Towards a conceptual framework for information security digital divide

By

Emmanuel Chisanga

Submitted in accordance with the requirements

for the degree of

MASTER OF SCIENCE

in the subject

COMPUTING

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Prof EK Ngassam

OCTOBER 2016

Declaration

Student Number: 48123412

I declare that TOWARDS A CONCEPTUAL FRAMEWORK FOR INFORMATION SECURITY DIGITAL DIVIDE 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.

SIGNATURE (Mr E. Chisanga)	DATE

Acknowledgements

My work was carved out of the philosophy of two Nobel Prize winners, "*One believed, it seems impossible until it is done"* (**Nelson Rolihlahla Mandela**). The other, "*The whole of science is nothing more than a refinement of everyday thinking"* (**Albert Einstein**). This dissertation is indeed a refinement of my everyday thinking over the last three and a half years, which at times seemed impossible. With that said, I would like to express my heartfelt appreciation to the following:

- First and foremost, God the Almighty, for the tenacity to keep going even when it seemed farfetched
- My priceless wife **Roswitha Chisanga,** who stood by me all the way and looked after our lovely son while I worked long hours day and night
- My son **Chileka Tuaundja Chisanga,** who I did not see grow up the way I would have wanted because of this commitment
- **Rosa-Stella Mbulu,** for the critique and editing of my work with a smile
- **Nguza Siyambango,** for the courage and help to kick-start the research
- **Uncle Robert Nasilele,** for the elegant editing touch
- **Jonathan Chanda,** for the glimmer of hope when it seemed dark, especially when funds dried up
- **Etambuyu Mutalife,** for the prayers and well wishes
- **Dr van Niekerk,** for the urge to fight on
- My mom, **Luwisa Chisanga,** for silently sending those prayers
- **Diebold South Africa,** my employer, for the time off during demanding days
- **Gabani Mwale,** Johannesburg would have never been my third home without you around
- I am also grateful to organisations that allowed me to test my innovation on their systems including all survey participants
- My academic supervisor, Professor **Ernest Ketcha Ngassam,** there is none like you; blatantly put, you were a light in the dark with your positive feedback and guidance during our correspondence over the last three years. Our many one-on-one contact classes in Johannesburg, Pretoria and Centurion have no equal

- **Khomotso Bopape** of Let’s Edit, for helping with the editing of my dissertation
- To my dad, **Christopher Kangwa Chisanga,** my role model in life – a man I have always looked up to; ***I am happy you have lived to see this family legacy***
- Finally, to all my family members and friends that I have not listed but were an essential part of this amazing milestone

Abstract

In the 21st century, information security has become the heartbeat of any organisation. One of the best-known methods of tightening and continuously improving security on an information system is to uniquely and efficiently combine the human aspect, policies, and technology. This acts as leverage for designing an access control management approach which not only avails parts of the system that end-users are permitted to but also regulates which data is relevant according to their scope of work. This research explores information security fundamentals at organisational and theoretical levels, to identify critical success factors which are vital in assessing the organisation's security maturity through a model referred to as "information security digital divide maturity framework". The foregoing is based on a developed conceptual framework for information security digital divide. The framework strives to divide end-users, business partners, and other stakeholders into "*specific information haves and have-nots*". It intends to assist organisations to continually evaluate and improve on their security governance, standards, and policies which permit access on the basis of each end-user or stakeholder's business function, role, and responsibility while at the same time preserving the traditional standpoint of confidentiality, integrity, and availability. After a thorough review of a range of frameworks that have influenced the information security landscape, COBIT^{TM} was relied upon as a baseline for the development of the framework of the study because of its rich insight and maturity on IT management and governance. To ascertain that the proposed framework meets the required expectation, a survey targeting end-users within three participating organisations was carried out. The outcome revealed the current maturity level of each participating organisation, highlighting strengths and limitations of current information security practices. As such, for new organisations relying on the proposed framework for the first time, the outcome of such an assessment will represent a benchmark to be relied on for further improvement before embarking on the next maturity assessment cycle. In addition, a second survey was conducted with subject matter experts in information security. Data generated and collected through a questionnaire was then analysed and interpreted qualitatively and quantitatively in order to identify aspects, not only to gauge the acceptance of the proposed conceptual framework but also to identify areas for improvements. The study found that there was a general consensus amongst experts on the importance of a framework for benchmarking information security digital divide in organisations. It also provided a range of valuable input relied upon to improve the framework to its final version.

Keywords: Capability Maturity, Digital Divide, Information Security, Information Systems, Critical Success Factors, Information Security Digital Divide, Information Security Maturity Level, Frameworks, Benchmarking

Table of Contents

List of Figures

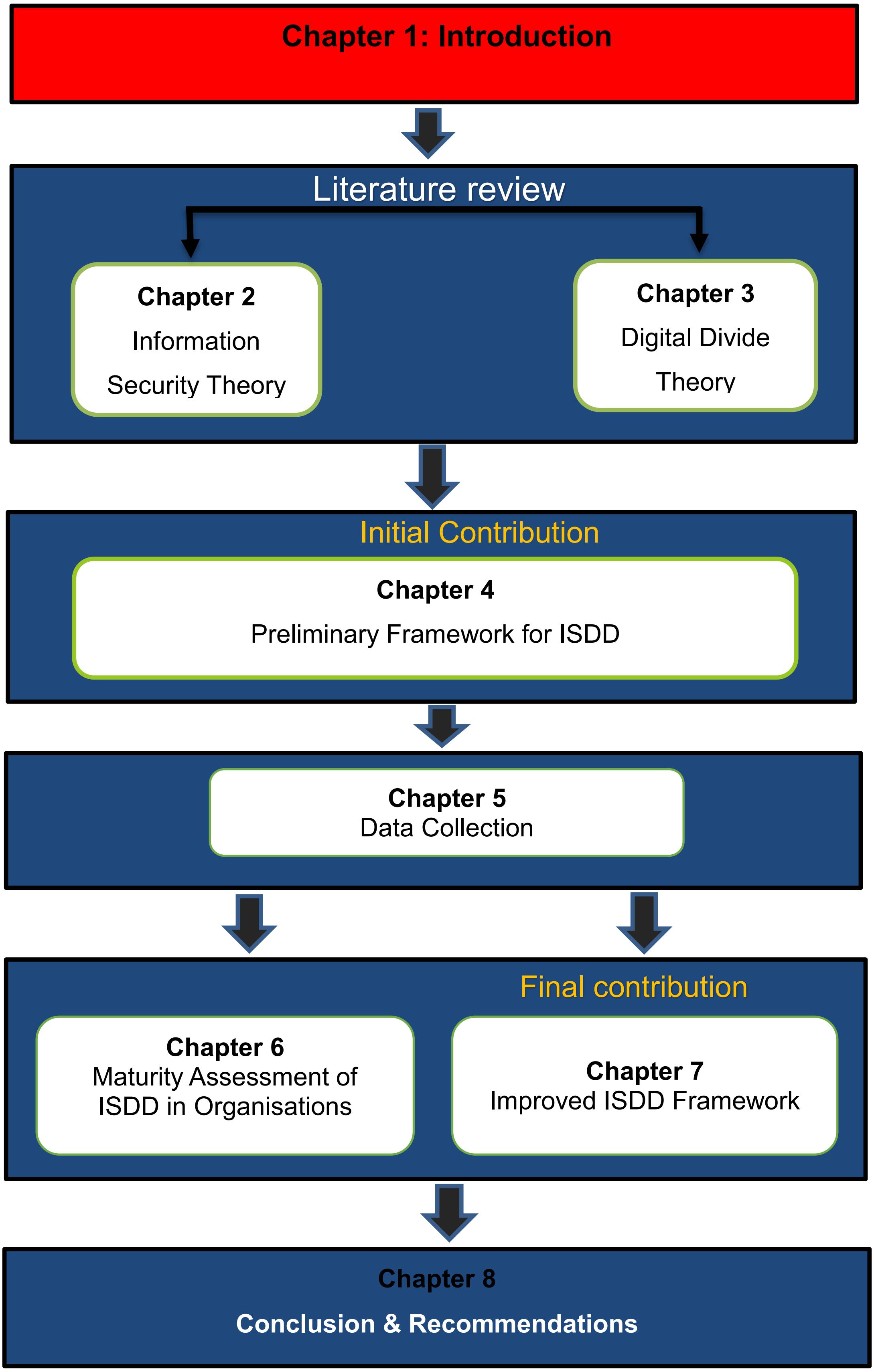
List of Tables

List of Abbreviations and Acronyms

API	Application Programming Interface
BCP	Business Continuity Plan
CEO	Chief Executive Officer
CIA	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CRM	Customer Relations Management
CSF	Critical Success Factor
DD	Digital Divide
ERP	Enterprise Resource Planning
EWF	European Federation for Welding
F2F	Face-to-Face
FFIEC	Federal Financial Institutions Examination Council
HR	Human Resource
ICT	Information and Communication Technology
ICT experts	Information and Communication Technology personel from various ICT sectors well vested in Security
ICT4D	Information Communication Technology for Development
ID	Identification
IS	Information System
ISACA	Information Systems Audit and Control Association
ISDD	Information Security Digital Divide
ISDDMF	Information Security Digital Divide Maturity Framework

KPA	Key Process Area
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITS	Information Technology Systems
LAN	Local Area Network
MIS	Management Information Systems
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic co-operation & Development
OSE	Operational Security Environment
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act
RDP	Remote Desktop Protocol
SOE	Sony Online Entertainment
STOPE	Strategy, Technology, Organisation, People, and Environment
VPN	Virtual Private Network
WAN	Wide Area Network

Chapter 1: Introduction



1.1. Introduction

Over the years, heavy dependency by enterprises on information systems for business operations has made information security a key ingredient in the quest for success and long-term survival. Traditionally, information security is about preserving confidentiality, integrity, and availability of corporate data. However, this traditional security standpoint alone does not provide much defence in terms of access control and preventing information from leaking to unauthorised end-users within and outside the domain of an organisation.

This research focuses on information security at organisation level. It investigates the segregation of end-users, business partners, and other stakeholders into "*specific information haves and have-nots*" based on a relatively new concept referred to as information security digital divide (ISDD).

Usually, the digital divide in the digital world concerns the unequal access to and usage of new technologies which are important for economic development in any country. This trend falls in the ambit of Information and Communication Technology for Development (ICT4D) (Fuchs & Horak, 2008). In the context of ICT4D, a high divide in any economy is considered bad for development because the poor and so-called "*information have-nots*" will seldom take advantage of the digital world. This would put them at a disadvantage, while a low divide would promote development because everyone, whether from "*the haves*" or "*have-nots*", would have access to the same kind of technology and information. With that noted, this research, however, introduces digital divide from a different perspective. It narrows down the concept to information systems security at enterprise level.

Unlike in ICT4D where a high digital divide is not good for development and the opposite is, in the context of this research, in order to promote a highly secured information system with decent access control among all end-users, both internal and external, a high ISDD appears very effective for organisational growth. On the other hand, a low ISDD is bad for any such organisation because it leaves information exposed.

By tapping into the rich insight of COBIT^{TM} on IT governance and associated metrics, the concept of ISDD can be used to develop a self-appraisal tool which determines the degree of vulnerability of aspects of the organisation’s information systems.

1.2. Background and Motivation

The motivation for this research is driven by first-hand experience on the devastating impact a security breach may inflict on a business. It is not only dollars and cents that are at stake. Aside from the financial burden of having to deal with a security incident, other factors could severely damage an organisation’s ability to operate (Caballero, 2009). While working with a number of organisations within Namibia, implementing Information and Communication Technology (ICT) and digital divide- (DD) related projects, the researcher was fortunate to interact with several information systems, management teams, information ICT experts, as well as information system end-users of various organisations. It was during this phase that the researcher realised the need to devise a concept within information systems that would ensure extra security urge. The concept would aid to curb information overlap, which often emanates from uncontrolled ability of end-users and stakeholders to access information according to the boundaries of their business roles and functions.

An organisation consists of its members and their interactions. Each member has his or her own role to play and sphere of responsibility, which contribute towards realising the organisation’s goals (Albrechtsen & Hovden, 2009). It is important, from a data and information access point of view, to ensure that, these members are segregated correctly. Often, organisations with low ISDD are characterised by frequent security breaches that can cause revenue loss, system crashes, information leakage, ruined reputation, and theft.

This research aims to develop a framework for benchmarking ISDD to be relied upon for assessing the maturity of ISDD in organisations. The framework can be used to measure the effectiveness of organisations’ information systems in order to determine their compliance when compared to other proved state-of-the art systems referenced in literature review. High ISDD entails a highly secured information system, while a low ISDD is a sign of a highly exposed environment. The tool strives to align all end-users and stakeholders in organisations, to use information within and outside the organisation based on the relevance to their roles and responsibilities. Finally, the idea is to issue them access to information resources but not more than they need to perform their roles and responsibilities (CA Technologies, 2015).

1.3. Problem Statement

According to Jaquith (2007), a security programme can only be improved if it is measurable. In any given organisation, all stakeholders have various roles and responsibilities which have an influence on the success of information security and, therefore the organisation's success as a whole. These stakeholders require access to corporate data, information, and systems at different levels according to their roles and responsibilities in order to achieve organisational vision and mission. However, in real-life contexts, organisations seldom put in place structured and standardised information security policies and governance instruments on which stakeholders should rely upon throughout undertaking their respective duties. Besides standard systems security practice that often comes with the vendor of the system, lack of a structured and well-defined set of principles that obligate the organisation to regularly perform self-assessment for systems' vulnerability minimisation remains a concern at corporate level. It is in this context that development of an appropriate framework aiming at regularly assessing the organisation's maturity level and identifying areas for improvement concerning information security appears to be of high importance in literature.

1.4. Research Objective

The main objective of this research is to *develop a framework for benchmarking information security digital divide.*

The premise of the research will be people, processes, and technology at organisation level. As such, the developed framework will be used by organisations to measure their current ISDD maturity level for further improvements should the need arise. Such an assessment will form the basis for the identification of various vulnerability issues and promote the implementation of counter-measures adequately designed to manage the ever-changing business ecosystem from a security perspective.

The framework is also intended to promote the understanding of ISDD among all stakeholders and help to secure information systems. It will ensure that end-users, stakeholders, and partners according to their business roles and responsibilities understand their part in the implementation, compliance, and evaluation of a successful conceptual framework. It will also contribute to formulating recommendations on the best approach to manage the digital divide to the benefit of the organisation. The foregoing main objective will be achieved through the sub-objectives that follow.

1.4.1. Sub-objectives

The sub-objectives below pertained to this study.

Sub-objective 1: *Investigate the state-of-the-art with regard to theory and practice of information security in organisations* – This sub-objective forms part of the literature review whereby research will be undertaken not only on the understanding of the functioning and structure of organisations in general but also the approach used to define critical success factors with regard to information security.

Sub-objective 2: *Understand the theory of digital divide and its contextualisation to information security*: This sub-objective intends to provide a contextual definition of ISDD by merging both theories of digital divide and those of information security critical success factors. The intention is to baseline the concept of ISDD in order to contribute to the realisation of the main objective of this research.

Sub-objective 3: *Develop and validate a conceptual framework for assessing ISSD in organisations* – This sub-objective will be achieved by relying on the aforementioned sub-objectives as well as a critical analysis of existing frameworks so as to conceptualise an appropriate framework for ISDD. Reliance will also be placed on a range of case studies in real-life context for the validation and improvement of the framework in organisations.

1.5. Research Question

Based on the aforementioned problem statement as well as the main objective of this research, the main research question is formulated as follows:

- *How can a framework for assessing the maturity of ISSD in organisations for further improvements be developed?*

1.5.1. Sub-research Questions

Secondary research questions of the study are as follows:

- **Sub-research question 1:** What are the current information security organisational practices and how is success measured in such context?
- **Sub-research question 2:** How can the concept of digital divide be leveraged positively in the context of information security at organisation level?
- **Sub-research question 3:** How can a framework for assessing ISDD capability maturity be developed and validated in real-world context?

1.6. Limitations and Delimitations

Only three target organisations in three different sectors participated in this research. This research can, however, be extended beyond those three organisations and even sectors different from those they hailed from. Only COBIT was relied on as a reference framework in order to develop the ISSD framework, but many other well-established reference security frameworks and standards such as ITIL, ISO/IEC 27001:2013, ISF, and others could have been used to the same effect.

1.7. Deliverables and Outcomes

The main deliverable of this research will be an integrated conceptual framework that will be validated and adjusted based on outcomes which will emanate from case studies targeting ICT experts and system end-users within selected organisations in Namibia. The proposed conceptual framework will form a benchmark for organisations to establish the maturity of ISDD. Further, it will weigh the effectiveness of their information systems in order to make well-informed decisions with regard to improvements.

1.8. Research Methodology

This research relied on mixed methods of both interpretive and positivist due to the nature of the questions that had to be answered, i.e. the “what and how”. Co-jointly, mixed methods use a combination of two methodologies with one feeding off the other (Wright & Losekoot, 2010). Some researchers now consider qualitative and quantitative methods as complementary rather than as opposites that cannot work together (Thomas, 2003; Creswell, 2003; Jack & Raturi, 2006).

Interpretive research entails the attempt by the researcher to understand phenomena through accessing the meanings participants assign to them (Walsham, 2006). Interpretivist is characterised by, first, the researcher – who is the main factor; they interpret data gathered in a context; and then they analyse it and finally draw a conclusion (Clarke, 2009).

Positivist, on the other hand, is based on quantification in the collection and analysis of data; it has a deductive relationship between theory and research and has an objectivist conception of reality (Wright & Losekoot, 2010). Positivist possesses the following characteristics: the researcher identifies a research problem, performs a literature review on it, collects data in a certain context, and analyses it statistically and interprets it to answer the research questions.

In line with joint characteristics of both interpretive and positivist characteristics discussed in the literature in this study, literature was reviewed particularly directly filtering out applicable material. The material was on, amongst others, information security, digital divide, COBIT, capability maturity, and information systems with the sole purpose of coming up with a contextual framework based on an interpretation of the reviewed literature.

In addition to the above, case studies were conducted in participating organisations, data was collected and analysed, with the determination of reporting the relevance of the framework based on feedback from system end-users mainly statistically to understand quantifiable trend patterns of end-users. Also, for checks and balances on the quality of framework produced, non-quantifiable data involving ICT experts within the ICT space were gathered, analysed, and interpreted, thus resulting in improvements representing the final contribution of this research.

Furthermore, it is worth mentioning that apart from the mixed research methods complementing each other to produce a robust result, it also provided an added advantage for the validation of data collected through cross verification, which is regarded as a powerful tool by many researchers in an effort to minimise inconsistencies (Creswell, 2014).

1.8.1. Sampling

In this study, assessing ISDD attributes such as the culture of protecting information or observing standard security practices among all end-users in participating organisations took long. It was for that reason that a small target of 90 participants was the sample across all three participating organisations. Of that 90, only 65 participants took part in this first survey, whereby Organisation X represented 29%, Organisation Y represented 25%, and Organisation Z represented 46%.

Furthermore, there was quantitative data gathered from ICT experts whose main aim was to assess the quality of the proposed framework. In this second survey, a total of 35 ICT experts were approached; however, only 25 participated. Quantitative analysis was more appropriate in this case because the intention was to understand the occurrences, sizes of responses on certain qualities of the framework, and the volume of agreements as opposed to disagreements on areas that needed change to make improvements on the proposed framework.

1.8.2. Data Collection

The most common sources of data collection in both quantitative and qualitative research are interviews, observations, questionnaires, and review of documents (Creswell, 2009; Locke, Silverman & Spirduso, 2010; Marshall & Rossman, 1999). The combined data collection methods that follow were used to collect data in this study.

1.8.2.1. Documentation Review

In accordance with the literature review performed on the critical success factors of information security, security policy as a living document was singled out to be a must-have for every organisation as a first line of maintenance. The document also needed to be relevant to the setup of systems. For that reason, a review of the content of the security policy and how often it gets updated was performed in all participating organisations with findings recorded as part of ISDD metrics. Furthermore, other reviews on important aspects of information security such as business continuity plans for disaster recovery purposes were also entertained.

1.8.2.2. Interviews with Structured Questions

Interviews were conducted with ICT experts who represented participating organisations only in order to understand areas such as systems landscape, types of security available, awareness and training programmes, access control management, and management support.

1.8.2.3. Observation

Observation as a data collection approach was used to monitor system end-users in all participating organisations. This was done randomly to observe the culture of protecting information on, amongst others, ISDD basic principles such as password use and sharing. It was also done to observe the culture of physical access to business functions using access control in areas such as access cards, keys, or biometrics.

1.8.2.4. Questionnaire Surveys

Two types of case studies were considered in this research. The first case study involved testing the relevance of the framework by engaging system end-users in all three organisations. This was achieved through a carefully designed questionnaire with mostly close-ended questions distributed to selected participants. The second case study consisted of a survey targeting ICT experts from the ICT space, using a questionnaire set to scrutinise the quality of the proposed framework. Their contribution provided an incentive to improve on the proposed framework to make it more consensual.

1.8.3. Data Analysis

According to Oira (2013), data analysis and interpretation is the process of assigning meaning to the collected information and drawing conclusions, significance, and implications of the findings. To efficiently validate data generated, this study depended on method triangulation. In both surveys involving system end-users and ICT experts respectively, data collected was both of a qualitative and quantitative nature.

Qualitative research centred on narrative and performance analysis in order to discover similarities in the respondents' responses was used. This was largely applicable to ICT experts discovering common opinions that would add value to the initial framework. Quantitative data analysis, on the other hand, focused on mathematical approaches such as statistics to examine and interpret data collected. This was better suited when measuring the relevance of the framework, whereby end-users' responses were quantified to observe certain patterns on how well they complied with ISDD attributes such as the use of passwords when accessing computers or to simply measure the general culture of protecting information.

1.9. Reliability and Validity

According to Joppe (2000), reliability in research is the degree to which results are consistent over time and results can be replicated using the same methodology. For the purpose of this study, the simplest approach to reliability and validity was to use the split-half method as suggested by Oats (2006:227). Questions in questionnaires were divided into two equivalent groups. The score of a respondent in one half is compared to the score in the other half. If the questionnaire is reliable, the two scores should be the same (Oats, 2006:227). In the context of this research, 22 random end-user questionnaires were coded in one table of two columns. The two columns were split into two halves, one with even numbers and the other with odd numbers. To find out the reliability of the responses on certain ISDD assessment within participating organisations, reliance was placed on SPSS whereby the table was imported and tabulated automatically. Given 22 value cases of respondents with each having 34 ISDD items (questions), the Spearman-Brown prophecy formula retained a coefficient equal to 0.74, which is considered respectable for the small number of participants involved.

As a further validation and reliability approach, retest reliability was also performed on applicable instruments used such as both end-user and expert questionnaires. Second opinions by suitable experts on the subject matter, were also done on data collection instruments such as, interview questions and observation sheets. Data collected was subjected to retests to further check for inconsistency and discrepancy in the result. Interviews can have a tendency of delivering inaccurate results, thus to reduce the chances of that happening, data triangulation was used, which was made easier by the fact that this study used both qualitative and quantitative types of data. Finally, findings were to be taken back to participants to ensure they agree that it represents the true situation, as a validation and reliability method.

1.10. Ethics

Because ISDD is a very sensitive issue, ethics needed to be highly considered in this research. Ethics ensure target organisations do not suffer any loss, physical or non-physical, or disadvantage them as a result of the research. Additionally, there is always a concern about breach of confidentiality, but the following measures were taken during this study to address the issue:

- Names of respondents were not to be revealed to anyone.
- Respondents were informed of their rights to withdraw from the survey if they felt uncomfortable continuing with participation at any point.
- What individual respondents told the researcher was guaranteed not be revealed, neither was the organisation they were representing made known or revealed.
- Respondents were not singled out for marketing purposes because they participated in the survey.
- As shown in Appendix A, ethical clearance was obtained from the University of South Africa and the approval communicated to participating organisations before engaging in various surveys.

1.11. Significance of the Study

This study contributes to the maturity and understanding of information security in organisations. An applied framework delivers the capability maturity level of information security and provides ample opportunities for further research. Further to that, the framework is meant to be used as a guideline tool by organisations when assessing the maturity of ISDD. It will help organisations to improve on security policies, standard, governance, and practice so as to strengthen ISDD. Auditors would benefit by using the framework as a guideline to perform quality assurance and control from an IT audit perspective, which will save both auditors and organisations time and money. The research will also contribute to the body of knowledge on how the various stakeholders, irrespective of roles and responsibilities, and position, can harmonise and work towards enforcing ISDD with the intention of safeguarding corporate information.

1.12. Research Process

Figure 1.1 summarises the research process layout as follows: Chapter 1 introduces the research problem, objectives, questions, and limitations. Chapter 2 contains a literature review on information security and its importance to business operations. The third chapter focuses on the overview of the digital divide; it also formulates literature on information security digital divide as a concept and reiterates how it re-enforces security. Chapter 4 concentrates on the development of the proposed framework. Furthermore, Chapter 5 sets the context for the validation of the proposed framework in terms of instruments used to perform data collection. In Chapter 6, an analysis of data collected from the first survey involving system end-users to measure ISDD is performed. Chapter 7 presents the second survey involving ICT experts whose primary purpose is to use the outcome to improve on the proposed framework. Finally, Chapter 8 summarises the entire research including the findings and recommendations.

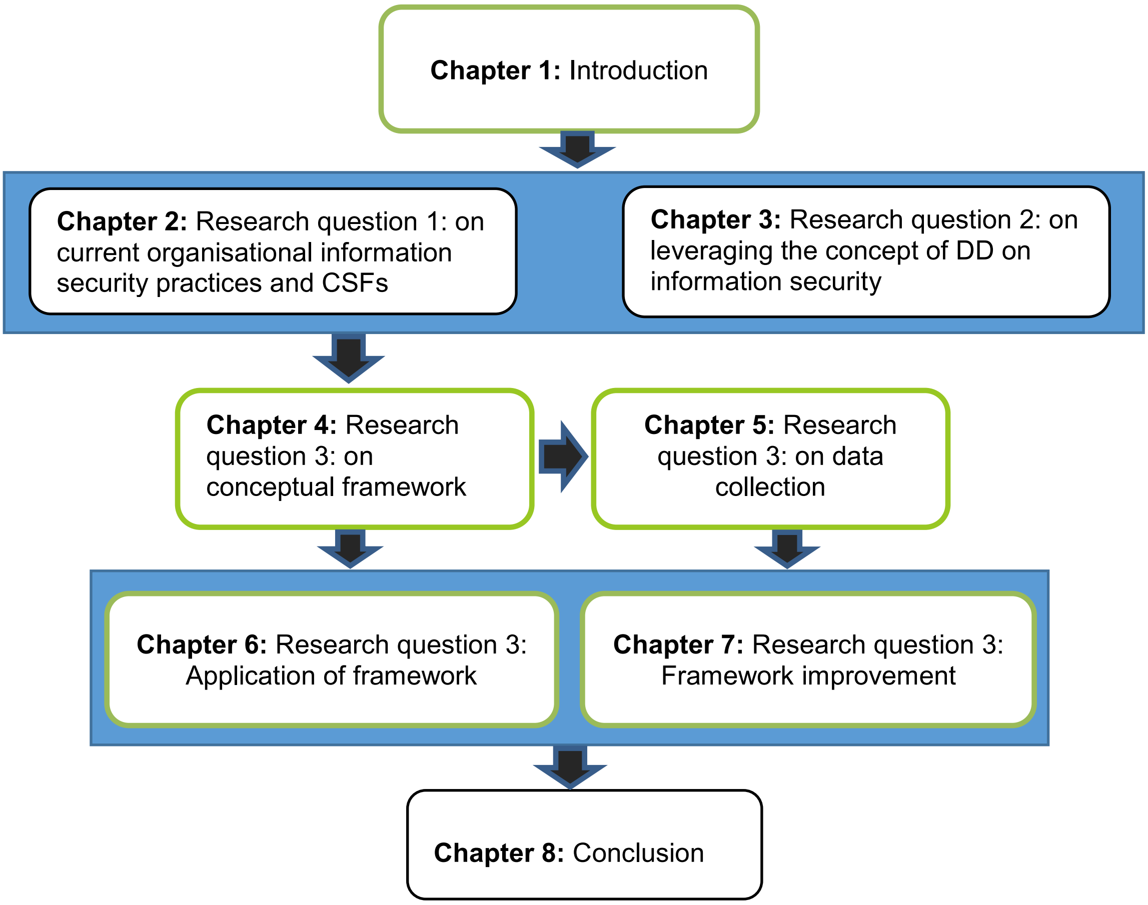

Chapter 1: Introduction
Chapter 2: Research question 1: on current organisational information security practices and CSFs
Chapter 3: Research question 2: on leveraging the concept of DD on information security
Chapter 4: Research question 3: on conceptual framework
Chapter 5: Research question 3: on data collection
Chapter 6: Research question 3: Application of framework
Chapter 7: Research question 3: Framework improvement
Chapter 8: Conclusion

Figure 1.1: Research process flow

1.13. Conclusion

This chapter introduced the research topic under consideration. It discussed the background and motivation on the need to explore information security digital divide at organisation level. A research problem was identified, leading to the formulation of research objectives to be achieved as well as research questions thereof. The most appropriate research strategy required to answer the research questions was discussed, as well as the reliability and validity of the research. The chapter further discussed ethical considerations, the significance of the research, as well as the layout of the study in the form of a research process. The next chapter focuses on an extensive literature review of information security at organisation level.

1.14. Definition of Key Terms

Benchmarking – establishing the basis for evaluation. Enabling organisations to rely on self-assessment for further improvement

ICT4D – Information Communication Technology for Development, access difference to telecommunication facilities among natives of an economy

Information security digital divide – A technique for regulating access control to information system resources on the basis of a stakeholder's business role, responsibility, and function

Information System – A combination of hardware, software, infrastructure, policies, and people, with the intention of collecting, processing, and storing corporate data. The purpose is to provide information for supporting business operations

Information security – The act of defending information from unauthorised access within and outside an information system by both authorised and unauthorised parties

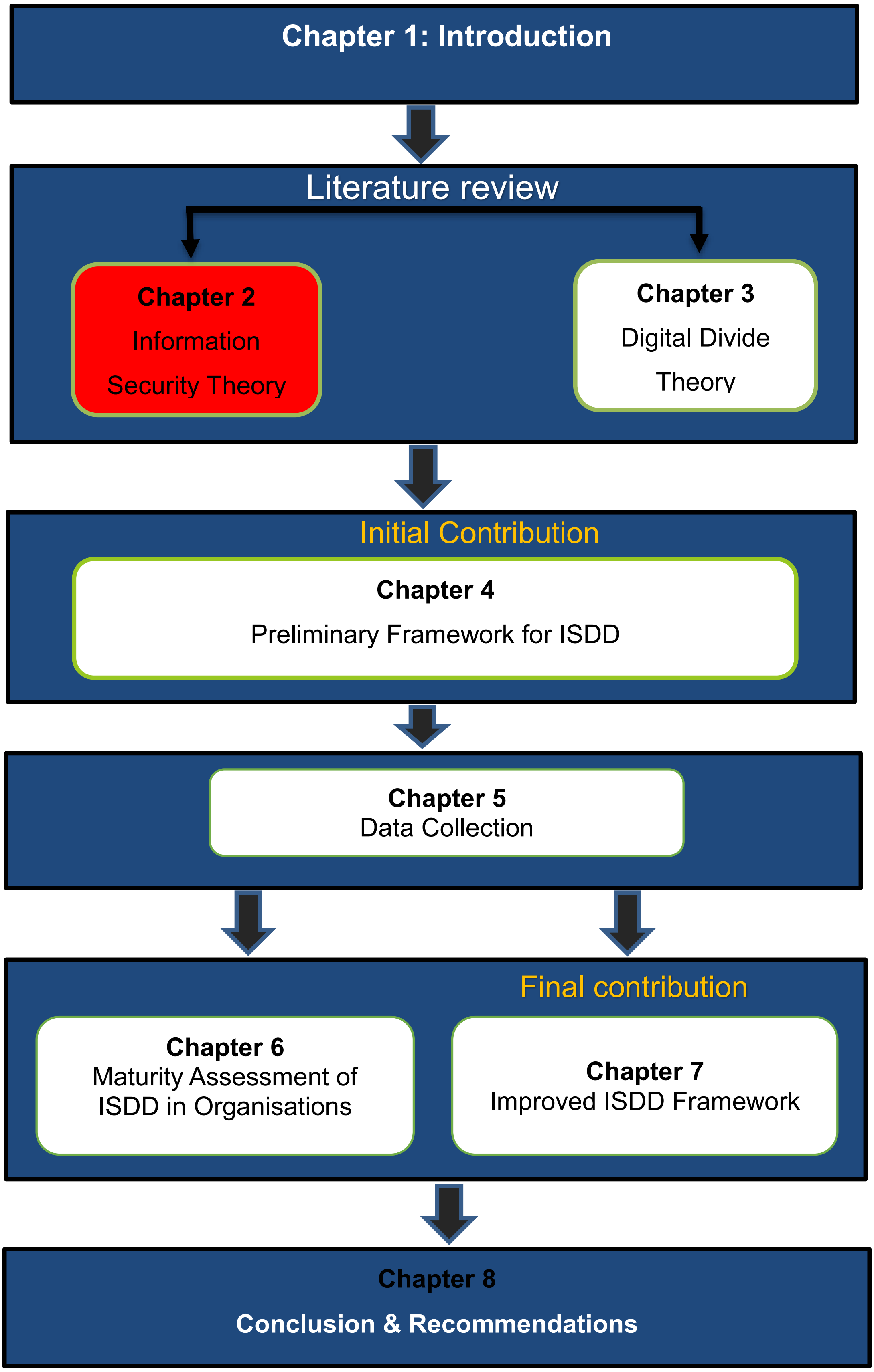
Capability Maturity – Specifies a series of steps for development for the purpose of benchmarking

Critical Success Factors – Areas in an activity or project that must be attained at all cost to realise the intended goal

Framework – A basic conceptual structure mainly composed of theory on how something should be formed

Mature ISDD - A well-organised, established, and appropriate mechanism for the management of the ability to access and process information and data within an organisation in such a way that security breaches are well contained

Chapter 2: Information Security in Organisations



2.1. Introduction

The previous chapter provided an introduction and background to the study. This chapter explores the literature on enterprise-wide information security basics that are relevant to understanding the concept of information security digital divide (ISDD). The chapter is significant to the research because it showcases a range of information and communication technology (ICT) infrastructure that are key in supporting business objectives and how this infrastructure needs to be protected in order to sustain the organisation. Additionally, it justifies how segregation of access and usage of an organisation's IT infrastructure improves information security. In so doing, it conceptually suggests a method of dividing end-user access in an attempt to only let them access what is required for them to perform their routine duties.

The purpose of this chapter is to answer the first research question on current enterprise information security practices as well as the identification of critical success factors and metrics thereof. The answer to the research question would thus require a thorough understanding of organisations at both structural and functional levels. Such an understanding will enable a seamless alignment to its entire ICT infrastructure needs from a security perspective. Of course, the exercise will not be materialised without exploring the literature on information security in general followed by its alignment to organisational requirements. The outcome of these investigations would result in a seamless identification of a range of information security-centric critical success factors aimed at contributing to the significant reduction of information security vulnerability.

The chapter begins with an overview of a generic organisation, its purpose, structure, and operations in Section 2.2. It proceeds in Section 2.3 to discuss the generics of information systems in organisations, their infrastructure, and how they complement business operations. An overview of information security is detailed in Section 2.4 where information systems threats, vulnerabilities, and risks are explored. The identification and description of critical success factors are provided in Section 2.5, with emphasis on what constitutes a secure information system. The chapter is summarised in Section 2.6.

2.2. Organisations and their Structure

An organisation is a collection of people or a group that is arranged in such a way that a specific objective is achieved through collective effort (Business Dictionary, 2015). All organisations, small or big, have a management structure that aligns these people or groups between the different activities, roles, functions, and responsibilities to carry out specific tasks.

2.2.1. Definition of an Organisation

According to Buchanan and Huczynski (2010), an organisation is a social structure for achieving coordinated performance in pursuit of collective goals. Also, all organisations are structured in a way that determines relationships between personnel (Business Dictionary, 2015). Furthermore, organisations can be affected by the environment in which they operate, but in return, they also induce some effect on that environment. Irrespective of their type or operational environment, all organisations have a sole purpose of achieving a common goal, which is often to attain the mission and vision goals of that enterprise.

2.2.2. Purpose of an Organisation

The purpose of a business is articulated in its vision and mission statements. In most cases, organisations are largely profitable, manufacturing or selling products and services. While profit may not be the major objective of a business, it is imperative that the aim be to make a profit for the owners and also in order to survive in the long run (GCSE Business Studies, 2004:2). This research, however, works towards any kind of business, be it profit or non-profit-orientated, provided it operates in a competitive environment. Irrespective of the purpose of an organisation, it must have a structure.

2.2.3. Composition of an Organisation

An organisation can be compared to a system (MacNamara, 2015). Organisations have major sub-systems, such as departments, programmes, divisions, and teams. Along with other subsystems, each of an organisation’s sub-systems has a way of doing things to achieve the overall goals of the organisation. Often, these systems and processes are defined by plans, policies, and procedures. In the simplest form, an organisation is a social system that contains inputs, process, and output (Illinois State

University, 2010). Input basically refers to resources such as raw materials, personnel, and technology. Inputs go through processes or procedures in order to be transformed into output, which is the tangible product or services to consumers.

For clarity purposes and in the interest of this study, a generic structure of personnel used by a European organisation called European Federation for Welding (EWF) has been adopted. According to observations (European Federation For Welding, Joining & Cutting, 2014:5; Chun & Mooney, 2009), the majority of organisations globally are structured in a similar fashion with the sole purpose of managing interactions between the various parts that make up the entire organisation.

2.2.4. Structure of an Organisation

An organisational structure shows the relationship between the internal departments and sub-systems (Petrauskas, 2006). Essentially, it is the operating manual that tells members how the organisation is put together and how it works (Smit, 2014). An effective organisational structure facilitates management and clarifies relationships, roles and responsibilities, levels of authority, and supervisory or reporting lines. Most organisations follow the traditional organisational structure style, where the hierarchy resembles a pyramid (Rishipal, 2014) as shown in Figure 2.1.

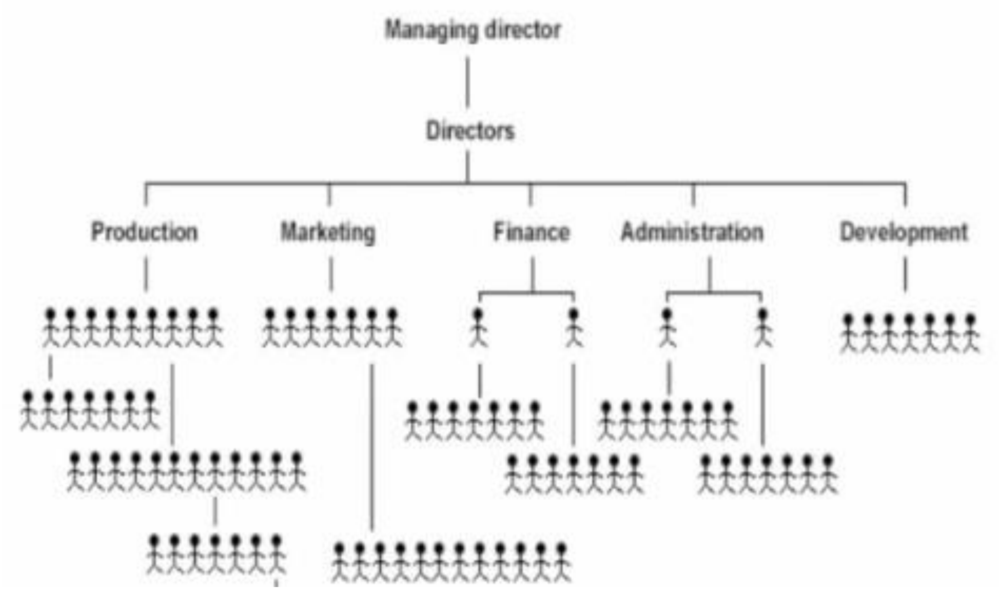


Figure 2.1: Generic traditional organisational structure

Source: Adapted from Organisational Development (2000)

The pyramid organisational structure in Figure 2.1 shows how the organisation is managed and controlled. It also highlights the delegation of authority across different positions. Figure 2.2 provides a further breakdown of this organisational structure to show the different levels of authority and responsibility.

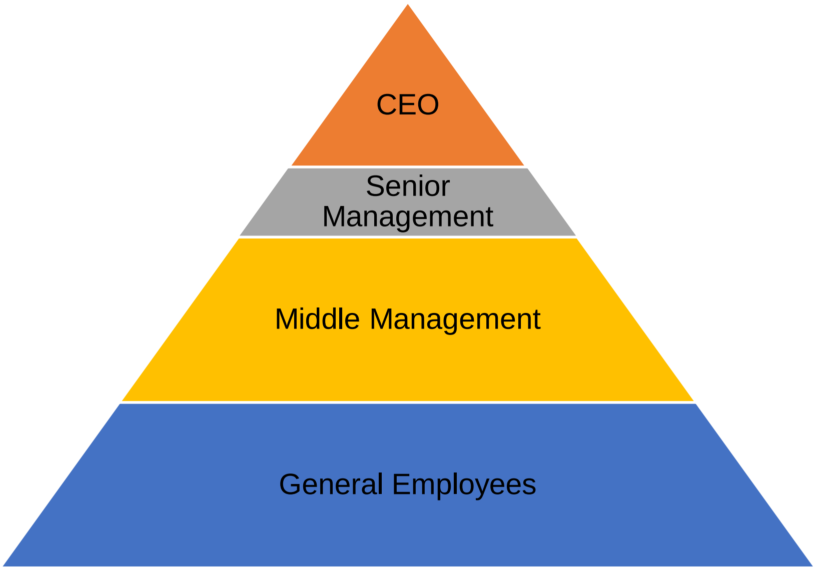


Figure 2.2: Four-tier structure representing the chain of command of labour

Source: Adapted from Smit (2014)

According to Figure 2.2, the chief executive officer has the greatest responsibility over the other three tiers below the hierarchy. As the levels move down from senior management to middle management and general workers, the levels of authority and responsibilities also diminish (Smit, 2014). All business roles, functions, and responsibilities of personnel in an organisation combine as a system towards one common goal. That goal is articulated in the form of a vision and mission statement. For that to successfully happen, the roles and responsibilities of employees need to be coordinated in accordance with the laid-down structure that is aimed at meeting the objectives of the organisation.

From a business operations perspective, as the flow of power, privileges and responsibilities diminishes, as depicted in Figure 2.2, so should the level of accessibility to certain types of information resources. This links to the notion that an employee should be allowed access to an organisation's data and information based on the merit of their business roles, function, and responsibility.

2.2.5. The Operation of an Organisation

Business operations involves all the activities required to propel a business to generate its desired output for profit purposes while delivering goods or services to clients (The Open University, 2011:1). In modern times, these business activities are efficiently supported by the use of technology in the form of information systems which support businesses through distribution, storage, processing, and management of data and information. According to Shipsey (2010), businesses nowadays depend on the usefulness of information systems to reach their desired goals and also gain competitive advantage. However, in an exchange of fortune, it is also inevitable that information systems are also beneficiaries of businesses because they become a product of businesses that conceive them.

Having provided an outline of an organisation and its operation in this section, it is common knowledge that such an operation should be supported by technology for efficiency purposes. In the next section, information systems are explored as the technological, operational backbone of an organisation.

2.3. Information System

An information system is a group of interrelated components that work collectively to carry out input, output, storage, and control actions in order to convert data into information (Hardcastle, 2008). In the same vein, Joseph and Schneider (2010) complement the definition further by arguing that information systems constitute a logical combination of hardware, software, and telecommunications to purposefully make up a system that can be used to gather, create, process, and distribute data in an organisation. Figure 2.3 shows the composition model of an information system.

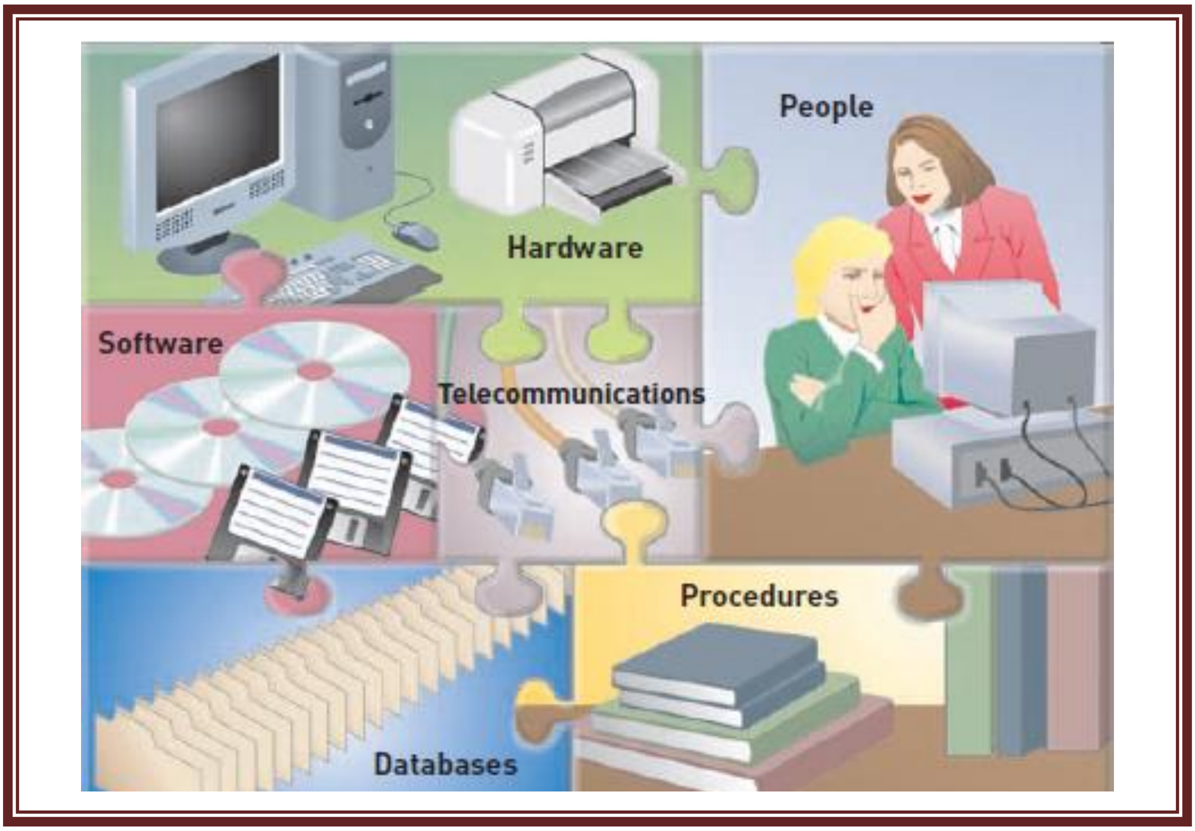


Figure 2.3: Computer-based information system model

Source: Stair and Reynolds (2012)

2.3.1. Primary Function of an Information System

The primary function of information systems is decision support, with the intention of guiding the organisation and operations on timely and correct information (Shipsey, 2010). As such, an information system is intended to execute business processes in line with the mission and vision statements of the organisation. Above that, Whitten, Bentley, Dittman and Bentley (2004) also contend that information systems also improve business knowledge, which is a product of information and data. It additionally improves business communications, which represents how the system interfaces with its end-users and other information systems, as well as how people communicate and collaborate with one another. There are many components that are combined to produce an information system.

2.3.2. Building Blocks of an Information System

Information system building blocks can be broken down into four categories. These include the database, applications, processes, and interface.

2.3.2.1. Database

A database is a collection of information that is organised so that it can easily be accessed, managed, and updated. The database management system allows managers and decision-makers within an organisation to perform qualitative analysis on the company's vast stores of data in databases, data warehouses, and data marts (Jefrey, 2006). Furthermore, a database management system at heart is the administrative tasks associated with the storage, modification, and retrieval of data held within a database. Significantly, it can also link to external databases to give managers and decision-makers even more information and decision support (Holt, Ramage, Kear & Heap, 2015:163). External databases can include the Internet, libraries, government databases, and more. Access to a combination of internal and external databases can give key decision-makers a better understanding of the company and its environment.

2.3.2.2. Application

Application software is an essential part of an information system because it interfaces the system with the end-users. Bourgeois (2014:9) considers an Enterprise Resource Planning (ERP) as a good example of an application which is useful because it links the front-end of the system to the back-end.

2.3.2.3. Interface

The interface of a system is the layer that allows system end-users to interact with the information system directly. For example, on a Microsoft^{TM} platform, the most popular interface is the operating system, e.g. Microsoft Windows^{TM} or Small Business Server^{TM}. Other supporting applications that form interfaces could be an application such as QuickBooks^{TM}, which enables departments such as Finance, Marketing, and Sales to manage payroll, inventory, sales, and other needs. Further to that, the software's features include marketing tools, merchant services, product and supplies, and training solutions. It is then easier for end-users in the aforesaid departments to manipulate data and use the system.

2.3.3. Information System's Processes and Services

These are categorised as constant business activities that support and complement the entire business operations. They consist of sub-functions, processes, as well as tasks. Business processes are activities that respond to business events. Such activities and services may include the front-end and back-end office activities and services. Front-end office interacts directly with customers; a good example can be marketing, sales, and customer relations departments. On the other hand, the back-end office is internal – behind the scenes; it does not interact with clients directly but offers support to the front-end office, e.g. human resource, inventory control, and finance.

2.3.4. Infrastructure Required for an Information System

2.3.4.1. Hardware

Hardware in information systems incorporates all physical infrastructures that facilitate a computer network. It includes items such as computers, laptops, access points, servers, printers, scanners, mobile phones, and routers.

2.3.4.2. Software

Software complements and controls hardware such as servers, computers, routers, and many others. Examples of the software may include the operating system, such as Microsoft Windows Small Business Server^{TM}, which operates servers; Microsoft Windows 8^{TM}, which operate personal computers for network end-users; and word processor, internet web browsers, spreadsheets, and many others (Microsoft Inc., 2015).

2.3.4.3. Services

These include telecommunications infrastructure such as telephone lines that facilitate the Internet. Internet service providers then provide lease lines from that and make dedicated internet traffic to networks.

2.3.5. Information System Infrastructure of an Organisation

This subsection discusses some of the devices that form part of an organisation's internal information system. These devices are embedded with software that supports the operations of an information system. They are listed and briefly described next.

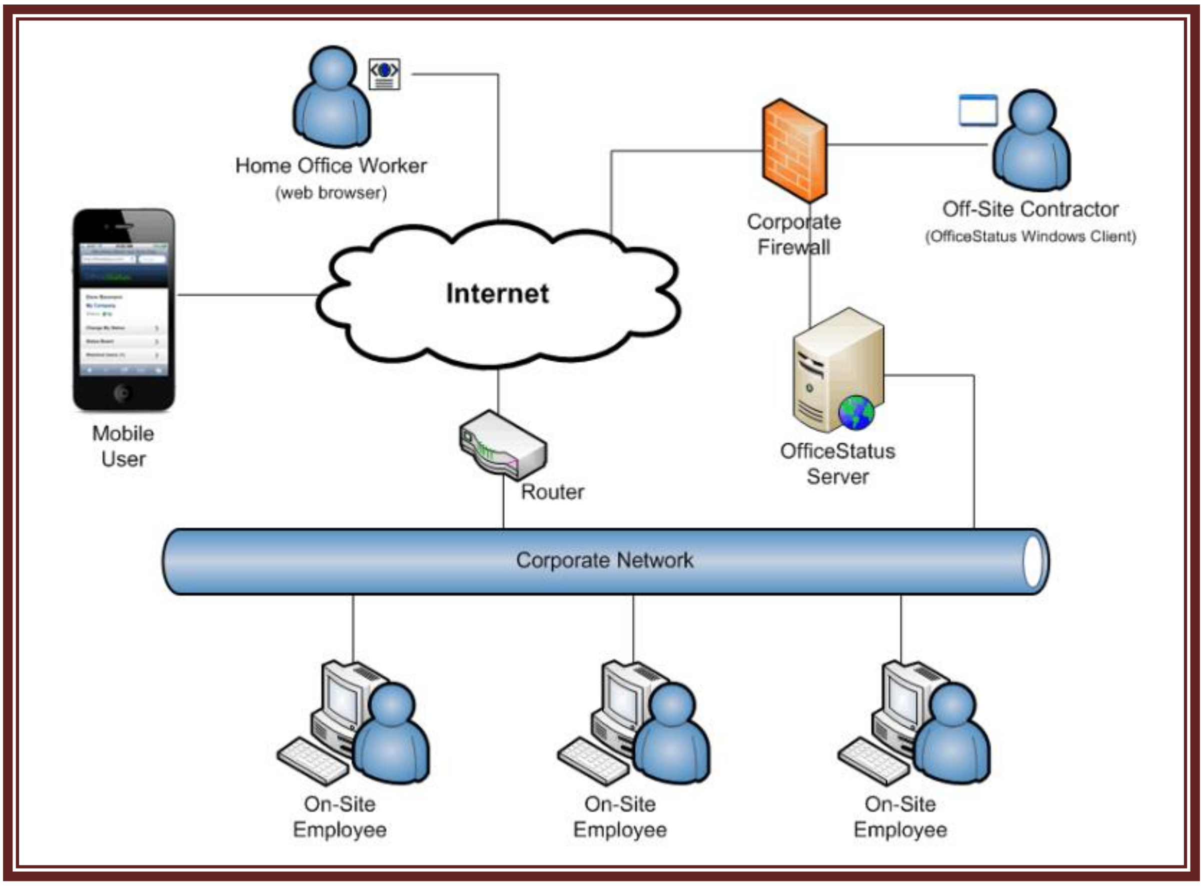


Figure 2.4: ICT infrastructure prone to attacks

Source: Microsoft Inc. (2015)

Figure 2.4 illustrates the components that are interconnected to form a local area network (LAN). According to Cisco (2015), a network router is a device that forwards internet traffic from one network to another. An Ethernet switch, on the other hand, connects all devices on the network such as servers, printers, computers, and other devices. For client computers and other network resources to operate, they need a special service; this is the role of a server.

A firewall is the security centre of a network; it sits on the edge of the network to screen traffic into and out of a network. Access points provide wireless access to a wired network; it is connected to an Ethernet switch, which it then converts into wireless signals. Finally, handheld devices such as personal digital assistants (PDAs), smartphones, and tablets also make up part of the infrastructure.

All the aforementioned network components combine to support and sustain an information system. To a large extent, these components can also span over a larger geographic area to form what is called a wide area network (WAN).

Information systems can also extend to incorporate other systems that are geographically far off but belong to the same organisation or partners. According to one IT department (CISCO, 2015), a wide area network is a computer network that geographically extends over a kilometre and has computers that are interconnected.

All network components shown in Figure 2.4 are prone to various security challenges such as hacking, viruses, disgruntled employees, ignorant employees, and many other known threats as well as risks. The security of information systems is discussed in the next section.

2.4. Information Security Overview

Various authors reserve various definitions for information security. Most authors associate information security with three well-known characteristics, namely, confidentiality, integrity, and availability. However, achieving these three characteristics is not a guarantee that a secure environment will be established (Saleh, 2010). “In its most basic traditional definition, information security means protecting information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction” (Fuchs, Pernul & Sandhu, 2011:748). Furthermore, the confidentiality, integrity, and availability of information are protected against threats and damage caused by faults in hardware and software, natural events, and wilful, negligent or accidental events (OECD, 2003).

Whitman and Mattord (2008) perceive information security as the safeguarding of information including its elements that are considered crucial. However, Ashenden (2008) argues that information security is merely not about the confidentiality, integrity, and availability of information alone, it should stretch beyond to accommodate real business benefits such as protecting while facilitating the controlled sharing of information and managing the associated risks across a changing threat and risk environment.

In light of the preceding section, organisations can implement information security protective measures through ISO/IEC 27001:2013 accreditation. The ISO/IEC 27001:2013 is an internationally recognised information security management standard that emphasises the three characteristics (Confidentiality, Integrity, and Availability – CIA) of information security (Caballero, 2009).

2.4.1. Characteristics of Information Security

2.4.1.1. Confidentiality

Information assets are believed to possess confidentiality when they are protected from disclosure or exposure from unauthorised individuals or systems. In easier terms, it determines the level of secrecy. Furthermore, it also ensures that only those with rights and privileges to access the assets are able to do so. Besides, when unauthorised individuals or systems can view information, confidentiality is breached (Whitman & Mattord, 2012). One of the best ways of preserving confidentiality is using a method called encryption, which according to Padmapriya and Subhasri (2013) is a technique of concealing sensitive information by converting it into a code to protect it from unauthorised persons.

2.4.1.2. Integrity

Of the three CIA aspects, this aspect of information is the most critical (365 Computer Security, 2010). Information assets are considered to possess integrity if they can only be modified by authorised parties or in acceptable ways, and this applies to data, software, and hardware (Zissis & Lekkas, 2012).

2.4.1.3. Availability

Availability refers to the ability of a system or information assets to be accessible and usable upon demand by authorised personnel. Additionally, it points out the willpower of a system to carry on operating even when authorised personnel abuse it. The system must have the pedigree to continue operations even during eventualities such as security breach. Availability not only refers to data or software but also hardware being available to authorised end-users upon demand (Zissis & Lekkas, 2012).

Figure 2.5 summarises the three fundamentals of information security graphically. If the three fundamentals of information security are maintained and upheld, a highly secure and reliable information system is possible in any such organisation because the preservation of information is guaranteed when all principle attributes of information protection, namely, confidentiality, integrity, and availability are conserved during the life cycle of information (ISO/IEC 17001:2013)

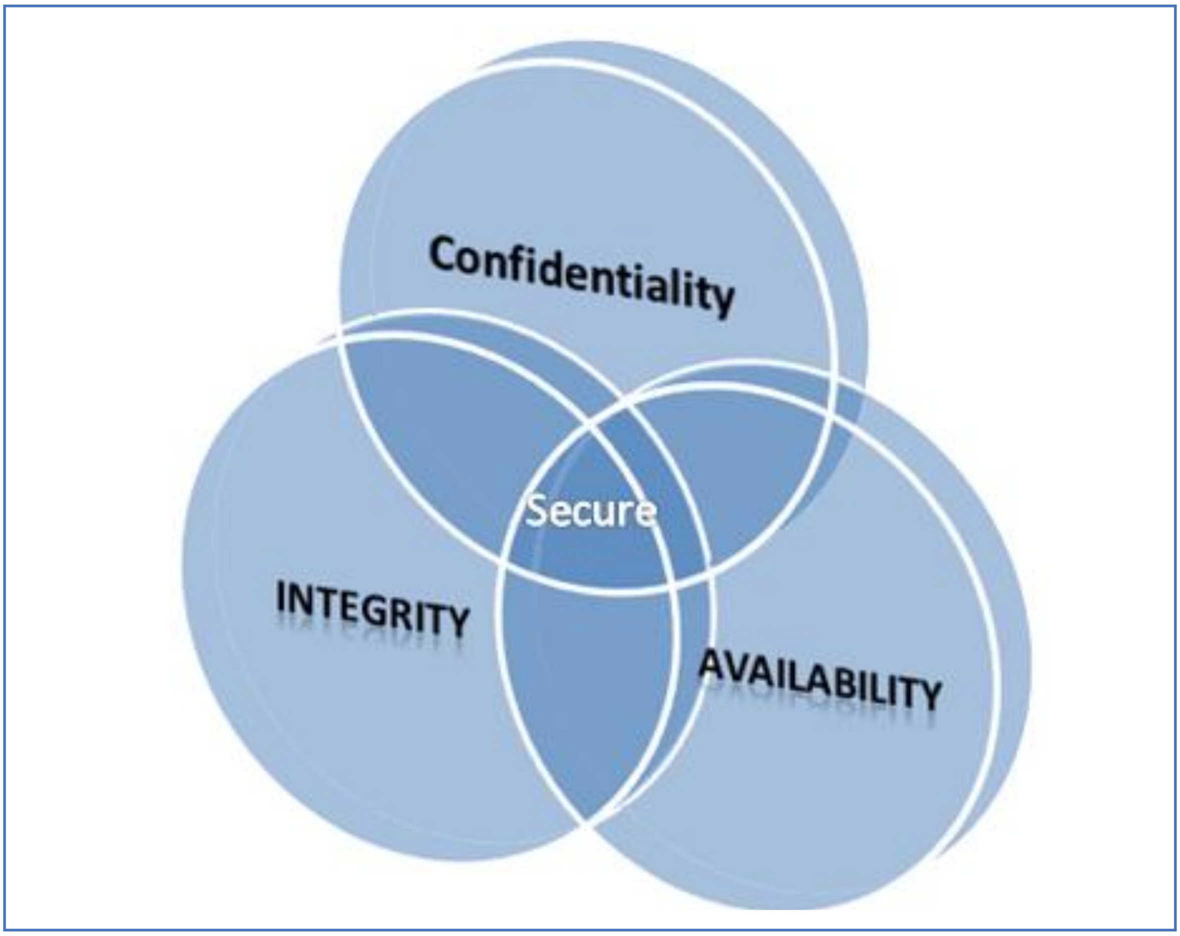


Figure 2.5: The relationship between integrity, confidentiality, and availability

Source: Adapted from ISO 27001:2013

The three characteristics of information security as depicted in Figure 2.5 (Confidentiality, Integrity, & Availability) form the so-called CIA triangle. The CIA triangle has to be preserved for the safety of data at various phases within an information system as summarised in Table 2.1.

Table 2.1: Phases of information through a system

Status	Description
In Transit	Protection of data while being transmitted between the various components of an information system
In Process	Protection of data while being accessed by end-users or applications in the information system
At Rest	The protection of data while it is in its storage areas waiting to be used or processed

Source: Whitteker (2014)

Consequently, if the characteristics of information security (CIA) already discussed are not adhered to during the information stages mentioned in Table 2.1, it exposes corporate data to threats which have the ability to affect the overall operations of an organisation

2.4.2. Information System Threats

In this subsection, information system threats are reviewed to fully understand how they hamper the general operations of a business in an effort to compete successfully. The subsection further relates these threats to potential business risks.

According to Bishop (2003:6), “a threat is a potential violation of security”. Accordingly, threats can cause incidents that may lead to both information system and organisation harm (ISO/IEC 27001, 2013). Intentionally through acts of terrorism or hacking, threats can be deliberated towards an organisation’s ICT infrastructure. Sometimes, these threats are unintentional through accidental occurrences by ignorant employees, or they can also be perpetuated by natural occurrences such as floods, fire, earth earthquake, and many other natural disasters.

2.4.2.1. Classification of Threats

In organisations, information security managers need to know and understand potential threats that can consequently impact their ICT assets. This is mandatory for them in order to perform a forecast to determine what they need to do to prevent attacks by selecting appropriate mitigation or recovery plans. Organisations possess unique attributes and specialise in different products and services; therefore, each organisation will face different threats and vulnerabilities (Layton, 2009). On that account, threats are exploited with a variety of attacks, some technical, others not so much (Caballero, 2009). Threats also affect systems differently according to the design and intention of the threat agent (Microsoft Inc, 2015). These threats can be classified as malicious, non-malicious, or natural as shown in Figure 2.6.

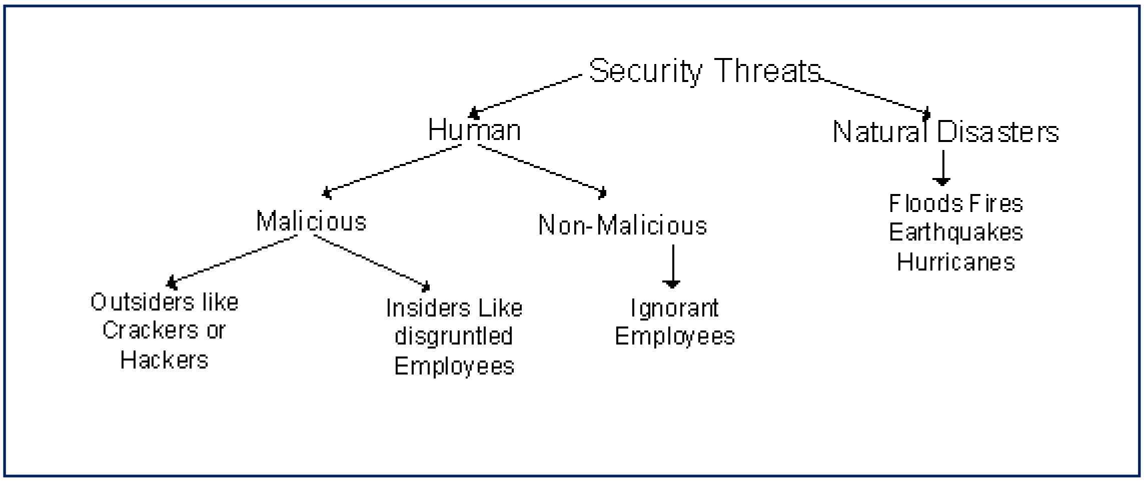


Figure 2.6: Classification of threats

Source: Microsoft Inc. (2015)

The classification in Figure 2.6 indicates that threats may come in different types and formats. They may hamper information systems in different ways. Whether the threats depicted in Figure 2.6 are of an intentional nature or not, they are likely to emanate from either internal or external sources. To provide a proper defensive mechanism, organisations need to understand these sources carefully. In the next subsections, internal and external threats, as well as general threats to information systems, will be briefly discussed.

2.4.2.2. External Threats

External threats to an organisation’s information system can be individuals who operate from outside the organisation attempting to gain unauthorised access to the information system through the Internet or other means. A good example of a threat agent is a hacker as shown in Figure 2.7.

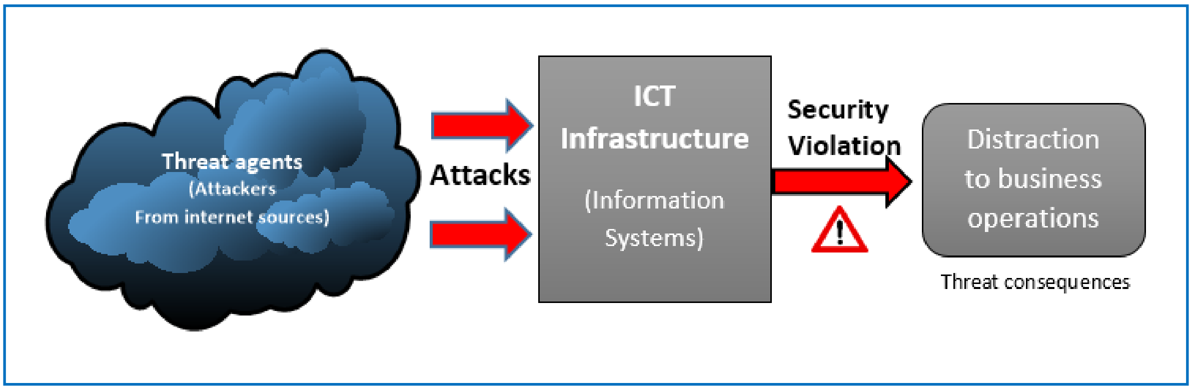


Figure 2.7: Demonstration of external threats to an information system

Source: Adapted from Huang and Behara (2014)

Figure 2.7 shows threat agents that may target an organisation’s information system using a variety of methods. It further shows that a security breach towards an information system has very damaging consequences towards the business; thus, a strong defensive mechanism is mandatory to protect a business and its ICT assets from threats.

- **Hackers**

According to Pfleeger (2007), a hacker is a computer genius who in most cases non-maliciously carries out illegal hacking work into a computer system for their gain or access to sensitive information or resources. Usually, they perform this act on behalf of someone with hidden intent. They use many different techniques to achieve this objective such as worms, backdoor Trojans, horses, and many other false pretences.

- **Malware**

Malware is software designed to destroy, steal private information, or spy on an information system without the prior consent of the owner (Meskovska, 2008). Its most popular form could be viruses, Trojans, adware, spyware, spam, and rootkits. These threats have the ability to perform and cause some of these activities:

  - steal user identifications (IDs) and passwords
  - remote control of computers and other network resources
  - theft of customer data
  - induce reduced network performance and bandwidth
  - increase internet traffic and changes to internet browser home pages and search engines

- **Social Engineering**

Social engineering is categorised as a non-technical intrusion approach that hackers use to exploit system vulnerabilities (Kaspersky, 2015). It is mainly dependent on human interaction and often involves tricking system end-users into defying security procedures.

- **Phishing Mail**

Phishing qualifies as a method of identity theft. Agents may use emails that look legitimate to lure system end-users into giving out sensitive personal or business information, such as a credit card, bank account, social security numbers, or other sensitive personal information (Trend Micro, 2015).

- **Web Exploits**

These take the form of malicious websites that threat agents use to exploit computer networks. They use features such as cookies, worms, and other spying means to extract information from information systems. They target end-users by using false pretences.

2.4.2.3. Internal Threats

An internal threat may be caused by an employee, staff, management, onsite contractor, or other members of a host institution that operates a computer system to which the insider has legitimate access (Humphreys, 2008). Insiders, as a result of legitimate access to their organisations' information, systems, and networks, create a significant risk to employers (Bellovin, 2007). Ironically, insider threats are an important yet often overlooked aspect of security (Williams, 2008). This potentially results in poor handling of the information system at the hands of internal system end-users with little or no computer and system know-how.

- **Untrained Employees**

The majority of reported security lapses and incidents which often lead to breach of corporate information security are perpetrated internally by members within the organisation. In this regard, internal end-users are perceived as the weakest link in information security (Warkentin & Wilson, 2009). The main threat to the integrity of corporate data primarily comes from legitimate system end-users or employees who are not aware of the result of their activities while interacting with the system (Microsoft Inc., 2015). Consequentially, an inside end-user without security awareness is a liability to the business (Logan and Clarkson, 2005).

- **Disgruntled Employees**

According to Humphreys (2008:247), a disgruntled employee is someone who might be resentful, be annoyed, or not content because of unfair treatment. This is the reason for the employee attempting to sabotage an IT system, to destroy company files and information assets, to speak badly about the company or their superior, to steal from the company, or to take other actions to compensate for their grievance. This conduct qualifies as a malicious insider threat (Microsoft Ink, 2015). Insiders are likely to have specific goals and objectives, and have legitimate access to the system. Employees are the people most familiar with the organisation's computers, system, and applications, and they are most likely to know what actions might cause the most damage. Insiders can plant viruses, Trojan horses, or worms, and they can browse through the file system effortlessly.

2.4.2.4. Common Threats

According to Jouinia, Rabaia and Aissab (2014), a security threat can cause one or several damaging impacts to the information system such as destruction of information, corruption of information, theft or loss of information, or disclosure of information. All of these are outlined next.

- **Interception**

This is considered when an unlawful person has got access to an information resource. The illegal party could be a person, a program, or a computing system. Examples of this type of bad conduct can include copying of program or data files, or wiretapping to obtain data in a network. Although a loss may be detected quickly, a silent interceptor may leave no traces through which the interception can be readily detected.

- **Interruption**

Interruption to a system can be qualified when an asset of a system becomes unavailable, goes missing, or gets destroyed intentionally by unwarranted parties. A good example is spiteful damage to a system's hardware, manipulation of a program or data file, or alteration to an operating system to make it fail or function in a less efficient way.

- **Modification**

This refers to unauthorised change to information. For example, someone might change the values in a database, alter a program so that it performs an additional computation, or modify data being transmitted electronically. It is even possible to modify hardware. Some cases of modification can be detected through simple efforts, others not, and one may get modifications that they cannot do anything about.

- **Fabrication**

An occurrence is labelled a fabrication in systems when a third party creates fake objects to intrude a computing system with the intention of changing the original design and operation. The invader may do this by introducing false transactions to a network or include bogus records to an existing database. Sometimes these bogus additions can be detected as falsifications, but when committed by professional hackers, they are not distinguishable from the real thing.

In this subsection, information system threats have been discussed ranging from the classification, types, and how they affect systems. It is clear that if threats are not managed, they can impact business operations negatively. Threats excel easily where a system has vulnerabilities which make it easy for the threat agents to reach their objectives.

2.4.3. Information System Vulnerabilities

A vulnerability is a weakness that allows a threat to cause harm (National Institute of Standards and Technology, 2010). Examples of vulnerabilities are information systems without proper policies to protect the use of information resources, no security centre to perform activities such as internet content filtering, buildings without access control to information resources, or a network without a properly maintained antivirus. Other forms of vulnerabilities could surface from human errors or mistakes in handling data through, for example, careless working or lack of training. These are categorically system vulnerabilities that can threaten the integrity of information assets or lead to unknowingly disclosing corporate secrets (Humphrey, 2008:248).

According to Bernik and Prislan (2011:208), the only way to control vulnerabilities and threats to information security is to have a process of risk management in place. Such risk management enables organisations to manage threats.

2.4.4. Information System Risks

A risk is the possibility of suffering harm or loss (Conklin & White, 2012). It is inevitable at some stage that organisations will suffer an information security incident. Such a downturn of events may create multiple negative impacts, such as loss of company reputation and customer confidence, legal issues, a loss of productivity and direct financial loss (Tøndel, Line & Jaatun, 2014). Generally, information security risks are hazards that individuals and firms all face (Hyeun-Suk Rhee, Ryu & Kim, 2012). It is therefore ideal for organisations to have a risk management programme within their organisation.

Risk management refers to the overall decision-making process of identifying threats and vulnerabilities and their potential impacts, determining the costs of mitigating such events, and deciding what actions are cost-effective for controlling these effects (Conklin & White, 2012:538). Figure 2.8 highlights the steps involved in risk management. It shows a step-by-step explanation of what needs to be followed in order to manage an identified risk according to ISO/IEC 27001:2013.

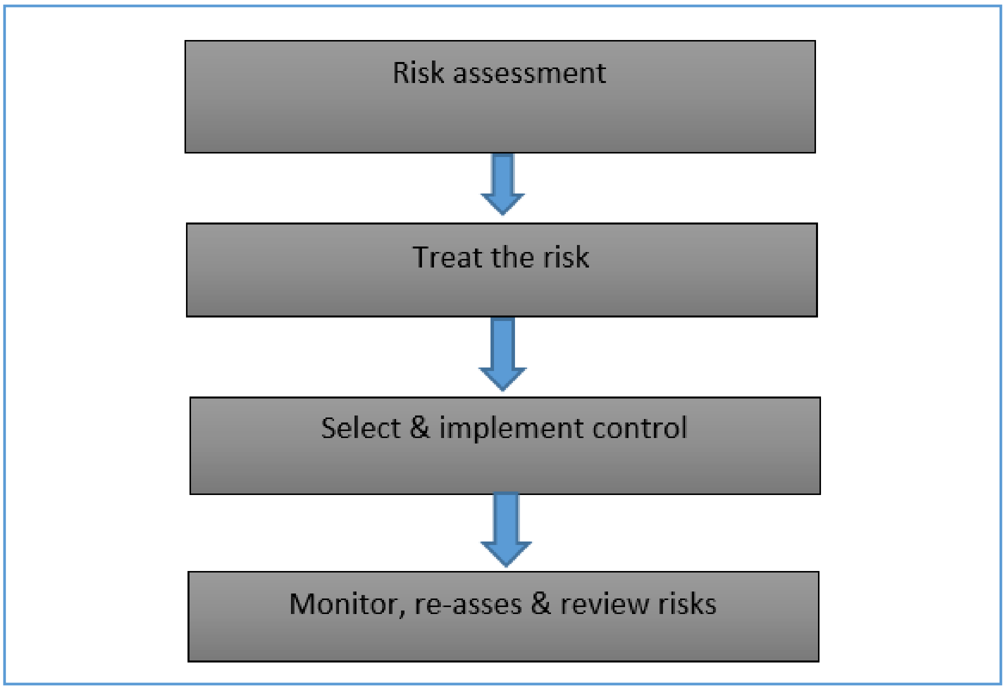


Figure 2.8: Risk management process

Source: Adapted from ISO/IEC 27001:2013

If a vulnerability is not attended to, it allows threats to progress and take advantage of the weaknesses in an information system. When threats succeed, it becomes a business risk that has the potential of creating a negative impact on the business.

2.4.5. The Impact of Threats on a Business

It is eminent that information technology (IT) and information system (IS) incidents have devastating consequences on a business and, as many examples show, may also have business-threatening impacts (Jarvelainen, 2013:583). Such destructive business incidents may result in multiple negative impacts, such as loss of company reputation and customer confidence, legal issues, loss of productivity, and direct financial loss (Tøndel et al., 2014:42). According to the observation of Brotby (2009), about 90% of organisations that lose their information assets due to the impact of successful threat attacks do not survive. This is so because the impact sometimes can create irretrievable damage to a business in so many different aspects.

The next subsection draws attention to potential consequences likely to result from successful threats to a business.

2.4.5.1. Economic Impact

One way or the other, information security attacks to any business setup may have negative effects on the organisation's financial position (Basani, 2012:32). Some attacks can have marginal effects on the organisation's business operations, while others may have enormous effects that may threaten its functioning and survival. In 2015, Bitstamp, a Slovenian company, once the world's biggest exchanges for trading the digital bitcoin currency lost around 19,000 bitcoins estimated at $650 million after a breach in its computer information security. The company was forced to suspend its services after the security breach (Reuters, 2015). The attack is believed to have targeted the UK-based exchange's operational wallets (also known as "hot wallets")

2.4.5.2. Financial Loss and Lawsuits

Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to substantial financial losses (Jouinia, Rabaia & Aissab, 2014). According to Kraemer et al. (2009), incidences of computer and information security vulnerabilities are on the rise, and the associated consequences have costly and business-threatening ramifications. A good example of high profile information security breach cases in 2014 involved Sony Incorporated and Bitstamp. The investigation that was carried out revealed that 25 million Sony customers' information on *Sony Online Entertainment* (SOE) was stolen and made available to the public (Mirror, 2011). The information leaked included names, addresses, emails, birth dates, phone numbers, and other information from PC games. Among all the clients whose information was accessed, at least 10 million also saved their credit card data therein. This incident highlights how data breach represents one of the major threats ICT systems face. Additionally, this has caused damages to a multinational company such as Sony, for millions of Euros in losses, and it also faces potential lawsuits by its clients for failing to protect their information.

2.4.5.3. Reputation or Confidence Loss

Negative publicity on an organisation has the ability to dent its reputation or brand, and could cause customers to lose confidence and loyalty, which prospectively may hand commercial rivals competitive advantage (Basani, 2012:81). For example, in the case of both Sony Incorporated and Bitstamp, existing customers who filed for lawsuits would never trust the safety of their private personal information at the hands of Sony or Bitstamp anymore. Even worse, the cost of capital in the effort to resurrect the corporate image and make up for the breach goes up.

2.4.5.4. Stakeholder Trust Loss and Legal Action

If an organisation reports a security breach, investors, customers, and stakeholders can use the courts to claim damages. It could even lead to some stakeholders withdrawing their shares, which could hamper business operations. After Bitstamp's hack attack in 2012 that saw the Slovenian business close for a while, Carney (2015), on his blog website, raises the following key concerns on behalf of Bitmap's clients:

- How will Bitstamp cover the $5 million loss, and is it currently running?
- Will it be through their own balance sheet?
- Will it be through insurance? If so, what kind of coverage does the company have?
- Will it try to recover through raising a new round of investment from existing or new investors, and has that been accomplished before?

From the foregoing, it is evident that the consequences of computer security breach through threats, vulnerabilities, and risks to any organisation have a very devastating impact. On that basis, it is a high priority that ICT infrastructure be protected in accordance with standard information security critical success factors to minimise the probability of successful attacks while increasing the chances of operating in a highly secure environment.

2.5. Information Security Critical Success Factors

Following the discussion in this chapter, there is no doubt that an organisation ought to invent a good security procedure for its information system and infrastructure to meet its operational target. On that account, Table 2.2 summarises the critical success factors (CSF) that are perceived to be of extreme importance when evaluating the maturity of the overall information security landscape of an organisation. While there is no single security formula that can guarantee 100% ICT infrastructure safety, to a certain extent, combining the CSFs in Table 2.2 obtained from ISO/IEC 27001:2013 and investigations offers a convincingly high degree of confidence that the overall information and communication landscape is highly secure.

A secure information system must be capable of preventing and detecting risks and threats, while at the same time, it crucially must possess the means to successfully recover from eventualities such as a successful attack (Saleh, 2007). To be able to comply with that, the factors in Table 2.2 need to be a reality.

Table 2.2: Information security critical success factors

	Description
CSF 1 **Security Policy**	It is mandatory for every organisation to have an information security policy document which is strictly enforced: this is the beginning of security. Many companies may have security policies, but the implementation to impose them on employees is weak (Kavanagh, 2006).
CSF 2 **Management Support**	Information security should be instituted as part of a strategy to protect a business, its operations, and assets. According to Caballero (2009), security in an organisation should not be looked at as an IT problem; it is in fact more a business problem. Layton (2009) further emphasises that information security strategy must be connected to an organisation's business plans to appropriately protect employees, assets, and future business plans. It must get full management support.
CSF 3 **Simplicity of Security Policy**	The security policy document must be comprehensively written using simple language understandable by even non-IT employees. System end-users must be acquainted with the security policy, procedures, and standard practice when they interact with the system.
CSF 3 **Security Awareness & Training**	Information security must be promoted to employees effectively (ISO/IE 27001:2013). The value of security to business must be highlighted to all employees who are end-users of the system, from the CEO right down to the cleaner so as to create the urge to work towards system safety whenever they interact with the computer system.
CSF 4 **Accountability**	An organisation's information security architecture must integrate a tradition of extending policy guidance to employees. For the most part, end-users must be aware of what is expected of them and what acceptable use entails, including accountability for non-compliance.

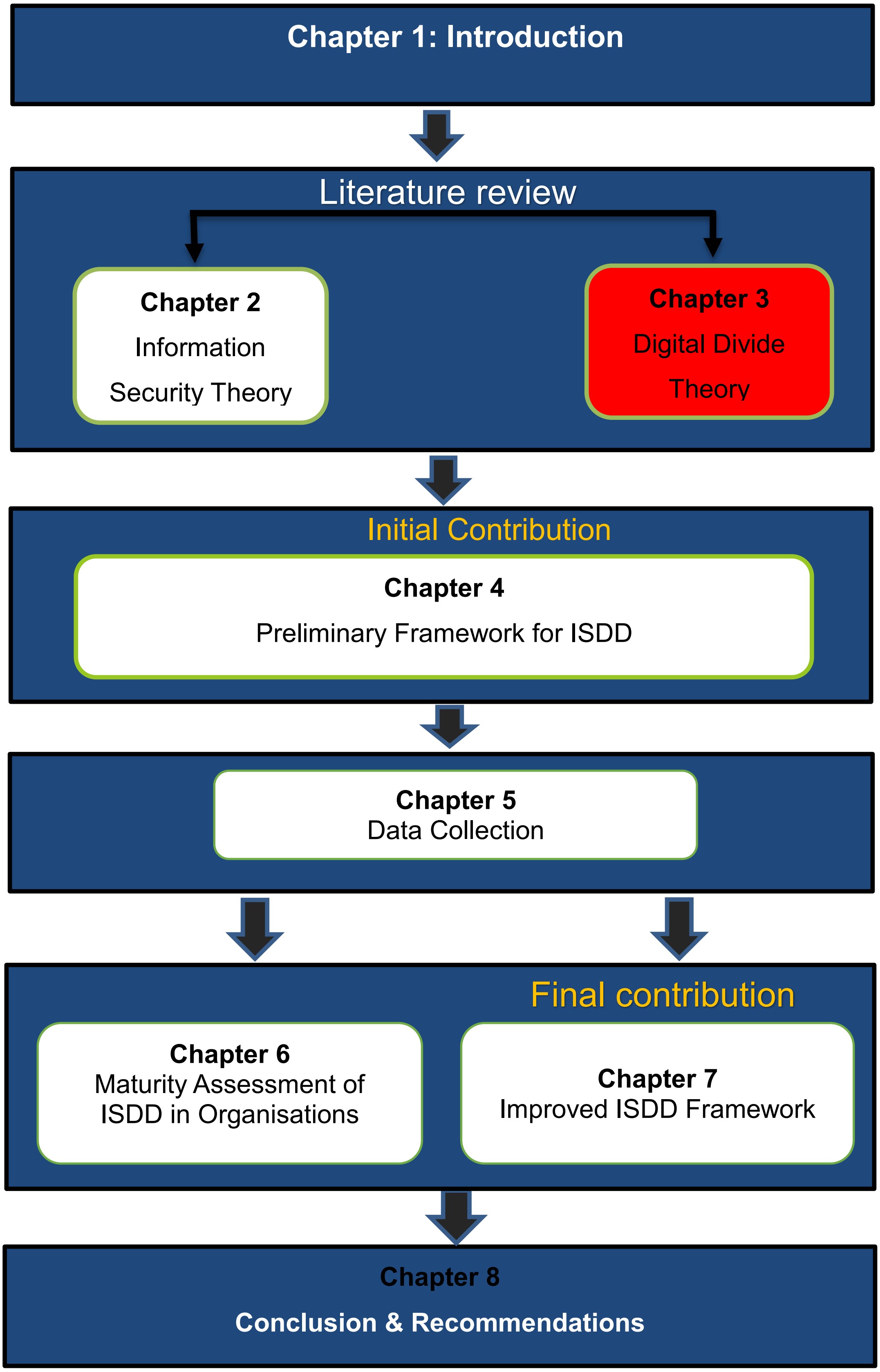
	Description
CSF 5 **Risk Management**	In every organisation’s security programme, there must be a focus on risk analysis and management structure plus a countermeasure plan to respond to eventualities. Information security personnel must have an inventory of the most valuable IT infrastructure as well as a forecast list of trending security risks which they must regularly sensitise end-users on how to respond to such risks.
CSF 6 **Performance Measurement**	A security architecture must be systematic and well-structured to a point where it is easy to track its performance by keeping abreast with improvement or lack thereof over time. Jaquith (2007) reiterates that one can only improve on a security programme if it is assessable.
CSF 7 **Self-assessment Tool**	An information security programme must have strong end-user control and monitoring. This must include a screening tool for new recruitments to measure their security awareness pedigree and check background to have a good understanding of their history security-wise.
CSF 8 **Business Continuity Plan**	In the event of a successful security breach that paralyses operations, a good security programme must have a swift recovery plan. This is often regarded as a business continuity plan or disaster recovery plan.

2.6. Conclusion

The purpose of this chapter was to explore literature on the information security landscape in organisations in order to identify its critical success factors to be relied upon in subsequent aspects of this study. This was achieved after an organisation business case in order to demonstrate the operations of an organisation. Furthermore, it was showcased how the business heavily relies on the support of ICT infrastructure to function competitively and meet its business goals. However, ICT infrastructure cannot be relied upon if it is not secured. To supplement that, the fundamentals of information security and how that is essential in safeguarding business information assets were explored. The chapter concluded with a discussion of critical success factors that are required in order to consider an information system reasonably reliable, safe, and able to meet the required minimum standards in accordance with existing security models such as ISO/IE 27001:2013 and COBIT.

The next chapter discusses the notion of digital divide and contextualises the concept to that of enterprise information security, leading to the relatively new concept of information security digital divide.

Chapter 3: Information Security Digital Divide in Organisations



3.1. Introduction

The preceding chapter explored organisations at structural and operational levels and justified the need to have a secured ICT infrastructure for supporting business operations. A range of critical success factors were identified in the framework of information security. Building on that, this chapter thus conceives the concept of information security digital divide as an additional re-enforcement measure to information security. This chapter is relevant to the research in the sense that it helps an organisation to relook at information resource accessibility and usage to measure control levels in order to upscale overall information security. This is achieved by first understanding the organisational ecosystem and then examining the flow of information in order to establish the best possible accessibility and information use control. In so doing, the research question "*How can the concept of digital divide be leveraged in the context of information security at organisation level?*" will be addressed. This ultimately will result in the identification of critical success factors for information security digital divide.

This chapter provides an overview of information security digital divide by first describing and then dissecting types of digital divides. It illustrates how information security and digital divide are combined to form the core concept of information security digital divide. The organisational ecosystem is then addressed for understanding the flow of information to determine how stakeholders interact in reference to their functions, roles and responsibilities, and how that affects accessibility and use of information together with the impact it may have on the overall organisation. The impact of accessibility and use is then introduced. Lastly, critical success factors (CSFs) of information security digital divide (an extension of information security) are explored before concluding the chapter.

3.2. An Overview of Digital Divide

Since the inception of the digital divide, it has become a topic that is researched more from an information and communication technology for development (ICT4D) point of view. Nevertheless, there are many varying definitions and types of digital divides. For instance, Van Dijk (2006:178) defines the digital divide as ‘‘the gap between those who have and those who do not have access to computers and the Internet’’. However, the most popular definition of digital divide is that of Partridge (2005), who explains that, traditionally, digital divide is globally perceived by many researchers with a socio-economic perspective, predominantly focused on accessibility to telecommunications technology, the Internet, and the capability to use this technology to fully participate in business. Figure 3.1 depicts an example of the digital divide in the context of ICT4D.

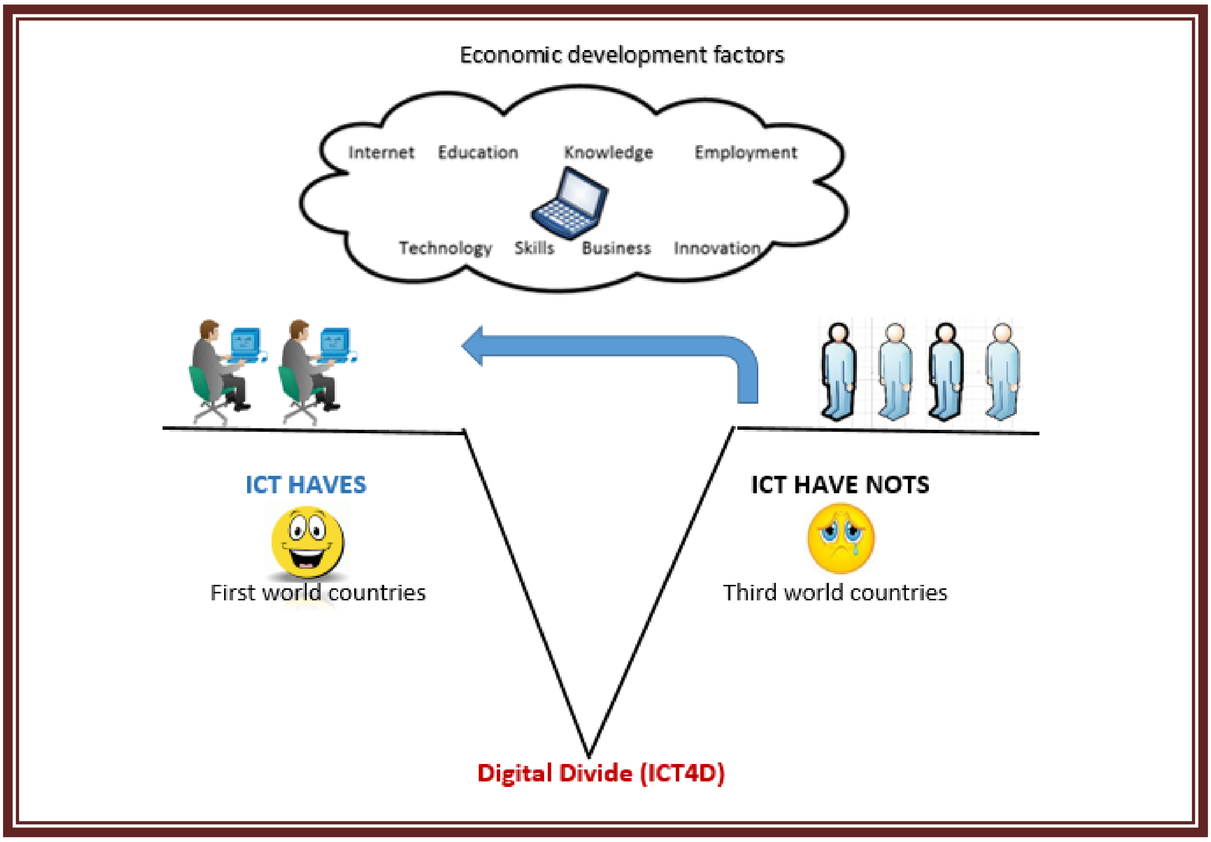


Figure 3.1: Digital divide overview indicating the haves and have-nots

Source: Adapted from Eubanks (2007)

In theory, according to Figure 3.1, if the technology accessibility gap between the haves and have-nots is too wide, it is not good for economic development. That said, the concept of digital divide can also be extended and used in other perspectives such as ICT security within an organisation, which is the focus area in the next segment of the chapter.

3.3. Digital Divide in the Context of Information Security

In addition to the literature in the preceding section on digital divide, Warschauer (2002) maintains that not only should digital divide be understood from a physical access to computers and connectivity viewpoint, it must also incorporate people's ability to make full use of systems. Likewise, Rao (2005) observes that digital divide could also be as a result of differences based on access to information and other information technologies, including the ability to use information. Albrechtsen and Hovden (2009:477-478) further substantiate this by positing that the digital divide is not only a question of access to information systems that have implemented adequate information security technology, it is also about considerable differences in skills, knowledge, roles and responsibilities, perceptions, and interpersonal relationships between various members of an organisation. Some of these differences, in effect, build towards the concept of information security digital divide (ISDD).

Based on the foregoing and in the context of this research, the digital divide is then contextualised in terms of accessibility and usage of corporate data by end-users, partners, and stakeholders. Primarily, this is supposed to be dictated according to the standard information security policy which regulates access and usability. It is further characterised by the alignment of system end-users, partners, and stakeholders to their business functions, roles, and responsibilities. This is similar to the concept of Role-Based-Access-Control (RBAC) where specific rules are defined for each individual within an organisation to restrict access to system resources according to their job or function (Fadhel, Bianculli, & Briand, 2015).

Therefore, in this research, information security digital divide will be defined as follows:

The control of access to corporate data and its use within and outside an organisation according to the relevance it has to an end-user, partner, or stakeholder based on their business roles and responsibilities, and functions within the structure of an organisation. Additionally, a partner, stakeholder or end-user is defined as a system operator or person who legally has permission within and outside an organisation to access and use certain relevant ICT resources and information.

In summarising both types of digital divides explored, it is evident that according to ICT4D, *a high digital divide is bad for economic development, whereas with* *information security digital divide, a high divide is good for the safety of corporate data*. Having defined and contextualised ISDD, the subsection that follows will combine the rationale of information security and digital divide to utilise this concept to demonstrate the value ISDD has in strengthening information security.

3.3.1. The Digital Divide Theory

Information security as discussed in Chapter 2 and demonstrated further in the CIA triangle in Figure 3.2 ensures information possesses confidentiality, integrity, and availability (CIA). In sum, the combination of confidentiality, integrity, and availability produces favourably safe corporate data and services.

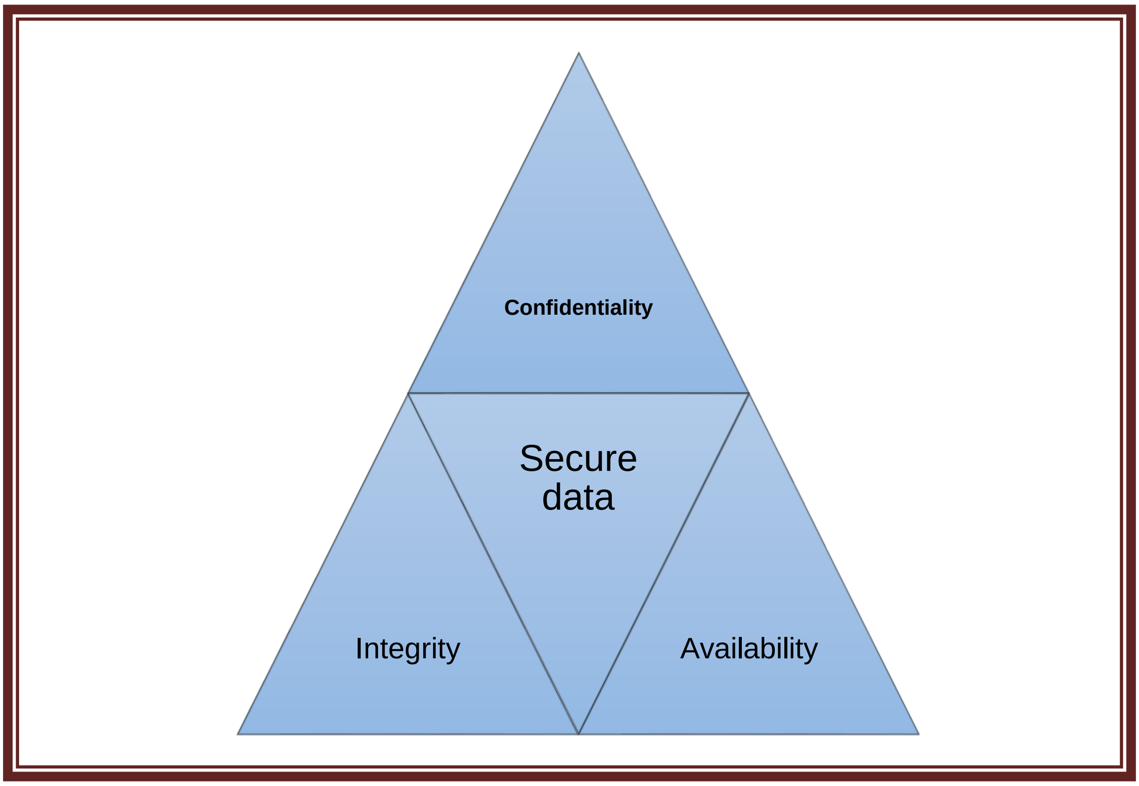


Figure 3.2: Information security requirements

Source: Adapted from Kaya (2012)

However, there is a range of assumptions that information security on its own does not completely provide answers to in the context of security, such as addressing ever-changing systems access control complexities and environment. But with the incorporation of ISDD, those concerns can be mitigated. These assumptions include:

- Information security on its own offers limited internal and external accessibility control techniques, while digital divide aims to create information accessibility haves and have-nots in harmony with what every end-user, partner, and stakeholder needs in order to perform their work. For example, internally, the finance department should only be able to have physical access to finance department computing resources. More so, such a divide is narrowed at individual end-user level to only provide accessibility and usage to those end-users who have the necessary credentials based on their functional role in the organisation. As such, those computing resources should be the only ones they can log on to and on top of that, these associated computers from a network perspective should only be able to view resources on specific servers and intranet resources.

- While information security protects ICT infrastructure, digital divide takes that information infrastructure and splits it into segments to safeguard it digitally. For example, in high technology organisations, certain departments that do not require access to the Internet can have computers that can connect to internal resources such as intranet, payroll checking, and many others, but they cannot surf the Internet.

- The human factor is considered the biggest threat to security (Gate Protect, 2015). However, information security focuses more on technical solutions such as firewalls, virus prevention, spam filters, and packet tracing. Digital divide, on the other hand, is a non-technical security approach that concentrates on the human factor, primarily on accessibility of information resources by end-users. Therefore, it will complement information security to improve overall security performance.

Combining Figure 3.2 and the assumptions raised in this subsection generates Figure 3.3. It also justifies the contextual definition of information security digital divide in this study.

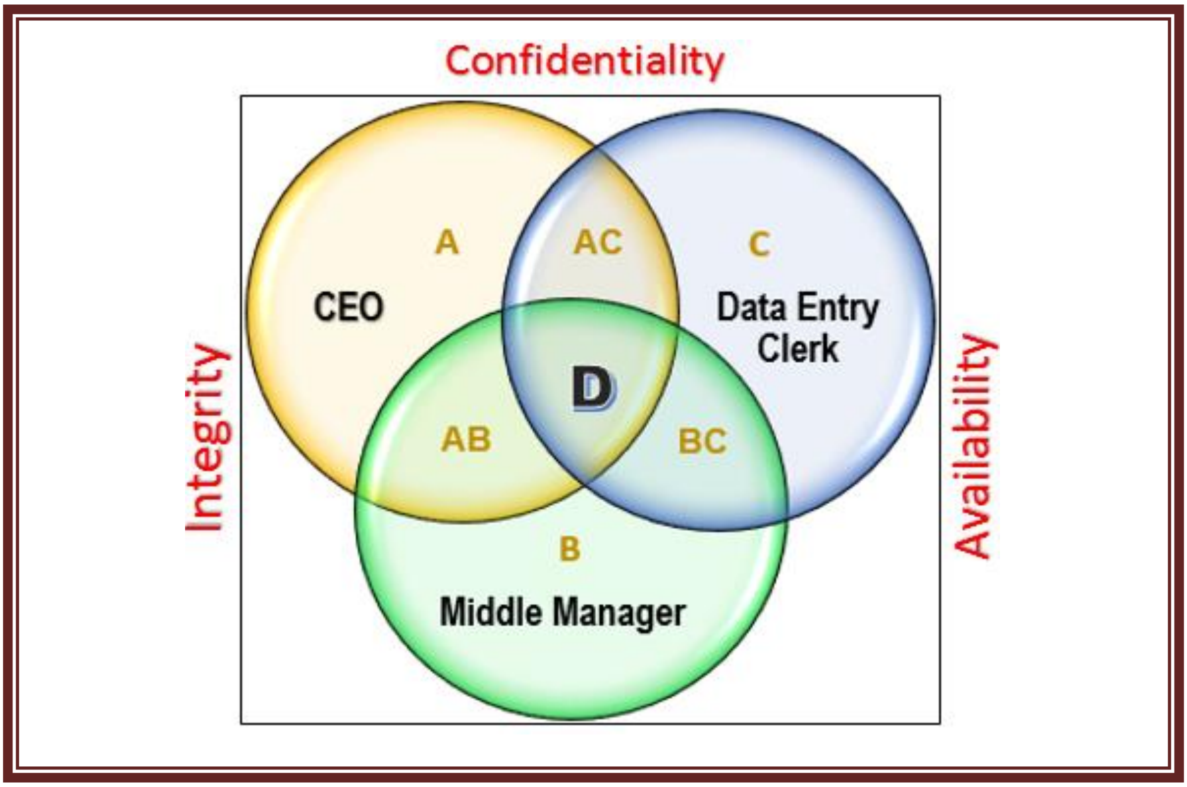


Figure 3.3: Information security digital divide and how it strengthens overall information security

Figure 3.3 illustrates the accessibility interrelationship of corporate data between internal stakeholders. For example, a high divide (**A, B, C**) is inevitable among all the three stakeholders, namely, chief executive officer (CEO), middle manager, and data entry clerk while ensuring the three characteristics of information security (CIA). The role of the divide is to ensure stakeholders have accessibility to corporate data according to the relevance. The relevance of corporate data to every end-user is guided by their business function, roles, and responsibilities, and it is explained in a living document called information security policy, which acts as terms of reference.

Further on, the intersection labelled **D** in Figure 3.3 indicates the common area that should be accessible to everyone in the organisation irrespective of business function, roles, and responsibilities. However, from a DD accessibility and usage perspective, the traditional information security proxies (confidentiality, integrity, and availability) alone fall short of defined strategy to efficiently isolate this corporate data in **D** in the event of a security breach by internal or external threats. Characteristically, **A** should only be exclusive to the CEO, while **B** to the middle manager and **C** to the data entry clerk. In the same order, information sharable between the middle manager and data entry clerk **BC** should be strictly unavailable to other stakeholders including, for example, the CEO. Although he is senior to the data entry clerk, he must not interfere in the scope of work by virtue of his seniority status on the organisational structure. However, when there is a need for the two business roles (CEO and data entry clerk) to work together, the system must temporarily make provision for such occasions. Equally, other aggregations in Figure 3.3 such as **AB** and **AC** must follow the same pattern. This demarcation matrix can extend to not only access to information but also the resources supporting them on an information system.

The level of maturity of ISDD in an organisation can then be determined based on how well accessibility is controlled and successfully highly restricted only to relevant end-users. For example, if IT support staff come and perform preventive maintenance on the CEO's computer, the profile used to access that computer must not be permitted to view any of the CEO's documents or explore any other areas not necessary for their role on that computer. However, given a circumstance where a business role may be required to break the principles of ISDD in order to perform a duty, e.g. IT support needing to resolve a failure on a hardware which directly stores the finance manager's sensitive data, such cases must be protected through a non-disclosure agreement to ensure no information accessed or viewed may be revealed or moved. All the aforesaid should be contained in the IT security policy.

The next subsection considers a sample of an information security template with accessibility policies that are aimed at demarcating end-users as well as act as a first line of security to a computer system. The sample used is inspired by that of another template (Trinity College Dublin, 2015).

3.3.2. Information Security Template Sample

Organisations invest a substantial amount of resources in order to support business operations through a sound information and communication technology landscape. It is therefore for this reason that criteria for protecting this vast investment should be instituted. This information security template applies to all computer system end-users including internal staff, company partners, stakeholders, and other external end-users not itemised. Everyone categorised herein must comply with all appropriate parts of the IT code of conduct as outlined in Table 3.1.

Table 3.1: Sample of security policy

I. Network Access Policy ✓ Only authorised network administrators or personnel may connect devices to the computer system ✓ Only authorised devices may be connected to the company system ✓ Authorised devices include PCs, laptops, handheld devices, and workstations owned by the company that complies with the configuration guidelines and standards of the organisation
II. Remote Access Policy ✓ Only permitted secure remote access technologies should be allowed, e.g. VPN, voice recognition, remote desktop connection, telephone ✓ All devices connecting to the company system must be approved by IT experts, and all such devices must comply with secure connection standards **II.(a) Non-standard Remote Access Connections** • External end-users who wish to use non-standard remote access technologies must obtain prior consent from the IT department for clearance • External end-users adopting third-party technologies must be made aware of the expectations from them of the ICT experts
III. Data Protection and Handling Policy ✓ All corporate data or programs formed/retained/stored by an end-user or connected to the computer system may be subjected to random inspection by IT support staff without any prior notice, especially when any breach of security is suspected
IV. Non-disclosure Agreement Policy ✓ All agents, contractors, partners, suppliers, and external end-users should be made to enter into a non-disclosure agreement for the purpose of security **V. Password Policy** ✓ End-users may not share a password or write it down where it is visible to others ✓ All passwords must meet the required minimum complexity of 10 characters mixed with lower and uppercase, numbers, and other special characters such as !@#$%^& ✓ Passwords must be changed every 90 days ✓ End-users that suspect passwords have been compromised must change them immediately

In Table 3.1, a security template with specific policies to manage aspects of security such as accessibility, non-disclosure agreement, data protection, and password management were briefly described. The next section will now present the flow of information within an organisation, taking into consideration all the various reporting structures in accordance with the design of the organisational structure. Often, the flow of data determines how the access matrix policy can be customised by internal information ICT experts.

3.4. Access and Usage of Information Resources within an Organisation

In this section, the focus is on information flow, how it is accessed and the use within and outside the organisation by relevant stakeholders. The section concludes with the impact of accessibility and usage of information resources on business operations. As a disclaimer, although the organisational structure discussed next was already introduced in Chapter 2, the fact that it is revisited in this section is for highlighting information flow necessary for the implementation of ISDD.

3.4.1. Organisational Structure

To facilitate cross-boundary information sharing within an organisation, an understanding of factors influencing information sharing is critical to establish and maintain collaborative relationships (Creswell, 2005; Gil-Garcia, Soon Ae, & Janssen, 2009; Pardo, Creswell, Dawes, & Burke, 2004; Zheng, Jiang, Yang, & Pardo, 2008). To realise that, one useful tool organisations could turn to is the organisational structure. An organisational structure shows the relationship between internal departments and subsystems (Petrauskas, 2006). Potentially, it is the operating manual that informs members how the organisation is structured and how it works (Community Tool Box, 2014). An effective organisational structure facilitates management and clarifies relationships, roles and responsibilities, levels of authority, and supervisory or reporting lines. Most organisations follow the traditional organisational structure style, where the hierarchy resembles a pyramid (Pathfinder International, 2014), as shown in Figure 3.4.

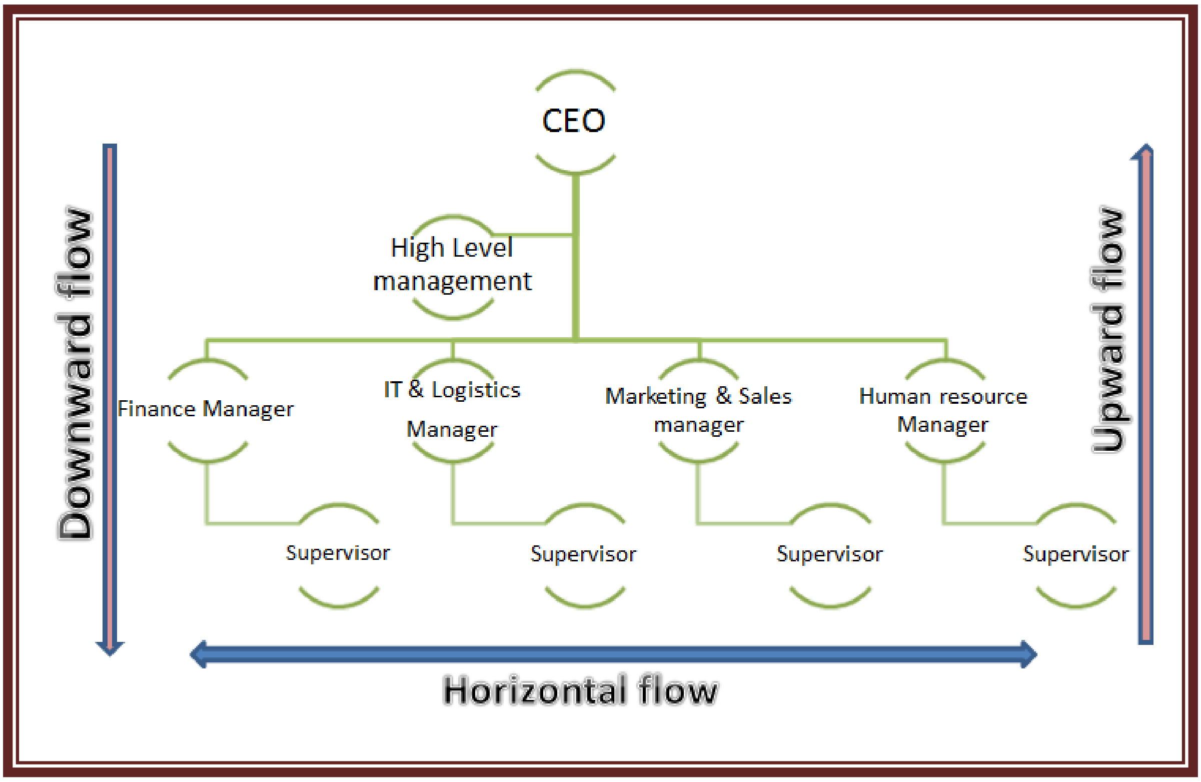


Figure 3.4: A generic traditional organisational structure

Source: Adapted from Organisational Development (2000)

Figure 3.4 is a summary of the different reporting lines according to business functions, and roles and responsibilities in harmony with the organisational structure. It will help in understanding some business functions and how business roles and responsibilities need to interact internally, in the process making them primary generation points of corporate data. On the other hand, while being considered consumers of data, which they rely on to interact with external stakeholders such as suppliers, partners, and third parties, some business roles also in return collect external data valuable to business operations. This makes them information generators.

3.4.2. Information Flow in an Organisation

"Information flow is so important to a business such that it can be compared to the value oxygen has to human life (Al-Hakim, 2008). Drawing on that reasoning, information sharing has been stressed as an important driver of organisational performance (Yang & Maxwell, 2011). According to Hatala and Lutta (2009), information flow relates to the movement of information or data between members of an organisation. In organisations, information flows in verbal, written, or electronic form

(Yazici, 2002). It can also be classified according to the direction of the flow (Rishipal, 2014). Traditionally, information in organisations flows upwards, downwards, or horizontally (Lunenburg, 2010). Vertically, information flows up and down among managers. For example, production supervisors constantly communicate with production line workers and their own managers. In contrast, in the horizontal case, information flows sideways among departments. One such good example is regional sales managers from the marketing department who set their sales goals by interacting with IT and logistics managers as shown in Figure 3.4 over a new product dependant on logistics and IT departments.

No matter how information is designed to flow in an organisation, it is required to do so freely among members if the organisation is to compete firmly (Hatala & Lutta, 2009). By examining the culture of information flow, one can get an idea of how well people in the organisation are cooperating, and also, how effective their work is likely to be in providing a safe operation (Westrum, 2014).

With the help of a graphic representation of an organisation's structure, a manager will be able to define tasks and determine information flow within the organisation effectively (Pathfinder International, 2014). This then enables the flow of business processes and workflows to be understood better because when information flow is uncontrolled, a client's sensitive and proprietary information about an unpatented business concept, business plans, customer list, salaries, trade secrets, and financial plan, just to mention but a few, cannot be protected (Demski, Lewis, Yao, & Yildirim, 2010).

Understanding information flow requires the understanding of stakeholders within and outside the organisation. In the next subsection, stakeholders are discussed as well as how they interact to the benefit of an organisation.

3.4.3. Stakeholders Interaction and Access to Information

Knowledge produced in organisations by individuals is the product of the interactions and information sharing of individuals within the environment (Vicka, Naganoa, & Popadiuk, 2015). It, therefore, makes knowledge sharing very critical to an organisation's competitiveness. Knowledge in an organisation may flow in two possible ways, namely, intra- and inter-organisational flow. The intra-organisational flow is confined to the boundaries of the organisation and is only available to internal stakeholders. On the other hand, inter-organisational knowledge flow extends beyond the organisation and involves external parties such as suppliers, shareholders, business partners, competitors, and industry regulators, amongst others.

3.4.3.1. Internal Stakeholders

Internal stakeholders are people or personnel who work within the organisation; they can be classified as employees, investors, and owners (Boundless, 2015). An employee is a person employed for wages or salary (Oxford Dictionary, 2015). Each employee has their own role to play and their own scope of responsibility, which contributes towards realising the organisation's goals (Albrechtsen & Hovden, 2009). Because of the uniqueness of their business function, roles, and responsibilities, employees require accessibility and use of corporate data for different reasons and at different levels. Examples include the CEO, senior managers, middle managers, supervisors, and data entry clerk, which are briefly discussed next.

- **Chief Executive Officer**

The CEO is qualified as the top executive on the hierarchy responsible for a firm's overall operations and performance (Business Dictionary, 2014). He or she is the leader of the firm, serves as the main link between the board of directors (the board) and the firm's various parts or levels and is held solely responsible for the firm's success or failure. During their day-to-day roles and responsibilities within and outside the organisation, CEOs interact with various stakeholders, and in the process, they access, generate, and use corporate data.

Internally, the CEO may interact upward, downward, or horizontally depending on what kind of information he/she may need to access or use. For example, if the CEO requires a financial report to present to the board of directors, he/she may request that from the finance manager. Figure 3.5 reveals how a CEO may channel instructions or request information within an organisation.

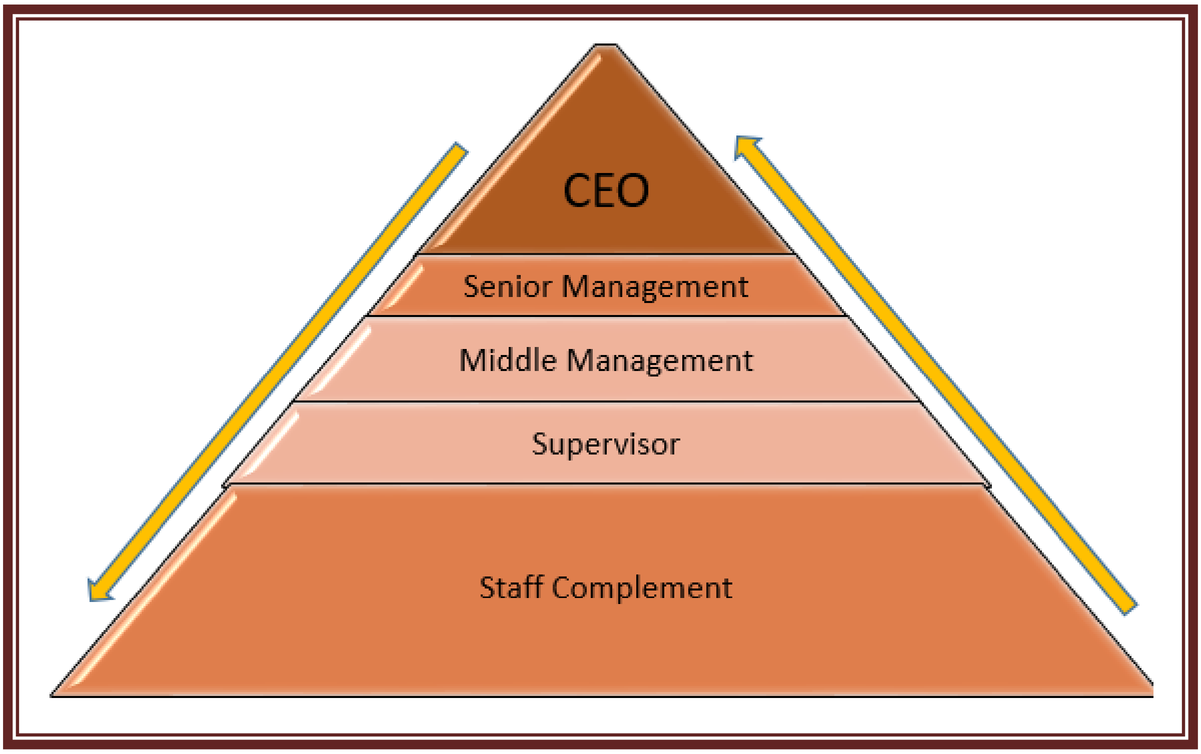


Figure 3.5: Information flow in an organisation

Source: Adapted from Liang (2011)

Externally, the CEO may engage other stakeholders for better understanding of organisational performance. When decisions are made in colaboration with stakeholder input, there is a greater chance of success. A CEO may then engage various stakeholders for first-hand experience in order to update the board on the progress the organisation is making or obstacles faced in an effort to meet the overall strategic objective.

As much as the CEO may be the highest in the hierarchy, from an information system standpoint, he/she should have no control over certain workflows. For example, he/she cannot approve leave for a system programmer without knowing whether there is a resource to continue business services anchored by that resource. This is because despite already not having knowledge of that department's operations, he/she may also fall short of correct technical insights to make that call. Such a decision is best made by well-placed personnel within the organisational setup, e.g. a qualified senior manager in the field. This is a befitting reason for not allowing a CEO to have control all across the organisation.

- **Senior Managers**

Senior managers are responsible for the vision of the organisation; they are more concerned with long-term strategic planning (Fergusson, 2013). To sustain their roles and responsibilities, they require interaction with all departments within an organisation to plan for future growth and the overall direction of the organisation. For example, they might need to plan for the marketing or sales department for the next five years. They also act as the link between the CEO and middle managers.

Their overall roles and responsibilities include managing both long- and short-term policies to sustain the business (FFIEC, 2015). To achieve this, senior managers may require access to certain information resources applicable to their line of duty from various departments, and in the process, also generating, accessing, and using corporate data.

Senior managers ensure the organisation produces results and that those results are produced consistently over time (Faust, 2012). Realistically, this means that most of the firms may decide to enter global markets, thus consequently improving their innovativeness (Smirnova, Kouchta, Podmetina, Vaatanen, & Rebyazina, 2009). Interaction with global markets by default means senior managers engage external stakeholders such as industry partners and suppliers. In the process, they generate access and use corporate data at almost all levels, since they also supervise middle managers.

Similar to the foregoing discussion on the CEO’s roles and responsibilities, even though senior managers may be placed above everyone in the organisation except the CEO, they should not be empowered to dictate all work processes above or below them on the hierarchy which they are not well-suited for or do not have expertise on. For example, a senior manager should not have the power to command a process change in the production department where he/she has no know-how. Such an activity must be in consultation with a well-qualified middle manager in that department.

- **Lower Managers**

Middle managers are mainly specialised in summarised information such as reports but may also be involved in decision-making. The information they require for their work may flow both vertically and horizontally within the boundaries of the organisation. They mainly work with budgeting and performance evaluation. They also focus on the implementation of long-term strategic plans raised by senior management (Darkow, 2015). Most crucially, they act as the link between the CEO, senior management, and the rest of the staff complement such as supervisors and data entry clerks.

Internally, middle managers receive instructions from senior management and pass that on to the staff complement below them on the organisational structure as an implementation process strategy. Equally, they make follow-ups to see whether this implementation is falling in place in accordance with its intended plan. They then resubmit this information through reports to senior management. They, therefore, access data in various places. In some cases, their responsibilities may require them to make contact with external stakeholders.

From a hierarchy perspective, middle managers should also be limited to profile expectations as guided by the organisational structure. They may not for instance initiate a payment process by electronically authorising online processes on behalf of the accounting department.

- **Supervisors**

Supervisors are generally individuals who on behalf of the organisation are skilled in making different groups work together in an organised way to achieve something (McNall, 2011; Cambridge Online Dictionary, 2015). They deal with up-to-date daily information which is primarily flowing vertically. All personnel that fall under a supervisor are directly responsible to the supervisor. Primarily, a supervisor's requirement for information mainly flows vertically.

Since they specialise in making groups within the organisation work together, supervisors on a daily basis generate performance-driven reports and information required by middle managers for their reporting to superiors (McNall, 2011). This requires supervisors to append existing reports as new data comes in. For example, data entry clerks verify and ensure data is accurate before it is dispatched to the system or sent over through email to relevant personnel. Supervisors in most cases only interact with internal stakeholders. They mostly generate information for internal usage.

Similar to the rest of the employees, supervisors should be limited to their roles and responsibilities by virtue of position on the organisational structure. However, because of eventualities such as a resource under them falling sick untimely, there should be a contingency plan improvised by the supervisor to maintain continuity. That plan could involve positioning some other resource to execute the duty of the ill resource in order to avoid taking the blame when business operations come to a standstill as a result of the unavailability of a resource.

- **Data Entry Clerk**

Data entry clerks in most organisations compile and transfer information for business and other organisations. The roles and responsibilities of a data entry clerk are summarised as compilation, entering, sorting, interpretation, and verification of data into the system (Nurse-Family Partnership, 2009). The nature of the job description leads to mostly generation of raw data while at the same time needing access and use of this same data.

In an organisation, the data entry clerk is at the front collecting information and updating it when necessary. Being the entry point of raw data, this responsibility requires the clerk to interact with other staff members such as field workers that may conduct field work for the organisation. This is important, for example, for brand popularity or consumer reference surveys which are done by word of mouth or interviews.

It is mandatory that the profile of a data entry clerk be confined to its duties by the system to avoid overlapping of information access. For example, a data entry clerk must not be allowed to change information on the middle manager’s profile after data is already processed and converted into meaningful information.

- **System Administrator**

According to Limoncelli, Hogan and Chalup (2007), a system administrator is a computer professional with access level to a system that exceeds that of a normal end-user. Their primary role is to upkeep and ensure that a system functions efficiently. They achieve this objective by installing, configuring, and supporting ICT infrastructure such as servers, routers, computers, and all the front- and back-end software applications that work with it.

The responsibilities of a system administrator allow them to generate information as they interact with both the system and its end-users on issues that affect their work. They can create documentation on end-user performance, network performance, threats, risks, and other new security trends. They use this information to create awareness campaigns and also to present to management on IT operations.

Further to their scope of work, system administrators are empowered to view and access all ICT infrastructure including servers and computers. However, it is mandatory that there be some form of control to ensure they are also regulated to only manage work processes that are in line with their scope of work as prescribed by management. For example, during their routine IT support maintenance or response to a fault on the CEO’s computer, their ability to view, access, or manipulate data without prior consent must be highly restricted. It could also be that they must not be given privileges to financial services of an organisation, be it physically or from an application point of view.

- **Super User**

A super user is an account on a computer system with elevated privilege levels that exceed an ordinary user account (Holme & Thomas, 2008). In most cases, this is allocated to a junior IT support staff or an advanced user that performs some simple IT support tasks such as creating new users, resetting passwords, connecting printers, and managing antivirus services.

This user may have mini-administrative duties to document any network activities as delegated by the system administrator or chief information officer. However, this delegation should not exceed any privileges beyond their technical expertise. Given an instance where the system administrator is unavailable, a junior IT support staff should not be empowered with delegation rights that permit them to fidget with highly critical server processes that need advanced skill sets to manage or rectify. Also, when he/she is tasked to check on an antivirus problem on a senior manager's machine, using his/her profile, he/she should not be able to view any of the manager's sensitive documents.

- **Chief Information Officer**

A chief information officer (CIO) is a dedicated IT director who is not only responsible for synchronising information technology, information security, and information strategy to business needs (Avison & Wilson, 2002). Today's CIO is also a business leader (Deloitte, 2004). This business function acts as the connection between business IT projects and the management of the organisation with the sole purpose of maximising returns from ICT investment to improve operation efficiency (Avison & Wilson, 2002; Deloitte, 2004).

Lawry, Wadell and Singh (2007) state clearly that the CIO is about designing strategy. That in itself is generation of data. Given that this position is executive, it must not, however, spill over its responsibilities. As an example, if the CIO wants to pay for a phase of a project, he/she must not have a direct role in the payment system – that must be handled by the finance director who owns the right procedures.

3.4.3.2. External Stakeholders

According to Avison and Wilson (2002), external stakeholders to a business could include customers, suppliers, shareholders, and investors. In accordance with their business functions, and roles and responsibilities, their interests in corporate data vary.

- **Customers**

Customers basically define the client base of the business. Their focus is always goods on offer, promotions, customer service, and the pricing of goods (GCSE Business, 2015).

Customers interact with the organisation's information system in different ways depending on the services and products they may require. They help the business generate information through activities such as leaving comments on website blogs on service delivery satisfaction or how to improve business.

Customers require access to the system, for example, through the portal to check on latest products, online shopping, pricing, promotions, or any information from the business that concerns them. Regardless of how they access business systems, it does have an impact on the security of business systems. As customers access the system through the portal, they should, for example, not be able to order goods from suppliers on behalf of the business. The system should not take any other service request other than what customers are defined to access.

- **Suppliers**

Suppliers are considered as trusted external end-users. They are very critical to most businesses today. Their relationship with the organisation is unique and direct because they also hold a stake in the business (Business Case Studies, 2014). They supply specific products which they agree on with the business (Cambridge Online Dictionary, 2014).

Since they have a stake in the business, suppliers may require access to business information systems in order to effectively perform their responsibilities such as to deliver goods and services on behalf of a business in a timely and reliable manner. They might need to know delivery schedules, places, and customer details. One way of achieving this could be to give them access to a Web portal, email, or instant messaging. However, these services such as instant messaging or email should be protected from risks that are associated with external connections into the internal system.

- **Investors**

An investor is a person who allocates a share of their capital to a business, with the expectation of financial gain in the future. Their role is to monitor their investment and the overall performance of the organisation (Cambridge Online Dictionary, 2015). Technically, investors are the owners of the business. Business owners refer to persons who have invested in an enterprise to own its’ stock, and that management are merely their employees (Aguila, 2014). This means that constantly they need to be kept up to date on the operations of the organisation through regular meetings, and quarterly and annual financial reports.

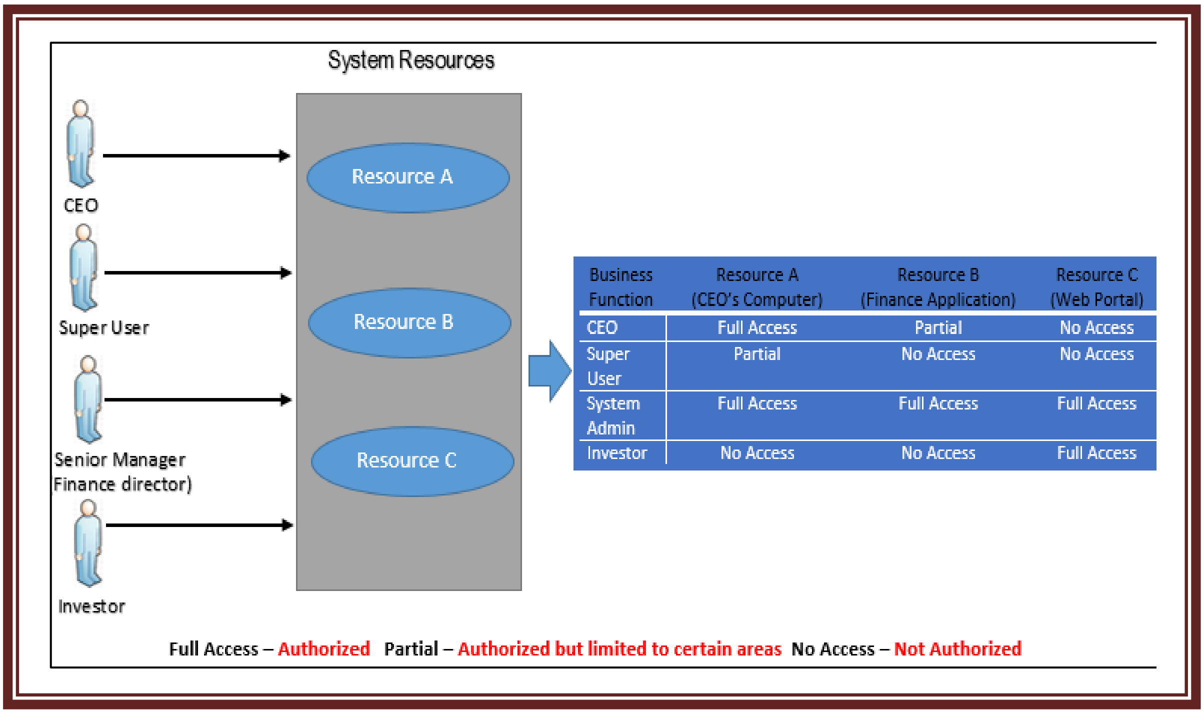
They interact with the board and management of the organisation through email, instant messaging, faxes, and the phone. They hardly generate data, since they are always feeding off reports from the organisation. They, however, require access to corporate data as and when they need it for their own use. Some of the data they need access to includes financial reports, future strategies, and news on potential competition in the market to understand threats to their investment.

This subsection explored the information flow amongst an organisation's stakeholders. This forms the basis for the advocacy for an information security digital divide. The next subsection focuses on accessibility control and the accompanying impact.

3.4.5. Information Access Control

Access control in computer systems and networks refers to a structure implemented and entrusted with the role of managing end-user access to information, resources, and services to counter malicious attacks (Zhang, He, Zhao, Huang & Liu, 2015:133). Ward and Smith (2002:358) further articulate that logical access control implementation on computer systems is considered an integral component in the protection of systems and information. However, installing a control mechanism in isolation is not advisable without first identifying what approaches should be adopted with regard to security across the organisation.

Given the above, user access management can then be summarised as the selective authorisation approach overseeing who can use, change, or view systems or information and the circumstances in which such access is permissible. Nevertheless, with increased emphasis on cross-functionality, teamwork, and multiple views of information (prescribed by job roles), it is more difficult to assign effective security parameters (Post & Kagan, 2007). For instance, within the same organisation, three personnel business functions from three different departments with three different roles and responsibilities need access to three varying resources authorised by the same information system. To avoid the overlapping of information, these end-users should not have the same access rights; their access must be carefully limited to resources that are required for their tasks, as illustrated in Figure 3.6.



Business Function	Resource A (CEO's Computer)	Resource B (Finance Application)	Resource C (Web Portal)
CEO	Full Access	Partial	No Access
Super User	Partial	No Access	No Access
System Admin	Full Access	Full Access	Full Access
Investor	No Access	No Access	Full Access

Full Access – Authorized Partial – Authorized but limited to certain areas No Access – Not Authorized

Figure 3.6: Accessibility to company information resource based on roles and responsibilities

Source: Adapted from Fuchs, Pernul and Sandhu (2011)

In Figure 3.6, given that resource **A** is the CEO's computer on the system, if a super user comes from the IT department to attend to a call on the CEO's computer, he/she should only be able to respond to the fault logged without being empowered by access level rights to initiate activities such as view sensitive data or applications. Additionally, an investor being an external stakeholder must not trigger an internal process such as preparing a payment voucher through resource **B** (Finance application). Also, resource **C** is not supposed to be used by a customer to procure goods for the organisation. In another example of access scenarios, the CEO must have some level of human resource (HR) roles in his scope of work, for example, it is in the CEO's interest to view whether HR policies are adhered to during recruitment of new personnel. This thus makes the CEO partners with the human resource department. That means the CEO should have some form of authorisation to view what is necessary in the human resource department; it could also be that he/she is supposed to be able to approve leave for the CIO or a senior manager using the HR system. Such an efficient access control management mechanism forms the backbone of the organisation becoming mature in ISDD.

3.5. Mature Information Security Digital Divide

A mature ISDD entails a well-organised, established, and appropriate mechanism for the management of the ability to access and process information and data within an organisation in such a way that security breaches are well contained. In this case, any access to information is fully traceable and aligned to the predefined security guidelines and policies established by the organisation. Within an organisation, ISDD is mature when the following key questions are answered and well-documented with regard to generation, access, and usage of information: “Who needs it?” “Why do they need it?” “How do they need it?” “For what purpose do they need it?” and “Is this in alignment to their business function, roles and responsibilities?” As such, by addressing the foregoing key questions, there will be a high degree of confidence that there is no overlap in the process of granting access to stakeholders. To that effect, only authorised access is experienced at any point in time. The following are a few examples of business rules for promoting a mature ISDD:

- The finance director should not be able to authorise leave on the system for a system programmer on behalf of the CIO. The finance director has no technical insight to understand the consequences of letting a system programmer go on leave without knowing whether there is a backup programmer to continue projects at the same level or not.

- Despite being the most senior personnel in an organisation, a CEO must not be empowered with credentials to view any information in the organisation such as tracking the cheque authorisation process – that is the work of the finance department.

- The system should not permit a cheque to be found in finance processing orders, which is the responsibility of the procurement department.

- IT support staff or system administrators, by virtue of their roles and responsibilities, should not be able to access or view the CIO’s sensitive information on the company’s business strategy when they come and perform routine maintenance.

- Employees must not be able to access one another’s computer profiles containing both work and private information such as electronic payslips, health status, trade secrets, and appraisals.
- A supplier’s interaction with the logistics department on the strategy to improve service delivery must only be available to relevant employees dealing with logistics.
- Investors cannot order goods for the organisation through the computer system nor should they be able to authorise a transaction on behalf of the finance director.

3.5.1. Impact of Accessibility and Use of Corporate Data

The impact of accessibility and use on corporate data can be divided into two sides: positive and negative. In the real world, every organisation would obviously want to have a positive side as opposed to a negative one.

3.5.1.1. Positive Side – Improved Business Operations

In this competitive business landscape, most businesses are profit-orientated. To that end, there is nothing as important as ensuring good service delivery to customers. According to Santouridis and Trivellas (2010), customer satisfaction with a business’ products and services is straightforwardly connected to good returns on investment. For any organisation to keep the competitive advantage, they must be well coordinated internally. Being coordinated goes hand in hand with the flow of information, especially the flexible accessibility in real time and using it to deliver that quality service. However, while flexible accessibility and usage are critical to business operations, they might also create a downside.

3.5.1.2. Negative Side

Relaxed access to and use of information can pose a danger to security and the system, especially if trade secrets, for example, end up in the hands of direct competition. Information can be exposed accidentally as discussed earlier in Chapter 2 through stakeholders, especially when they interact with external stakeholders or intentionally through internal end-users who are less informed about good use of information facilities.

The literature review in Chapter 3 provides a rich overview of how information flows through interactions among stakeholders within and outside the organisation. This creates a complex demand for accessibility and usage, which has the potential to weaken the traditional information security measures of confidentiality, integrity, and availability. It is then inevitable to look at the structure of the existing information security based on identity critical factors that must function appropriately to ensure that information accurately and correctly gets accessed by who legally needs it, why they need it, what they need it for, and how they need it.

3.6. Information Security Digital Divide Critical Success Factors

According to Frenzel and Frenzel (2004), CSFs are those few areas in a business where things must go right – they are an executive's necessary conditions for success. In the context of information security in an organisation, they relate to information technology (IT) executives, their subordinate managers, and to other relevant executives within. Table 3.2 lists 10 ISDD critical success factors relevant to this study which will be used in the next chapter to develop maturity level metrics.

Table 3.2: ISDD critical success factors

CSF	Description
CSF 1 – Ecosystem Information Flow	A clearly defined ecosystem according to the organisational structure (Fadhel, Bianculli & Briand, 2015). This will allow the assessment of workflow, data movement, as well as the way data should be accessed and used in order to promote a mature information security digital divide. Also, it allows individuals to observe their boundaries when dealing with the access, use, and sharing of corporate data.
	Security awareness as a culture is mandatory in every organisation that invests in a computer system (IS/IEC 27001, 2013). Security awareness must involve internal end-users, stakeholders, partners, and other external

CSF	Description
CSF 2 – **Culture of Security Awareness**	beneficiaries of the computer system in accordance with how they interact with it. This awareness should be tailor-designed to build protection according to the design of the specific IT landscape.
CSF 3 – **Business Function, Roles & Responsibilities Management**	Business functions, and roles and responsibilities of each individual must be structured according to the work scope as indicated by the organisational structure (Fadhel, Bianculli & Briand, 2015). This makes it easy for the system to be configured to allow individuals within and outside the organisation to access information resources according to how their work scope dictates. For instance, when the logistics manager works outside the workplace, he needs access to logistics-related information externally. Also, he needs to be able to use email to communicate to suppliers while outside the organisation.
CSF 4 – **Access Control Management**	A well-managed access control policy to corporate data or system resources is based on the relevance of the information to an individual (Humphreys, 2008). Every end-user must have an ID and password for authorisation. Uncontrolled access to information could result in security that could breach the divide policy. For example, individuals working in the finance department must be confined to finance-related resources only. A controlled environment reduces the risk of information leaking to other departments within the organisation that are not relevant to the operations of finance.
CSF 5 –	Standard information security policy custom-made to properly support accessibility and use of corporate information resources and information (IS/IEC 27001, 2013). This is a standard reference document that provides guidelines to all individuals and constantly reminds them of the dos and don’ts around the use of organisational

CSF	Description
Security Policy	information technology within and outside the premises of the organisation. It promotes a strong divide which is essential for the safety of corporate data.
CSF 6 – **Information Security Knowledge**	Among all individuals, sound information security knowledge, skills, and its application is a must (Nikolakopolous, 2009). Without good information security knowledge and its application, it is difficult for individuals to interpret some, if not all, the content of the information security policy. It also makes it hard for end-users to conduct themselves in a manner that promotes a mature information security digital divide. Unknowingly, they can engage in activities that can compromise the divide.
CSF 7 – **Physical Access**	Well-controlled physical access to information resources within the premises individual (Humphreys, 2008). Before access to information resources such as computers and laptops can be discussed, access to physical buildings where these resources are kept must be considered to ensure the concept of digital divide is upheld. Individuals' access must be carefully regulated, for example, issue individuals access cards or keys which only give access to offices and other places permissible according to the scope of their work. Finance department must only access computers within their department as well as interact with the part of the Intranet relevant to financial matters.
CSF 8 – **Audit Trail**	A comprehensive audit trail to enable the computer system to determine what resource was accessed, by whom, why, and when (Holme & Thomas, 2008). This security feature also reinforces the fact that all activities on a computer system may be closely monitored. This also enables breach to be identified early enough to counteract in order to minimise the extent of damage in cases of security breach.

CSF	Description
CSF 9 – Identity Management	Identity Management is the beginning point of access control on a computer system. It is a requirement that all end-users are authenticated and authorised before they can use the system (IS/IEC 27001, 2013).
CSF 10 – Culture of Protecting Information	System end-users and stakeholders must conform to a culture of using system resources according to the confines of the security policy (Da Veiga & Eloff, 2010). Such a culture promotes standards and best practice vital for mature ISDD.

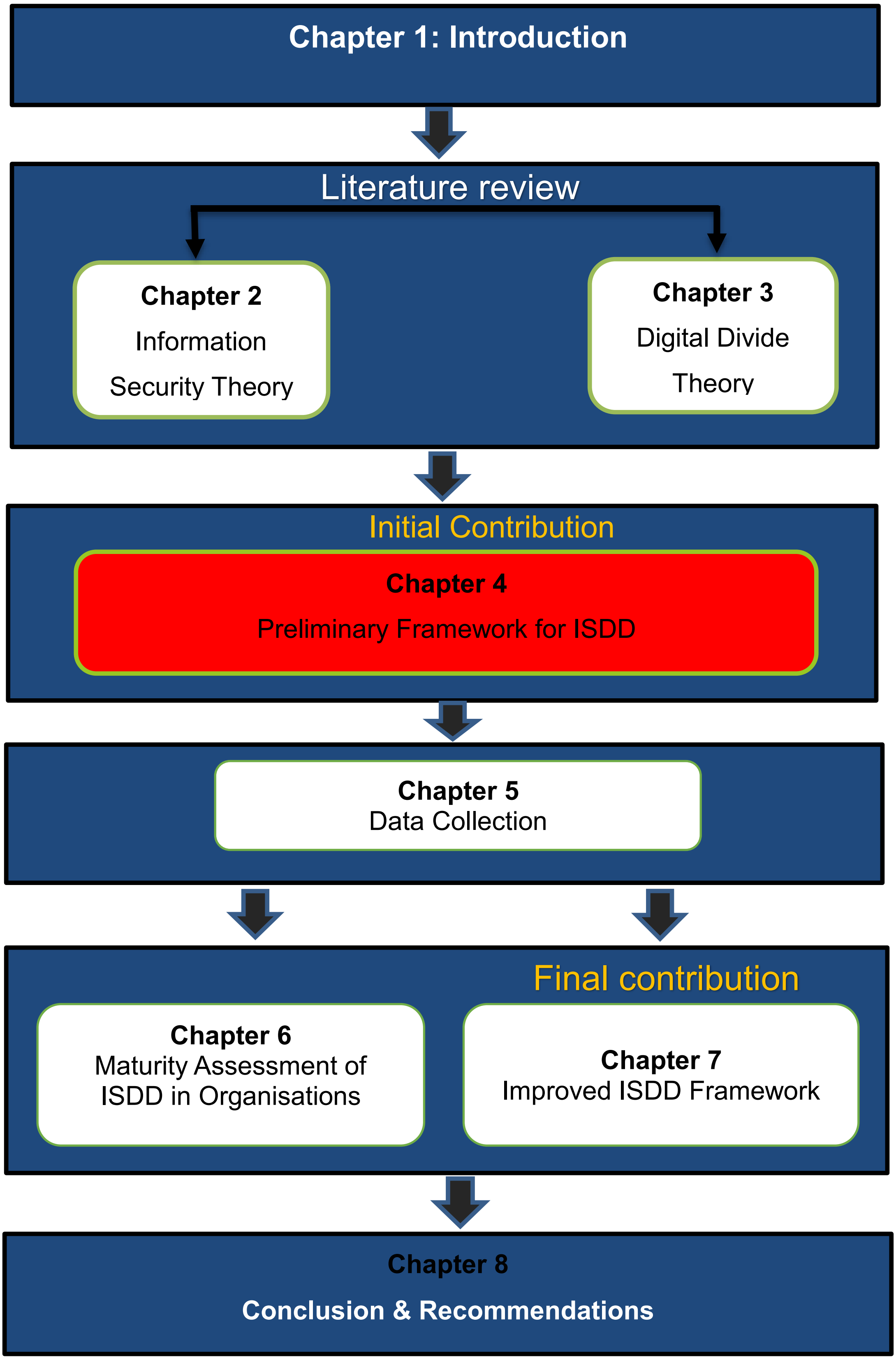
3.7. Conclusion

This chapter focused on accessibility and use of information systems and their alignment to the concept of digital divide to complement traditional fundamentals of information security (confidentiality, integrity, and availability). The concept of information security digital divide was derived by aligning information security and digital divide. To demonstrate the significance of dividing information to enhance information security, the organisation ecosystem was assessed, and stakeholders' interaction based on their roles and responsibilities was described. It was further highlighted that system stakeholders vary based on roles and responsibilities, some are more primary sources of information generation than consumers, others more consumers than sources. In some cases it can be both.

This analysis boils down to the fact that while all the users might need to access and use information, accessibility, and use must be regulated by the relevance of the information to their roles and responsibilities. It is then vital to realise that a high information access divide is good for the enhancement of information security, whereas a low divide is not. However, this is contrary to the concept of information and communication technology for development, which dictates that a low divide is good as opposed to a high divide.

The chapter that follows will address the theoretical foundation on which this study relies for the construction of a conceptual framework.

Chapter 4: A Framework for Information Security Digital Divide



4.1. Introduction

The foregoing two chapters (Chapters 2 and 3) focused on exploring information security and information security digital divide from literature in the context of this study. Building on that, the purpose of this chapter is to propose a theoretical framework for ISDD. The chapter thus seeks to answer the third research question on the development of a conceptual framework for benchmarking information security digital divide. The framework is intended to assess the maturity level of ISDD in any given organisation in a real-life context. This is achieved by relying on the maturity assessment approach of COBIT, which will be used as the roadmap for the characterisation of maturity levels.

The chapter begins with the definition of a framework, its objectives, characteristics, and life cycle in Section 4.2. It then provides an overview of COBIT in Section 4.3, as well as metrics that determine compliance levels. Section 4.4 deals with principles of software capability maturity and further explores the significance of capability maturity, focusing on conditions used to determine security capability maturity criteria. Section 4.5 presents the proposed information security digital divide framework and its various components are discussed. Compliance and maturity levels in the context of ISDD are further elaborated on in Sections 4.6 and 4.7 respectively. A conclusion to the chapter is provided in Section 4.8.

4.2. Overview of a Framework

An information security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in an organisation (Granneman, 2013). Granneman (2013) goes on to elaborate that frameworks are basically outlines for building an information security programme to manage risk and reduce vulnerabilities. In addition, an information security framework should not only focus on technological issues but also incorporate other mission-critical components within an organisation such as people, process, and business strategies which also dictate the need for information security (Patil, 2008:5). In security models, people, process, and technology must combine to increase security performance (Saleh, 2011), as depicted in Figure 4.1.

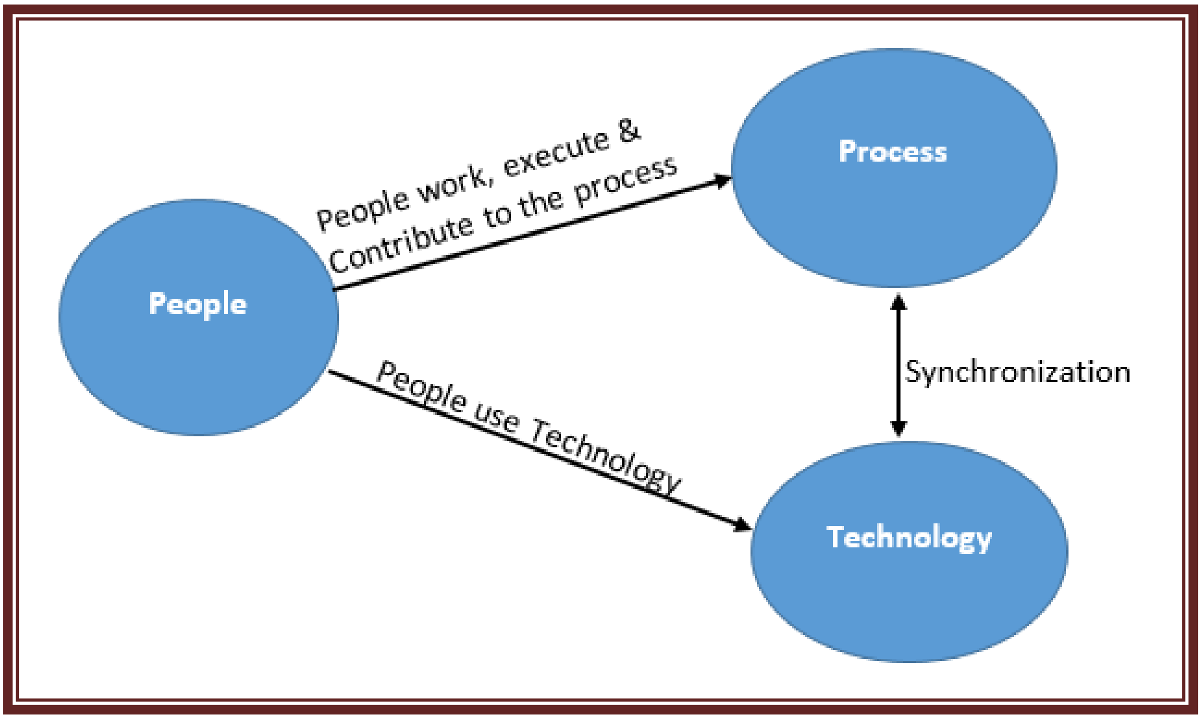


Figure 4.1: Relationship between, people, process, and technology

Source: Adapted from Kumta and Shah (2002)

Figure 4.1 is identical to the logic of Saleh, Abdulkader and Alfantookh (2011) on security, which underlines the reality that combining essential information security factors enhances standards of security practice and is fast becoming a popular trend. Saleh et.al (2011) furthermore spot the example of the strategy, technology, organisation, people, and environment (STOPE) framework, which entails combining all the aforesaid factors to create a good framework. The subsection that follows discusses the objectives of a framework.

4.2.1. Objectives of a Framework

The aim of an information security framework is to connect people, process, and technology in order to deliver practical IT guidelines for standard practice (Patil, 2008:8). However, even with the best planning and implementation, it is often impossible to obtain a perfect information security framework (Whitman & Mattord, 2008). Principally, the idea of a framework is to minimise the information security risk. This is also known as creating the operational security environment (OSE). The OSE is supplemented by all installed information security countermeasures. Figure 4.2 is a demonstration of the legacy concept of OSE which was masterminded by Von Solms, van de haar, von solms and Caelli (1994). A carefully designed framework should be able to sustain or at least come close to the ideal OSE because then the prescribed countermeasures would have been met. One way of attaining OSE in an organisation is by utilising a custom framework based on combining the capabilities of other existing frameworks such as IS0/1EC 27001:2013 and COBIT.

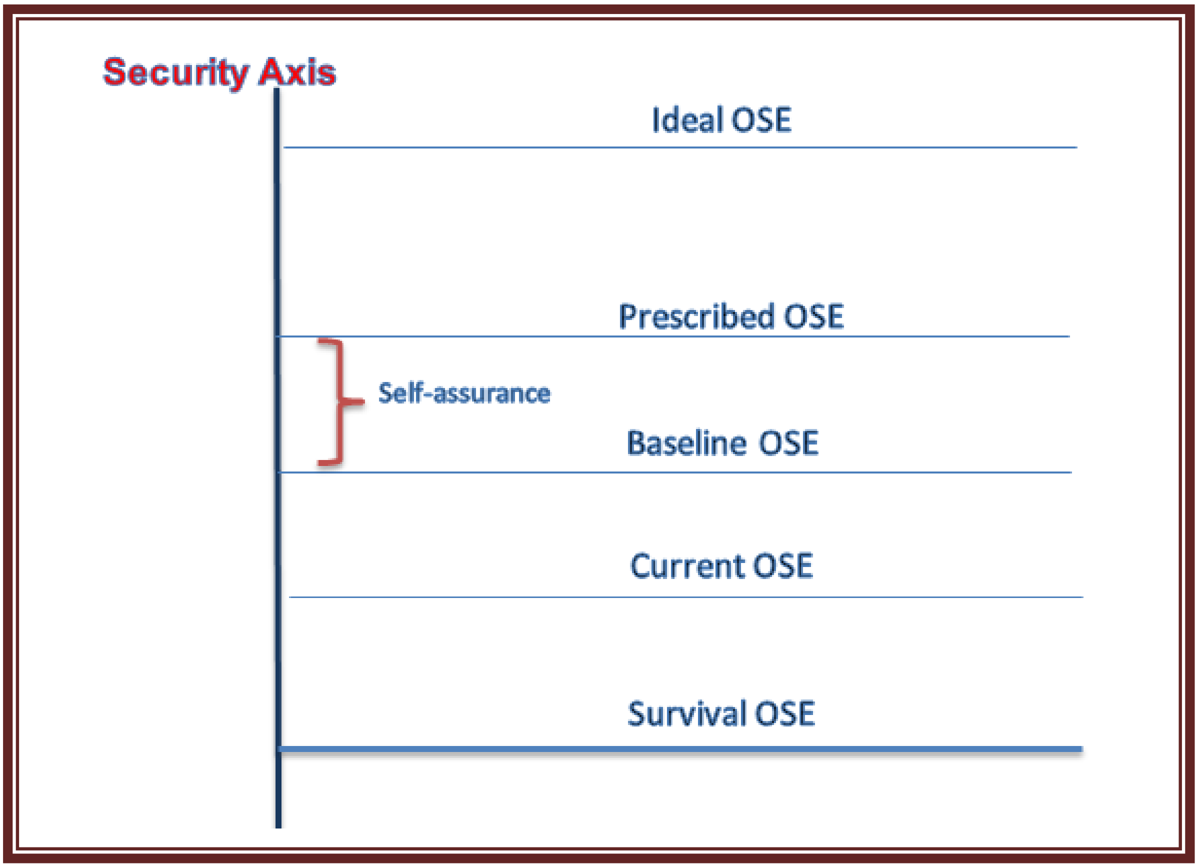


Figure 4.2: Operating security environment

Source: Adapted from Von Solms, van de haar, von solms and Caelli (1994)

According to Arora (2011:8), standard frameworks on information systems management can be dissected into information security standards or information security governance standards. COBIT is a high-level IT governance and management framework. It focuses on broader decisions in IT management and does not dwell on technical details. On the other hand, ISO 27001:2013 implementation concentrates on security controls, centred on a risk management approach. This implies that both COBIT and ISO/IEC 27001:2013 deliver foundations that are essential towards the development of a sound information security plan (Garcia, 2015). To get the desired security level, every custom framework requires going along with industry-approved characteristics applicable to the security of its business operations. The next subsection discusses framework characteristics.

4.2.2. Characteristics of a Framework

According to some authors (Patil, 2008:8; Basani, 2012), a well-designed information framework should at all costs integrate the following important components:

1) A life cycle: This contributes to ensuring that there is continuous improvement in a process by looking at its critical phases (Basani, 2012:6).
2) The next item must be a recommended and well-constructed information security governance that is complete. Patil (2008) points out that this is only realistic by, for example, putting in place properly organised and clearly outlined policies within an organisation.
3) Sound controlled access practices for, amongst others, stakeholders, processes, technology, and crucially information resources.
4) The use of popular, successful existing frameworks as guidelines. Good examples of those could include COBIT, IRSM, HIPAA, and ISO 27001:2013.
5) A guide of acceptable criteria on alternatives to helping in tailoring a framework to suit the operating information security environment in which it will be applicable.

4.2.3. Life cycle

To ensure that all aspects of information security are considered in a properly designed framework, it is essential that a framework follows an approach based on a comprehensive life cycle (Basani, 2012:108). One such example is the “Plan-Do-Check-Act-(PDCA)” process (Siponen & Willison, 2009; ISO 7799, 2002; Locke & Gallagher, 2010). It offers a good approach to be used as a guideline to develop and implement a successful framework. Table 4.1 is a summary of PCDA in combination with how the proposed ISDD framework of this study will benefit.

Table 4.1: The PDCA - based life cycle of a framework

	Activities
Plan	The first quadrant: Planning entails forming goals and having in place appropriate processes to get the desired outcome (Siponen & Willison, 2009; Basani, 2012). Planning in the context of ISDD in Figure 4.6 equates to points 1, 2, 3, and 4. The planning around how external stakeholders and busines roles according to which business functions they are attached to use technology 3 and 4 in a manner that complies with mature ISDD in the organisation.
Do	The second quadrant performs monitoring and measuring of the process performance in comparison to the objective of the improvement process. This stage incorporates point 5 in Figure 4.6 in the framework, and how people process and technology have been combined in accordance with the set performance target goals. Appraise targets according to the ISDD maturity level
Check	The third quadrant: Implementation of the appropriate processes and then assessing and measuring performance, and setting up for process improvement. Once planning of how to combine people, process, and technology is achieved to retain high ISDD as explained in the previous stage, all metrics that constitute roles, functions, and systems in point 6 in the proposed framework in Figure 4.6 need to be assessed and measured for compliance.
Act	The fourth quadrant involves actioning lessons learnt; corrective action must be performed to correct any irregularities (Mind tools, 2015). Using the outcome of the maturity level grading attained after going through all stages in the proposed framework, the organisation reflects on the wrongs identified during the entire cycle. They draw upon those mistakes and go back to the planning “table” to narrow down on faults identified and make amendments to enhance security.

Figure 4.3 is a graphical illustration of PDCA in accordance with the explanation offered in Table 4.1 regarding the transition of the four quadrants.

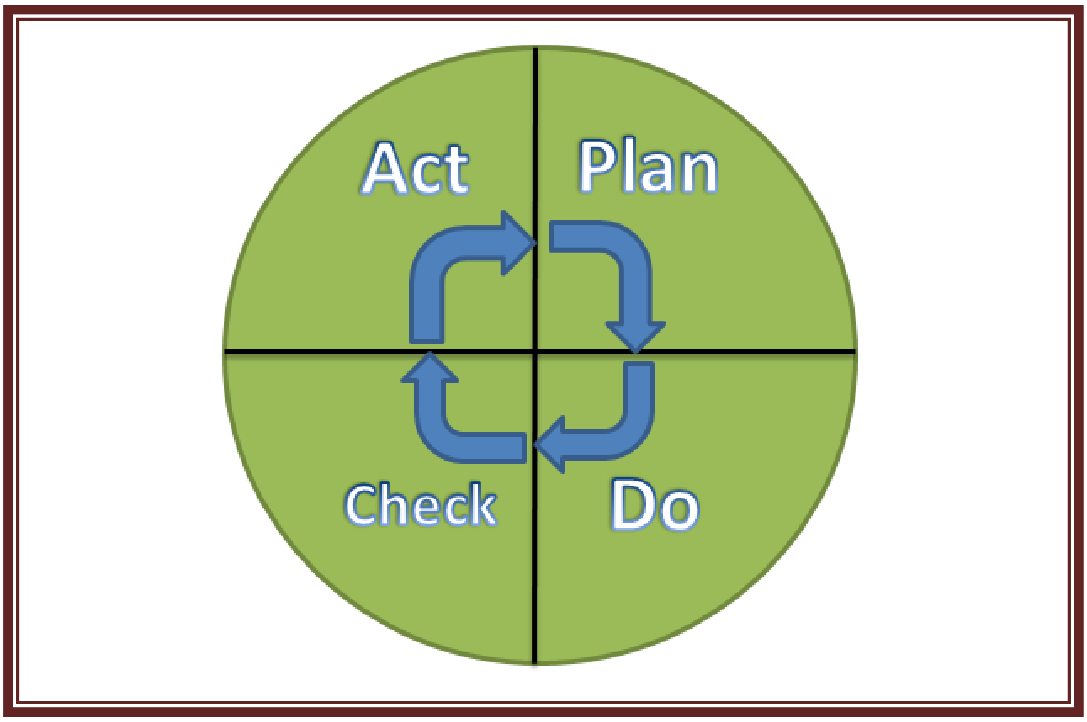


Figure 4.3: PDCA model

Source: Adapted from Humphreys (2008)

Directly or indirectly, most information security frameworks – one way or the other – incorporate the PCDA strategy discussed in Figure 4.3. One such successful and industry-approved framework is COBIT; it uses this methodology to develop the concept of capability maturity level in IT.

4.3. The COBIT Framework

The business orientation of COBIT by default is more concerned with linking business objectives to information technology goals (ISACA, 2008:5). It further provides leverage and maturity metrics to measure a security programme's overall performance. It does this by clearly identifying key IT processes and business functions critical in building a solid, measurable security programme as illustrated in the flow chart in Figure 4.4.

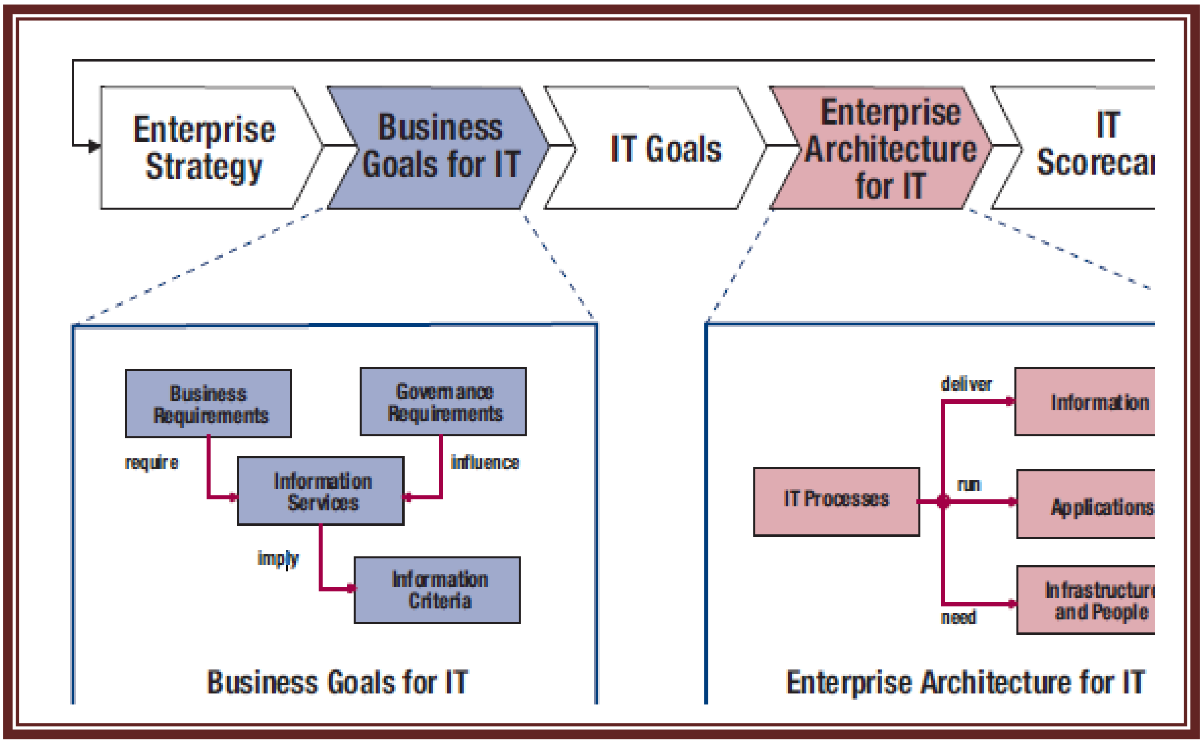


Figure 4.4: How COBIT links IT to business corporate strategy

Source: IT Governance Institute (2008)

As depicted in Figure 4.4, in order to integrate IT into corporate business strategy, COBIT delivers clearly defined policies and good practice for internal information technology control. It also allows organisations to measure internal processes, manage resources, infrastructure, controls, and procedures against industry standard metrics reliable enough to allow organisations to weigh the maturity level of their control (Arora, 2010). It is for this reason that COBIT has been selected as the foundation of this study. The foundation on which the COBIT metrics are based is highlighted next.

4.3.1. COBIT Metrics that Determine Compliance Levels

COBIT derives its maturity model by using 34 generic processes. The basic principle of these processes is to act as a means to determine the current level of an IT programme and how to set its priorities for potential improvement. Appendix G in the appendices section shows the critical success factors on which COBIT bases its maturity model. Based on these metrics provided in Appendix G, COBIT uses maturity levels indicated in Table 4.2 as a summary of the various suitable levels.

Table 4.2: COBIT Maturity Levels

Maturity Level	Description
Level 1 **Initial**	Process need is acknowledged but not defined.
Level 2 **Repeatable**	Processes are defined and can be tracked but still immature.
Level 3 **Defined Process**	Processes are well-defined and properly tracked but not quantitative.
Level 4 **Managed and Measurable**	Processes are well-defined, tracked, and quantitative.
Level 5 **Optimised**	Processes are well-defined, tracked, quantitative, and continuously improving.

Source: Xiao-yan, Yu-qing and Li-leic (2011)

The next section presents the notion of software capability maturity. This will lead to the benchmark for the criteria used to develop compliance metrics to be used in developing similar levels to that of COBIT in Figure 4.2.

4.4. Software Capability Maturity Level

According to Kerrigan (2013:20), generally, capability maturity is a concept that enables one to grade the extent to which an organisation applies formalised processes to the management of its various business functions. Equally, Goksen, Cevik and Avunduk (2015:209) charectarise capability maturity by stating that it is a fact built on principles that people, organisations, functional areas, and processes over time change towards an advanced maturity, in the process passing through various distinct levels. Most critically, just as the name indicates, the concept is about capability and the accompanying maturity improvement strategy of an enterprise (Pooley & Wilcox, 2004). In other words, it simply identifies the critical success requirements that a process needs to exhaust in order to improve both capability and maturity. In recent years, according to Kerrigan (2013), a couple of reference models have surfaced from different authors describing the techniques and processes involved in capability maturity. By default, most capability maturity models use a five-tier approach as described in Figure 4.5, showing an advancement path from a chaotic and immature process to a fully developed orderly process (Kumta & Shah, 2002).

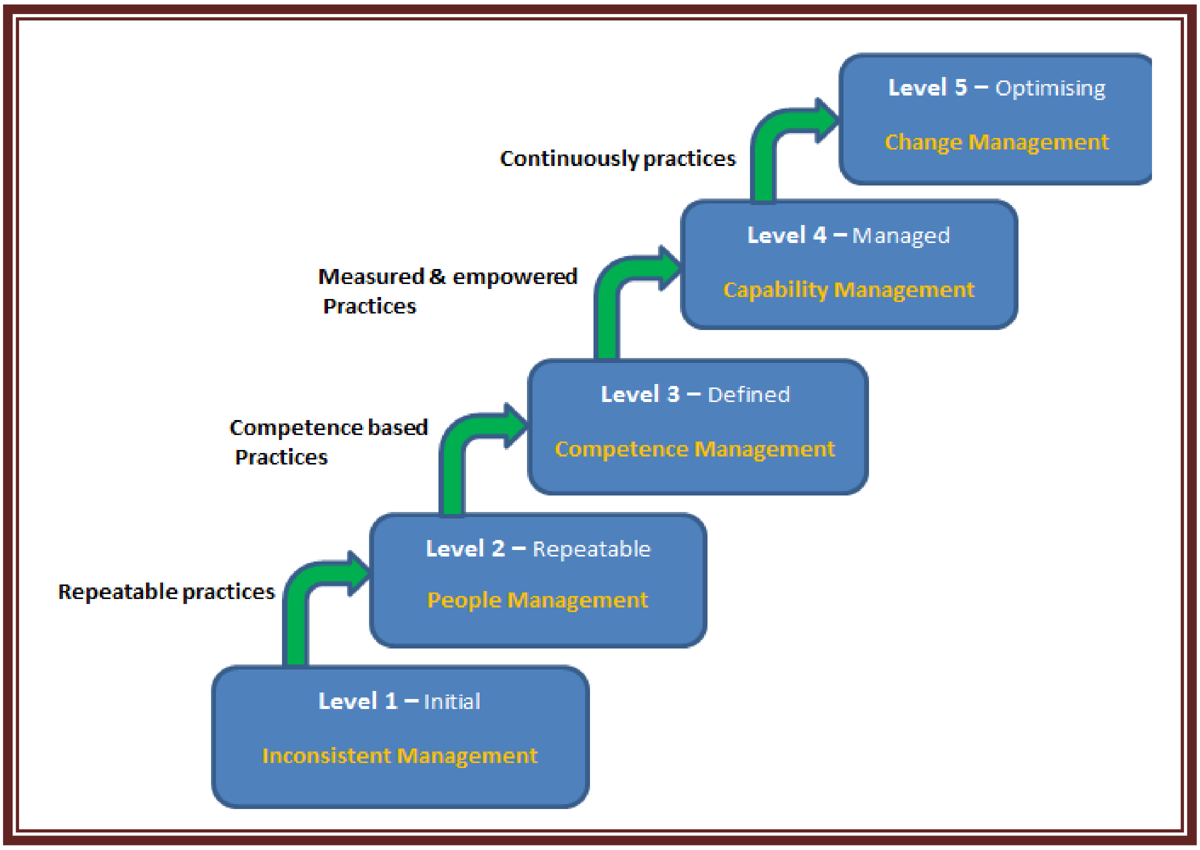


Figure 4.5: The five levels of Capability Maturity Model for software development

Source: Adapted from Curtis, Hefley and Mille (2009) and Pooley and Wilcox (2004)

Each of the maturity levels 1 to 5 shown in the iterations in Figure 4.5 comprises a number of key process areas (KPA). Each of the KPAs has a succession of related activities which require working together in order to attain a set of goals. According to Pooley and Wilcox (2004), it is a must that all set targets of a KPA be reached to satisfy that KPA and consequently accomplish a certain desired level of maturity in the framework. With a view to determining key process areas required in each of the levels from 1 to 5 in Figure 4.5, there are special sets of metrics that are used as parameters that must be considered.

4.4.1. The Significance of Capability Maturity Models

To benchmark the importance of information security models, Carney (2013) lists the reasons as:

1) First, they set direction which develops a decisive roadmap. It further carves out a foundation for building a concrete security programme.
2) Second, they ensure that priority is placed on all information and communication technology valuable assets.
3) Third, they show security gaps. This provides for the perfect opportunity to fully develop a security programme to the required industry standard and better management of security.
4) Fourth, they aid in articulating the security programme's value alongside its associated progress. This value ensures continued evaluation of the programme versus best practices.

In this section, the theoretical foundation of capability maturity was defined. In its entirety, capability maturity is the heartbeat of this research. To achieve this objective, a generic framework in accordance with information security is first outlined, then the characteristics of a good framework are considered. To demonstrate how capability maturity is determined to come up with various compliance maturity levels, COBIT as a tried-and-tested framework is explored. Finally, the section is closed off with the advantages of capability maturity. With the theory of COBIT and the capability maturity levels having been explained, the next section will develop the preliminary framework based on the concepts discussed herein.

4.5. Information Security Digital Divide Framework

Based on the lessons resulting from previous sections on the theoretical foundation of software capability maturity, together with the critical success factors of both information security and ISDD which were the focal points of Chapters 2 and 3, this section will now devise a model for determining ISDD maturity metrics for a security programme. The section is the cornerstone and the main contribution of this study. It describes key process metrics which will enable the model to achieve its intended objective by categorising five varying ISDD levels of capability maturity.

Every capability maturity level is custom designed to measure an organisation's security profile, with level 1 representing non-existence of ISDD, level 2 the base entry, all the way to the highest attainable level, which is level 5, a reflection of mature ISDD. This framework subscribes to a security principle by Saleh (2011:321), which states that what cannot be measured cannot be managed. Invariably what cannot be managed also cannot be improved on. Much as the framework may base its capability maturity ideology on COBIT and ISO/IEC 27001:2013, it does not, however, try to reinvent the wheel of either framework; it comes up with an approach in a different technique while not defying the principles of both.

The proposed information security digital divide maturity framework (ISDDMF) in this study is intended as a self-assessment tool to help organisations to appraise their information security programme. The model helps in suggesting where an organisation should be and informs on issues leveraging IT maturity to reach an acceptable maturity. The proposed model furthermore carefully outlines key processes that govern, evaluate, and regulate all facets of information accessibility and general security in accordance with critical success factors of ISDD. Largely, it triggers a security structure that ensures it is able to prevent, detect, and react to security threats and risks efficiently. To accomplish this, the framework pivots on five basic indicators called compliance metric levels, with level 5 representing an organisation with a mature information security digital divide. These compliance metric levels are mapped to the critical success factors that were discussed in Chapters 2 and 3. Figure 4.6 highlights a breakdown of the building blocks of the entire framework.

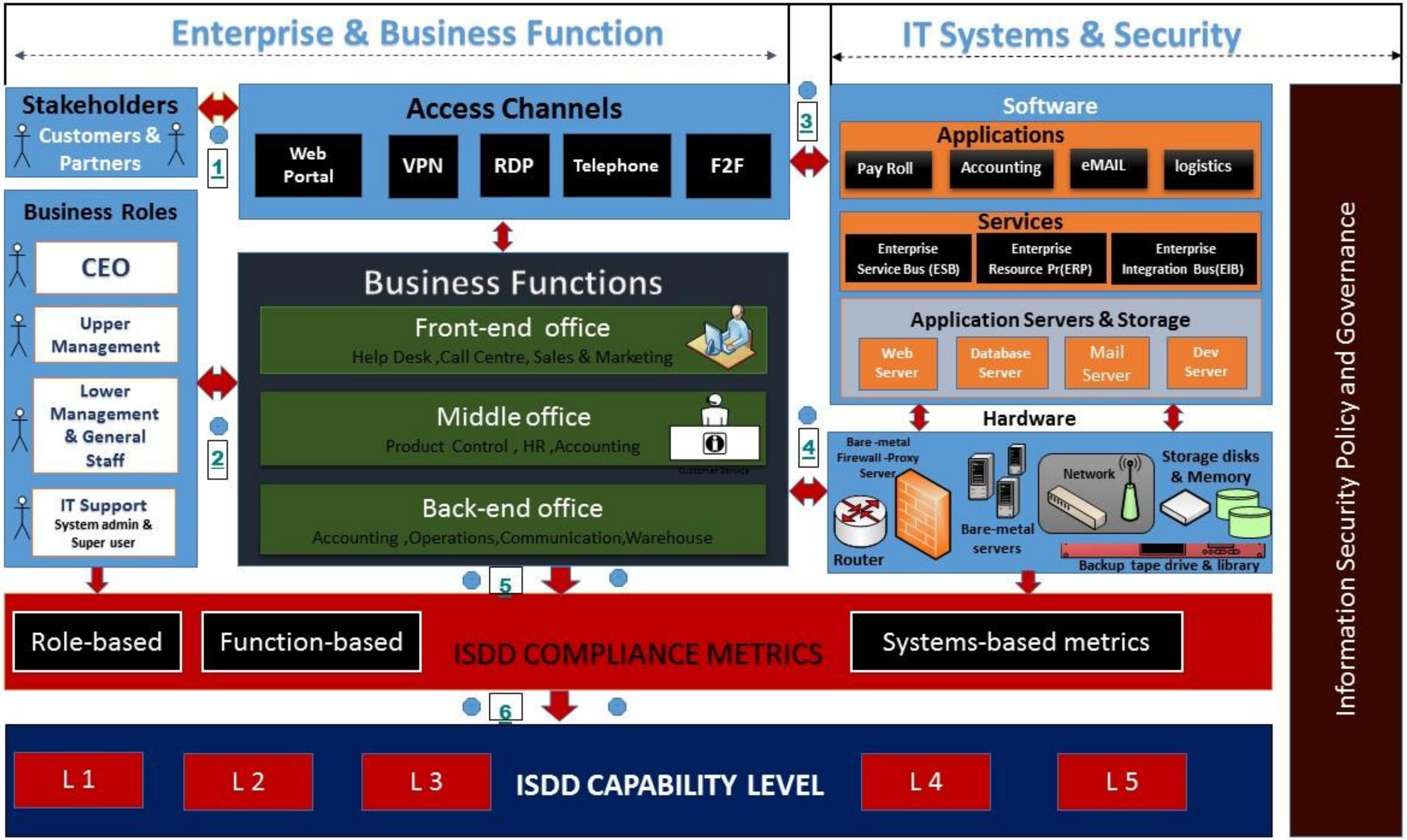


Figure 4.6: Information Security Digital Divide Maturity Framework

Figure 4.6 reflects the alignment of business, information technology, and information security in order to apply ISDD policies that help in decision-making on the capability of an organisation's security programme. The different building blocks of the framework will also be discussed.

4.5.1. Enterprise and the Business Function

An enterprise is simply a business organisation (United States International Trade Commission, 2010). Additionally, a business consists of its members and their interactions. Each member has their own role to play and their own sphere of responsibility, which contribute towards meeting the mission of the organisation. The core of any enterprise lies in how people, processes, and technology combine to deliver business goals according to the mission statement. Each stakeholder has a role to play and is assigned to a business function. Every stakeholder undertakes their routine duties through the use of technology, for example, the HR manager assigned to the middle office in the human resource department uses a laptop that has a front-end application such as Payroll. Through the intranet, HR is able to access back-end services to manage employee records, recruit new staff, evaluate the performance of individuals, and make monthly payments. Human resource also uses email to contact external stakeholders for routine services that support the business.

Human resource is the most valuable asset to any business. A business organisation relies on internal service roles combined with external stakeholders to manage it. These service roles and external stakeholders make use of technology to drive their associated business functions and roles which, in turn, creates a successful business. Collectively, an enterprise, its associated functions, and technology is made up of the following building blocks:

1) External stakeholders who require system access externally

2) Business service roles that require internal and external system access

3) Business functions within an organisation that work separately but routinely while supporting one another to attain the mission of the organisation; equally, information here must be confined to business functions it is relevant to

4) Access channels provide system access methods for all internal and external stakeholders; these channels must be used correctly on devices they are accessed from to prevent any security breach

5) IT systems support all business operations technologically

6) Security strives to provide defence mechanisms to facilitate smooth operation without any breach that may compromise systems, at the same time ensuring data is made available correctly based on its need to business roles

The next subsection will narrow down the building blocks of the proposed framework.

4.5.2. External Stakeholders

An external stakeholder could be a person, group, or organisation that is not directly involved in the business but affected by decisions and operations of the enterprise (Business Dictionary, 2015). These may include customers, suppliers, and other partners. While they are not directly involved in the business, their services are very important to operations such that they require access to systems. For example, transport suppliers may require access to a company's Web portal, VPN, or email system to verify delivery or pick information of goods. However, the system should be accessible to such suppliers using an access channel strictly authorised within the confines of their business involvement. The supplier must access the system on the basis of a trackable profile that requires authentication. All these measures must be incorporated into the organisational security policy.

4.5.3. Business Roles

Business roles is a general term that describes personnel that belong to various business functions. These roles range from chief executive officer, upper management, middle management, lower management, and the rest of the staff complement. They all integrate into the business functions according to their work scopes to meet the mission statement of the enterprise. For example, the CEO may be the head of the organisation, but system-wise, he should not be able to access and control the accounting department's payment system because it is not part of his work profile to process and release payments through accounting applications.

4.5.4. Business Function

A business function is an operation that is performed routinely to carry out a part of the mission of an organisation. It can be broken down into three areas, namely, front-end office, middle office, and back-end office.

4.5.4.1. Front-end Office

Front-end office is the part of the business that directly interacts with clients. Examples include service desk, marketing, and sales departments. As much as the front-end office work relies on both middle and back-end offices for certain support, e.g. if a customer enquires from a sales person at front desk on how far an application for the purchase of a product on hire purchase is, the sales person may through a written undertaking or telephone contact personnel in the middle office that handles processing of such to get an update of issue to the client; front-end office personnel should not be able to track middle office processes system-wise directly. However, they should be able to view incidents that may be in line with their roles.

4.5.4.2. Middle Office

In a business setup, this is a part of operations that provides support to both the front- and back-end offices and also draws on resources of both. Such departments could be product control, IT, legal, or compliance. Given an incident where an IT support staff receives a support request to rectify a software issue on a computer in the HR department based in the back-end office through their profile which they use to gain access on the HR computer with the fault, IT support staff may not possess the ability to view sensitive data or manipulate services such as leave applications on the payroll application.

4.5.4.3. Back-end Office

The back-end office acts as a support system to the front-end office. Work is escalated to them from the front office. For example, service desk may pass on a new application to human resource for processing. In the real world, an accounting department in the middle office may not be able to view at what level an application on the HR system has reached because of access restriction levelled against their profile. However, through enquiry in writing or a phone call, the personnel may engage the HR department through permitted procedure.

In conclusion, stakeholders and business partners need to interact with part of the enterprise or business function suited to their business involvement. This interaction is facilitated by an assorted choice of available access channels.

4.5.5. Access Channels

Access channels interface system end-users, be it internal or external to the system. This avenue details how business service roles and other stakeholders such as partners, customers, and suppliers are able to access an organisation's information system.

4.5.5.1. Access Channels for External Stakeholders

Externally, a number of access options are available including Virtual Private Network (VPN), Remote Desktop Protocol (RDP), internet, telephone, and face-to-face communication. For example, a customer can – through online shopping – log on to an organisation's Web portal to purchase goods which they have delivered to their residence. However, such access by the client must be highly secure and only available to that unique client and nobody else. In another circumstance, a supplier providing delivery of goods through transportation must also be able to access the same organisation's system through a Web portal to check delivery bookings; the system must limit both the client and transport supplier to what is necessary in order to avoid information overlap.

4.5.5.2. Access Channels for Internal Stakeholder

Internally, the majority of internal end-users depend on the intranet to access the system irrespective of the service role and business function they operate in. For instance, a manager in the finance department uses a laptop with an accounting application required to access accounting information stored on back-end servers. However, if a manager in the research department wishes to access information in order to prepare a report, they might have access to the same intranet, but they need to request that information from the finance manager because they do not deal with financial matters; hence, they have no need for financial applications to be installed on their devices.

All access channels discussed herein are facilitated by an information system. This information system makes it possible for end-users and other stakeholders to access information resources as at when and where they need them.

4.5.6. Information Technology Systems

Information Technology Systems (ITS) such as Management Information Systems (MIS) which are supported by components such as the ones in Figure 4.6 support business operations. For example, it can provide a marketing manager with real-time information or reports on clients' response on a new product launched in order to know whether to continue or discontinue the product or campaign. The CEO can use MIS reports to compare overall organisational performance to previous years.

The previous section explored ITS, which also rely heavily on a combination of both software and hardware to successfully support business operations.

4.5.7. Software

In general, software is a collection of computer instructions that offer precise desired functionality or output to a user (Schach, 2011:24). Software applications facilitate the smooth operation of mission-critical business processes without which any business cannot operate efficiently.

4.5.7.1. Application Software

These can also be referred to as the front-end or client program because it is what the end-user interacts with directly. Application software interface the end-user to the back end, e.g. Payroll, Microsoft Dynamics, Microsoft Outlook, QuickBooks, Enterprise Resource Planning (ERP), and Internet Explorer. In a more applicable example, an email program such as Microsoft Outlook is what an end-user depends on to send and receive emails. However, this software does not perform everything by itself; it is dependent on a back-end application server such as Microsoft Exchange Server.

4.5.8. Service

These are components of applications such as ERP, customer relationship management (CRM), and third-party application programming interface (API) which can be consumed by system end-users and stakeholders as a service.

4.5.9. Application Servers and Storage

This is the back-end or server-side of an application. The end-user does not come into contact with this, but they will always rely on it to perform a function within an organisation. For example, Microsoft Exchange Server hosts the mailbox of an end-user who only accesses it through front-end application software such as Microsoft Outlook. The entire software landscape discussed operates on a combination of various hardware.

4.5.10. Hardware

Hardware is an integral part of any information system infrastructure (Prenhall, 2015). The hardware layer is what supports all software such as applications, application services, and servers. An operating system such as Microsoft Windows Server 2011 acts as the master program controlling this hardware to work with all software. If the HR person of an organisation opens the Payroll application program on their laptop and queries an employee, the logical database hosted on a hardware supplies the employee's records for the Payroll program to present to the HR person.

To sum up, both software and hardware require IT security governance in order to be protected from threats and attacks. Governance is best managed by starting with a comprehensively written information security policy.

4.5.11. Information Security Policy

An organisation's policy on security is a plan outlining what an organisation's critical information assets are and how they must be protected (Pfleeger & Pfleeger, 2007). This is the first line of defence for the organisation's information system. Its primary agenda is to clarify what is being protected, why it is being protected, how it will be protected, and by whom. In a nutshell, it provides the do's and don'ts an end-user and stakeholder should be aware of when they work with the system. This ensures minimised risk of system attacks and failures, thus securing the company's critical systems. To summarise, a security policy is a living document which acts as reference for everyone using systems and information resources defined as potential targets.

4.6. Information Security Digital Divide Maturity Framework Compliance Metrics

To derive the appropriate compliance metrics that will define the different capability maturity levels which will befit this model, people, processes, and technology are combined carefully to ensure the security principle of preventing, detecting, and reacting is attainable by security programmes. In Table 4.3, seven decisive critical success factors of both information security and digital divide are used to map out metrics.

Table 4.3: ISDDMF Mapping Metrics

Phase /Level	Eco-System (Work flow & data movement)	Access Control Management (System & Physical)	Alignment of System End-users & Stakeholders to business roles and functions	End-user Skills, Security Awareness & Training	Security Policy, Procedure & Standard	Culture of Protecting information	Performance target (ability to prevent, detect & correct)
1	Being a small or one-man firm, the need for an organisational structure is not a priority and so there is no information and process flow	Password use is not mandatory, being a one-man or small firm. Physical access control to information resources is not practical as often everyone sits in one place	No alignment of any form exists. It is a small or one-man firm; thus, there are no unique business roles and functions. One person assumes multiple roles	End-user skills required to operate the system without exposing it are very low; some rely on trial and error. Security awareness and campaigns are non-existent. There is no training programme	There is no policy on security present to provide guidance. No standard procedure is followed when using information resources. End-users rely on what they know to protect information	There is no ISDD culture among end-users and stakeholders. They do not seem aware, responsible, and willing to act in ways that benefit ISDD	Security processes are non-existent; therefore, the environment is not quantifiable and measurable

2	The need for an organisational structure is being considered. Workflow and movement of data are beginning to be given attention but are still disorganised	There is a desire for authentication through password when using the system. In the same vein, the need to partition business roles and functions is beginning to take its toll on operations	System ability to permit access to information according to end-user roles and functions is being looked at but not implemented	There is a realisation that end-user upskilling, security awareness, and training is mandatory and is imminent, but there is no understanding of how this should be done	Security policy, procedure, and standard is introduced but is not comprehensive and lacks proper implementation	End-users and stakeholders seem to begin entertaining awareness, responsibility, and action towards ISDD attributes	Performance targets are set but not measurable entirely. Only certain aspects of ISDD are measurable
3	An organisational structure is now present, but information flow and data movement processes do not conform to the organisational structure	By default, password authentication is instituted by the system but lacks consistency. Business roles and functions are physically partitioned but still lack strict control approach	System ability to permit access by end-user role and function is implemented but not structured, hence not effective	End-user skills, security awareness, and training are made part of the strategy. The organisation is beginning to realise the need to develop training plans according to the environment	Security policy, procedure, and standard begin to be implemented but in a chaotic fashion that makes it ineffective. The policy is not written in low-level language and not updated regularly	End-users and stakeholders now embrace awareness, responsibility, and actions necessary for mature ISDD. However, it is not uniform across all end-users and stakeholders	Performance targets are visible and can be measured, but not entirely

4	A clear and precise organisational structure is present. Both information flow and data movement are available but not completely firm	Password authentication is a standard policy and enforced by the system but not enhanced. Business roles and functions are well-segregated but lack continuous improvement	System's ability to permit access according to end-user roles and business function is fully effective but lacks continuous improvement	Understanding of the full value of end-user skill, awareness, and training is high. Incentives to motivate end-users to upskill user levels is present. Most end-users are minimum intermediate users	Security policy,procedure, and standard are now implemented and effective too but do not evolve with the changing environment	By standard, end-users and stakeholders comply with mature ISDD requirements but lack the element to continue observing activities that alter ISDD maturity with the changing environment	Performance targets are set and measurable. However, continuous improvement lacks
5	A perfect organisational structure which flawlessly regulates information and process flow is automatic. Process	Password authentication is strictly enforced. All end-users and stakeholders comply with password policy. Business roles and functions are well-partitioned and	System's ability to permit end-user roles and business functions to information is highly efficient and continuously improves with the changing	End-user skills, security awareness, and training is enforced at recruitment. All end-users are advanced users. End-user skill set is made a part of	Security policy, procedure, and standard compliance have reached the ultimate best. Best practice among end-users and stakeholders is a culture. Policy is	All end-users and stakeholders are completely mature and ISDD compliant and continuously strive towards new, mature ISDD trends instituted	Performance is highly measurable and spans the entire organisation. Continuous improvement is an automated part of the enterprise culture

	management keeps on improving	controlled. There is continuous improvement	environment. It is well-documented too	annual appraisal. Improvement is constant	updated regularly and continuously to accommodate change in the risk and threat spectrum	according to the environment	and is well-documented

The ISDDMF compliance metrics in Table 4.3 helped in pairing some critical aspects of IT which define various suitable compliance metrics profiles discussed in the next section.

4.7. Information Security Digital Divide Capability Maturity Levels

Capability maturity levels help organisations to weigh the strength of their information system security by identifying key critical success factors of various aspects of information technology which work dependently to mount a watertight security structure. Figure 4.7 portrays five high-level guidelines useful for continuously and operationally improving a security programme.

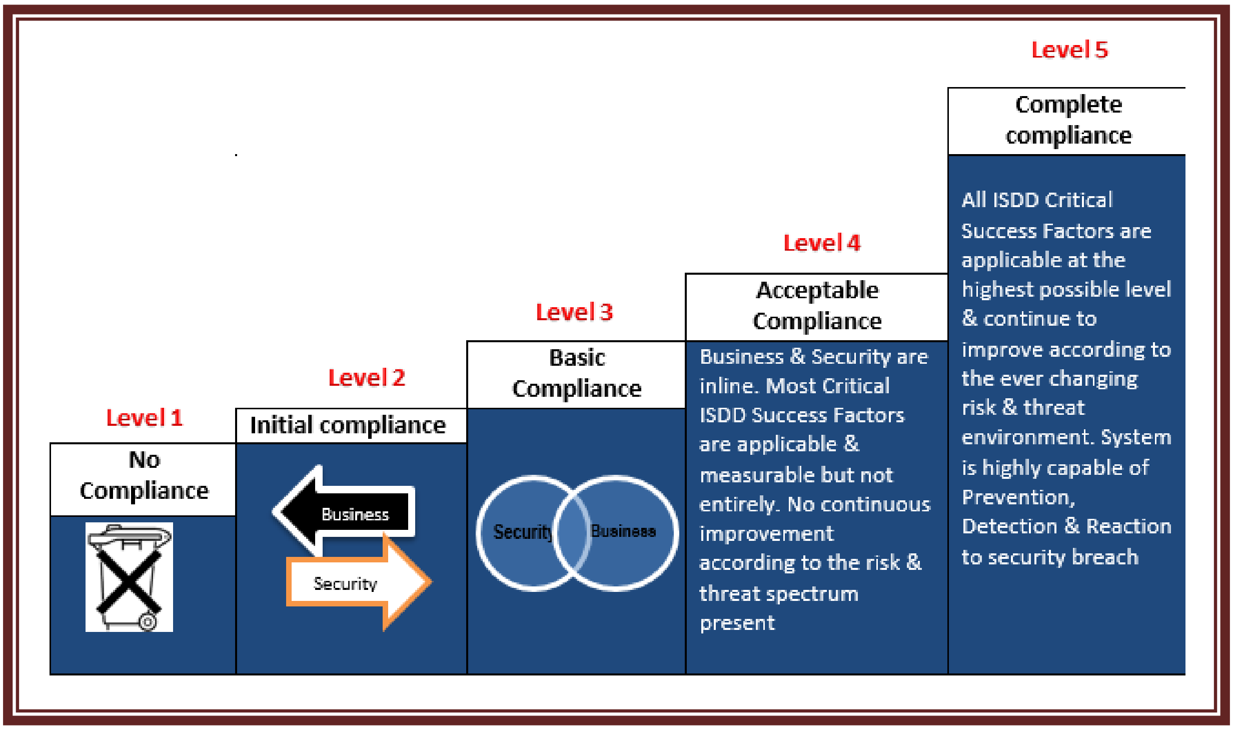

Level 1
No Compliance
Level 2
Initial compliance
Business
Security
Level 3
Basic Compliance
Security
Business
Level 4
Acceptable Compliance
Business & Security are inline. Most Critical ISDD Success Factors are applicable & measurable but not entirely. No continuous improvement according to the risk & threat spectrum present
Level 5
Complete compliance
All ISDD Critical Success Factors are applicable at the highest possible level & continue to improve according to the ever changing risk & threat environment. System is highly capable of Prevention, Detection & Reaction to security breach

Figure 4.7: Demonstration of ISDDMF maturity levels

In Figure 4.7, it is clear that the lower the security profile of an organisation, the higher the risk of successful attacks and damaging threats to its business operations. In the next part of this chapter, the transition of ISDDMF compliance levels is summarised.

Level 1: Non-compliance (ISDD Immature)

At this capability level, ISDD maturity is non-existent. There are no policies or procedures to protect the business. The organisation completely does not see and acknowledge the value of ISDD to its business operations. Business and security are parallel concepts. This kind of organisation does not subscribe to any of the principles of ISDD critical success factors identified in Table 4.3. Potentially, these could be one-man or small enterprises without any need for the use of software or information technology as a backbone to business operations.

Level 2: Initial Compliance (ISDD Immature)

At this capability level, business and security are parallel concepts. However, it marks the entry stage to mature ISDD for any organisation because there is acknowledgement of the value ISDD has to business. Nonetheless, despite acknowledging the importance of security, there is no incentive to adopt this useful security approach by instituting the necessary policies and procedures for the purpose of securing the business. The organisation may seem overly concerned about ISDD in times of security breach, but the approach can be summed up as being reactive instead of proactive.

Level 3: Basic Compliance (ISDD Mature)

Proper security towards business safety begins here. At this capability level, the organisation has realised the need and benefit of fully embracing ISDD. Business and security are now synchronised to work towards a common goal of protecting the business. As a result, ISDD critical success factors are adopted but still unstructured, and funding towards IT systems is not fully dedicated. An information security policy template may exist, but it is not regularly updated and not written in low-level language to easily guide end-users, partners, and stakeholders on industry standard practice. End-user skills range between entry and intermediate. Generally, ISDD maturity is attained but still in its infant stage.

Level 4: Acceptable Compliance (ISDD Mature)

At this capability level, ISDD critical success factors are almost fully adopted and documented. Information security is now completely recognised and treated as a core business function, and is also integrated into corporate strategy. There is a well-outlined IT security policy to that effect to guide end-users on standard practice. Access control, training, and security awareness are all proactively initiated and carefully managed. Management of information security is well-coordinated and funded. End-user training and security awareness are instituted to upskill end-users to a minimum of intermediate level. Generally, ISDD is mature but lacks continuous improvement.

Level 5: Full Compliance (ISDD Mature)

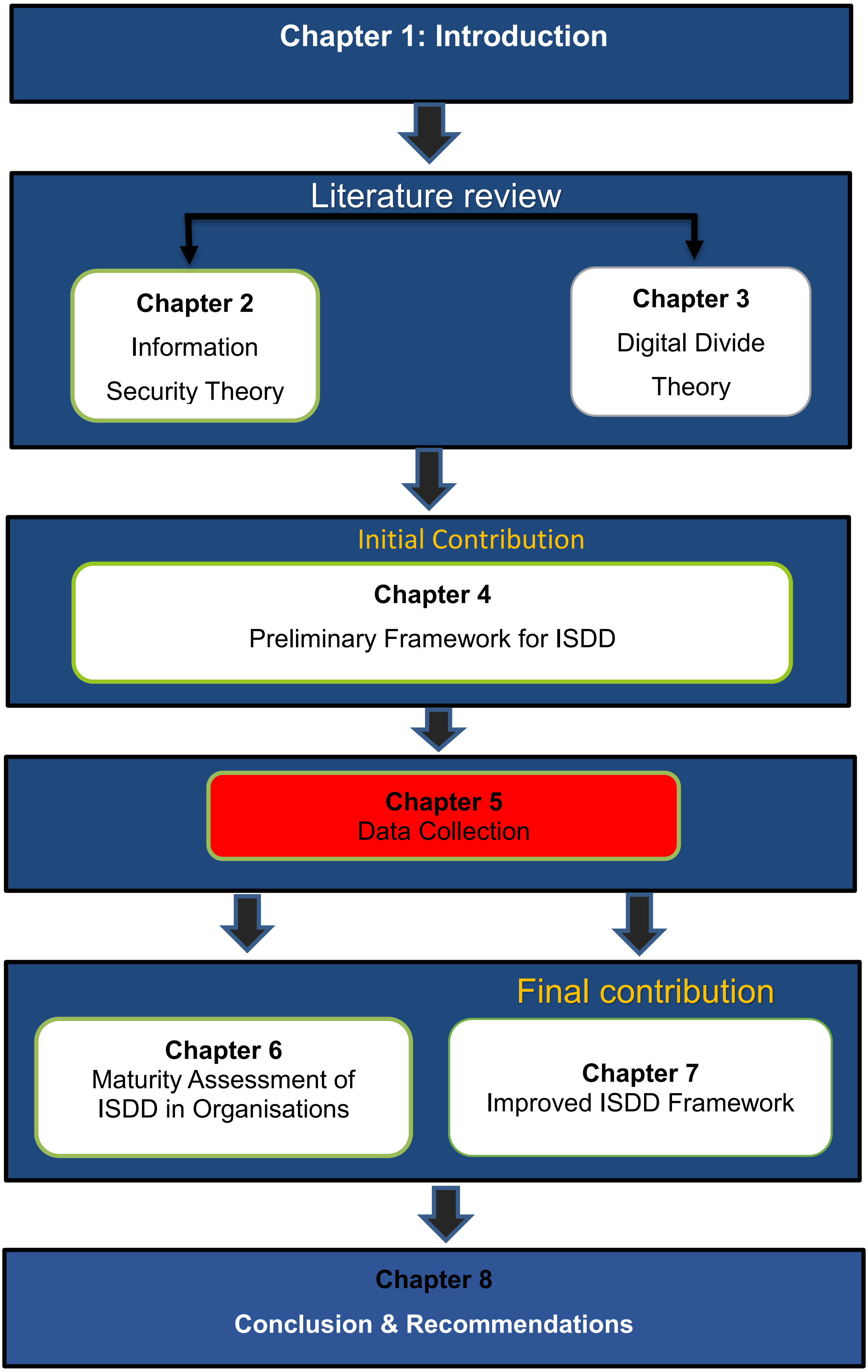
This capability level is the ultimate highest attainable level. The organisation is fully ISDD mature. ISDD critical success factor processes are fully measurable and manageable. Security is by default fully in synchronisation with the business requirements and integrated into corporate governance. Information technology is allocated to a fully equipped department with personnel that are highly trained and suitably qualified. Additionally, a sound budget is allocated to IT. System end-users range from intermediate to advanced. A well-developed information security code of conduct exists and gets updated regularly to allow the organisation to adjust to latest security threat trends. The organisation as a whole manages its information security above expectations by executing every critical success factor proactively. Technically, the system is so proactive that it can detect, resolve, and correct any potential threats and risks it encounters with little effort.

4.8. Conclusion

The purpose of this chapter was to develop a conceptual framework for benchmarking ISDD. This contributed to answering the third research question, “How can a framework for assessing ISDD be developed and validated in a real-world context?” This was achieved by drawing on the theoretical capability maturity theory contribution of COBIT as well as guidelines from ISO/IEC 27001:2013 to produce the information security digital divide maturity framework (ISDDMF), which strives to combine people, process, and technology in the best possible way to safeguard a business. Furthermore, following the capability maturity assessment technique used by COBIT, it was possible to use a combination of critical success factors of information security and digital divide to come up with an assessment compliance metrics that led to defining the ISDD compliance levels. Theoretically, reliance has been placed on COBIT to produce the information security digital divide framework. With that, the objective of developing a tool for benchmarking ISDD in organisations pending validation means in a real-life context has been reached.

The next chapter will develop a case study to practically validate the framework.

Chapter 5: Data Collection



5.1. Introduction

Until this point, the research has undergone a range of essential logical stages in iteration, including a literature review on the structure of an organisation which gave insight into information flow within an enterprise. Continually, an overview on both information security and digital divide together with their respective critical success factors was touched on in relation to how they combine to protect information. The previous chapter tackled principles around which the proposed theoretical framework was produced. Based on all the aforesaid theories, a proposed theoretical framework was presented. The framework strives to combine people, process, and technology in a way that guides organisations on standard practice to exclusively promote mature ISDD. However, the proposed framework still remains theoretical; hence, it needs to be validated in a real-life context by experts and end-users.

The main objective of this chapter is to set the context for the application and validation of the proposed framework in terms of instruments used to perform data collection. To meet this objective, case studies were conducted at three distinct target case enterprises in various environments, namely, government sector (Organisation X), ICT sector (Organisation Y), and non-profit sector (Organisation Z). A survey targeting 30 independent information ICT experts was also carried out. First, a pilot on the two sets of questionnaires was conducted, one for system end-users and stakeholders, and the other for ICT experts. This was intended to improve on initial questionnaires. Finally, the final questionnaires were amended and circulated to participants.

This chapter begins with an overview of the case study in section 5.2, specifying how the research strategy was used and why it was deemed the best, with an inclusion of the following subsections: data generation, description, and quantitative and qualitative data. Section 5.3 discusses research instruments, questionnaire structure, validation of questionnaires, and survey tool employed. Section 5.4 conveys the sample design by highlighting the population and sampling frames, sampling techniques, and sample size. A conclusion of the chapter is provided in Section 5.5.

5.2. Case Study

One of the contributions of this study is to produce a self-appraisal tool which organisations can depend on to measure both ISDD and the effectiveness of their information system. Selecting the most suitable strategy to use when collecting data is pivotal in any research. Saunders, Lewis and Thornhill (2009:600) define research strategy as an overall plan stating how the researcher intends to answer research questions. To explore further on that, a combined table (Table 5.1) illustrates some of the most applicable qualitative and quantitative research strategies and questions to help in the selection of the most appropriate strategy (Oates, 2006; Yin, 2003).

Table 5.1: Choosing appropriate research strategies

Strategy	Form of research question	Requires control of behavioural events	Focuses on contemporary events
Experiment	How, why?	Yes	Yes
Survey	Who, what, where, how many, how much?	No	Yes
Case study	How, what, why?	No	Yes
Archival	How, why?	No	Yes/No
History	How, why?	No	No

Source: Adapted from Oates (2006) and Yin (2003)

An appropriate research strategy has to be selected based on research questions and objectives (Saunders, et al., 2009). Accordingly, Starman (2013) reiterates that case studies are relevant when one's research addresses either a descriptive question such as "what is happening" or an explanatory question such as "how did something happen". Considering the strategy selection guide provided in Table 5.1 and also the fact that the main question and sub-questions of this research subscribe to both descriptive and explanatory questions ("How can a framework for assessing the maturity of ISDD in organisations for further improvements be developed?" "What are the current information security organisational practices?" and "How is success measured in such context?") A survey-based case study is the most appropriate inquiry strategy. Furthermore, case study as a data collection strategy complements this research even more because it advocates for the use of both quantitative and qualitative data collection methods (Yin, 2009:19- 20). A case study can be summed up as an empirical inquiry concerned with investigations of a contemporary phenomenon in depth, especially concerning issues that concern exploration and understanding of complex issues in real-life context (Yin, 2009; Zainal, 2007). To answer this study's research questions and meet the objectives, three case studies in random organisations from various sectors were conducted, as well as a survey among ICT experts in different fields on the quality of the framework. Figure 5.1 illustrates the structure of the case study.

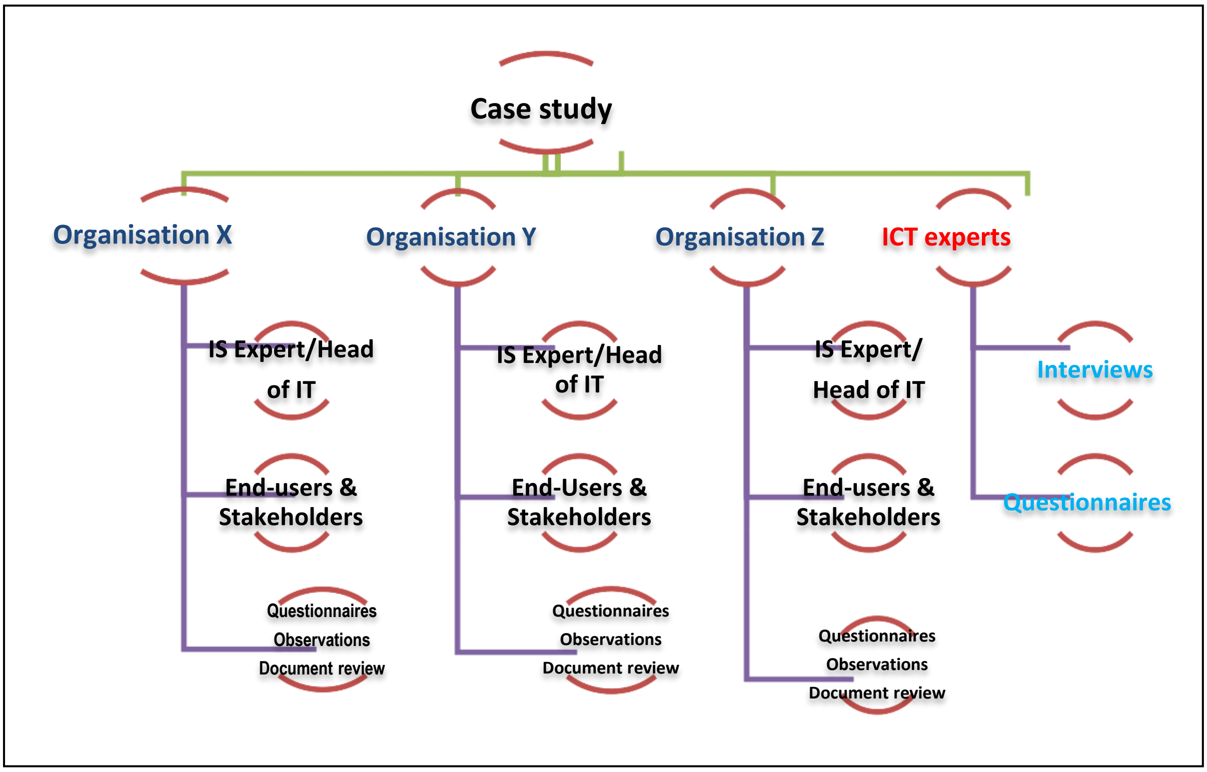


Figure 5.1: An illustration of the structure of the multiple case study used for data collection

Three organisations were assessed for ISDD and system effectiveness using both quantitative and qualitative data collection methods through questionnaires, interviews, review of documents, and observation. This was to understand how the organisations fare when measured against core system metrics and factors. Independent ICT experts and heads of IT departments or internal ICT experts within these participating organisations were part of the sample to help with the screening of the framework developed with the vision of making it extensively consensual. In the next section, data gathering is looked at in detail to give clear insight of the approaches used and why they were used.

5.2.1. Data Gathering

Even though case studies are more often considered a part into qualitative research, they may also be a combination of both qualitative and quantitative (Starman, 2013). Some of the strengths of using a case study to perform research include the following: they engage a diverse approach of evidence including review of documents, interviews, artefacts, observation, and archival records (Yin, 2003). The following multiple data collection methods were used in this study for all three case organisations plus the ICT ICT experts where applicable: questionnaires, review of documents, observation, and Interviews.

5.2.1.1. Questionnaires

Questionnaires in research refer to a set of structured questions with a choice of answers aimed at collecting specific information from respondents (Kaptein & Avelino, 2005). The idea is to translate the researcher's information obligation into easy-to-understand questions that respondents are able and willing to answer.

5.2.1.2. Questionnaire Administration

In this study, questionnaires were emailed to various identified end-users in all three participating organisations. Also, physical distribution of printed forms directly to respondents was done through the researcher as well as focal personnel that volunteered to help. In other distribution cases, social media such as Facebook was used to reach some respondents, especially ICT experts all around the world. Questionnaire samples can be found in Appendix C of this research.

5.2.2. Review of Documents

Review of documents is a qualitative method of data collection which involves relevant documents which might aid in achieving the objective of the study (Elmusharaf, 2012). It is considered an ancient way of data collection but is still useful in some research types. In this research, documents such as IT security policy, business continuity plan, and brochures were targeted and looked at if present or otherwise indicated as a not present ISDD metric.

5.2.3. Observation

Participant observation is a qualitative research approach which particularly works as a data collection method where people or processes are analysed by the researcher by also making themselves part of the situation or what is being investigated. According to DeWalt and DeWalt (2002), the intention of using participant observation as a method in research is mostly to come up with a complete understanding of the phenomena under study that is as objective and accurate as possible given the limitations of the method. Additionally, observation can either be structured or unstructured. This study used unstructured observation method of data collection, placing the culture of protecting information and security awareness around the system top of the list.

5.2.4. Interviews

According to Simpson (2011), most of the time interviews are used to get information on an individual’s experience. In this study, interviews were relied on to get some qualitative data which was done through structured questions with a few open-ended questions. Mostly interviews were for follow-up investigations on study scenarios that involved observation.

5.2.5. Data Description

For both sets of respondents (experts and end-users), data was collected in its raw format through the use of survey questionnaires designed using Microsoft Office Word 2013. It was then cleaned up in preparation for it to be exported into both Microsoft Excel and SPSS tables. Using Microsoft Excel and SPSS, data was then imported according to either Experts or End-user tables with suitable categories, then manually entered into Microsoft Excel spreadsheets according to question categories. Most data was tabulated in rows and columns, e.g. business roles that require external access to systems after work hours were collected from a completed questionnaire and summarised in the Excel spreadsheet in Table 5.2.

Table 5.2: Access need to system by internal end-users externally

	Access need from external by end-users – Question 5.2.4					
	Org X	**Org Y**	**Org Z**	**X%**	**Y%**	**Z%**
Not at all	13	6	4	68	33	15
Sometimes	5	7	14	26	39	52
Occasionally	0	1	0	0	6	0
All the time	1	4	9	5	22	33
Total	19	18	27	100	100	100

Descriptive statistics such as the mean, mode, and median were used to analyse the data statistically in order to give it full meaning or interpretation. In the case of Table 5.2, to find out per organisation the external access needs by personnel outside of normal working hours or when they are in the field, the formula that follows was used. Mode is the number or item that appears the most (DevMaths, 2016), e.g. The following options were given in a question for respondents in Organisation X to choose "Not at all" – 13, "Sometimes" – 5, "Occasionally" – 0, or "All the time" – 1. If the responses are arranged in ascending order, "not at all" was the most frequent response. This means that the majority of the employees in this organisation do not require access to the system most of the time.

MS Excel spreadsheet formulas were used in producing Table 5.2, to calculate the highest response percentage = (B6/B8)*100. This gave an indication that in Organisation X, 68% of the respondents indicate they do not require access to the system externally. Using the same table, the mean can also be worked out to know what the average response towards external access is. The response choices in Organisation Y towards external access to the system were not at all – 6, sometimes – 7, occasionally – 1, and all the time – 4. According to DevMath (2016), the mean is simply the average which is calculated by adding a series of numbers and dividing the sum by the frequency. In the case of Organisation Y, 6+7+1+4 = 18, 18/4 = 4. Using that response, it can be deduced that the average number of employees that need access to the system outside working hours and also during working hours but externally is four.

5.2.6. Response Rate

Out of a total of 35 information ICT experts who were surveyed for their response to a range of ISDD questions, a total of 25 completed questionnaires successfully, translating into a response rate of 71%. On the other hand, 90 end-users was the ultimate target aimed, but only 64 completed questionnaires successfully, giving a response of 71%. Table 5.3 below summarises the sample target size, number of responses and the percentage of responses.

Table 5.3: Target sample size, number of responses & percentage of responses table

	ICT Experts	End-users
Target Population Size	35	90
Number of Questionnaires administered	35	90
Number of Responses	25	64
Percentage of Responses	71%	71%

5.3. Case Organisation 1 – Enterprise (X)

This laboratory is a government department in the veterinary sector, which focuses on research in animal disease occurring in Namibia for economic importance. The services it provides to the nation include livestock, pasture, and botanical research. It also provides diet and nutrition of livestock, as well as ecology and utilisation.

To manage laboratory operations, Organisation Y utilises a Laboratory Management Information Reporting System that was developed in collaboration with an externally based consortium. This reporting system is composed of the following open source tools: Oracle 10g database as the back-end application; Apache Tom Cat web server using Java; Jasper report for report generation; and Firefox web browser as the front-end application.

The aforementioned computer system collects and manages all necessary information on samples, tests, and test results. The system involves the entry of sample data on arrival, as required by Namibian sampling plans; the tracking of samples through the various sections of the organisation; the collection of test results, generation of test reports, and monitoring of outbreaks through data interrogation functions; and eliminating multiple registrations of the same data on paper records. It is a fundamental component of the Namibian veterinary information system.

Organisation Y has a staff complement of 50 and comprises the following internal subsections: Food hygiene; Toxicology; Serology; Clinical Microbiology; Rabies; Pathology; and Biotechnology.

5.3.1. Case Organisation 2 – Enterprise (Y)

This is an international ICT-based enterprise in Southern Africa, especially in Namibia and South Africa. In the context of South Africa, its client base includes 14 of the 25 enterprises listed on the Johannesburg Stock Exchange. Additionally, it employs over 2,200 highly qualified IT professionals within Southern Africa. Its core business function concentrates on application services, infrastructure configuration, and implementation. The following departments exist in its Namibia Head Office: Finance; Accounting; Customer service; Sales and Marketing; Human Resource; Software and Training; and Information Technology.

The IT department consists of 10 staff members serving over 60 end-users in its head office in Windhoek, Namibia, and many more spread across the country. All customer support engineers, consultants, and other travelling stakeholders are given laptops, PDAs, tablets, and other handheld devices, while the rest of the general staff complement are allocated both desktop and laptop systems. Fileshare and email servers in use are Microsoft Windows-based. The system further uses Microsoft SQL Server for its database. Back-end Software Application used includes Enterprise resource planning (ERP) with the following modules: Service Desk, Sales and Marketing, Customer Relationship Management, and Financial Accounting.

A brief profile of the first case study enterprise has been provided. The next subsubsection considers the category and type of questions that were focused on and what the objectives of the questions were.

5.3.2 Case Organisation 3 – Enterprise (Z)

Organisation Z is a non-profit humanitarian organisation that is dedicated to alleviating human suffering by providing assistance to victims of disaster all across the 13 regions of Namibia. Its core values include: promoting human values; disaster response; disaster preparedness; and health and community care.

The organisation has its headquarters in Windhoek, with branch offices all across the country, which are linked through an information system which supports mostly communication channels using various technologies. Structurally, it consists of the following departments: Human resource; Logistics; Disaster Management; Programmes; and Finance.

Being a humanitarian organisation focused on alleviation of human suffering, the organisation heavily depends on efficient communication on and off the ground through field workers and supporting staff in regional offices and headquarters. Communication is sustained by an information system that links regional offices and also links headquarters to donors across the universe to facilitate real-time reporting.

5.4. Research Instruments

According to Abawi (2013), research instruments are technically fact-finding strategies used for the collection of data such as questionnaires, interviews, review of documents, and observations. This study used two sets of questionnaires to execute two distinct objectives: one questionnaire was intended for information ICT experts to help in screening the quality of the framework and offer suggestions on improvement avenues, and the second questionnaire was for system end-users and stakeholders, which according to the measurement methods defined in the framework would indicate at what ISDD level the organisations were ranked and operating at.

5.4.1. Questionnaire Content

Considering the primary objectives of the survey of both ICT experts and end-users discussed, the questionnaire content will next be expounded on.

5.4.1.1. Expert Questionnaire

The majority of the questions in this questionnaire targeted the core and context of the framework for improvement purposes, e.g. question 5.15 explores the use of a security model in an organisation being mandatory as a starting pointing for security, while question 5.1.8 and 5.1.9 both address the value of having an organisational structure and the flow of information when designing access control among end-users. On the other hand, question 5.1.19 investigates types of access channels most recommended for both internal and external end-users, and question 5.1.25 evaluates access by business role and function. A complete set of the questions are provided in Appendix C.

5.4.1.2. End-users' Questionnaire

This subsubsection measures general ISDD within the organisation among system end-users. Randomly, questions that showcase ISDD measurement are sampled. Questions 5.2.4 and 5.2.6 collectively check the need for external system access by business roles after business hours and which access channels they make use of. Question 5.2.5 inspects the frequency business roles interact with external stakeholders. Further, question 5.2.8 checks on security culture on password use, while question 5.2.13 deals with physical access control to information resources, and finally, question 5.2.14 measures computer user skill to assess their ability to operate a computer and work with the system without compromising security. The questionnaire and its full content can be viewed in Appendix C.

5.4.2. Expert Questionnaire Structure

The first section of ICT experts' questionnaire consisted of demographic information to provide insight on the respondents including the industry they represent, years of experience, and their specific occupation. Further to that, the remainder of the questionnaire carried the following subsections aimed at scrutinising the quality of the framework:

1. Importance of security in an organisation
2. Information system access management
3. Policy formation, standard practice, and compliance
4. Structure of an organisation and information flow

The ultimate target of these questions was to enable ICT experts to criticise the framework and also offer counter solutions to areas they felt lacked in terms of security.

5.4.2.2. End-user Questionnaire Structure

In the end-user questionnaire, the following was the content: demography on each respondent's business role, duration of stay in the organisation, and finally the business function they report to. The rest of the questionnaire consisted of these subsections:

1. Information system access management
2. Computer skill set, and security awareness and training
3. Procedure and standard practice
4. Application use and know-how
5. Culture of protecting information

5.4.3. Category of Questions to be Administered and their Objectives

This part takes a deeper dive into the types of questions addressed in end-user questionnaires and the intention thereof.

5.4.3.1. Organisation X

Being a critical laboratory, the primary focus on questions was on access control to the reporting application by end-users according to business roles and functions. Focus was also on information system access and use of data by various departments. The ecosystem and information security policies on application and information system were articulated. Here most of the questions determine application access control level measurement from an application point of view by evaluating whether laboratory employees are allocated rights according to their departments, and roles and responsibilities. Furthermore, questions weighed how well-structured control is by the application administrators and also whether the application administrators are empowered to modify the modules of the application from a back-end perspective.

Overall, the primary objective of all questions in this organisation was to measure access control management and how the system is designed to safeguard its information.

5.4.2.2. Organisation Y

Organisation Y offers ICT solutions and services to various organisations with diverse business environments. In light of that, how the organisation regulates its IT environment from a systems standpoint will be dealt with. How the system limits workflow control by portfolios from both a front and back-end application control point of view was randomly looked at. For instance, can the CIO access and regulate workflow processes outside the scope of their role? Additionally, an attempt is made to consider professional ethics by IT consultants and other professionals as system end-users with regard to standard practice and conduct when handling client resources at client sites as well as when they access the organisational intranet. Does Organisation Y have a non-disclosure agreement with its clients to ensure their personnel do not divulge trade secrets, patents, and other highly sensitive data they interact with when they have access to it due to the nature of their work?

The main objective of the questions in line with this organisation's environment was to understand the digital divide among individuals as well as how the system is set to filter that divide. It was also to understand standard practice within and outside the organisation in terms of access control at all applicable levels including network access, application use, and other services among especially all general staff.

5.4.3.3. Organisation Z

Organisation Z is mainly a field-orientated environment dealing with humanitarian-related projects. Given that background, the target questions here were mainly on communication to and from the field and how that is managed in and out of the information system that supports the organisation. Generally, it is more about whether the system limits end-users correctly according to what information is necessary to perform their roles in the organisation or whether the system over-tightens security to the point that it interferes with employees' progress.

The main objective was to assess how accessibility is managed according to the various business roles and functions. Also, what kind of technologies and applications were deployed at field level to handle corporate data, and finally, how the flow of information was used to determine access control levels.

In this subsection, questions administrated by all organisations and their objectives were looked at. Despite the differences in the concentration of questions for individual organisations, the intention is to measure system security strength irrespective of sector, magnitude, budget, organisational structure etc., as detailed in proposed future work under section 8.4.

5.4.4. Choice of Measuring Scales

In general, a measuring scale can be defined as an instrument for weighing (Oxford Dictionaries, 2016). Based on that definition and considering the fact that the main objective of this study was to establish the level of ISDD in organisations and also to appraise the effectiveness of their information systems, it was inevitable to adopt a method for this research to efficiently rely on to measure ISDD and reveal the effectiveness of systems.

1. Table 4.3 shows ISDDF mapping metrics derived from literature referenced on what the state-of-the-art security systems adopt as critical success factors
2. Table 5.4 on ISDD system measuring scale is derived by summarising mapping metrics in table 4.3 into categorised key process areas necessary for ISDD measurement
3. Table 5.5 further streamlines table 5.4 to create 5 easy ISDD levels which categorise an organisation according to how it fared against key performance areas

On the basis of the outcome of data analysis and interpretation on end-users in Chapter 7, ISDD is measured in a real-world context according to the framework core indicators and metrics set out in Table 4.3. Every question or statement contained in Appendix C was measured in relation to these core indicators and metrics, and a score was allocated to determine how well an organisation complies with that particular benchmark. Questions were split into sections and subsections that would be combined at the end to indicate the overall rating which reflects on compliance with this framework. In Table 5.4, ten different ISDD capability maturity metrics categories are shown. Each category has a list of 10 items, the combined maximum ISDD maturity score obtainable is 100. Then, an actual ISDD level and system effectiveness is denoted using stars in Table 5.5. One star is a symbol of non-compliance to any level of ISDD defined in this framework, and two stars is entry level all the way to the highest obtainable level (five stars), which is a symbol of full mature ISDD compliance and a highly effective information system.

Table 5.4: ISDD and system measuring scale

Overall rating	**Org X**	**Org Y**	**Org Z**
1. Information flow	0	6	4
2. Standard Practice, Policies & Procedures	8	8	4
3. Management Support	0	9	4
4. Security Types in Place	7	10	7.5
5. Security Awareness and Training	0	0	0
6. Access Control Management	9	9	4.5
7. Culture of Protecting Information	4	8	8
8. System Appropriateness	4	6	4
9. Business Continuity Plan (BCP)	0	3	6
10. Performance Target & Continuous Assessment	2	2	2
Combined rating	34	60	48

Table 5.5: ISDD maturity and system effectiveness summary table

Assessment Rating	Star	ISDD Level
0 - 20	*	Non-compliance
21 - 40	**	Initial compliance
41 - 60	***	Basic compliance
61 - 80	****	Acceptable compliance
Above 80	*****	Full compliance

Source: Adapted from Saleh(2011)

5.4.5. Validation of Questionnaire

An important component in the data collection process is piloting (Monette, Sullivan & DeJong, 2002). Before the final survey of this research was conducted, a pretest of survey questionnaires with closed-ended questions was done by circulating them to five ICT experts from different sectors, and also to six random end-users from all three organisations belonging to different business functions and occupying unique roles. According to Scholar Bank (2010), the main purpose for piloting a survey is to test the questionnaire to ensure it is coherent and comprehensible. In line with that, this study piloted the survey to get views and concerns before the final survey, which would lead to amendments suitable to improve the relevance and value of the survey questionnaires. Directly, that benefited the relevance and quality of the final survey together with the research.

Following the piloting of survey questionnaires, a couple of suggestions that required changes to both sets of questionnaires were identified as follows:

- **Expert Questionnaire:** Incorporate middle management as a business role; also add expert years of experience on demographics; change the one external stakeholder's access channel from Web portal to internet; remove some closed-ended questions; add some closed-ended questions to contextualise certain areas such as access control; and finally, remove some options questions with Yes or No options as answers to avoid a biased outcome.

- **End-users Questionnaire:** Adjust years of experience under demographics to include 8-10 years category, include middle management as a business role, and include voice recognition as an authentication option.

5.4.6. The Research Software Tools

Administration of survey questionnaires in this study was done using three software tools, namely, Microsoft Office Word, SPSS, and Excel. Microsoft Office Word was used to design the questionnaires which were delivered in person by the researcher to the respondents by hand and by soft copy through email and social media (Facebook). SPSS was used to perform data triangulation, and Microsoft Excel spreadsheets were relied on for entering data after it was cleaned up and prepared for interpretation and translation.

5.5. Sample Design

This section discusses the techniques used in the execution of this research. In doing so, sampling and participant profiles are briefly looked at.

5.5.1. Population

Choosing the right participants is an essential part of research. Participant selection is mainly influenced by the applicability of the information needed from relevant individuals by the researcher. Participants in this study were split into two: the first group was end-users of the information system in every target organisation, and then the second comprised ICT experts within and outside of the enterprises.

A total of 110 participants took part in this survey. Of the 110, 25 participants were independent ICT industry experts and the remainder system end-users from the three case organisations split as follows: 19 respondents from organisation X, 18 respondents from Organisation Y, and 30 respondents from organisation Z.

Staff in all participating organisations were targeted to better understand the applicability of information security digital divide. On the other hand, experts' involvement would provide input on the relevance of the framework to the work environment.

5.5.2. Sampling and Sampling Frame

Sampling is the act of choosing a portion of a population with the intention of generalising the findings to the entire population sampled from (Kitchenham & Pfleeger, 2002). Sampling is applied in many types of research because in some cases, collecting information from the entire population is costly, time-consuming, and in most cases impossible. Tashakkori and Teddlie (2003) state that probability sampling techniques are key in quantitative-based research and involve selecting a relatively large number from a population or from specific subgroups of a population. To compound that, Teddlie and Yu (2007) go further to stipulate that probability sampling aim at getting as much representation as possible, which highly reflects the degree to which the sample accurately represents the overall population sampled from. In contrast to probability sampling, purposive sampling techniques are primarily used in qualitative research and are often about selecting a section of the sample purposefully well-placed to aid in providing answers to the research question (Teddlie & Yu, 2007).

To get an accurate representation of both ICT experts and end-user populations, Systematic random sampling method was adapted in this research. Both samples were broken into intervals by taking the total target population and dividing by a number to create intervals. E.g organisation X had a total of 120 system end-users, we divided that by 4 to get 30 intervals which ensured a rational representation of end-users to take part in the survey, and the pattern was applied to the remaining two participating organisations. For ICT experts, they were also divided into 5 intervals by dividing the overal target population by 5 in order to increase the chances of a wide range of ICT expert representation. Information system end-users helped the researcher to determine the level of ISDD and measurement in the appropriateness of the information system, while ICT security expert engagement assisted in making the framework largely consensual.

A sampling frame in research refers to a record of the population from which a sample is taken (Singh, 2015). In simpler terms, it could be people or items forming a population from which these people or items are taken. ICT experts were the first sample. The second portion of the sample constituted all system end-users that interact with the systems of all the organisations, this included all external stakeholders such as suppliers, partners, contractors, customers, and consultants.

5.5.3. Data Preparation and Cleaning

Data preparation entails editing, coding and tabulating. In this research, data collected through the survey from ICT experts and end-users was of both a qualitative and quantitative nature. This data was logged in and checked for consistency and transformed into a format readable by tools which were used to manipulate and translate it into meaningful information that the researcher used to translate and interpret research findings in order to answer questions and reach objectives. A detailed explanation of data analysis will be provided in Chapter 6.

5.5.4. Validity and Reliability

Reliability in research entails the stability, equivalence, and consistency of a tool used to conduct research from one assessment to another (Roberts, Priest & Traynor, 2006). Primarily, if the same result can be replicated under a similar method, then the tool used can be considered reliable. This research took on the split-half concept whereby the Spearman-Brown prophecy formula was implemented and the outcome retained a coefficient equivalent to 0.74 as detailed earlier in section 1.9 which is a demonstration of the reliability and validity of the research method used over time.

5.5.5. Limitations

In addition to limitations discussed in Chapter 1 (Section 1.6) regarding the participation of only three organisations in this study and COBIT's principles as the sole base reference framework, the intended sample was not met because some participants offered to take part but did not complete the questionnaires; this altered the envisaged outcome. In other few isolated cases in the last case organisation, respondents did not answer questionnaires in accurately and to the best of their ability due to time constraints, which made data analysis difficult.

5.5.6. Ethical Considerations

In addition to ethical considerations touched on in detail earlier in Chapter 1 (Section 1.10), high ethical standards were adhered to during this entire study. Permission in writing was sought from UNISA's ethical clearance committee, and clearance was issued as per Appendix A. Also, permission was requested in writing from all three target organisations to perform surveys and collect all necessary data required to complete the research; all three organisations agreed to the requests in writing as well. All participants from various organisations were informed of what the research was about including its objectives. Participants were further enlightened on their rights to withdraw from participation if they felt uncomfortable or not willing at any point to continue with the participation. They all signed the consent form that is included in Appendix E.

5.5.7. Permission to Conduct Research

It is mandatory for institutions to make sure that all ethical review is in place and adhered to before giving any form of research a go-ahead in order to protect the integrity of organisations and respondents (Chilengi, 2009; Terre Blanche & Durrheim, 2002). In the context of this research, an application was made to the research ethics committee. The research ethics committee at University of South Africa reviews and grants permission to do research when ethics standards need to be met. Proof of application and approval for this research can be found in Appendix A.

5.5.8. Consent Forms

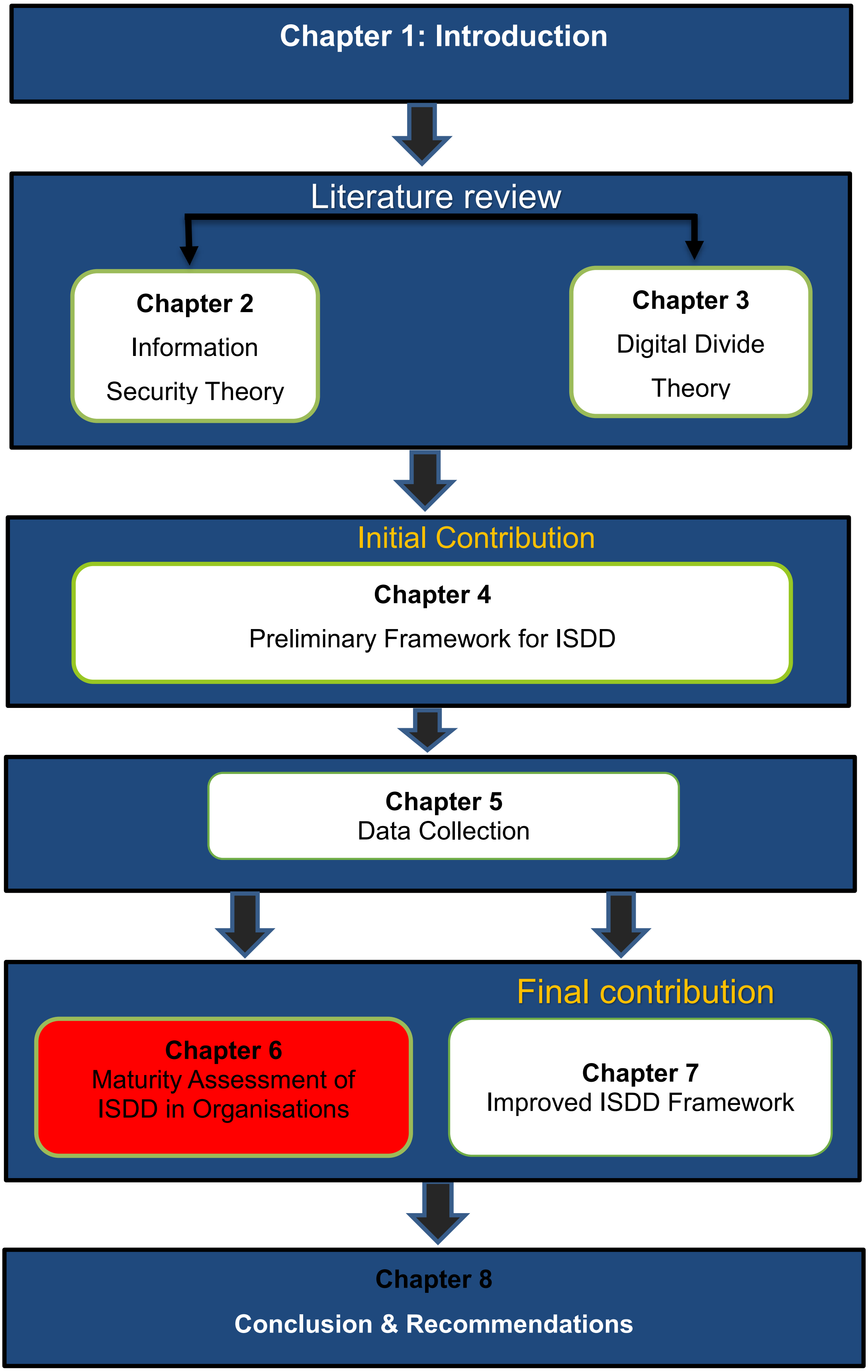
Any research conducted involving respondents must have an informed consent provision for the participants. In that respect, all participants who agreed to participate in this research were given a breakdown of what the research was about. Based on that, they willingly signed the consent forms to indicate their acceptance to participate. Further to that, they were made aware of the fact that they could withdraw at any given time if they felt uncomfortable and/or were not willing to continue with participation. A sample of the consent form can be found in Appendix D.

5.6 Conclusion

In this chapter, data collection was covered. First, the best research strategy applicable to this study's research type was determined. Case studies, research instruments, sampling, and data description were then discussed. Details were also provided on both end-user and ICT expert's questionnaire structures, the content of which is available in Appendix C. Furthermore, validation of questionnaires was touched on. The purpose of the chapter was to discuss tools aiming not only at testing the framework in a real-life context but also to validate it by using ICT experts for further improvement.

The chapter that follows will focus on the outcome of the ISDD maturity assessment of case enterprises and draw a conclusion as proof that the framework can indeed be relied on in a real-life context.

Chapter 6: Maturity Assessment of ISDD in Organisations



6.1. Introduction

The preceding chapter presented the layout of the instruments used to gather data as well as the context for the validation of the proposed framework. The main purpose of this chapter is to analyse data from the first part of the survey involving system end-users in order to determine the capability maturity of case organisations. This objective is reached by analysing responses from end-users and stakeholders ranging from CEOs, upper and middle management, including general staff in each organisation in order to measure ISDD among all and generalising that to the entire population. In doing so, the objective of testing the conceptual framework in a real-world context to see if it can be relied upon to measure ISDD maturity is also achieved.

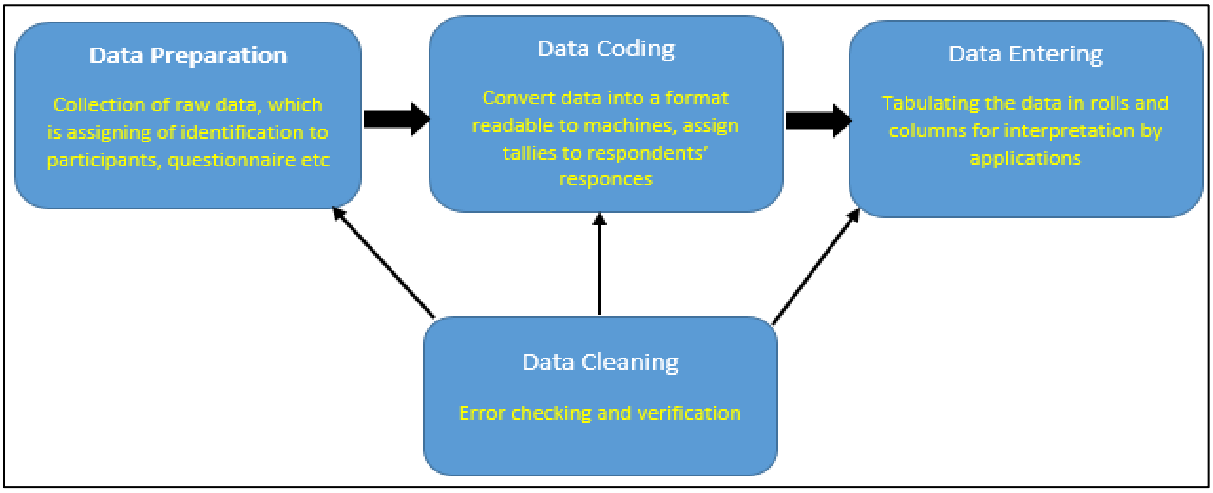
The chapter begins with data analysis in detail including quantitative and qualitative data analysis as well as steps involved thereof in Section 6.2. Section 6.3 focuses on survey results for end-users; it covers aspects such as demography, access control, computer use skill set, and others. Section 6.4 covers ISDD maturity level assessment, touching on various framework metric categories such as security awareness and training, standard practice and policies, management support, security types, and many others. The section also derives the maturity assessment rating of ISDD per case organisation. Finally, the conclusion of the chapter is provided in Section 6.5.

6.2. Data Analysis

Data analysis and interpretation is the process of assigning meaning to the collected information and determining the conclusions, significance, and implications of the findings (OIRA, 2013). For all the case organisations discussed in Chapter 5, data analysis and interpretation will be the same. This study used the method of triangulation to validate data generated. Data collected was both of a qualitative and quantitative nature. Qualitative research centres on narrative and performance analysis in order to discover similarities and insights in the responses. It is worth mentioning that a quantitative approach was used more in this research, since the bigger picture of the study involved sampling from a population and generalising the findings to the overall population. Quantitative data analysis generated for this study relied on statistics to examine and interpret the data collected from respondents.

6.2.1. Quantitative Data Analysis

Quantitative data analysis is a representation of data in numerical form (Schulze, 2003). Its main purpose is the quantification of data following statistical procedures to process data in order to give it meaning. The outcome of quantitative data is often measured in relation to a quantity (Nikolakopoulos, 2009). Durrheim (2002) sums up quantitative data analysis stages as involving, coding, entering, and cleaning of data. Figure 6.1 shows steps involved in quantitative data analysis.



Data Preparation
Collection of raw data, which is assigning of identification to participants, questionnaire etc
Data Coding
Convert data into a format readable to machines, assign tallies to respondents' responces
Data Entering
Tabulating the data in rolls and columns for interpretation by applications
Data Cleaning
Error checking and verification

Figure 6.1: Steps in quantitative data analysis

Source: Adapted from Durrheim (2009)

The limitation of quantitative research is exposed when there is a need to investigate many varying realities in assorted contexts (Pickard, 2007). However, Choy (2014) counters that by asserting that the strength in quantitative research lies in its ability to produce concrete frameworks with data that is in a format easier to translate and analyse. This study mainly involved looking at trends and patterns in end-users' activities when interacting with information systems. Therefore, quantitative research was more suited for the study even though qualitative was also required in some cases.

6.2.1.1. Steps in Quantitative Data Analysis

Step 1: Preparing the Data

Quantitative data is a representation of data in its raw form; it consists of numbers that represent scores on variables (Wright & Losekoot, 2010). Being in its raw state, it is unstructured, not in order, and may contain flaws and missing values which need to be corrected in order to convert it into a machine format that is executable. In this study, most of the data is primary, as it was collected through questionnaires with mostly closed-ended questions; however, in a few cases secondary data was also collected through observation.

Step 2: Coding the Data

Data coding is considered as the transformation of data into a state that computers and accompany application programs can understand and translate. In the case of this study, items from questionnaires were transformed into a format readable by computer applications. For example, information ICT experts were asked to rank how critical information security is to the operations of an organisation, with option 1 being “not critical”, option 2 – slightly, option 3 – fairly, option 4 – critical, and option 5 – very critical. The responses were assigned scores. The scores of all items were combined to produce a summed score to indicate the overall picture. Combined scores represented the thought of the various ICT experts on the value of information security to the operations of an enterprise.

Step 3: Entering the Data

Through the use of statistical application programmes, interpretation of data occurs through numerical data collected from questionnaires. In this study, using a combination of SPSS and Microsoft Office Excel spreadsheets, data was entered in row and column fashion on variables under investigation. Variable labels entered in the computer applications were identical to those in questionnaires to make it easy for reference and error correction.

Step 4: Cleaning the Data

Occasionally errors in data may occur. According to Schleicher and Saito (2005), cleaning of data is critical before analysis. In addition to that, data cleaning involves checking for any potential errors and correcting them accordingly. In this study, a random sample consisting of 10% of the data collected was cross-checked to ensure it was error-free.

6.2.2. Statistical Data Analysis

Having prepared the data by cleaning and converting it to computer application acceptable format, the next step was to analyse the data through statistical means. There are two main types of analysis, namely, descriptive and inferential data analysis.

6.2.2.1. Descriptive Data Analysis

Descriptive statistics is the conversion of raw numerical facts and figures into a state that will be easy to understand and interpret (Zikmund, 2003). On top of that, Larson (2006) claims that it is a mere summary of various aspects of the data that gives details about the sample and provides information about the population from which it was sampled. This refers to rearranging, ordering, and manipulating data to generate descriptive information (Zikmund, 2003). In the context of this study, calculations ranged from the mean, mode, and median, which helped in understanding concepts such as the central tendency of standard IT practice when system end-users interact with the system.

6.2.2.2. Inferential Data Analysis

Inferential statistics in research helps in making inferences about populations on the basis of samples collected. It is useful in making estimate population parameters and also testing hypothesis (Terre Blanche & Durrheim, 2002). It can also be split into parametric and non-parametric.

In the foregoing section, literature presumptions on approaches used to analyse both qualitative and quantitative data were presented. The next section focuses on the data analysis in a real-world context of data collected from end-users of target organisations.

6.3. Results of First Survey for Case Organisations X, Y and Z

This part of the chapter interprets data and establishes ISDD levels. The response ratio as opposed to the target is calculated, followed by a brief analysis and interpretation of ISDD metrics and core indicator questions.

6.3.1. Response Rate and Demography

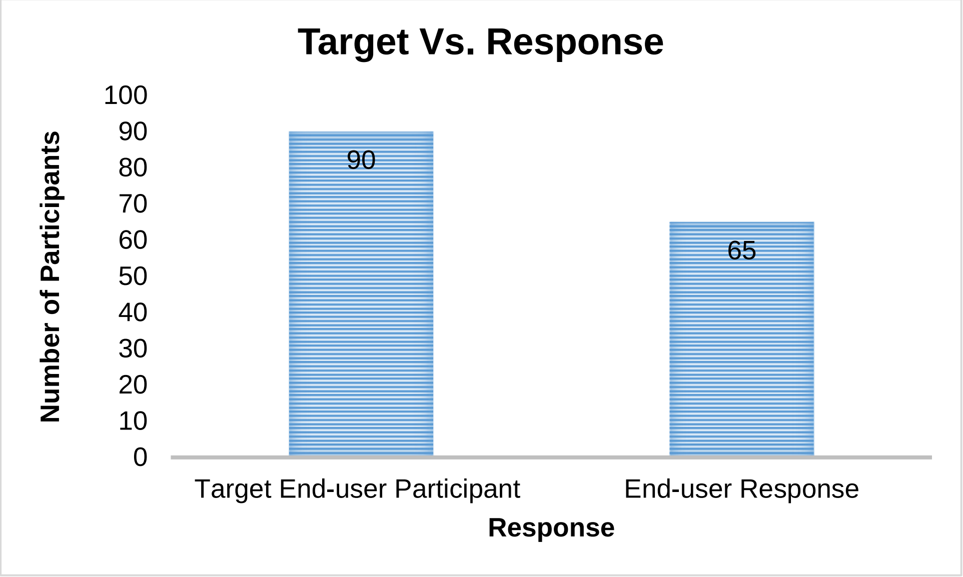


Figure 6.2: End-user participant response

The target in this study was to reach out to approximately 30 end-user participants per organisation, as indicated by the total of 90 in Figure 6.2. However, it turned out that more than 50% of the target was reached for each organisation (96% for Organisation Z, 60% for Organisation Y, and 63% for Organisation X), which is above average and as such satisfactory.

6.3.2. End-user Participation

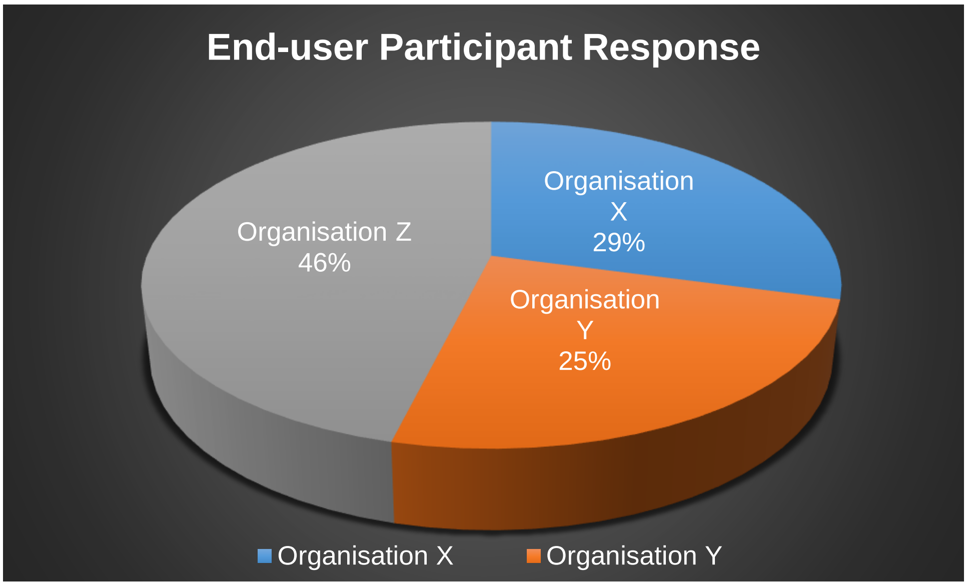


Figure 6.3: Participant response by organisation

According to Figure 6.3, regarding the distribution between target organisations, out of 65 end-user participants, 25% of them were from Organisation Y, 29% from Organisation X, and the final 46% from Organisation Z. This was a satisfactory distribution.

The next subsection is the analysis of the remaining random set of questions for this part of the survey. The question numbering highlighted in brackets next to the subsection is consistent with the questionnaire numbering in Appendix C.

6.3.3. Role-based Questions

Some of the role-based questions in this study follow.

- **Question 5.2.1 –** *Please state your business role within the organisation*

The purpose of this question was to have a clear picture of the role placed by end-user participants within the organisation and demonstrate the importance of such role in the context of ISDD. Figure 6.4 quantitatively depicts the various roles followed by discussions on the results obtained.

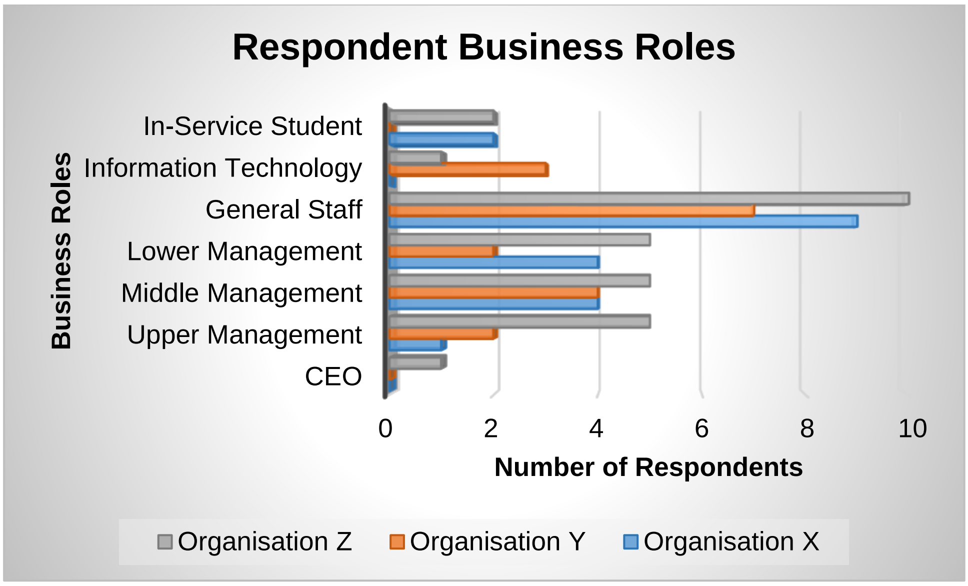


Figure 6.4: Business roles of respondents

Organisation X had a total of 19 participants, as indicated in Figure 6.4. Five per cent of them were part of upper management, 20% was from middle management, another 20% came from lower management, 45% was the representation of general staff, and 10% was made up of in-service students. There was no IT representation.

Organisation Y had a total of 18 participants who took part. Figure 6.4 shows that 11% of them were upper management, 22% middle management, and 11% consisted of lower management. The majority of the population that participated were general staff at 39%, and 17% of them were members of the information technology (IT) team.

Organisation Z had a maximum of 29 participants who responded. Of that population, the distribution was as follows: 3% from upper management, middle management and lower management all comprised 17%, 34% was general staff, 3% from IT staff, and 7% in-service students.

- **Question 5.2.2 –** *State how long you have been in this organisation*

In this question, the aim was to understand the duration of each participant in the organisation in order to relate ISDD understanding according to length. Figure 6.5 presents duration in the organisation per participant and discusses the findings.

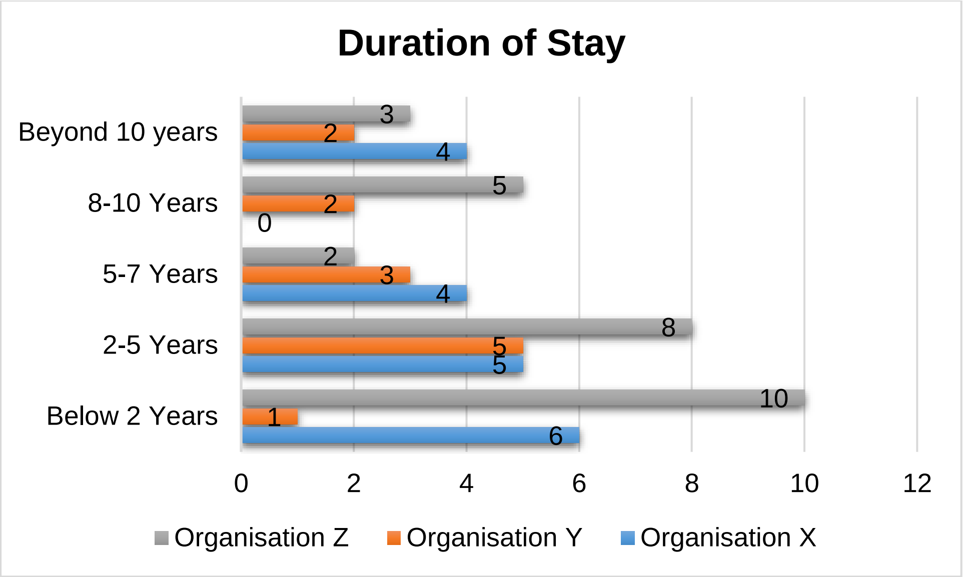


Figure 6.5: Duration of stay at organisations

Organisation X – According to Figure 6.5, the majority of the respondents have been at the organisation for less than 2 years (32%). The second majority (26%) has been there for 2-5 years, and the third and fourth groups making up 21% each represent 5-7 and beyond 10 years.

Organisation Y – In Organisation Y, 8% of the respondents have been there for less than 2 years. Thirty-eight percent of the respondents have been there for 2-5 years, 23% for 5-7 years, and participants who have been at the organisation for 7-10 and beyond 10 years represented 15% each.

Organisation Z – This organisation had the majority (36%) at below 2 years, 29% between 2 and 5 years, 7% for 5-7 years, 18% for 8-10 Years, and finally 11% for beyond 10 years.

- **Question 5.2.3 –** *Which business function do you report into*?

The purpose of this question was to measure ISDD according to a business function that an end-user should be confined to in accordance with the organisational structure. Discussions around the findings follow regarding Figure 6.6 including a quantitative depiction.

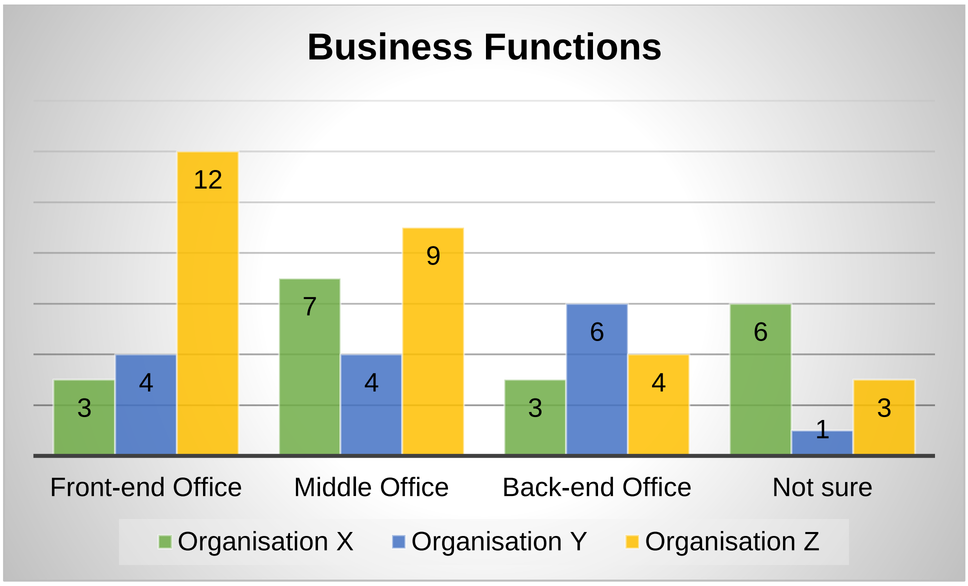


Figure 6.6: Respondents according to business function

Organisation X – Figure 6.6 reveals that 37% of the respondents in Organisation X fall into middle office, 32% of them were not sure where they belong, and 16% each stated front- and back-end offices.

Organisation Y – Most respondents make up the back-end office (47%), while front-end and middle offices share 27% each, with 7% not sure where they are classified.

Organisation Z – Organisation Z had 43% front-end office representatives, 32% middle office, 14% back-end office, and only 11% of them were not sure of their business function placing.

The demography of the participants was the centre of this subsection. With that done, the next item involves analysing digital divide-related responses to some of the set metrics, specifically the handling of access control.

6.3.4. Access Control-based Questions

The focus of this subsection is on access control-based questions, which are explored next.

- **Question 5.2.4 –** *Does your business role require you to access the system from outside the organisation?*

The purpose of this question was to place the number of business roles that need external system access so as to understand ISDD risk through devices used to access the system in such cases. Measurably, in Figure 6.7, end-users that require external access are shown and the accompanying explanation thereafter.

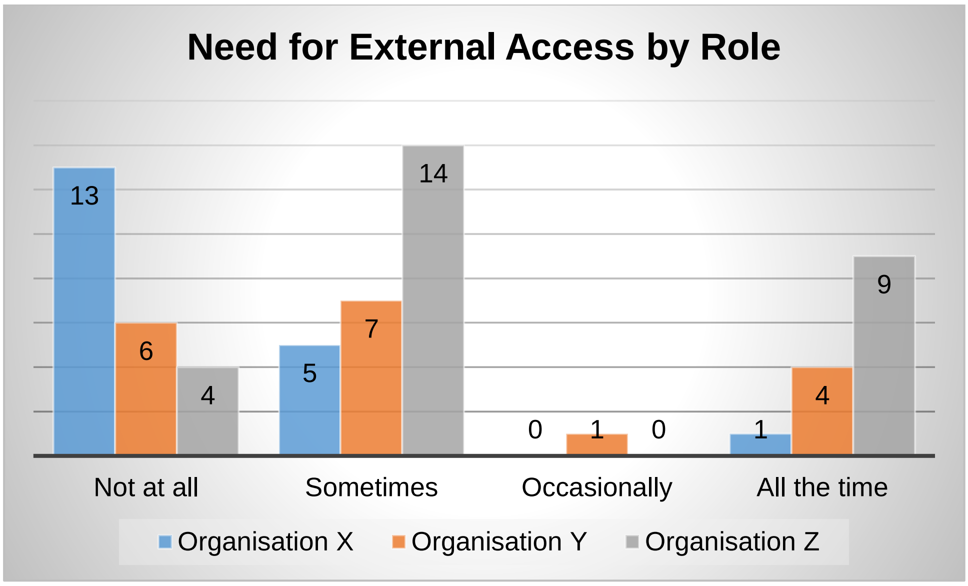


Figure 6.7: Need for external access to the system by employees

Organisation X – End-users were asked about the need to access the system externally according to their business role. Sixty-eight per cent declared that they do not require access at all. However, 26% sometimes require access, with only 5% of those who exclusively need access all the time.

Organisation Y – Over the same question, respondents in Organisation Y fared differently, as 39% need access to the system externally sometimes, whereas 33% do not need access. It came to light that 22% need access at all times, while 11% need occasional access as well.

Organisation Z – In this organisation, the majority of the respondents (55%) sometimes need external access to the system, while the second-largest number of respondents (33%) need access at all times. The least group (15%) has no need for access at all.

- **Question 5.2.6 –** *Which access channels do you use to access the system when you are outside the organisation?*

In this question, the focus was on all end-users whose business roles and functions require them to access the system externally. It had to be established what kind of access technology they make use of and how the system manages access in relation to authentication and isolation according to roles and responsibilities which constitute ISDD critical success factors. Figure 6.8 depicts the findings.

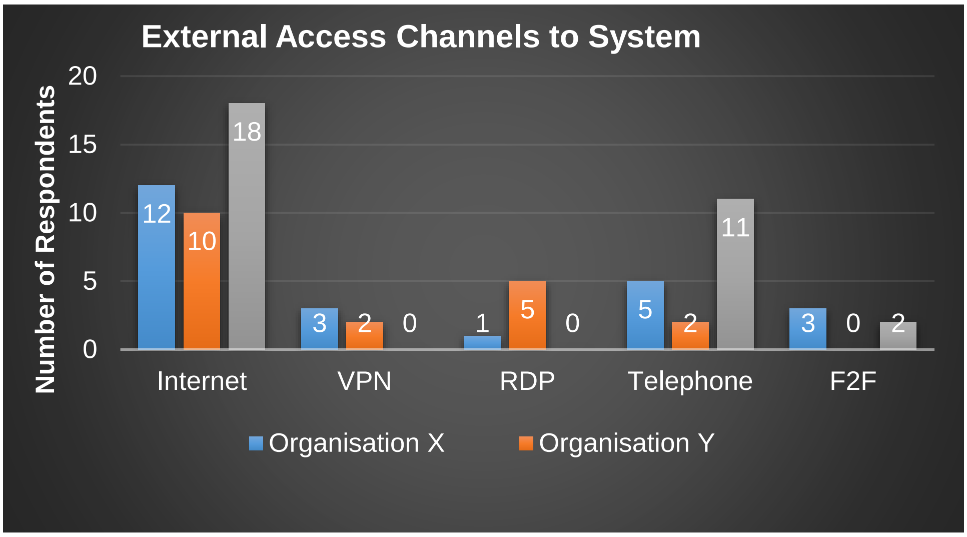


Figure 6.8: External access channels used by end-users

Organisation X – According to Figure 6.8, half of the respondents (50%) who use the system externally do so through the Internet, whereas 13% use VPN, 4% RDP, and the second largest (21%) use the traditional telephone method.

Organisation Y – In Organisation Y, it is shown that 53% resort to the Internet for external access, with the second most (26%) using RDP, while 11% each prefer VPN and telephone.

Organisation Z – The response for Organisation Z was as follows: 58% uses the Internet, 35% uses telephone, and 6% uses face-to-face (F2F) channel.

- **Question 5.2.7 –** *Which access channels do you use to access the system internally?*

The purpose of this question was to highlight how end-users access the system internally including physical restriction to information resources which are all part of factors that ISDD is measured on. Figure 6.9 demonstrates the outcome graphically and the interpretation comes thereafter.

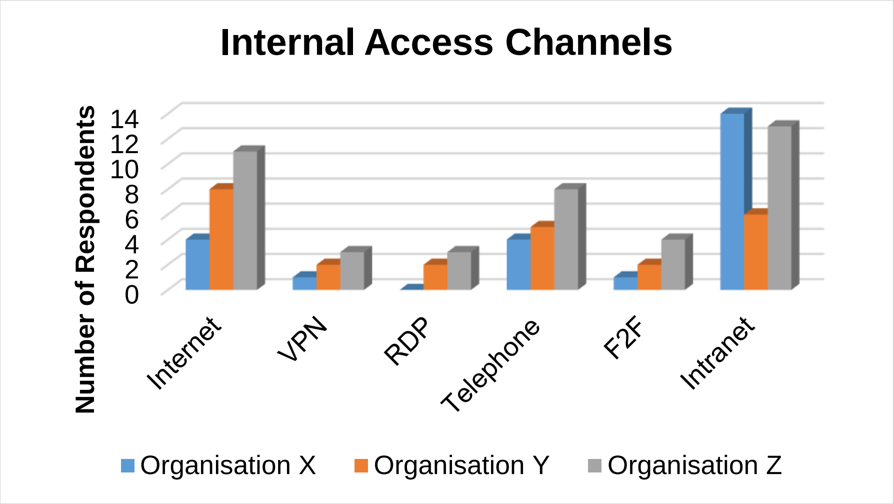


Figure 6.9: External access channels available to the system

Organisation X – In Organisation X, 17% of the respondents use the Internet to access the system internally, 4% VPN, 17% telephone, 4% face-to-face, and 58% intranet.

Organisation Y – Respondents in Organisation Y responded as follows: 32% uses the Internet, both RDP and VPN are at 8%, 20% uses telephone, 8% uses the face-to-face channel, and 24% uses intranet.

Organisation Z – Organisation Z presented the following responses: 26% internet, VPN and RDP both 7% each, 19% telephone, face-to-face channel at 10%, and finally 28% intranet.

- **Question 5.2.8 –** *In accordance with the access channels available, which authentication do you use?*

The essence of this question was to investigate authentication methods available to the given access methods to analyse access control as a basic of ISDD measurement. Statistically, Figure 6.10 illustrates the outcome, and further to that, discussions are detailed around authentication.

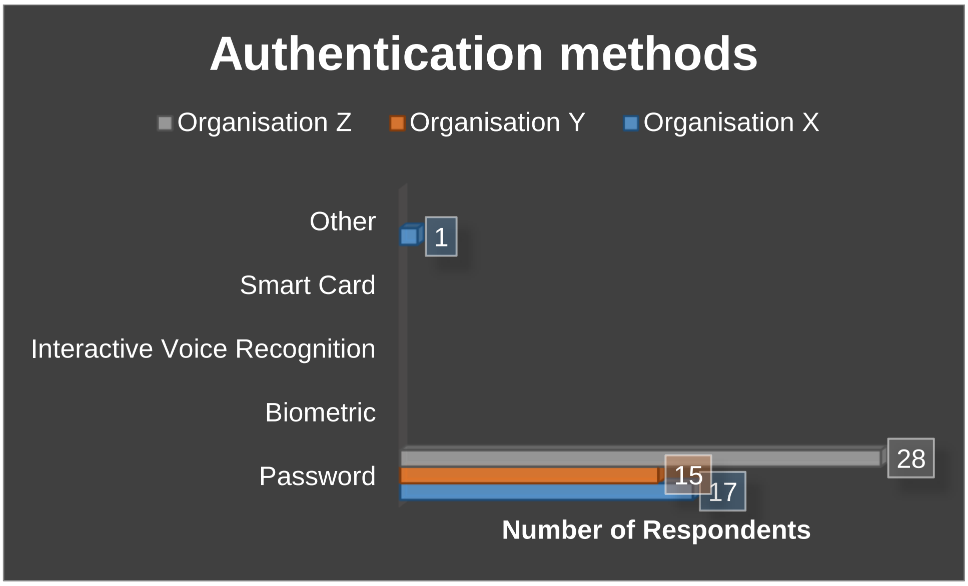


Figure 6.10: Authentication type used by end-users accessing the system

Figure 6.10 indicates all organisations (X, Y, Z) use the same authentication methods when accessing the system, both internally and externally. Organisation X showed that 94% of the respondents used a password with one other unstated method. Organisations Y and Z had a 100% password use response.

- **Question 5.2.9 –** *In your opinion, does the organisation's system limit your access to what is relevant to your work scope?*

The purpose of this question was to enquire from end-users how they felt over the access restriction rendered by the system in relation to their business roles and functions.

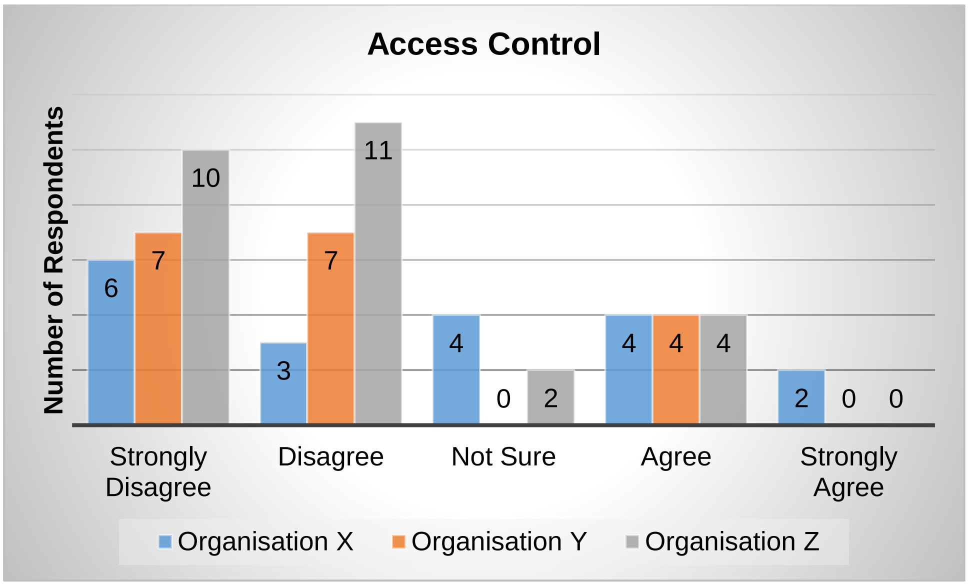


Figure 6.11: Access control according to business roles

Organisation X – From the responses in Figure 6.11, close to half of the respondents are of the opinion that the system does not limit their access according to their work scope, while 32% of them strongly disagree and 16% disagree. On the contrary, 21% of them think the system limits them according to their work scope, whereas another 21% of the respondents think they are not sure. The last group thinks strongly that the system limits them accordingly.

Organisation Y – In Organisation Y, 39% also strongly disagree with the fact that the system limits them to what is relevant to their work scope. A further 39% also disagrees, and contrary to that 22% agrees.

Organisation Z – In this organisation, 37% of the respondents strongly disagree, 42% disagree, 7% are not sure, and only 15% agree to the fact that the system limits them according to the relevance of the resources to their work.

- **Question 5.2.13 –** *Which physical access restriction method to information resources do you use in your business function?*

Fundamentally, here the physical partitioning of business roles and functions was the objective especially to control physical access to information resources – a quality necessary for ISDD. Figure 6.12 highlights the statistical responses and a discussion continues thereafter.

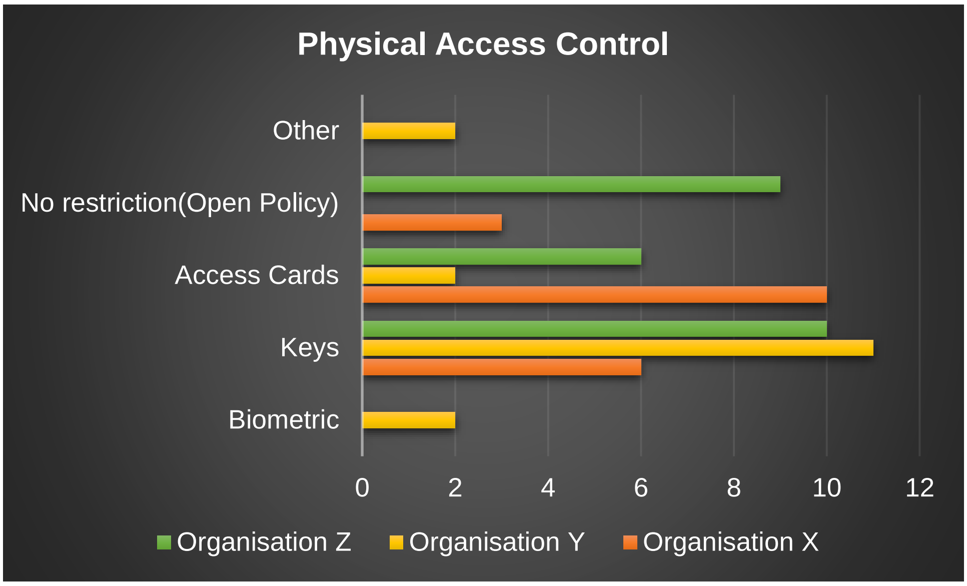


Figure 6.12: Physical access control techniques

Organisation X – Fifty-three per cent of the respondents use access cards in order to physically access information resources within the organisation. Further, 32% resort to keys, and the minority (16%) operates in open policy workspaces.

Organisation Y – This organisation has 65% of staff using keys to access information resources, 12% uses biometrics, 12% uses access cards, and another 12% uses other methods not mentioned.

Organisation Z – Keys are the most prominent at 40%, while 36% of the respondents indicate they operate in open policy offices, and 24% uses access cards.

6.3.5. Computer Literacy-based Questions

Questions that are computer literacy-based will now follow.

- **Question 5.2.15 –** *Where do you rate your computer use skill set?*

Primarily, the question addressed the computer usage competencies of all end-users and equated their responses statistically, as shown in Figure 6.13, to their ability to interact with the system without compromising it.

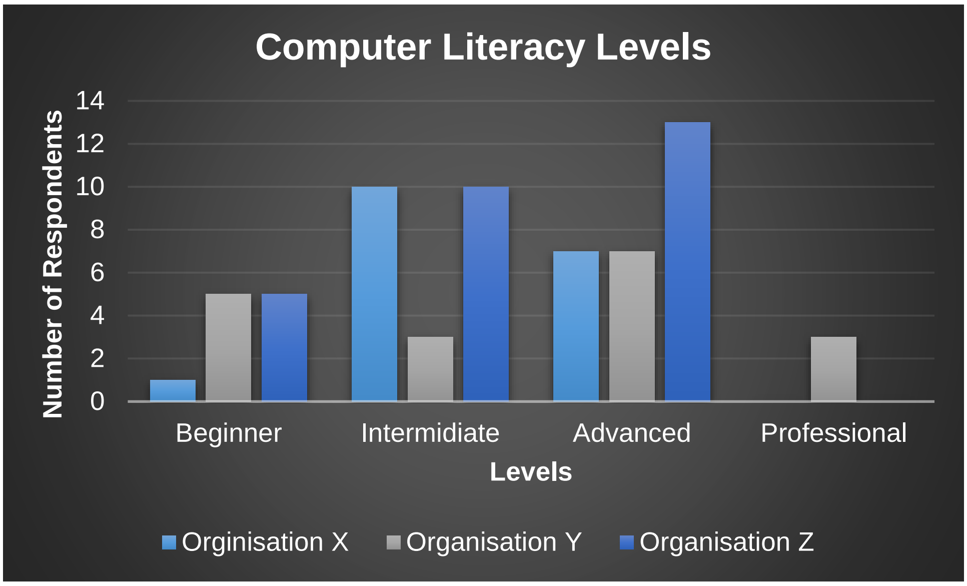


Figure 6.13: Computer use skill set levels

Organisation X – Computer literacy-wise, most of the respondents in Figure 6.13 are at intermediate level (56%), followed by advanced (39%), and finally beginners make up the smallest population (6%).

Organisation Y – In this organisation, advanced users make up the biggest portion (39%), then comes beginners (28%), and finally professionals and intermediate split into 17% each.

Organisation Z – Organisation Z reports advanced users as the majority (46%), with 36% being intermediate users, and finally the minority (18%) are beginners.

6.3.6. Culture of Protecting Information

The question that follows pertains to the culture of protecting information.

- **Question 5.2.16 –** *I fully understand the consequences of my actions while interacting with/or accessing the system*

The intention of this question was to measure end-users' awareness of their actions when accessing the system. The graphical depiction in Figure 6.14 is explained in detail in the discussion that follows.

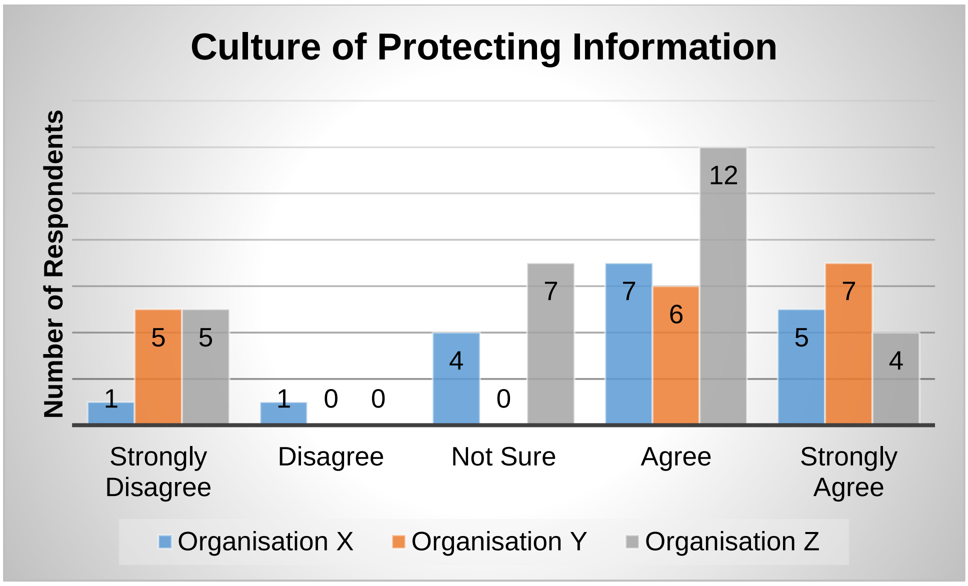


Figure 6.14: End-user understanding of consequences of system misuse

Organisation X – Of all the respondents who took part in the survey, the majority (39%) merely agreed that they understood the consequences of their actions while interacting with the system. A further 28% strongly agreed, 22% was however not sure, while a split of 6% each of the respondents indicated that they were in strong disagreement and merely disagreed.

Organisation Y – In this organisation, more agreement than disagreement was the outcome, with 39% who strongly agreed, 33% who agreed, and 28% who disagreed.

Organisation Z – Forty-three per cent agreed to the fact that they knew the effect of their interaction with the system. However, 25% of the respondents were not sure, 18% strong disagreed, and the least strongly concurred with that statement.

6.3.7. Security Awareness and Training

The questions that follow have to do with security awareness and training.

- **Question 5.2.17 –** *Have you ever received information security awareness or training within the organisation before?*

In-house capacity building tailor-designed to suit the security structure of the organisation as well as activities that subscribe to strong ISDD conduct among all end-users was the purpose of this question. Figure 6.15 represents quantitative findings, and further down an explanation to that effect is given.

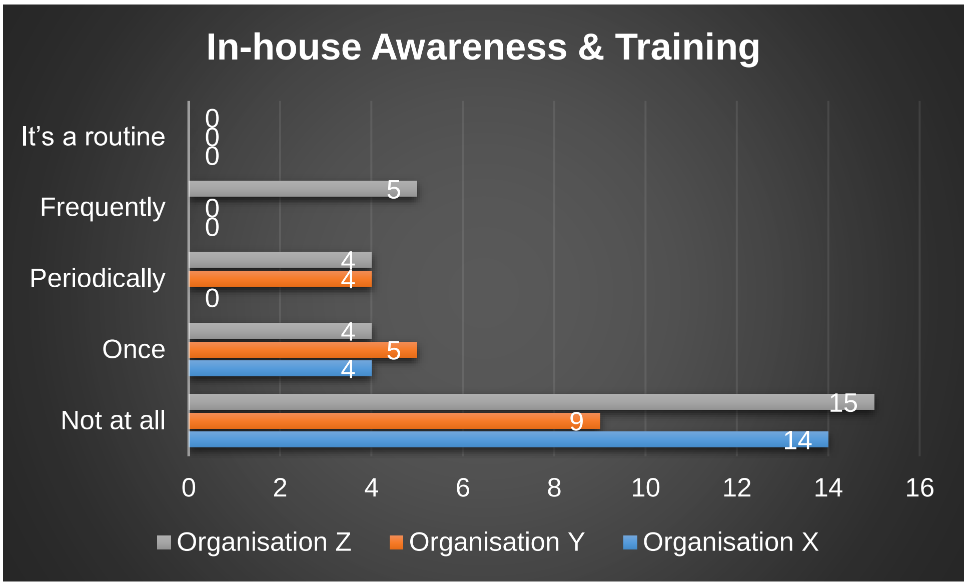


Figure 6.15: In-house employee computer awareness & training

Organisation X – Data collected on computer awareness and training shown in Figure 6.15 indicates that the majority of the respondents (78%) in Organisation X have never received training as opposed to 22% who have.

Organisation Y – Fifty per cent of the respondents in Organisation Y stated that they have never received training at all, 28% of them said they did but only once, and the remainder (22%) periodically did receive training.

Organisation Z – In this organisation, 54% of the respondents have never received training during their time at this organisation. Additionally, 14% of them said training was frequently received, those who indicated periodically represented 18%, and another group of 14% said that once only they received training.

- **Question 15.2.32 –** *On a scale of 1-5, what is your security awareness knowledge on the latest threat trends such as viruses, hacking, and spyware?*

End-user awareness to identify and detect suspicious latest security threat activities that are capable of breaching security when entertained on the system was the concentration of this question. Figure 6.16 depicts the outcome, and then an explanation follows after it.

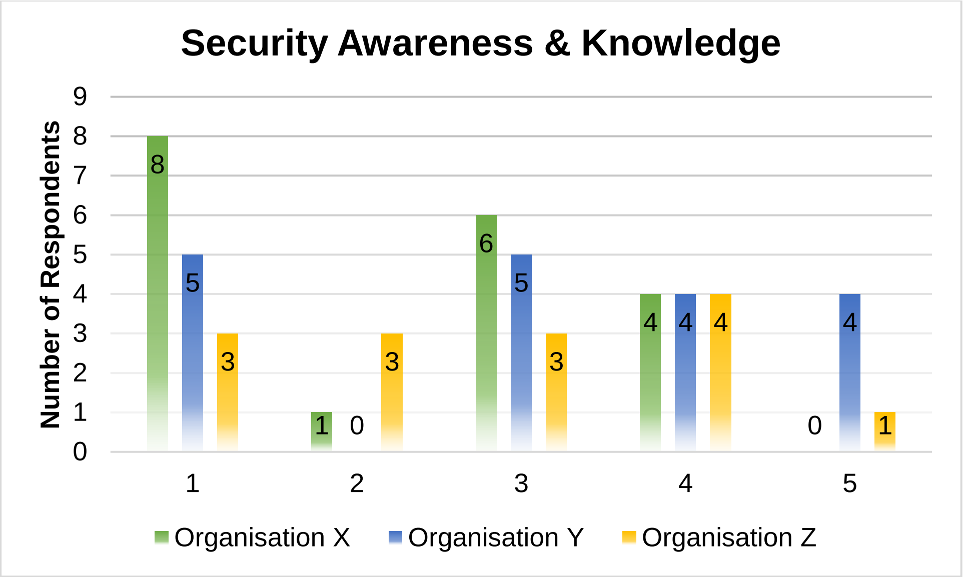


Figure 6.16: Security awareness knowledge

Organisation X – When reviewing statements according to Figure 6.16, many of the respondents (42%) in this organisation have very little knowledge and awareness of the latest threat trends. On the other hand, 32% of the respondents represented the second-largest response of those who indicated that they considered themselves average, 21% of them thought they were good, while 5% of them were of little knowledge and awareness as well.

Organisation Y – Twenty-eight per cent of the respondents indicated that they have very little knowledge and awareness on the latest threat trends. In contrast, another 28% claimed to be average. A split of 22% each of the respondents showed that they had good and very good awareness and knowledge of the latest threat spectrum.

Organisation Z – In this organisation, there was a 29% claim of having good awareness and knowledge of activities threatening systems. Quite the opposite to that, two second-best responses highlighted very little and little awareness and knowledge both at 21% each. Another 21% had average knowledge and awareness, with only 7% of the respondents confidently claiming they were good in knowledge and awareness of the risk space.

- **Question 5.1.20 –** *In your organisation, where can you find information regarding standard practice, access, and acceptable use when using the system?*

The purpose of this question was to understand end-user awareness with respect to the presence of a security policy or document meant to guide them on standard use, compliance, and acceptable use on the system. Statistically, in Figure 6.17, the outcome is presented and then explained.

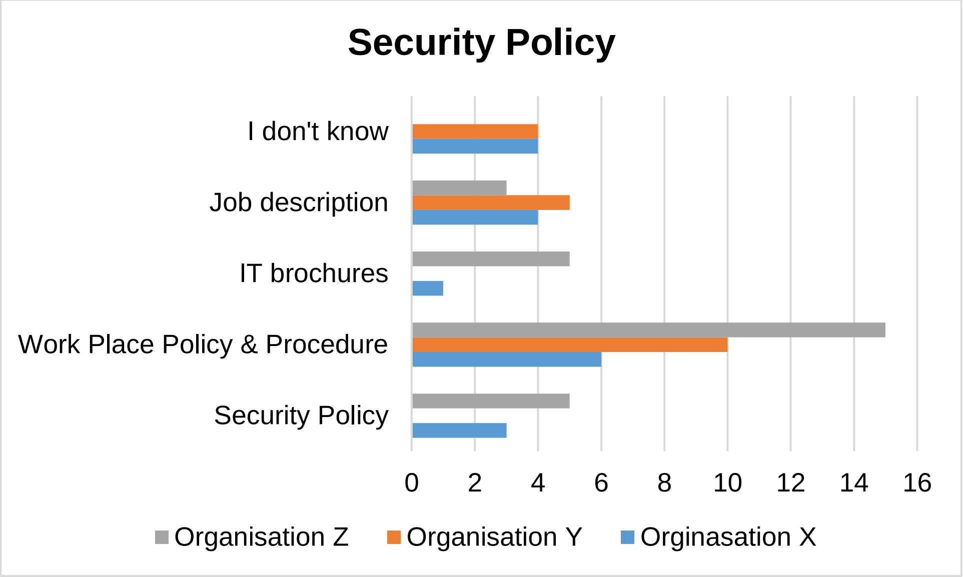


Figure 6.17: System use reference document by end-users

Organisation X – Figure 6.17 shows that only 17% of the respondents are aware of the presence of a security policy. Most of the respondents (33%) referred to workplace policies and rules for guidance, 22% did not know what to reference, another 22% pointed towards their job descriptions, and finally 6% spoke about brochures from IT department.

Organisation Y – At Organisation Y, 53% of the respondents acknowledge workplace rules and policies as security guidance, 26% of them mentioned their job description as guidance, and 21% of them do not know what to turn to.

Organisation Z – Fifty-four per cent of the respondents referred to workplace rules and policies, 18% to security policy, 18% to brochures from IT, and 11% to job description.

6.3.8. Standard Practice, Policy and Procedure-based Questions

Questions based on standard practice, policy, and procedure are dealt with in this subsection.

- **Question 5.2.23 –** *Do you understand the need for standard practice and acceptable use when interacting with the system?*

In a continuation of question 5.1.20 highlighted in Section 6.3.7, the idea behind this question was to see how end-users perceive the value of standard practice and acceptable use when using system resources. A graphical interpretation in Figure 6.18 reveals the result and thereafter the narration.

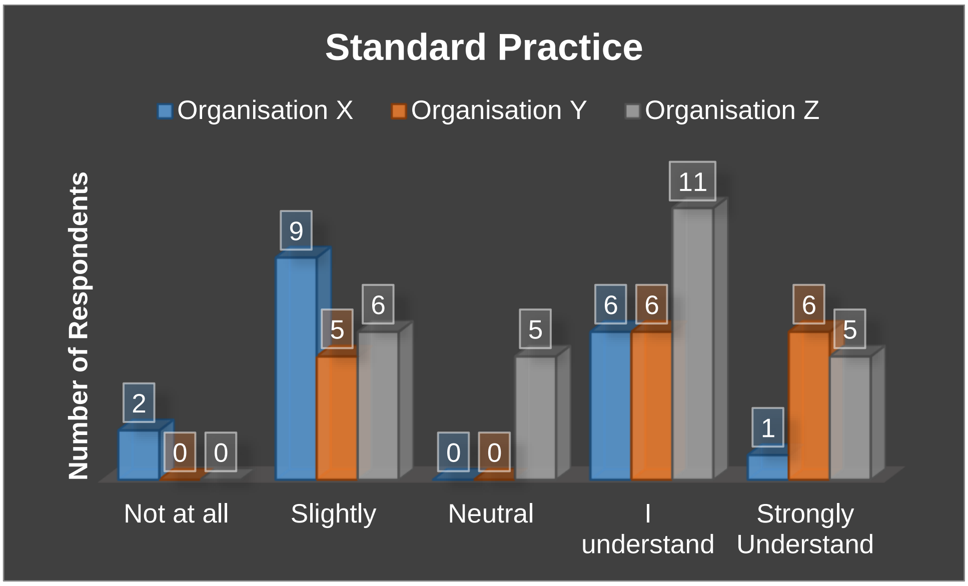


Figure 6.18: Standard practice

Organisation X – Most of the respondents (50%) understand slightly with a doubt the need for standard practice and use while using system resources, whereas 33% understands without a problem. On the contrary, 11% of the respondents state that they do not understand, and 6% of them strongly understand.

Organisation Y – This organisation exhibits more understanding of the need for standard practice by showcasing that 35% of the respondents understand, while an additional 35% of them strongly understand. Twenty-nine percent of the respondents were for the option they understood only slightly.

Organisation Z – From those in this organisation, 50% understand, 27% slightly understand, 23% are neutral, and 23% also understand strongly the need for standard practice.

- **Question 15.2.31 –** *For what purpose do you access your organisation's information system?*

The purpose of this question was to have a clear overview of the reason for needing access to the system by end-user participants. Further on, participants demonstrate the importance of understanding the need for access in the context of ISDD. Figure 6.19 quantitatively depicts the access reasons followed by discussions on the results obtained.

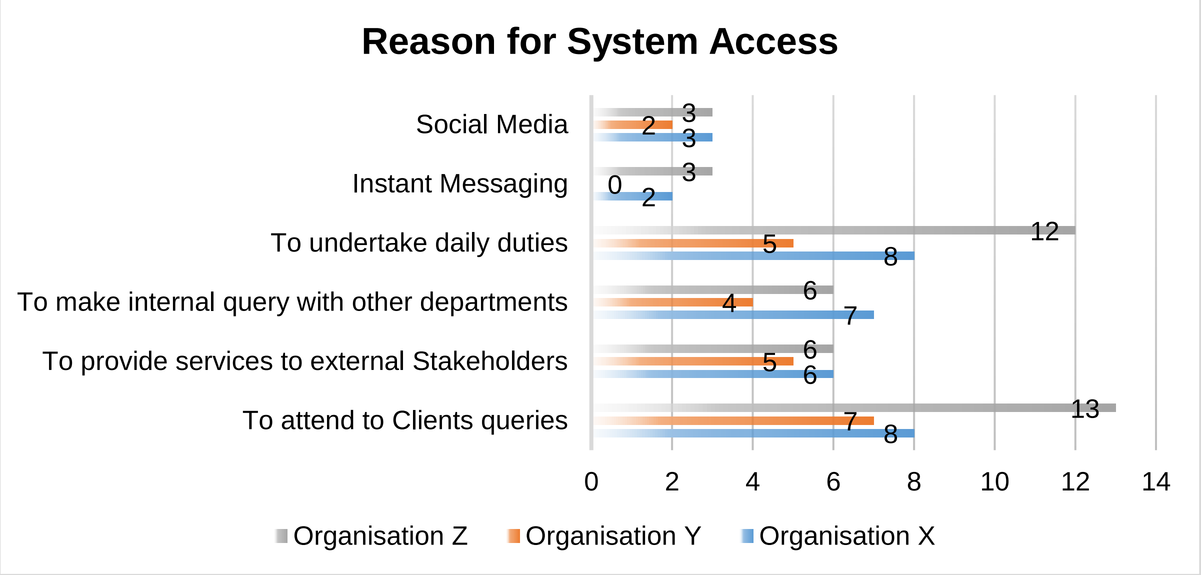


Figure 6.19: Reasons why end-users access system

Organisation X – Twenty-four per cent of respondent purely access the system for attending to clients queries, 18% to provide services to external stakeholders, 21% to make internal queries with other departments, 24% to undertake their daily duties, 6% for instant messaging, and 9% for social media.

Organisation Y – The majority of the respondents (30%) showed that they access the system for the purpose of attending to client queries, while 22% of them use it to provide services to external stakeholders. On the other hand, 17% of them use it to make queries within the organisation with other departments, another 22% to go on with their day-to-day duties, and finally 9% of the respondents use it for social media

Organisation Z – The majority of the respondents (30%), according to Figure 6.19, use the system for attending to clients queries, secondly (28%) to undertake their daily roles, while a split of 14% each to provide service to external stakeholders and make queries with other departments internally. A further split of 7% each represents instant messaging and social media.

6.4. ISDD Maturity Level Assessment

In the previous section, questions that directly relate to the measurement of ISDD according to the framework core indicators and metrics were discussed. Every question or statement was measured in relation to these metrics and a score allocated to determine how well an organisation complies with that particular benchmark. Questions were split into sections that would be combined in the end to indicate the overall rating to reflect compliance with the framework. In the next subsections, all case organisations will be rated.

Based on the foregoing analysis done and the interpretation made including qualitative data gathered from review of documents and observations, the rating sheet that follows will be used to gauge all three case organisations accordingly.

6.4.1. Information Flow – Ecosystem

From the literature explored in Chapters 2 and 3 earlier, as a security enhancement strategy which promotes high ISDD, segregation of information on the basis of business roles and functions is mandatory. This is reflected by CSF 1 in Table 3.2 in collaboration with associated metrics in Table 4.3. Furthermore, evidently it is mandatory to understand the flow of data, processes, and associated reporting structures as indicated by an organisational structure of every organisation. This emanates from Section 2.2.4 on the structure of an organisation and how that integrates into an information system. In this subsection, information flow compliance according to the design of the framework is what Table 6.1 is about. The rating scored per organisation is based on valid proof of data collected to measure the appropriateness of information flow in the effort to design a watertight ISDD structure. The measurement of information flow is constant all across organisations irrespective of the type of organisational structure. If an organisation complies with a critical success factor, a score of two is allocated, otherwise a zero.

Table 6.1: Appropriateness of information flow

Appropriateness of Information Flow			
Information flow accuracy, is it standard? Y= 2, N = 0	**OX**	**OY**	**OZ**
6.4.1.1. A proper organisational structure exists	N	Y	Y
6.4.1.2. Organisational structure clearly depicts reporting structures to make it easy to understand the work and data flow system-wise	N	Y	N
6.4.1.3. Roles and responsibilities of end-users are clear and precise according to the organisational structure to guide access control	N	N	N
6.4.1.4. Organisational structure conforms to the traditional design of data flowing upwards, downwards, or horizontal	N	Y	Y
6.4.1.5. All end-users know and understand their business roles and functions to enhance system security	N	N	N
Average Assessment …………………………………………………	0	6	4
Comments on priority areas of improvement …………………………………………………………………………………… ……………………………………………………………………………………			

Based on the evidence collected from the end-user survey, the information flow compliance metrics of every organisation were checked for compliance. The following were the scores per organisation: Organisation X = 0, Organisation Y = 6, and

Organisation Z = 4. In the subsection that follows, security management is screened against ISDD metrics compliance. Security Management

This subsection is based on a combination of CSF 1 in Table 2.2 and ISDD metrics discussed in Chapter 4 based on Table 4.3. The rationale is to use the table to measure general IT management and also adherence by end-users to procedures, standard practice, and compliance when using the system. The rating scored showcases whether security management by custodians of IT in organisations is upheld according to the design of the ISDD framework. The evaluation is based on the proof provided by data collected; for every metric, a score of either 2 for Yes or 0 for No is issued based on findings of evidence collected in the end-user survey. The metrics are then summed up to find the average score per organisation in Table 6.2.

Table 6.2: Security management

Standard Practice, Policies & Procedures Yes = 2, No = 0	**OX**	**OY**	**OZ**
6.4.2.1. A properly defined information security policy exists	Y	Y	Y
6.4.2.2. Security policy is written in low-level language for easy understanding of end-users	Y	Y	Y
6.4.2.3. End-users are compliant with security policy	N	Y	N
6.4.2.4. Security policy is updated to accommodate the changing risk landscape	N	N	N
6.4.2.5. End-users have signed a non-disclosure agreement each as a part of workplace rules	N	Y	N
Average rating ……………………………………………………………………	4	8	4
Comments and areas of priority ………………………………………………………………………………………………….. …………………………………………………………………………………………………			

In accordance with general security maintenance compliance conducted in Table 6.2 based on end-user data collected from the survey combined with review of documents, the following is how organisations fared: Organisation X = 4, Organisation Y = 8, and Organisation Z = 4.

6.4.3. Management Support

Caballero (2009), through CSF 2 in Table 2.2, states that security should not be looked at as an IT problem; it is a business problem. It is against that background that Table 6.3 reviews management support towards security in organisations. Based on review of documents and interviews with relevant participants applicable to this section in all three organisations such as IT officers, System administrators, Helpdesk and Technicians. The ratings in Table 6.3 indicate whether metrics listed are adhered to and to what extent.

Table 6.3: Management support

Management's commitment to IT Yes = 2, No = 0	**OX**	**OY**	**OZ**
6.4.3.1. Information Technology is acknowledged by management as a core function and important part of business strategy	N	Y	N
6.4.3.2. Management allocates sufficient budget to IT	N	Y	N
6.4.3.3. Management fully supports enforcement of security policies	N	Y	N
6.4.3.4. Management fully attends security-related awareness and training and encourages other end-users to do so	N	Y	N
6.4.3.5. Security is looked at as a business and not an IT problem alone by management	N	N	N
Average rating	0	8	0
Comments and areas of priority			

In this subsection, using set ISDD metrics, organisations were measured against management's involvement towards security. Organisation X scored 0, Organisation Y scored 8, and Organisation Z scored 0.

6.4.3.1. Security Types

Table 2.2 lists security types as a part of security architecture. This aspect is a critical success factor. ISDD metrics in Table 6.3 equally adopted that quality. In ISDD context, rating allocated to organisations in Table 6.4 indicate whether security types listed are present in organisations and how well they match industry standards.

Table 6.4: Security types

Indicate the security type by acknowledging whether they exist or *not (Yes = 1 for main question, 0.25 for sub-question, No = 0 for all)*	**OX**	**OY**	**OZ**
6.4.4.1. Antivirus software is present	Y	Y	Y
6.4.4.1.1. Antivirus software constantly has the latest updates	N	Y	Y
6.4.4.2. A firewall is present (Security centre)	Y	Y	Y
6.4.4.2.1. The firewall is regularly updated and policies tweaked to suit environment (latest patches and content filtering)	Y	Y	Y
6.4.4.3. Password authentication is enabled by default on the entire system	Y	Y	Y
6.4.4.3.1. Password authentication is strongly enforced and monitored against violation	Y	Y	Y
6.4.4.4. Encryption of data is enabled on the system by default	N	Y	N
6.4.4.4.1. All handheld and mobile devices have encryption software installed	N	Y	N
Average rating	8.5	10	8.75

Comments and areas of priority

……………………………………………………………………………………………….

……………………………………………………………………………………………….

In terms of security types in the context of ISDD, Organisation X scored 8.5, Organisation Y scored 10, and finally, Organisation Z scored 8.75.

6.4.4. Security Awareness and Training

To avoid making costly errors on a system, end-users must be trained (Broadie, 2008). ISO/IE 27001:2013 in CSF 3 (Table 2.2) also allude to that by stating that information security must be promoted effectively to employees. In this framework, in order for an organisation to have end-users that are well-equipped to operate the system effectively in a way that by-passes threats and risks, training and awareness are a top priority to uphold high ISDD attributes. To measure organisations on that aspect, scores in this subsection makes it possible to indicate whether this framework metric is observed and to what extent. For every metric in this table, a Yes carries a score of 2, while a No is equivalent to 0. An average score is issued by summing all metrics at the end.

Table 6.5: Security awareness and training

Mark the option with a Yes or No, where Yes = 2, No = 0	**OX**	**OY**	**OZ**
6.4.5.1. A self-assessment tool is available for screening of end-users at recruitment to weigh security risk to the system	N	N	N
6.4.5.2. All end-users are screened for computer skill set at recruitment	N	N	N
6.4.5.3. Management prioritises company-wide security awareness and training which is performed according to latest threats and risk trends	N	N	N
6.4.5.4. Prior to joining the organisation, all end-users received security awareness and training from credible institutions or, if not, were upskilled upon recruitment	N	N	N
6.4.5.5. All end-users range from minimum intermediate to advanced users	N	N	N

Average rating ………………………………………………………………….. 0 0 0

Comments and areas of priority

…………………………………………………………………………………………………..

………………………………………………………………………………………………….

Summing up the performance of organisations against the aforementioned metrics came to the conclusion: Organisation X = 0, Organisation Y = 0, and Organisation Z = 0.

6.4.5. Access Control Management

Access control is a major component of ISDD assessment. This is highlighted in CSFs 3, 4 and 9 of Table 3.2. In the context of this research, access control regulates who accesses information when and where in accordance with their business roles and functions. The scoring issued to organisations in this subsection indicates whether the organisation complies with the framework metrics and to what extent. In this part, every question has a sub-question. On the main question, a score of 1.5 represents a Yes, while 0 is a No. The sub-question carries the weight of 1 for a Yes, otherwise 0 for a No. A summary of the total is given at the end in Table 6.6.

Table 6.6: Access control management

Access compliance by End-users and General system customisation Main Question: Yes = 1.5, No = 0, Sub-question: Yes = 1, No = 0	**OX**	**OY**	**OZ**
6.4.6.1. Every employee has their own distinct password	N	Y	Y
6.4.6.1.1. Every end-users’ password meets minimum requirement, e.g. complexity, strength, history, and expiry date	Y	N	N
6.4.6.2. Physical access to system resources is strictly regulated by keys, biometrics, or access card	Y	Y	N

6.4.6.2.1. Physical access regulated according to business function and role	Y	Y	Y
6.4.6.3. All end-users have access cards or keys only usable when accessing their business function areas	Y	Y	N
6.4.6.3.1. Extra cards, keys, or biometrics solutions to offices is/are available on standby for end-users who forget or lose theirs	N	N	N
6.4.6.4. System by default enforces password minimum requirements, e.g. strength, complexity, expiry, and history	Y	Y	N
6.4.6.4.1. System locks out non-complaint end-users until IT support manually intervenes	N	Y	N
Average rating ………………………………………………………………	6.5	8.5	2.5
Comments and areas of priority …………………………………………………………………………………………….. ……………………………………………………………………………………………			

In Table 6.6, access control management was weighed in all case organisations as follows: Organisation X = 9, Organisation Y = 9, and Organisation Z = 4.5.

6.4.6. Culture of Protecting Information

The culture of protecting information is a critical success factor regarded highly on the list in an effort to enforce security as shown in Table 3.2. In this framework, the culture of safeguarding information is an attribute that requires consistency and correct attitude by all end-users and enforcement to complement other critical success factors necessary for striving towards high ISDD. In this subsection, the score indicates whether the organisation complies with the framework metrics and to what extent. A Yes carries a weight of 1, while No is equivalent to 0.

Table 6.7: Culture of protecting information

Security Culture Yes = 1, No = 0	**OX**	**OY**	**OZ**
6.4.7.1. End-users at all levels understand the consequences of their actions when working with the system	Y	Y	N
6.4.7.2. All end-users know the name of the antivirus in use	N	Y	N
6.4.7.3. All end-users are concerned about information sharing, privacy, and protection according to their work scope	Y	Y	Y
6.4.7.4. All end-users understand the value of compliance	N	N	N
6.4.7.5. Ethical conduct among all end-users towards organisational information resources is acceptable	N	N	Y
6.4.7.6. Strategies to enforce security culture are in place by the organisation	N	N	N
6.4.7.7. Overall, the ISDD culture is acceptable in the organisation at individual level	N	N	N
6.4.7.8. End-users are willing to support processes including change instituted by custodians of security to minimise risks and threats within the organisation	Y	Y	Y
6.4.7.9. Ethically, end-users are willing to take accountability for their activities when using the system	Y	Y	Y
6.4.7.10. The organisation takes action promptly on non-compliant end-users	N	N	Y
Average rating …………………………………………………………….………………	4	5	5

Comments and areas of priority

……………………………………………………………………………………………………..

……………………………………………………………………………………………………

According to Table 6.7, compliance to culture of security was weighed as follows: Organisation X = 4, Organisation Y = 5, and Organisation Z = 5.

6.4.7. General System Security Appropriateness

System appropriateness concerns the general ability of the system to minimise ISDD vulnerabilities. In this framework, this aspect measures automated attributes necessary for a system that stays alert to vulnerabilities and risks. Rating on this aspect is based on proof presented through questionnaires, review of documents, interviews with IT personnel, and observation. For every metric, a Yes represents a score of 1 and a No stands for 0. The summary will follow at the end including the combined rating of the subsection.

Table 6.8: Security appropriateness

System Capability Yes = 1, No = 0	**OX**	**OY**	**OZ**
6.4.8.1. Applications are upgraded regularly to minimise exploitation openings by threats and risks	N	Y	N
6.4.8.2. System access audit is enabled and easily identifies unauthorised access or failed attempts	N	N	N
6.4.8.3. System limits end-users according to their roles and responsibilities	N	N	N
6.4.8.4. Application availability is controlled according to relevance and needs of end-users	Y	Y	Y
6.4.8.5. All devices require authentication by default	Y	Y	Y
6.4.8.6. System regulates authentication according to business function	N	N	N
6.4.8.7. Security structure accommodates external end-users efficiently, e.g. suppliers, contractors, partners, customers, and consultants	N	Y	Y
6.4.8.8. System is upgradable both software and hardware-wise to suit new trends	N	Y	Y

6.4.8.9. Data in and out of the system is captured by default using a firewall	Y	Y	Y
6.4.8.10. After hours the system is automated to make selective end-user access according to business role and function needs	N	N	N
Average rating ………………………………………………………………………………	3	5	5
Comments and areas of priority …………………………………………………………………………………………………….. …………………………………………………………………………………………………….			

Based on Table 6.8, the organisations were scored as follows with regard to the appropriateness of the system: Organisation X = 3, Organisation Y = 5, and Organisation Z = 5.

6.4.8. Business Continuity Plan

CSF 8 in Table 2.2 elaborates on business continuity planning, which is highly regarded as a significant component of security. In this framework, it is a disaster recovery plan that enables the system to regain operations after a successful security breach. The rating in Table 6.9 is based on documents reviewed and interviews conducted with IT personnel at case organisations during the surveys to match the application of business continuity planning required according to the metrics of this framework. Every metric present signifies a score of 2 otherwise 0. The summary of the outcome is presented at the end.

Table 6.9: Business continuity plan

Ability of the system to recover after a failure Yes = 2, No = 0	**OX**	**OY**	**OZ**
6.4.9.1. A regular backup schedule is present	N	Y	Y
6.4.9.2. Backup restoration is performed frequently to test disaster recovery	N	N	N

6.4.9.3. There is an offsite backup which is at least 5-10 km away from the system for recovery during natural disaster, theft, organised crime or fire	N	N	Y
6.4.9.4. All mission-critical services, infrastructure, and data are part of the disaster recovery plan and can be restored in the shortest period to preserve system uptime	N	N	Y
6.4.9.5. Alternate communication channels for all stakeholders are kept intact for eventualities when there is a major system outage	N	N	N
Average rating …………………………………………………………………………	0	2	6
Comments and areas of priority …………………………………………………………………………………………….. ……………………………………………………………………………………………………			

Organisations in the business continuity plan category of the framework in Table 6.9 were evaluated as follows: Organisation X = 0, Organisation Y = 2, and Organisation Z = 6.

6.4.9. Performance Target

Performance target is a metric represented in Table 4.3. According to the ISDD framework, this factor monitors how processes that support ISDD continue to improve to ensure the system subscribes to the notion of prevention, detection, and recovery from threats including overall system effectiveness processes. Based on data collected through document review, interviews with IT personnel and observation, scores in this segment validate performance target and measures continuous improvement. A Yes stands for a score of 1, and a No is 0. An average score and summary will then follow at the end of the Table 6.10.

Table 6.10: Continuous improvement

Performance Target and Continuous Improvement Yes = 2, No = 0	**OX**	**OY**	**OZ**
6.4.10.1. Security policy is updated regularly to suit the ever-changing risk spectrum	**N**	**N**	**N**
6.4.10.2. Employees are screened annually for the level of security risk on latest threat trends and are upskilled where necessary	**N**	**N**	**N**
6.4.10.3. Organisational structure and ecosystem are continuously updated to ensure the system too is kept high ISDD-compliant at all times	**N**	**N**	**N**
6.4.10.4. Management continues to get involved by supporting enforcement of policies and strategises IT as a business core function allocating sufficient funds	**N**	**N**	**Y**
6.4.10.5. Culture of strong security understanding is kept sound among all stakeholders through regular awareness and training to keep them up to date with latest threat and risk trends	**N**	**N**	**N**
6.4.10.6. Organisation keeps track and record of security incidents and outbreaks and evaluates to measure improvement	**N**	**N**	**N**
6.4.10.7. Physical access control is regularly reviewed and observed flaws improved on	**N**	**N**	**Y**
6.4.10.8. Access control is continuously reviewed as end-users leave the organisation, move business roles and functions due to resignation, promotion, temporal recruitment, and many others	**N**	**N**	**N**
6.4.10.9. Risk assessment approach is reviewed and updated according to the environment and threat spectrum	**N**	**N**	**N**
6.4.10.10. Business continuity plan is reviewed quarterly and recommendations made and documented	**N**	**N**	**N**
Average rating …………………………………………………………………………..	0	0	4
Comments and areas of priority …………………………………………………………………………………………….. ……………………………………………………………………………………………..			

Based on evidence collected in Table 6.10, Organisation X scored 0, Organisation Y scored 0, and Organisation Z scored 4.

6.4.10. Derived Maturity Level Assessment of ISDD Case Organisation

Given the scores of organisations in Tables 6.4.1 to 6.4.10 in the preceding section against ISDD core indicators and metrics, Table 6.11 will present the summarised total scores per organisation to indicate their ISDD levels.

Table 6.11: ISDD metrics score

Overall rating		**Org X**	**Org Y**	**Org Z**
1	Information flow	0	4	4
2	Standard Practice, Policies & Procedures	4	8	4
3	Management Support	0	8	0
4	Security Types in Place	8.5	10	7.5
5	Security Awareness and Training	0	0	0
6	Access Control Management	6.5	8.5	4.5
7	Culture of Protecting Information	4	5	5
8	System Appropriateness	3	5	5
9	Business Continuity Plan (BCP)	0	2	6
10	Performance Target & Continuous Assessment	0	0	2
Combined rating		26	50.5	41.2

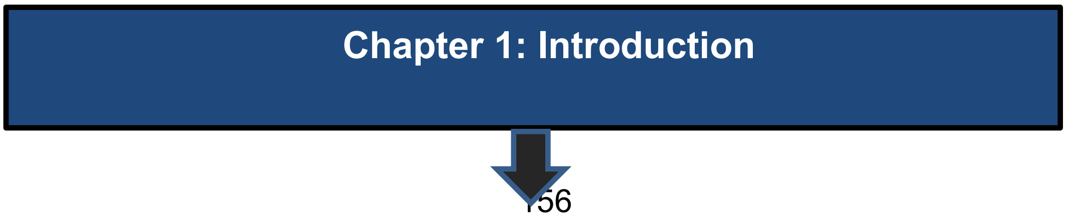
Table 6.12: Overall rating and ISDD compliance table

Assessment Rating	Star	ISDD Level	Description
0-20	*	Level 1	Non-compliance
21-40	**	Level 2	Initial Compliance
41-60	***	Level 3	Basic Compliance
61-80	****	Level 4	Acceptable Compliance
Above 80	*****	Level 5	Full Compliance

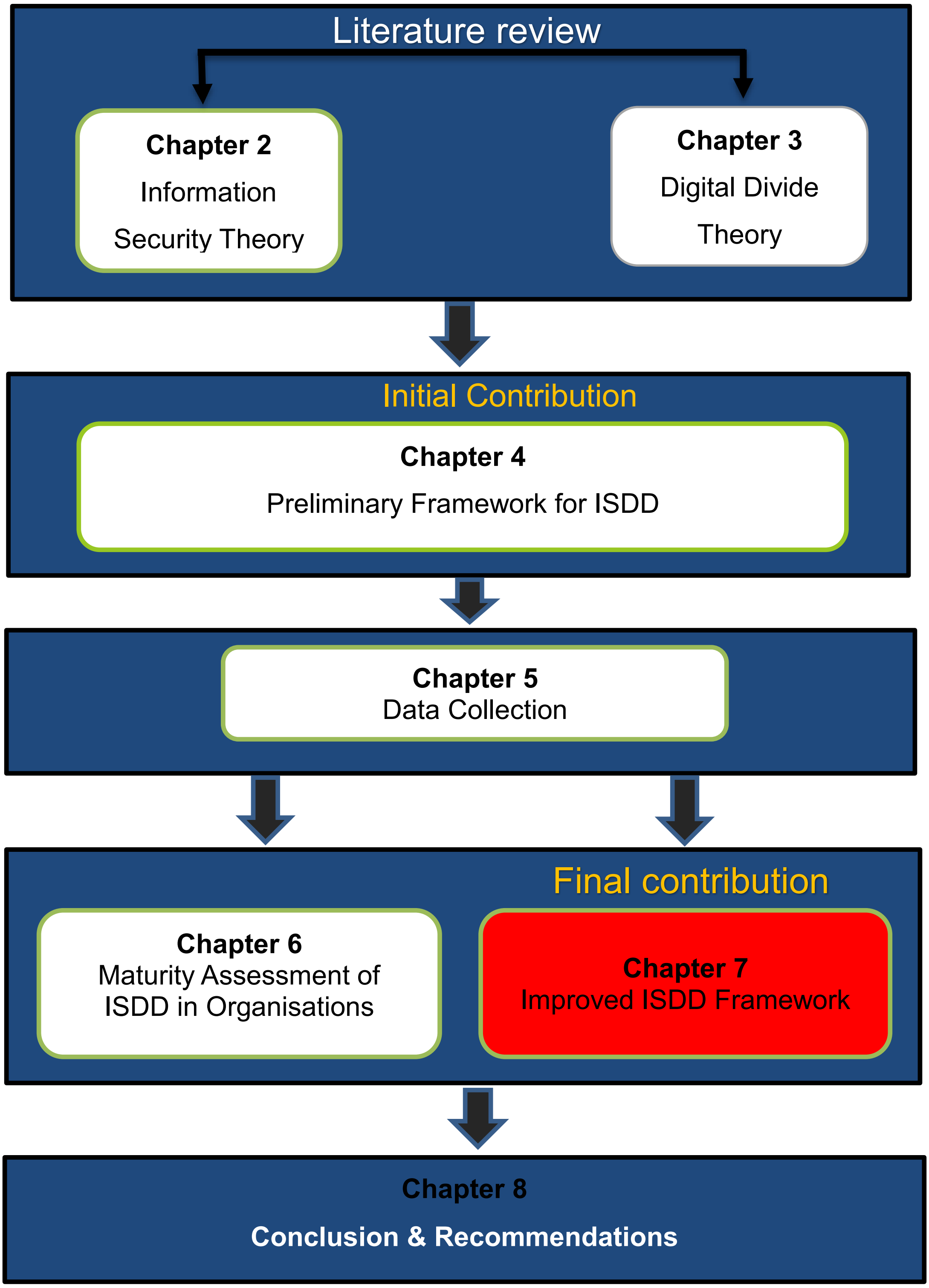
Going by the combined rating provided in Table 6.11, it can be concluded that Organisation X's ISDD stands at initial compliance (level 2), which marks basic entry stage to mature ISDD. The organisation is beginning to acknowledge the need for ISDD processes, but this need is not acted on. This is characterised by immature ISDD processes. The combined rating for Organisations Y and Z (50.5 and 41.2) puts both under basic ISDD compliance (level 3). This means these organisations have embraced ISDD critical success factors. An approach towards security processes has now started following a certain organised structure. Security is measurable, but not entire. Conclusion

In this chapter, the proposed framework was tried and tested in a real-world context by analysing the result of data gathered from end-users in participating case organisations. Results analysed revealed that the ISDD capability maturity level of organisation X is at 2 (initial compliance), meaning the organisation is ISDD immature; it needs improvement to upscale ISDD to a mature status. Further results also showed that Organisation Y and Z were rated at level 3 (basic compliance). This level translates into mature ISDD, but at entry level. This status acknowledges and implements CSFs, which is the beginning of ISDD maturity. The results obtained from this exercise demonstrated that the framework in this study can indeed be used in a real-life context to assess an organisation's ISDD maturity in order to measure continuous improvement. However, since the framework tested is still at its theoretical stage, expert validation is necessary. The next chapter is dedicated to the validation of the framework by experts with improvements thereof.

Chapter 7: Improved ISDD Framework



Chapter 1: Introduction



7.1. Introduction

In the foregoing chapter, the proposed framework was tested for applicability in a real-world context. Survey results on end-user data analysis performed on all organisations presented an opportunity to use the proposed framework to measure capability maturity in all organisations. Going into this penultimate chapter, the focal point is to analyse data collected from the ICT experts' survey, present the results, and use that to improve on the proposed framework in order to produce the final contribution of this study to the body of existing knowledge on ISDD. Most importantly, viewpoints on the proposed framework by ICT experts who were in some cases internal to case organisations and some that were not internal made the final proposed framework consensual and relevant to the field of information security.

Section 7.2 briefly outlines the data analysis approach of this study. Then Section 7.3 follows with a detailed analysis of collected data from expert participants. Section 7.4 provides a summary of the results, suggesting areas of improvement of the proposed framework. The improved version of proposed framework is presented in Section 7.5. Section 7.6 concluded the chapter.

7.2. Data Analysis

Data analysis in this section is a continuation of the first survey where system end-users were incorporated. The second survey incorporates viewpoints on the quality of framework by ICT experts.

The methodology used for data analysis was discussed in the previous chapter in which both qualitative and quantitative approaches were explored, and it was emphasised that data triangulation was used whereby various data sources of information were used in order to increase the validity of the study. The outcome of a survey administered to ICT experts so as to qualitatively and quantitatively provide insights aimed at improving this study's framework will be discussed. The outcome of the various analyses in this study will also be presented.

7.3. Questionnaire Responses by ICT experts

This section presents the analysis of the responses from ICT experts which focuses on the assessment of the quality of the preliminary framework. The intention is to be able to grasp a range of insights aimed at improving aspects of the proposed framework so as to come up with a vetted and improved version. Original question numbers as they appear in Appendix C are retained herein.

7.3.1. Response Rate and Demography

A total of 35 ICT experts were reached in this survey. Out of the 35 targeted respondents, only 25 took part in the survey, representing a return rate of 71% as depicted in Figure 7.1.

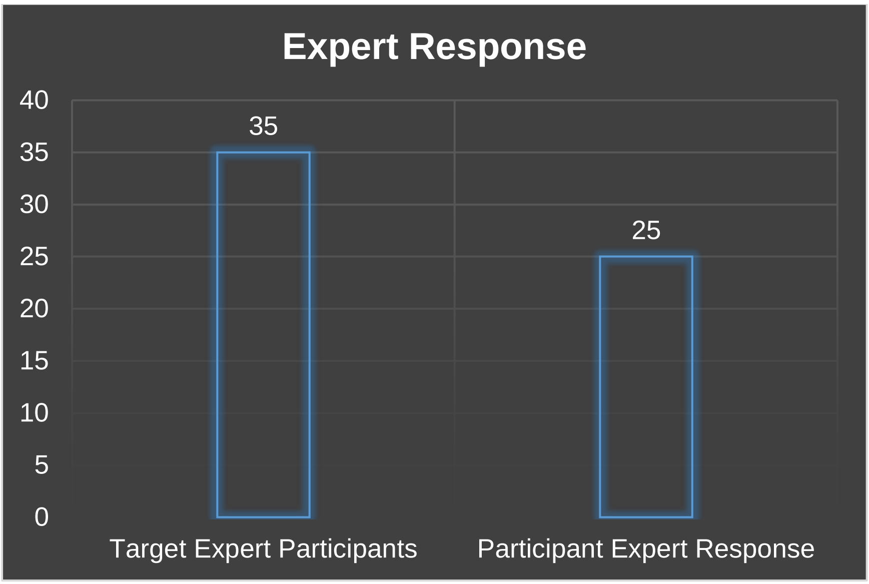


Figure 7.1: Expert participant response

According to Figure 7.1, a total of 35 ICT experts were reached in survey 2. Of the 35 ICT experts, only 25 responded and took part in the survey, representing a response of 71%.

- **Question 5.1.2 –** *Years of experience of security expert respondents*

The purpose of this question is to try to understand the years of experience in the field of security by experts that took part in the survey. It makes it possible to hear viewpoints on ISDD based on experience. Figure 7.2 presents the quantitative outcome and discusses the findings.

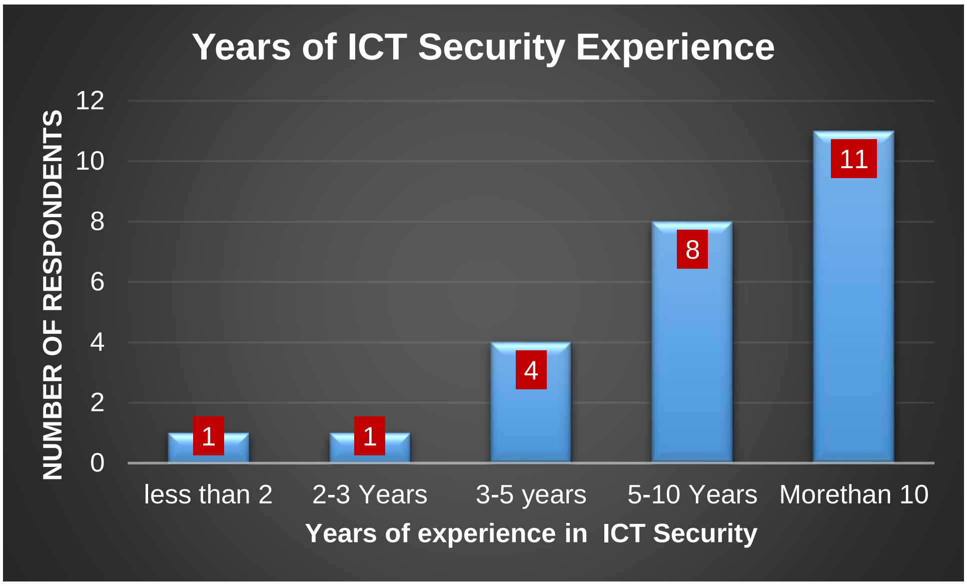


Figure 7.2: ICT years of security experience of the respondents

Based on Figure 7.2, the majority of ICT expert participants had more than 5 years of experience, whereby 32% had between 5 and 10 years, and 44% had more than 10 years. A small number had less than 5 years of experience including 16% of the ICT experts who had between 3 and 5 years, as well as those with 4% each, representing 2-3 and less than 2 years' experience respectively.

- **Question 5.1.3 –** *The occupations of information ICT experts who participated in the survey*

The rationale behind this question was to evaluate the areas of security represented by expert respondents, and then relate it to the context of this study with the purpose of improving the framework. Figure 7.3 is the quantitative depiction of respondents' occupation and the accompanying discussion.

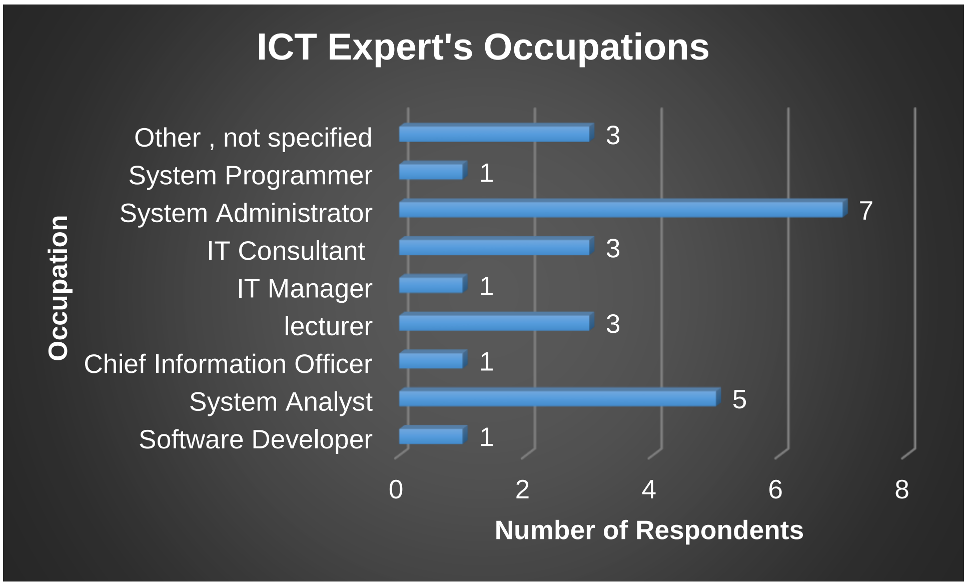


Figure 7.3: Respondents by occupation

As depicted in Figure 7.3, from the majority of ICT experts surveyed, five were systems analysts, seven systems administrators, and three IT consultants. The rest were as follows: one CIO, one system programmer, one IT manager, one software developer, and finally, from the academic sector, three lecturers. It was deemed relevant to include respondents from the academic sector in the sense that their theoretical contribution to the enhancement of the framework is equally relevant.

7.3.2. Importance of Information Security to Operations of an Organisation

This section articulates on the opinions of ICT experts about the value of information security to the operations of an organisation.

- **Question 5.1.4 –** *Viewpoint by ICT experts on how critical information security is to business operations*

This question was set up to paint a picture on the value of security to business operations while at the same time highlighting how that is enhanced by connecting to ISDD. Figure 7.4 illustrates the outcome and discussion thereafter.

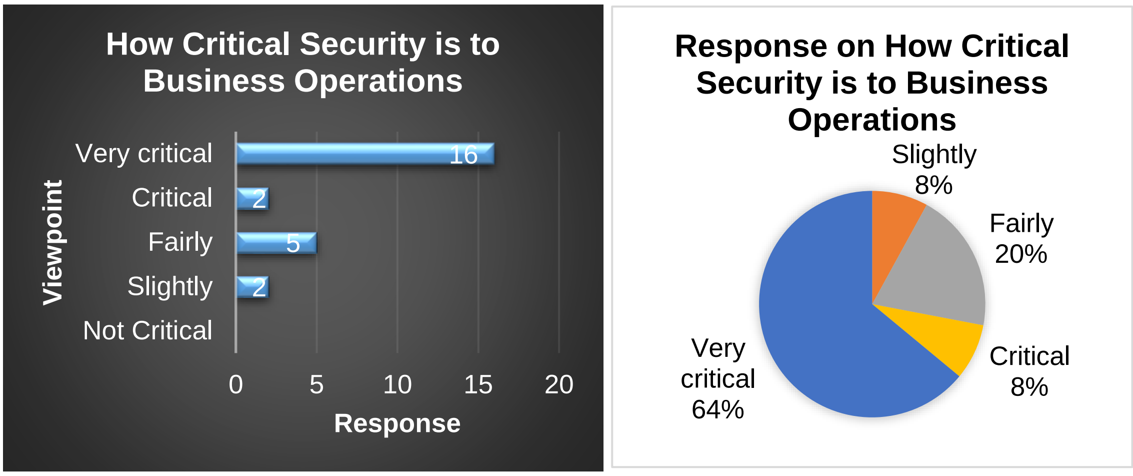


Figure 7.4: ICT experts' viewpoints on the value of security to business operations

Based on the responses to the question posed, Figure 7.4 show that the majority of the ICT experts (64%) acknowledged that security was very vital, 8% felt it was critical, 20% felt it was fairly vital and the rest of the ITC experts (8%) were of the opinion that it was slightly vital.

- **Question 5.1.5 –** *The view of ICT experts on the use of security models such as COBIT or ISO/IE 27001 in organisations*

The idea behind this question was to hear from ICT experts on the applicability and usefulness of security frameworks such as ISDD to businesses. Figure 7.5 portrays the quantitative response, followed by the summary.

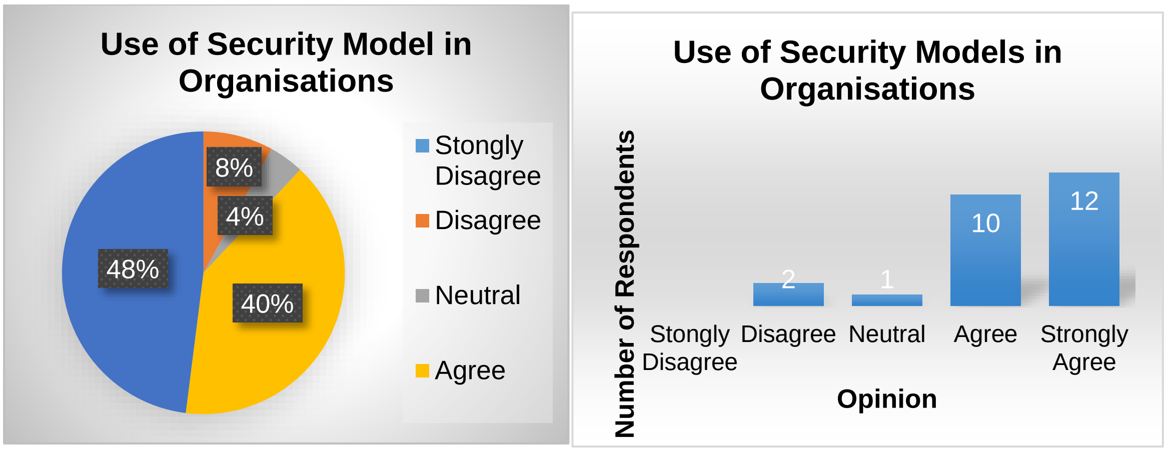


Figure 7.5: Expert opinions on use of security models

Of the 25 ICT experts who participated in the survey, Figure 7.5 reveals that twelve endorsed strongly the use of security models, which stands for 48%; ten respondents also agreed, which represents 40%; and one respondent (4%) was neutral, and two (8%) disagreed.

- **Question 5.1.6 –** *Highlights the most influential factors when managing information security*

The focus in this question was factors which must be considered first and should be acted upon when addressing security enhancement activities which are favourable towards preserving high ISDD status in an organisation. Figure 7.4 is a graphical interpretation of this and is accompanied by a summary of this interpretation.

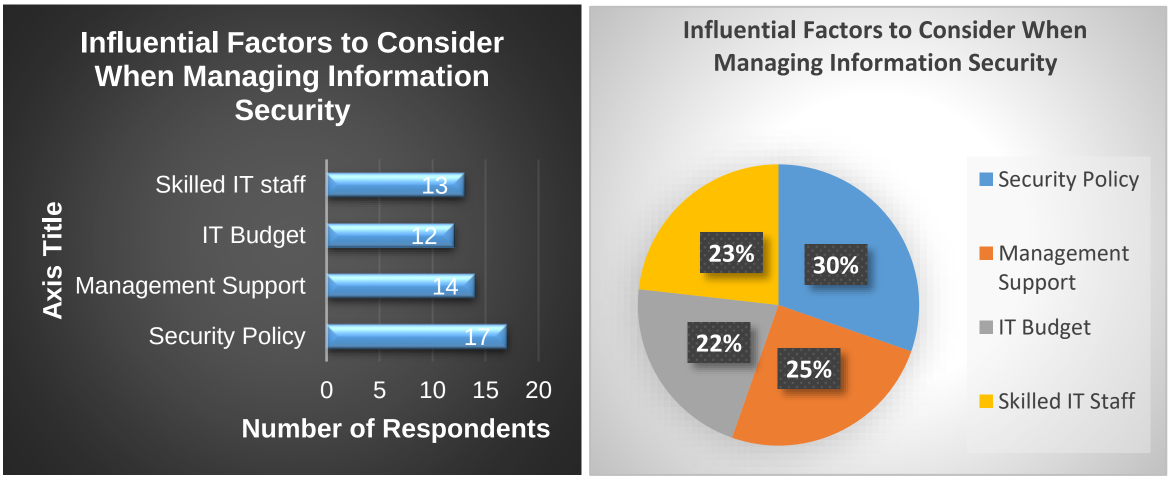


Figure 7.5: Common denominators in security management

Based on Figure 7.5, experts considered a security policy as the first line of defence and the most important factor in security management (30%). This was followed by management support (25%), while a skilled IT department and IT budget were rated 23% and 22%.

7.3.3. Access Control Management

This part of data collected and interpreted now integrates information security into the core and context of this research, namely, information security digital divide. Access control management through the system determines who has access to which information resources based on their business functions, roles, and responsibilities.

- **Question 5.1.7 –** *The importance of understanding the flow of information in access control management to information resources*

The purpose of this question was, through expert viewpoints, to highlight the value of understanding the flow of information when designing access control by end-users according to their business roles and functions which are held high on the ISDD list of CSF. Figure 7.6 presents the results, and a summary follows thereafter.

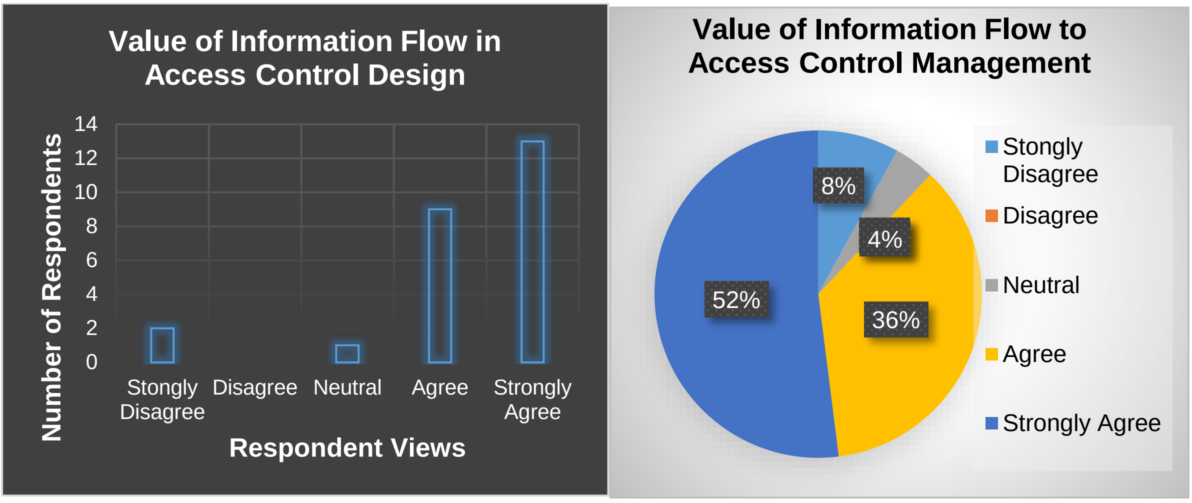


Figure 7.6: The role of information flow in planning access control management

Question 5.1.7 targeted how understanding the flow of information through reporting structures within an organisation was important to the designing of access control management in Figure 7.6. Responses provided show that 52% of ICT experts strongly agreed with the notion that information flow is a critical component of access control management, 36% additionally backed that by merely agreeing, and 8% strongly disagree, while 4% was neutral.

- **Question 5.1.9 –** *The structure of the organisation needs to be a strong point of consideration when assigning access credentials to end-users*

The aim of this question was to relate the organisational structure to end-user access control design. Expert response would illustrate that, as shown in Figure 7.7, and a discussion would then summarise the outcome.

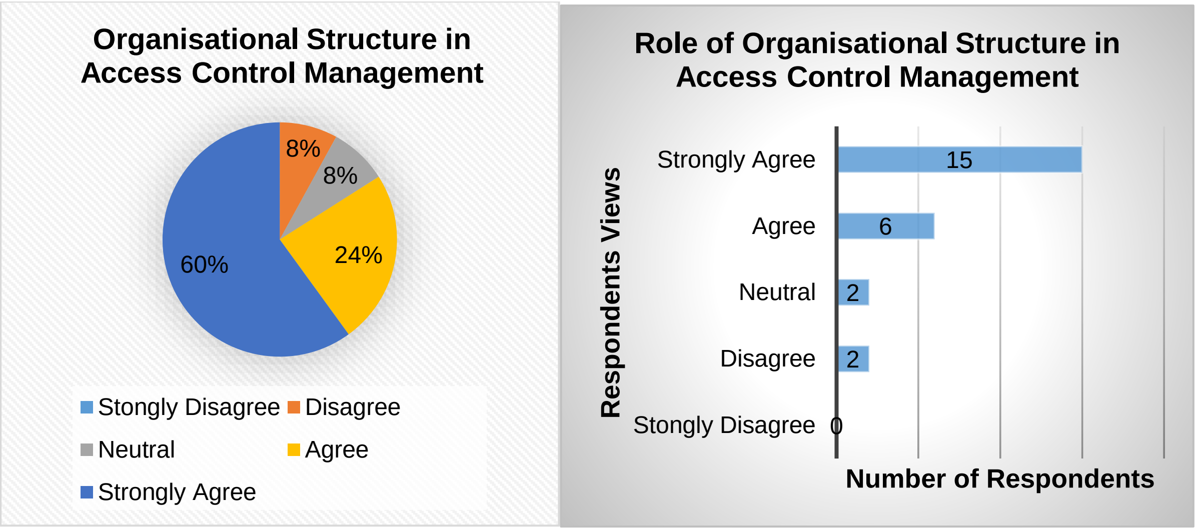


Figure 7.7: The role of the organisational structure in access control management

The biggest opinion (60%) on this question went towards a strong agreement that it was mandatory to have the organisational structure referenced during access control design. Figure 7.7 goes on to show that a further (24%) favoured the option, but 8% of the ICT experts reiterated that they were neutral, while another 8% represented ICT experts who disagreed.

- **Question 5.1.10 –** *The degree of accessing information by an individual in an organisation should depend on the complexity of their role and its complexity*

The objective of this question was to assess from the expert opinion on whether an end-user's job complexity should be a factor when determining access management. Figure 7.8 showcases the quantitative depiction, and then the summary sums it up.

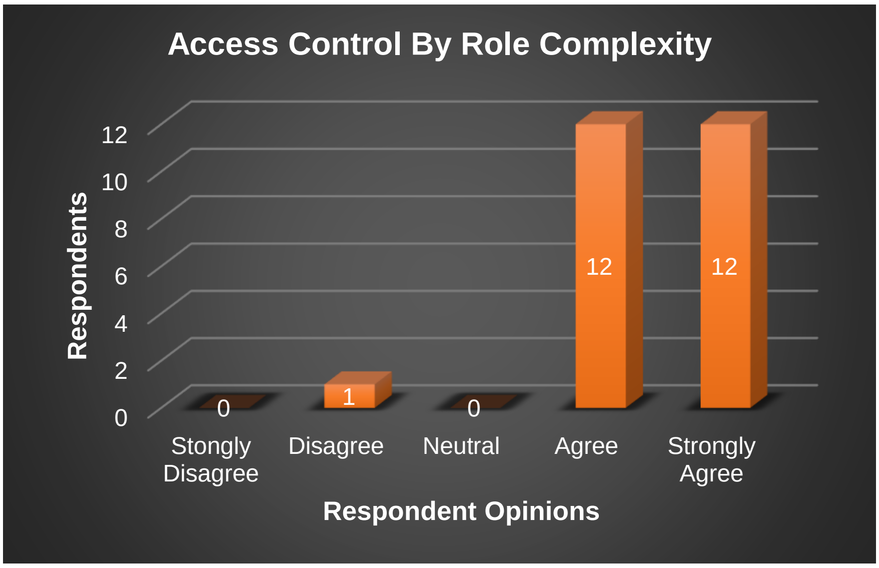


Figure 7.8: Access control by business role complexity

Forty eight per cent of the respondents favoured the idea strongly. A further 48% also agreed and only 4% disagreed, as highlighted in Figure 7.8.

- **Question 5.1.11 –** *For external stakeholders who need services from the back-end office through various access channels available, what do you think is the best authentication method to be followed?*

In this question, the most appropriate authentication option for external end-users and stakeholders when accessing the system was the target to understand what ICT experts would recommend creating a high ISDD. The outcome is revealed in Figure 7.9 and summarised thereafter.

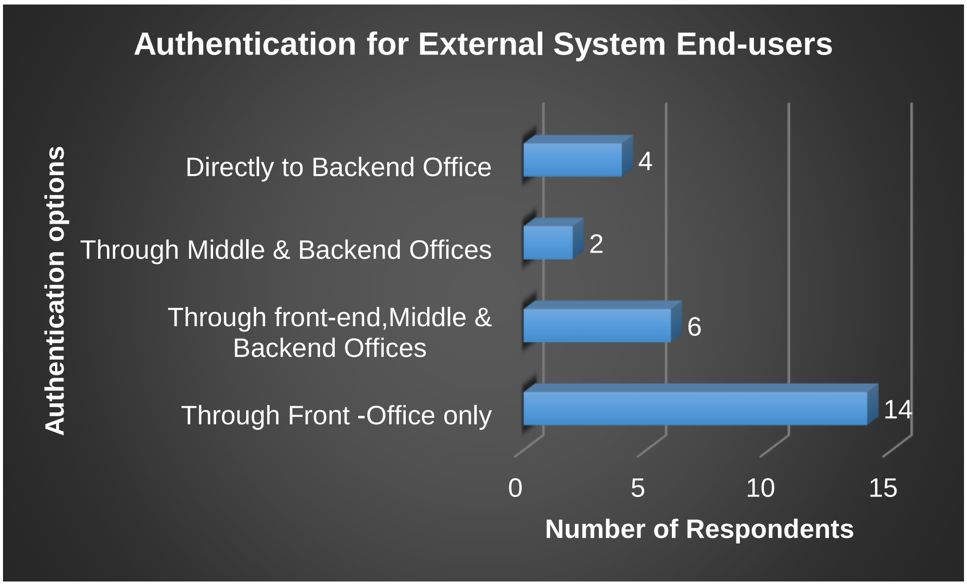


Figure 7.9: Authentication for external users to back office

As Figure 7.9 shows, the majority of the ICT experts (54%) viewed authentication through the front office only as the best method for external end-users because they felt anything more would prolong response time and productivity of end-users. Further on, authentication through all three offices, namely, front, middle and back end was second at 23%. Bypassing the front-end and middle offices straight to the back was opted as the third best option (15%), with middle to back-end offices being the least option (8%).

- **Question 5.1.17 –** *Which factors are the most applicable when information access matrix is planned in an organisation?*

In this question, the aim was to observe what ICT experts would cite as a particular order of factors that must be observed as top priority when deciding the access control matrix in order to create a high digital divide. Graphically, that is illustrated by Figure 7.10. A further explanation of the findings to that effect is also included.

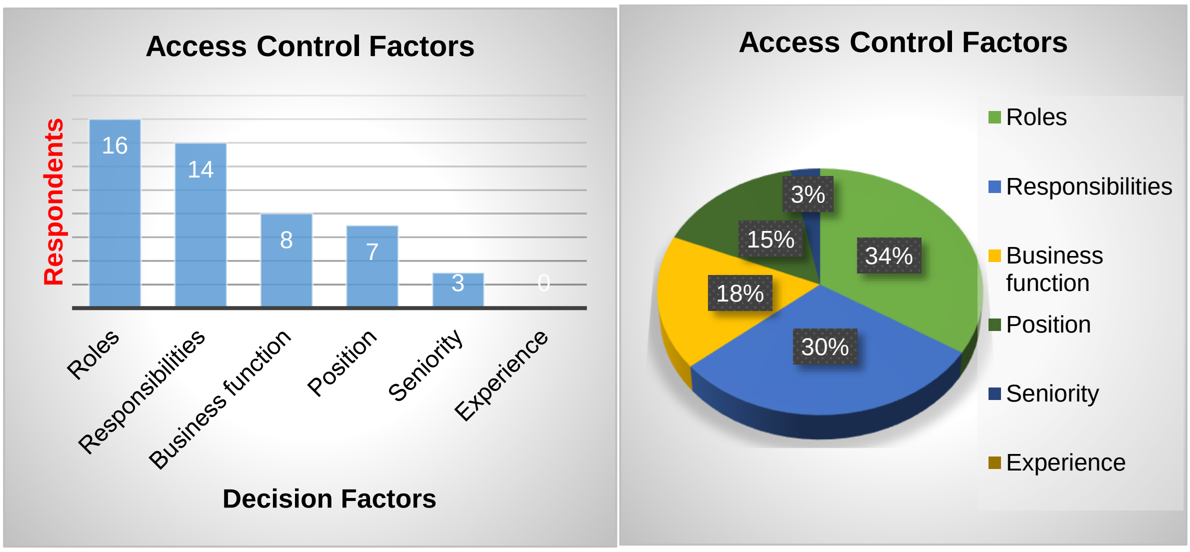


Figure 7.10: Factors that influence access control during planning

According to Figure 7.10, respondents' views indicated that business roles standout at 34%. Next, business responsibilities of an end-user are at 30%. 18% represented business functions, with the last 15% advocating for seniority.

- **Question 5.1.18 –** *Is access control management to information systems generally significant to business operations in your industry?*

The purpose of this question was to bring forth the significance of ISDD management in business operations in accordance with ICT experts' industry of representation. Figure 7.11 represents the opinions of the ICT experts and is then followed by a summary.

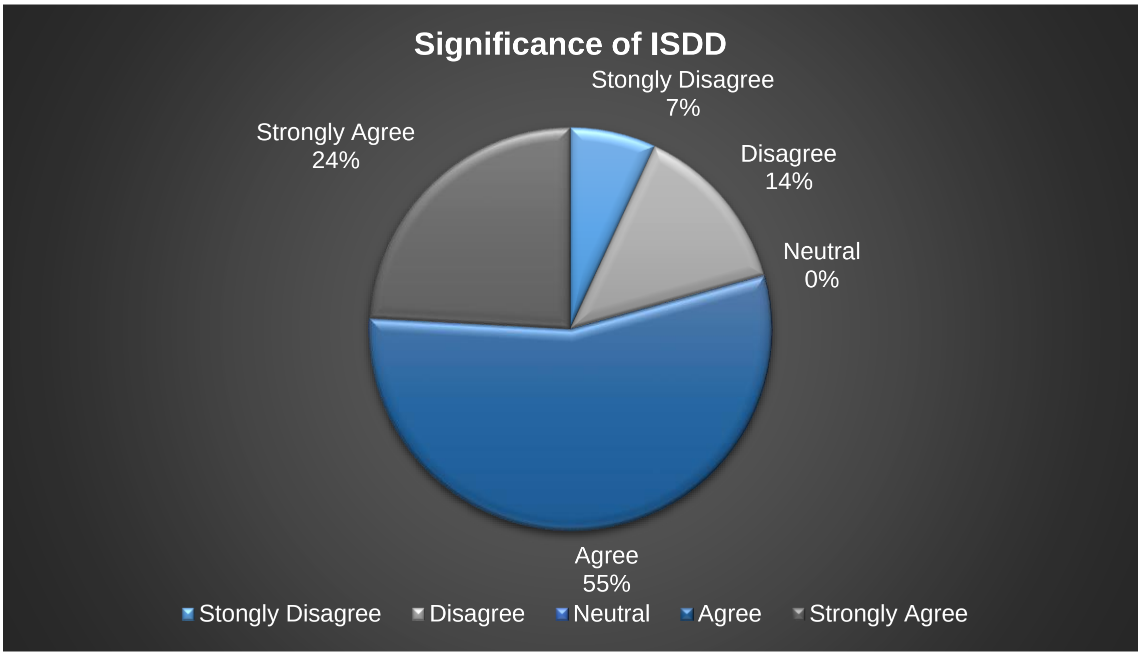


Figure 7.11: Significance of ISDD

According to ICT experts' opinions in Figure 7.11, 55% of them agree that it is very significant to security, and 24% strongly agree to significance. On the contrary, some ICT experts indicated that they disagree with the notion of dividing end-users according to roles and responsibilities, and that business function is important to business operations. This group of respondents represented 14%. A further strong disagreement represented 7%.

- **Question 5.1.19 –** *Access channels recommended for external system end-users*

This question was aimed at finding out what ICT experts' thought were the most appropriete access channels for external end-users. Figure 7.12 is a portrayal of the response, and after that, a summary follows.

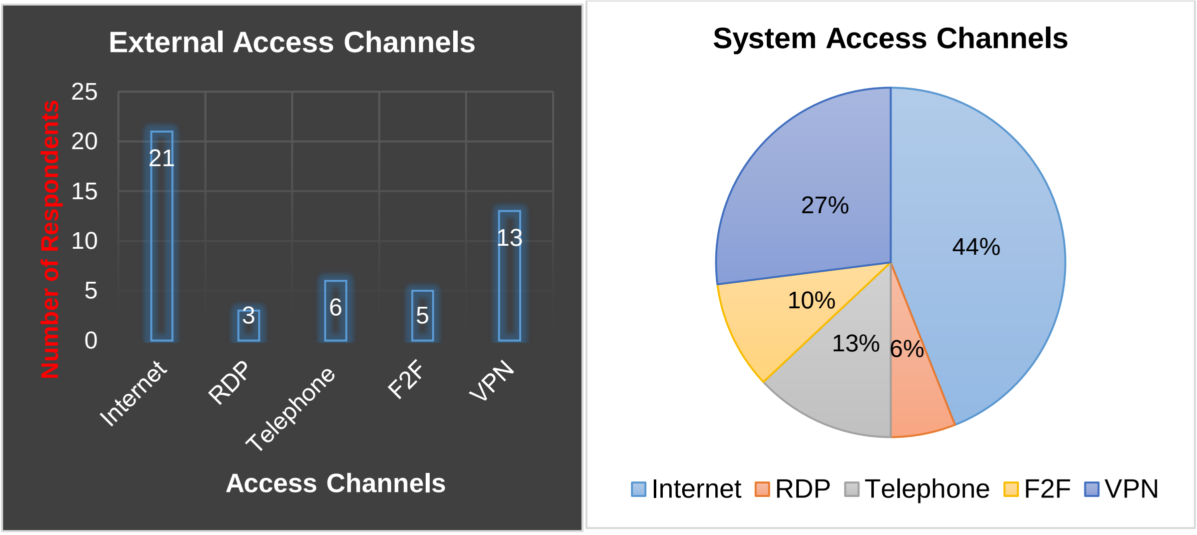


Figure 7.12: Access channels most applicable for external system end-users

As indicated in Figure 7.12, the most favoured external access channel according to ICT experts was internet (44%), while 27% chose VPN. Further, 13% endorsed the traditional telephone, 10% face-to-face (F2F), and the least (6%) recognised Remote Desktop Protocol (RDP).

- **Question 5.1.21 –** *Which one of the listed options is the most appropriate to access the system internally by end-users?*

Observing how ICT experts preferred accessibility options that offered the highest possible ISDD enforcement on internal end-users when they intend to access the system internally was the idea behind this question. In Figure 7.13, the outcome is shown quantitatively, and then a summary of the results is given.

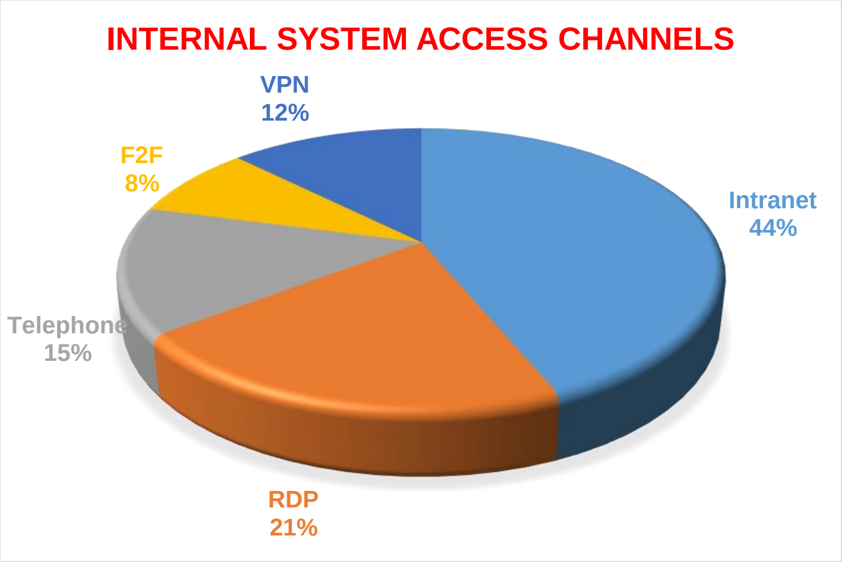


Figure 7.13: Access channels most applicable for internal system users

According to Figure 7.13, the intranet was the most favourite access channel at 44%. This was followed by RDP at 21%, telephone at 15%, VPN 12%, and finally, F2F received the least at 8%.

7.3.4. Security Policy

For an organisation to have an information system that by default ensures high digital divide among its business roles, it is mandatory to have a security policy that governs standard practice and compliance. A security policy is the starting point of any security programme, but for it to be relevant, it needs enforcement by the organisation. The next question engages ICT experts on items around policies, standard practice, and compliance.

- **Question 5.1.20 –** *An organisation must have a clearly defined access control mechanism to its systems. Based on this statement, which of the following must be enforced to ensure a highly secure system?*

The purpose of this question was to understand the preferred order of ISDD factors that a security policy must highlight according to ICT experts. Figure 7.14 presents the graphical depiction of the outcome, supported by a summary after that.

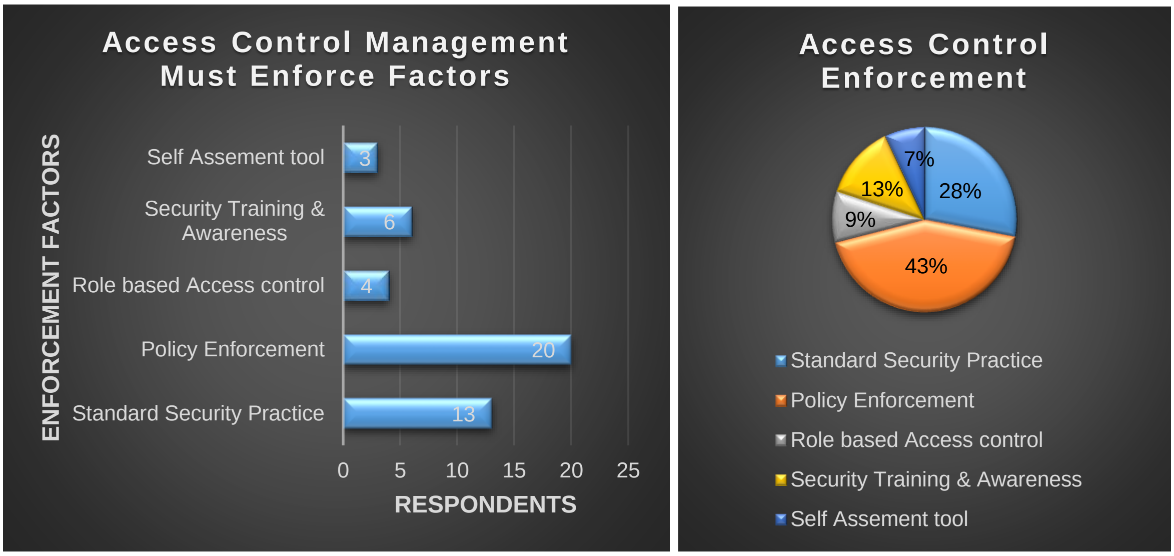


Figure 7.14: Factors that must be enforced to promote a highly secure system

From Figure 7.14, it is clear that security policy was the most prominent factor (43%) that must be enforced to promote a highly secure system, with standard security practice by end-users being the second most prominent (28%). Furthermore, security training and awareness ranked third (13%), while role-based access control (9%) and the use of a self-assessment tool to screen for computer and security skill sets (7%) were the least two factors.

7.3.5. Enterprise Structure

In this subsection, from a system benefit viewpoint, multiple opinions from ICT experts on the structure an organisation should take on including how the business roles and functions should be set up to facilitate a proper management of access control was the main aim.

- **Question 5.1.24 –** *For a standard enterprise, which business functions are mandatory between front-end office, middle office, and back-end office?*

This question was aimed at helping to consider the most common business function structure across organisations represented by ICT experts, hence generalising that to the framework. The choice of office setup makes it possible to improve the framework by understanding how the flow of information should be set up. Graphically, the illustration in Figure 7.15 presents results that are accompanied by a summary.

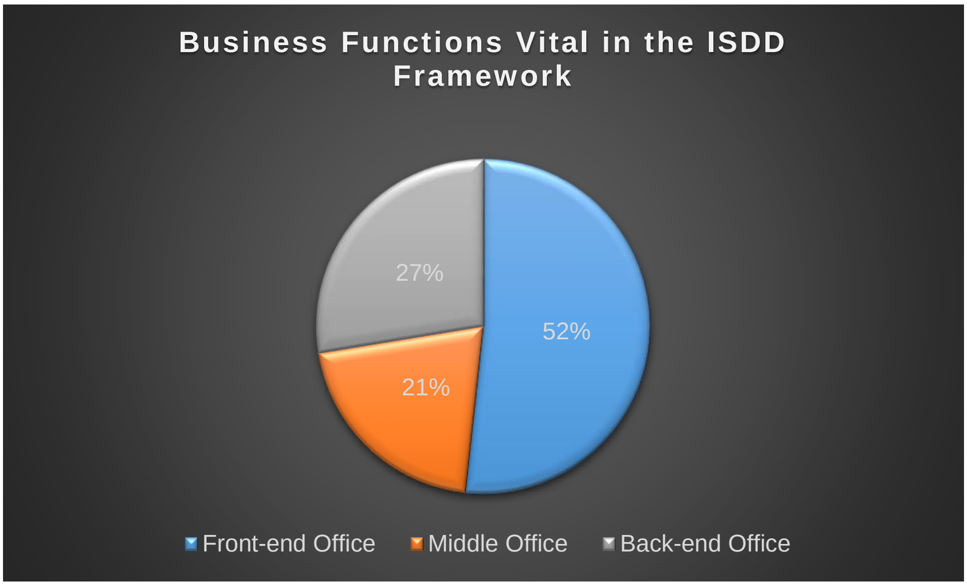


Figure 7.15: Business functions in an organisation

It can be observed from Figure 7.15 that 52% of the ICT experts endorsed front office as a must-have. Further, 27% proposed that an enterprise must have a middle office to support both front- and back-end offices. Finally, 21% of the ICT experts were in support of always having a back-end office to back the front and middle offices.

- **Question 5.1.25 –** *Suggest business roles which must be considered when planning the ISDD framework*

This question was for the purpose of getting an indication from ICT experts concerning which business roles must be made part of the framework and in which order of preference, if any, when planning a comprehensive access control management design.

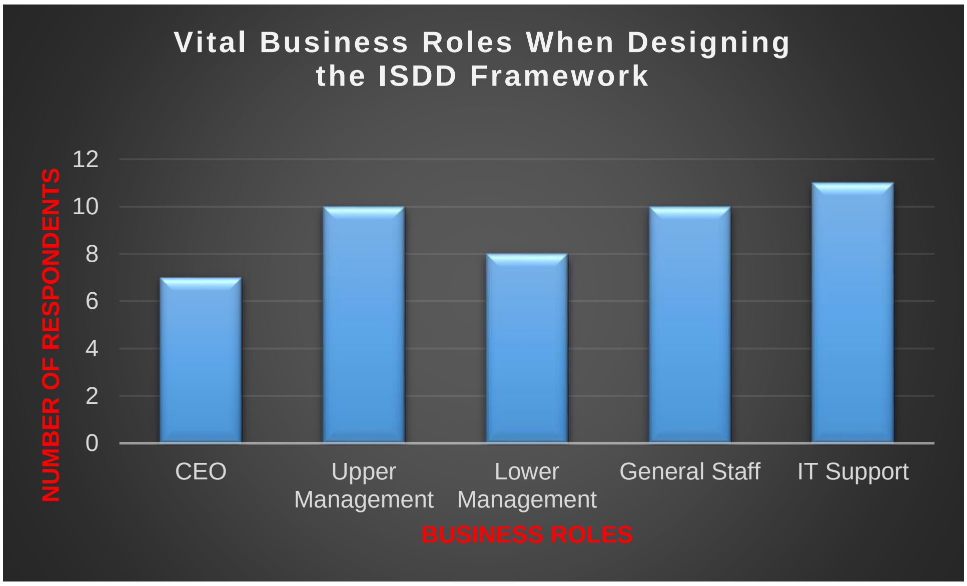


Figure 7.16: Vital business roles when designing ISDD

ICT experts listed the IT department as a top priority when designing ISDD according to business roles. This was followed by both upper management and general staff, with lower management together with CEO being of least priority.

- **Question 5.27 –** *Suggest the most commonly used front-end applications from the list*

The question was designed to entice ICT experts to state according to the sector they represented, the most common front-end applications and how they are protected and availed according to business roles. Figure 7.17 graphically depicts that, and the summary follows.

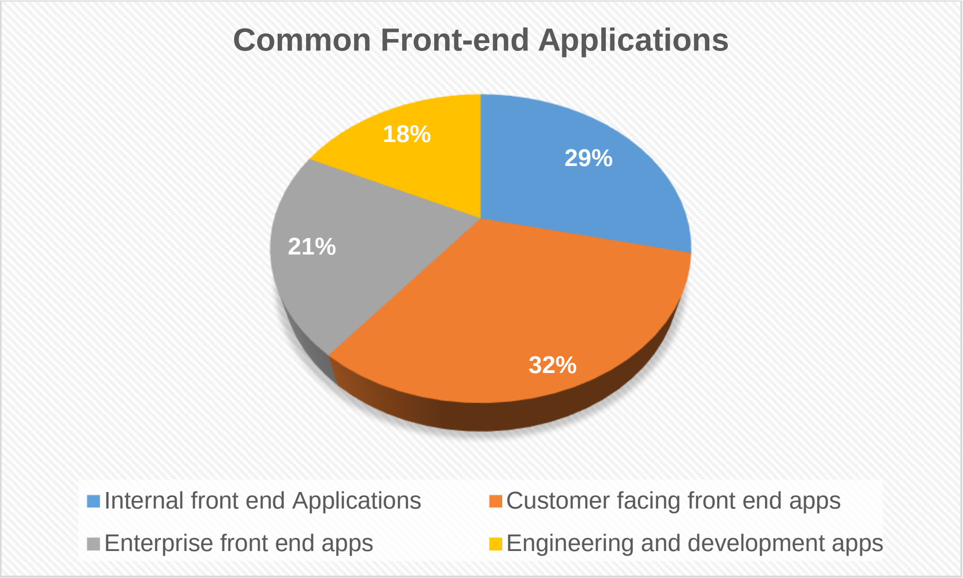


Figure 7.17: Common front-end applications

According to their sectors of representation, ICT experts thought the most common front-end application is customer facing front-end application (32%). Figure 7.17 shows that this was followed by internal front-end applications (29%), enterprise front-end applications (21%), and finally, engineering and development applications

- **Question 5.1.28 –** *In an enterprise, which one is the most common software that can also be consumed as a service*?

To better improve on the framework from a back-end application perspective, ICT experts were requested to identify the most consumed software as a service. A quantitative depiction in Figure 7.18 reveals the outcome, and this is followed by a summary.

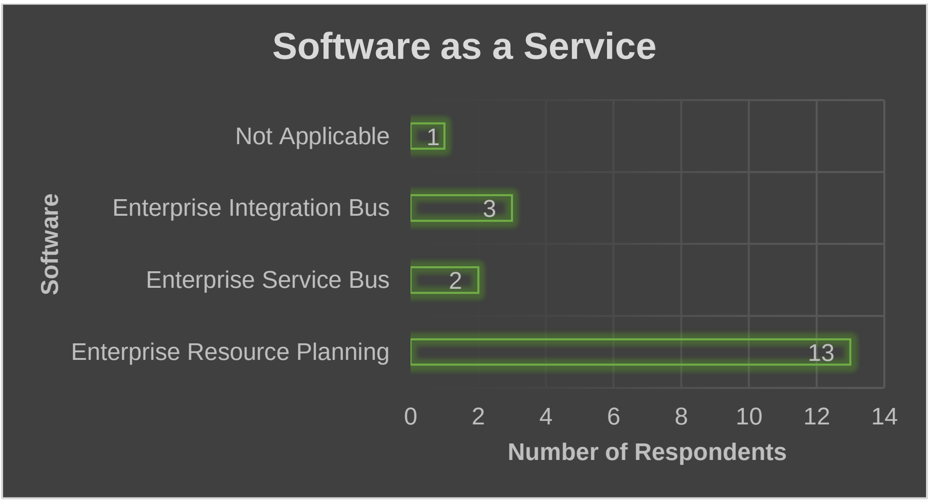


Figure 7.18: Software consumed as a service

The most favoured software was Enterprise Resource Planning (ERP). This was followed by Enterprise Integration Bus, and Enterprise Service Bus was the least favoured.

- **Question 5.1.29 –** *In your opinion, generally how applicable is the core and context of this framework to your area of expertise and sector?*

According to their areas of expertise and the sector they represented, the purpose of this question was to weigh the applicability of the ISDD framework.

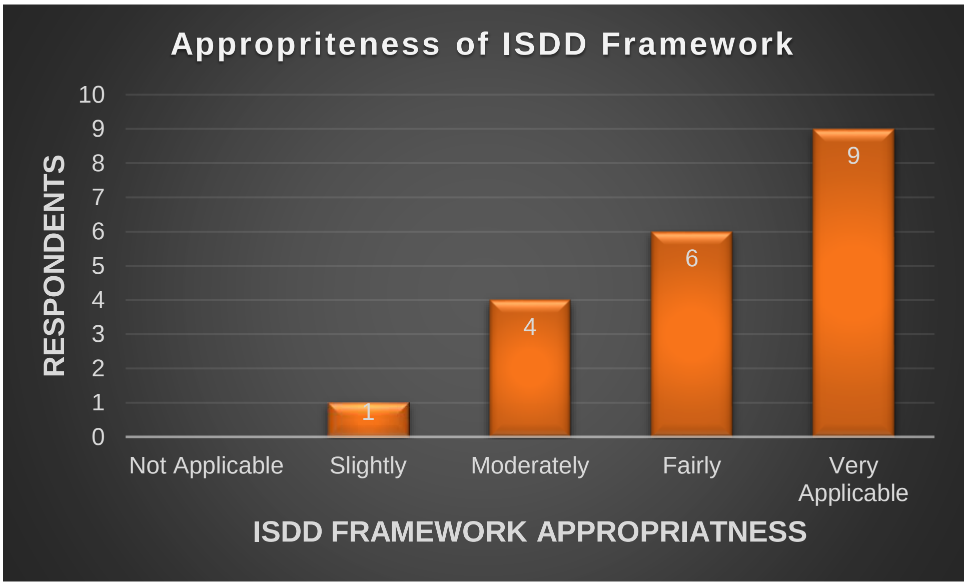


Figure 7.19: Appropriateness of ISDD to ICT expert sectors of representation

Of the twenty-five ICT experts, ten (40%) commended the framework because it was applicable to their sector and area of expertise, as brought out in Figure 7.19. Six (24%) ICT experts indicated that the framework was fairly applicable, and four (16%) said it was moderately applicable. Five (20%) leaned towards the framework being slightly applicable, and two of the ICT experts (8%) were of the idea it was not appropriate to their expertise and the sector they represented.

In this subsection, analysis and interpretation of data from ICT experts was the aim. The next section will focus on the pointers intended to be used for the improvement of the proposed framework.

7.4. Results Summary

In this section, the outcome of the survey is summarised so as to capture aspects aimed at improving the framework. The survey result is summarised in Table 7.1. As can be observed from the table, a number of improvement recommendations were noted as mandatory to accommodate the views expressed by ICT experts. The areas that follow were factored as important.

7.4.1. Generalisation of Access Mode by External Stakeholders

This access channel was represented by arrow 1 in Figure 4.6, renamed from Web portal to internet in order to generalise the access mode to any other that may fall under internet.

7.4.2. More Business Role in Middle Management

Additional business roles were included in middle management in the framework to cover a wider spectrum of end-users within an organisation.

7.4.3. More Business Roles in Upper Management

More business roles in upper management were also incorporated in the framework to ensure more management involvement in IT management and support.

7.4.4. Clarification of Business Roles

Business roles were clearly defined and organised according to complexity. This was made possible by having a comprehensively organised organisational structure that is precise so as to guide system access configuration.

7.4.5. External End-user Authentication

External stakeholders should only be authenticated at front-end office and nothing more to improve access response time. Otherwise, it might frustrate them because of a prolonged procedure before authentication.

7.4.6. Additional Business Roles

It would be ideal to incorporate an additional business role (middle management) between upper and middle management in order to complete a general outlook of business roles.

7.4.7. An ISDD-specific Security Policy in Low-Level Language

An information security policy that is written in low-level language that is easy for end-users to understand and work with, and also specific policies that zoom in on issues that support ISDD is necessary. Such policies may include a strict password policy that strictly enforces strong passwords, ones that change over time and making it clear sharing of passwords is a punishable offence.

7.4.8. Business Function Regulation

Business functions from both a physical access and system performance perspective need to be regulated according to business roles and their complexity.

7.4.9. Internal Business Roles Activation to Use External Access Channels

Internal business roles should also be allowed to use external user access channels given circumstances where their access devices, e.g. laptops, are unavailable or unable to work using their routine options.

7.4.10. Include Intranet as Access Channel for Internal End-users

It is advisable to add intranet as a primary access channel for internal end-users as depicted by arrow 3 in Figure 4.6. Nevertheless, there should be other access channels such as RDP or VPN as secondary for eventualities involving linking to other organisational departments or sites when normal channels are down.

This section suggested a couple of improvement recommendations based on ICT experts' responses observed as mandatory to making the framework of this study extensively consensual and further its enhancement and performance. Table 7.1 presents areas of concern as raised in survey responses concerning *framework properties in relation to ISDD critical success factors.*

7.4.11. Results and Contributing Questions to Improvement of Framework

Table 7.1: Framework properties and expert contributing questions matrix

		Population & Demography	Security Awareness & Training	Security Policy Standard Practice & compliance	Information Flow (Organizational structure)	IT Systems & Security	Computer Literacy	Access Control	Value of IS to organizations
Q 5.1.1		X							
Q 5.1.2		X							
Q 5.1.3		X							
Q 5.1.4									X
Q 5.1.5									X
Q 5.1.6				X					X
Q 5.1.7								X	
Q 5.1.8								X	
Q 5.1.9					X				
Q 5.1.10								X	
Q 5.1.11								X	
Q 5.1.12								X	
Q 5.1.13								X	

Q 5.1.14								X	
Q 5.1.15								X	
Q 5.1.16								X	
Q 5.1.17								X	
Q 5.1.18								X	
Q 5.1.19				X				X	
Q 5.1.20			X	X	X	X	X	X	
Q 5.1.21								X	
Q 5.1.22								X	
Q 5.1.23								X	
Q 5.1.24					X				
Q 5.1.25					X				
Q 5.1.26					X				
Q 5.1.27							X		
Q 5.1.28							X		
Q 5.1.29									X
Q 5.1.30							X		

In this section, areas of improvement based on expert survey outcome were presented. The next section takes those expert recommendations raised and incorporates them into the initial proposed framework to produce the final ISDD framework.

7.5. Improved Information Security Digital Divide Framework

In light of the improvement recommendations made by ICT experts in Section 7.4 on the areas of concentration and what can be altered to improve the quality of the framework, the final information security digital divide framework (ISDDF) depicted in figure 7.20 will now be presented.

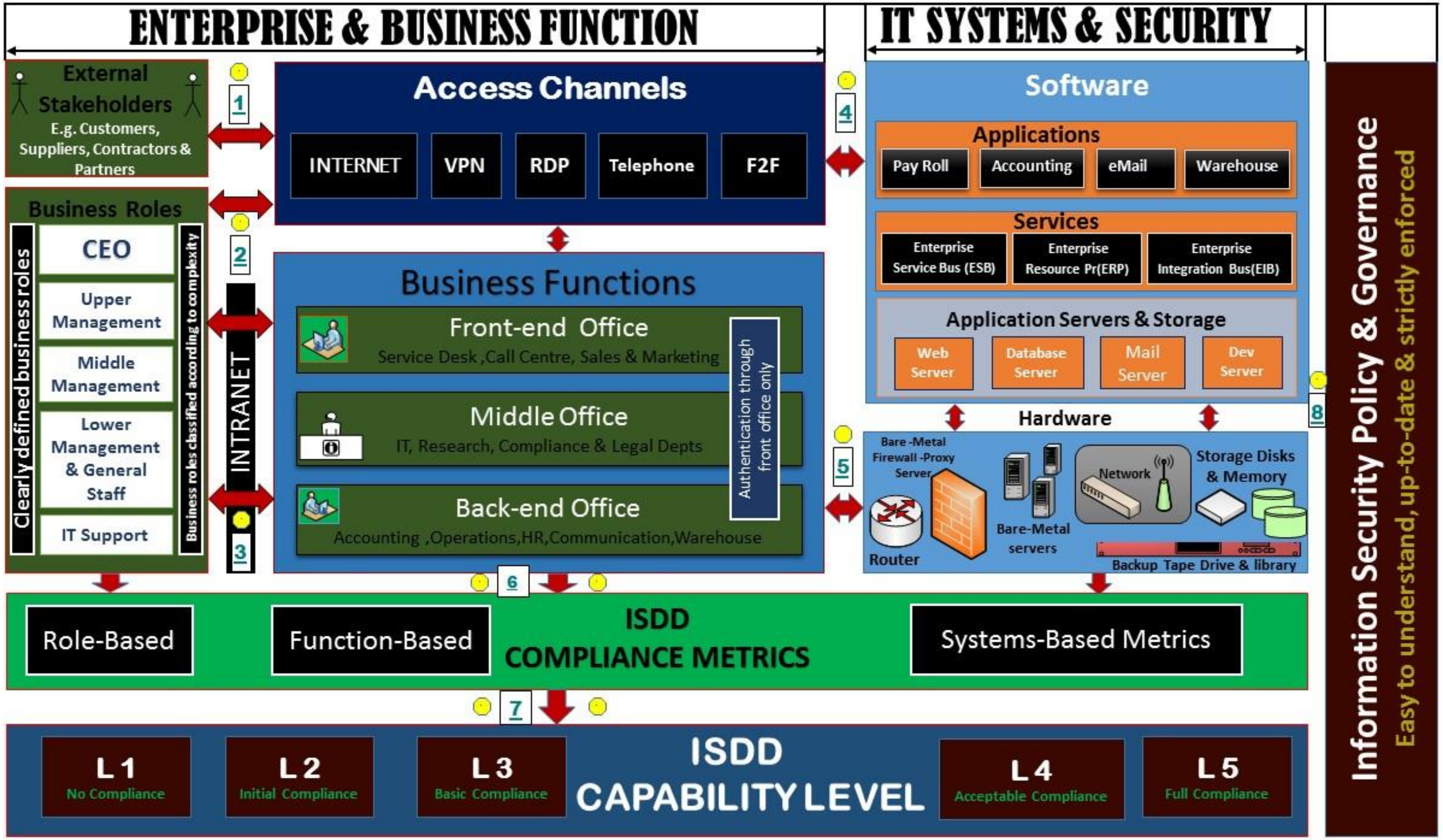

ENTERPRISE & BUSINESS FUNCTION
IT SYSTEMS & SECURITY
External Stakeholders
E.g. Customers, Suppliers, Contractors & Partners
Business Roles
Clearly defined business roles
CEO
Upper Management
Middle Management
Lower Management & General Staff
IT Support
Business roles classified according to complexity
INTRANET
1
2
3
4
5
6
7
8
Access Channels
INTERNET
VPN
RDP
Telephone
F2F
Business Functions
Front-end Office
Service Desk ,Call Centre, Sales & Marketing
Middle Office
IT, Research, Compliance & Legal Depts
Back-end Office
Accounting ,Operations,HR,Communication,Warehouse
Authentication through front office only
Software
Applications
Pay Roll
Accounting
eMail
Warehouse
Services
Enterprise Service Bus (ESB)
Enterprise Resource Pr(ERP)
Enterprise Integration Bus(EIB)
Application Servers & Storage
Web Server
Database Server
Mail Server
Dev Server
Hardware
Bare -Metal Firewall -Proxy Server
Router
Bare-Metal servers
Network
Storage Disks & Memory
Backup Tape Drive & library
ISDD COMPLIANCE METRICS
Role-Based
Function-Based
Systems-Based Metrics
ISDD CAPABILITY LEVEL
L 1 No Compliance
L 2 Initial Compliance
L 3 Basic Compliance
L 4 Acceptable Compliance
L 5 Full Compliance
Information Security Policy & Governance
Easy to understand, up-to-date & strictly enforced

Figure 7.20: Final ISDD framework

7.5.1. Improvement from Previous Framework as Value Thereof

The improved version as opposed to the initial one is more security and ISDD-centric through emphasis, amongst others, on:

- A wider coverage of end-user spectrum to ensure ISDD is strongly enforced all across the entire organisation
- A high concentration and control of the organisational structure, which is the basis of a strong and comprehensive access control management design
- Carefully streamlined business roles to align them to the appropriate business functions system-wise and also creating improved access modes for both internal and external end-users and stakeholders. Furthermore, a physical access control plan that regulates all end-user effectively according to their work scope
- Access channels are revised, changed and improved on to add a wider access opportunity for both internal and external end-users and stakeholders, which improves access efficiency while at the same time preserving a high ISDD
- A security policy template which is proposed to be efficiently written in a tone that makes it easy for end-users to apply it as a guideline while at the same time emphasising on how enforcement of policies by custodians must be firm

7.5.2. Usage of the Framework in Real-life Context

The importance of this framework is that it is a self-assessment tool that can be used by organisations to measure the level of ISDD and furthermore be relied upon to improve on what is noted as inappropriate. Organisations can use the framework by comparing their ISDD compliance against a checklist of metrics and core factors presented by the framework. At the end of compiling checklist scores, an organisation is able to know its level of ISDD compliance and accompanying recommendations to improve on the shortcomings identified.

7.5.2.1. Step-by-Step Process to Measure Capability Maturity

This framework was curved on the concept of perfectly combining people, process, and technology to minimise security risk and threats. As such, capability maturity was measured using the structure of Salaski (2013) as follows:

- **Step 1:** Identify ISDD capabilities to be assessed – These capabilities are covered in Section 6.1 to 6.10, and the processes are summarised in Table 6.11.
- **Step 2:** Create a unit of measure – Every capability table covered in Section 6.1 to 6.10 used different score scales ranging from 1 to 2.5 per metric question. The total score or rating per category was equal to 10.
- **Step 3:** Identify who to add in the assessment – A wide range of end-users and stakeholders whose business roles require them to mostly interact with the system were selected.
- **Step 4:** Perform the assessment – An assessment was performed by way of a range of questionnaires issued to mostly impacted system end-users who were selected carefully. This was covered in Chapter 6. In some cases, the assessment took some form of interviews with structured questions to make inferences on certain aspects of ISDD not obtainable by end-user questionnaires. Furthermore, observation was also resorted to so as to weigh ISDD applicability.
- **Step 5:** Report the results – Combined rating in Table 6.11 and assessment rating in Table 6.12 presented the results.

7.5.2.2. Continuous Improvement

Continuous improvement involves ensuring that key performance indicators continue to improve over time. In this framework, all factors presented in Table 4.3 are key performance indicators that are summarised in Table 6.1 to 6.10. The measurement of continuous improvement in this framework follows the Plan-Do-Check-Act tool discussed earlier in Chapter 2 whereby:

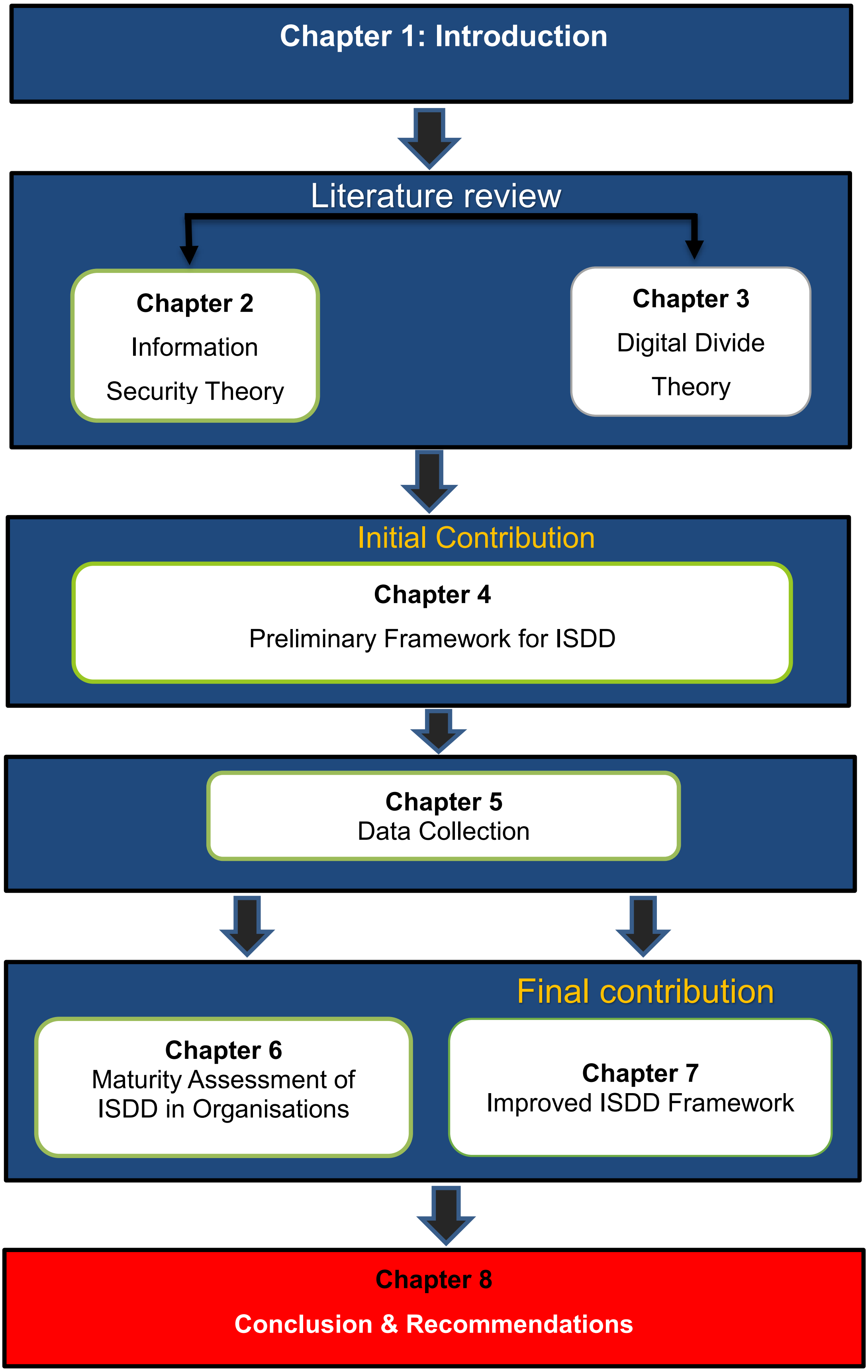
- **Planning** involves identifying all key change processes involved in sustaining factors presented in Table 6.1 to 6.10 and planning for potential change.
- **Do** means implementing the change to the process identified in Table 6.1 to 6.10 in moderation.
- **Check** has to do with monitoring in order to observe the performance of the change after application in the previous stage.
- **Act** concerns actioning lessons learnt in all processes undergone from Table 6.1 to 6.10 and making corrections where set targets did not happen as planned.

7.6. Conclusion

The objective in this chapter was to analyse data collected from ICT experts from different sectors and occupations within the ICT space. The idea was to interpret results so as to identify recommendations which would provide additional value to the proposed framework. The summary of the survey result was used to improve on the initial proposed framework. Additionally, usage of the framework in real-life context was presented, including how capability maturity is measured alongside continuous improvement.

The chapter that follows will provide a conclusion and recommendations of this study.

Chapter 8: Conclusion and Recommendations



8.1. Introduction

The main objective of this study was to develop a self-assesment tool which organisations can rely on to measure ISDD capability maturity. The tool provided as a framework would be dependent upon for benchmarking ISDD in organisations and use such a benchmark for future improvements. This was achieved by first reviewing literature on information security and its role in business operations, followed by a contextualisation of ISDD and a presentation of its critical success factors. The foregoing provided a reasonable ground for the suggestion of a theoretical framework based on principles of COBIT. To assess the relevance of the framework for this study at organisation level, suitable data was collected from selected stakeholders and analysed with conclusions drawn in order to assess the relevance of this study's framework and also explore avenues for its improvement.

The purpose of this chapter is to summarise this study in order to demonstrate how the objectives set out in Chapter 1 were achieved. It also provides a range of future works that are deemed necessary to pursue in order to enrich the literature on ISDD.

This chapter begins with research findings in Section 8.2, followed by a summary of this study in Section 8.3. Section 8.4 then explores future works, and then Section 8.5 concludes the study.

8.2. Research Findings

The findings revealed in this study follow. They are primarily applicable to participating organisations. However, they can be extrapolated to the overall body of knowledge on organisational structure, information security digital divide, and ISDD Capability Maturity Assessment. The findings are as follows:

1. Organisations must be structured in a specific order that by default complements system access control and strive for a mature ISDD. Preferably, organisations must be structured into upper-middle-lower management in order to take advantage of the concept of ISDD.

2. In the same alley as the previous findings, systems need to be architected in a manner that is aligned to the overall concept of front-end office, middle office, and back-end office. This enables them to efficiently and effectively

manage ISDD in a segregated manner and view information security in a decoupled manner in order to minimise vulnerability and at the same time be able to identify flaws whenever they arise and, in turn, take remedial action flawlessly.

3. ISDD is important in all organisations that make use of information systems for business operations. While digital divide is perceived as bad in the context of information communication technology for development (ICT4D), it was demonstrated throughout the study that ISDD is good for organisations to safeguard corporate data.

4. A variety of existing IT frameworks in literature such as COBIT can be exploited to build new frameworks in various aspects of ICT at organisational level for the purpose of continuously improving on challenging ICT aspects of the organisation.

5. Allocating ISDD capability maturity levels from 1 to 5 and defining them with key assessment criteria appears to be a key contribution to this study in the sense that it can be used in a real-life context to measure ISDD maturity level assessment and therefore continuously improve on security challenges at organisation level.

6. Organisations can use the ISDD framework for self-assessment and continuous ISDD improvement. Furthermore, such a tool can be used as a governance and best practice tool for continuous improvement.

7. Organisations can make use of the ISDD framework tool to conduct independent auditing for IT compliance.

8. The main and final finding in this study was the developed framework consensually improved by the contribution of information ICT experts.

8.3. Research Summary

This study was initiated to equip organisations with a valuable governance tool aimed at not only determining their current status with regard to ISDD but also to rely on such evaluation to constantly improve on information security-related shortcomings in the organisation, thus resulting in graduation to the next maturity level. The main objective as depicted in Chapter 1 was to develop, experiment, and evaluate an ISDD framework for maturity assessment at organisation level. A range of sub-objectives were identified to which appropriate research questions were aligned so as to collectively achieve the main objective. In the subsections that follow, each of the sub-objectives (and therefore research question) will be revisited, and they will briefly be expanded on how they were achieved in this study.

8.3.1. Sub-objectives

The sub-objectives of this study were as follows:

- **Sub-objective 1**

Investigate the state of the art with regard to theory and practise of information security in organisations: The intention in this objective was to thoroughly investigate theoretical and practical management aspects followed by some of the best performing security systems in organisations. Based on that observation, the aim was to replicate their approach in order to identify best techniques applicable and befitting this study. This sub-objective was attained earlier in literature review in Chapter 2, whereby, the general composition of an enterprise and information systems were thoroughly investigated.The outcome then steered this study to identifying critical success factors suitable for guiding the study to produce further consolidated CSF for ISDD in Chapter 3.

- **Sub-objective 2**

Understand the theory of digital divide and its contextualisation to information security: This sub-objective defined what digital divide was and how it combined with information security to conceive the core concept of ISDD. In chapter 2, this sub-objective was achieved by means of the following: theory on organisational information flow and structure was studied in detail. Then mostly in Chapter 3, the generic concept of digital divide (DD) from an ICT4D perspective was exploited and aligned to information security as well as information flow in an organisation to provide a contextual definition of ISDD that promote the segregation of information access at enterprise level. The foregoing culminated in the description of CSF for ISDD that formed the basis for the definition of ISDD core metrics used for obtaining maturity assessment.

- **Sub-objective 3**

Develop and validate a conceptual framework for assessing ISSD in organisations: In this sub-objective, the intention was, based on literature review, suggest a theoretic ISDD framework and then set the context for validating it and finally testing it in a real-world scenario. Practically this was the main contribution of this research. Achieving this objective spanned across four chapters: to begin with, relying on COBIT as the base framework, the ISDD conceptual framework was developed in Chapter 4. This was followed by the exploitation and evaluation of parts covered in Chapter 5 on data collection approaches for application of the framework in a real-life context and its validation by ICT experts. In Chapter 6, the framework developed was subjected to a case study in three case organisations which revealed the current ISDD maturity of each participating organisation and also demonstrated the relevance of this study's framework. Finally, by means of Chapter 7, evaluation of the developed framework by ICT experts ensued, resulting in an improved version of the initial framework.

8.4. Future Work

This research formed the basis for the maturity assessment of ISDD in organisations. As a matter of future work, listed below is a range of research of varying degree of complexity which can be conducted in order to contribute not only to the body of knowledge but also to the specialised field of information security.

- **Framework automation:** A plausible next step of this research would be the conversion of the suggested framework into an automated system. Such a system can be regarded as a capability maturity measurement tool which can be relied upon by ICT experts to benchmark ISDD and generate appropriate reports.
- **Framework expansion:** This study relied on COBIT to produce its final product; however, there are other IT governance frameworks which can also be considered to produce similar results. Such frameworks may include Information Technology Infrastructure Library (ITIL), the business process

framework (eTOM), and ISO/IEC 27001, which is a family of standards that can be trusted to secure system assets. As such, the proposed framework of this study could be expanded to produce a more comprehensive framework consisting of more CSFs that can be relied upon for the derivation of appropriate metrics. The combination of those metrics will contribute to enriching the definition of maturity level for more complex and accurate assessment and decision-making.

- **Framework specialisation:** This study only relied on organisations structured in terms of lower-middle-upper management. However, not all organisations may be organised in that format. It would be interesting to conduct a similar study on larger organisations that may not conform to such an organisational structure.

- **Localisation of the framework:** This study only targeted organisations based in Namibia. It would be interesting to observe how its applicability would fare in a different country. It would be worthwhile to perform a comparison on how effective the framework is on organisations with sufficient resources as opposed to small organisations experiencing budget constraints.

- **Framework replication:** While this work may have solely focused on ISDD, the same framework can be developed in other aspects that are not necessarily in the IT governance space, e.g. quality assurance, banking, and any other fields that can conform.

- **Doing the same work but in unrepresented sectors:** This framework was tested in a real-life context in only the following sectors: government, non-profit, and IT. It would be interesting to investigate the relevance of the same framework in other sectors such as banking, telecommunications, and logistics.

8.5. Conclusion

The main purpose of this research was to produce a self assesment tool suitable for organisations to use as a benchmark when measuring information security digital divide maturity. This would indicate to an organisation the safety of their information system, and further offer countermeasures to close security gaps identified. This was achieved by combining Information Security and Digital Divide to conceptualise the idea of Information Security Digital Divide (ISDD). This further culminated into a framework called Information Security Digital Divide Maturity Framework (ISDDMF). To develop the metrics for ISDDMF, COBIT IT Governance was used as a baseline framework, which resulted in the defining of a 5-level Capability Maturity Framework which can be used in the assessment of ISDD capability maturity. To ensure that all aspects of information security were considered in the design of ISDDMF, the Plan-Do-Check-Act (PDCA) life cycle approach was adapted. To empirically validate ISDDMF, a survey study, using questionnaire, interview, observation and document review as instruments was conducted. End-user staff from three organizations, and a number of ICT experts were respondents. The proposed framework which was also tested in a real world context constitutes a significance contribution in providing a tool for management of business organizations for continued monitoring of their capability to address information security threats to which they could be vulnerable, towards continuous capability improvement.

References

365 Computer Security, 2010. 365ComputerSecurity. [Online] Available at: https://www.youtube.com/channel/UCONoZM9jqOK799q20GtIsEg [Accessed 10 April 2015].

Abawi, K., 2013. The sexual and reproductive health and human rights of people living with HIV. [Online] Available at: http://www.gfmer.ch/SRH-Course-2013/sti/SRH-HR-PLHIV-Abawi-2013.htm[Accessed 11 April 2015].

Aguila, L.A., 2014.Looking at Corporate Governance from the Investor's Perspective.[Online]Available at: https://www.sec.gov/News/Speech/Detail/Speech/1370541547078[Accessed 27 August 2015]

Albrechtsen, E. & Hovden, J., 2009. Computers and Security. The information security digital divide between information security managers and users, 28(6), p. 476–490.

Al-Hakim, L., 2008. *Modelling information flow for surgery management process.* International Journal of Information Quality, 2 (1). pp. 60-74

Arora , V., 2010. Comparing different information security standards: COBIT v s. ISO 27001. [Online] Available at: https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf [Accessed 18 June 2015].

Ashenden, D., 2008. Information Security management: A human challenge?,. Information Security Technical Report, 13(Issue 4), pp. 195-201.

Avison, D., & Wilson D.N., 2002. IT failure and Colapse of one. Tel. Information Systems. The e-Business challenge - Kluwer, pp 31 - 46

Basani, M., 2012. Towards a framework to ensure alignment among information security Professionals, ICT security Auditors and Regulatory officials in implementing security in South Africa.University of South Africa, Pretoria: University of South Africa.

Bellovin, S. M., 2007. Insider Attack and Cyber Security. Beyond the Hacker. Columbia: Columbia University.

Bernik, I. & Prislan, K., 2011. Information Security in Risk Management Systems: Slovenian Perspective. VARSTVOSLOVJE, Journal of Criminal Justice and Security, 13(2), pp. 208-221.

Bishop, M., 2003. Computer Security – Art and Science. New Jersey: Pearson Education,Inc.

Bourgeois, D. 2014. Information systems and beyond. [Online] Available at http://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%

20and%20Beyond/Textbook.htm[Acessed 13 February 2015]

Brotby, K., 2009. Information Security Governance. A Practical Development Approach and Implementation. New Jersey: John Wiley & Sons Inc.

Buchanan, D. & Huczynski, A., 2010. Organizational Behaviour: An Introductory Text. 7th ed. s.l.:FT-Prentice Hall.

Business Case Studies, 2014. Building on Stakeholder Support To Achieve Dynamic Growth & support. [Online] Available at: http://businesscasestudies.co.uk/aldi/building-on-stakeholder-support-to-achieve-dynamic-growth-success/suppliers.html#axzz4NTH19Hqh

Business Dictionary, 2014. [Online]Available at http://www.businessdictionary.com/definition/organization.html[Accessed 20 May 2015]

Caballero , A., 2009. Managing Information Security. Second ed. Waltham: Terremark Worldwide.

Cambridge Dictionaries, 2014. Meaning of “coordinator” in the English Dictionary. [Online] Available at:http://dictionary.cambridge.org/dictionary/english/coordinator?a=british[Accessed 1 February 2014].

Cambridge University Press, 2009. ICT4D - Information and Communication technology for Development. London: Cambridge University Press.

Carney, C., 2013. Measuring the Maturity of your Information Security Program Impossible? [Online] Available at: http://secure360.org/wp-content/uploads/2013/05/Measuring-the-Maturity-of-InfoSec-Program-Mark-Carney.pdf (Accessed 20 November 2015)

Carney, M., 2015. With BitStamp back online, serious questions about its solvency and security remain. [Online] Available at: https://pando.com/2015/01/12/with-bitstamp-back-online-there-remain-serious-questions-about-its-solvency-and-security/[Accessed 27 April 2015].

CA Technologies, 2015. Digital technology, the need for connection, and the role of national memory institutions. [Online] Available at: http://news.gc.ca/web/article-en.do?nid=1018799 [Accessed 15 May 2015].

Centre for Disease Control, 2016. Analysing Quantitative Data for Evaluation. [Online] Available at: http://www.cdc.gov/healthyyouth/evaluation/pdf/brief20.pdf [Accessed 5 May 2016].

Chilengi, R., 2009. An ethics perspective on responsibilities of investigators, sponsors and research participants.112 (1), p.53 - 62

Choy, T. L., 2014. The Strengths and Weaknesses of Research Methodology: Comparison and Complimentary between Qualitative and Quantitative Approaches. IOSR Journal Of Humanities And Social Science (IOSR-JHSS) , 19(I4), pp. 99-104 .

Chun, M. & Mooney, J., 2009. Information and Management. CIO roles and responsibilities: Twenty-five years of evolution and change, 6(6), pp. 323-334.

CISCO, 2015. Introduction to Wide Area Network Protocols. [Online].Available at: www.cisco.com/networkers/nw00/pres/2303.pdf[Accessed 21st June 2015].

Clarke, R., 2009. INTERPRETIVIST RESEARCH TECHNIQUES. [Online]
Available at: www.rogerclarke.com/Res/53-Int.ppt[Accessed 27 August 2016].

Commission, U. S. I. T., 2010. Small and Medium-Sized Enterprises: Overview of Participation in U.S. Exports Washington, DC 20436 .. [Online]
Available at: www.usitc.gov [Accessed 23rd October 2015].

Community tool box, 2014. Section 1. Organizational Structure: An Overview. [Online] Available at: http://ctb.ku.edu/en/table-of-contents/structure/organizational-structure/overview/main (Accessed 2nd June 2016)

Conklin, A. W. & White, G., 2012. Principles of Computer Security. 3 ed. New York: McGraw Publishers.

Cresswell, J. W., 2014. Research Design: Qualitative, Quantitative and Mixed Method Approaches. Fourth ed. Los Angeles: Sage Publications.

Cresswell, W. J., 2003. Research Design: Qualitative, Quantitative and Mixed Method Approaches Thousand. Los Angeles: Oaks: Sage.

Creswell, J. W., 2009. Research design: qualitative, quantitative, and mixed methods. Third ed. Los Angeles: Sage.

Curtis, B., Hefley, B. & Miller, S., 2009. People Capability Maturity Model (P-CMM) Version 2.0, Second Edition, Hanscom: Mellon University.

Da Veiga, A & Eloff, J.H.P. 2010. A framework and assessment instrument for information security culture. Computers & Security 29(2010) 196 – 207. University of Pretoria

Darkow, L., 2015. The involvement of middle management in strategy development — Development and implementation of a foresight-based approach. Technological Forecasting and Social Change, Volume 101, pp. 10-24.

Deloitte, 2004. CIO 2.0.The changing role of the chief information officer. [Online]
Available at: http://www.providersedge.com/ehdocs/ehr_articles/CIO_2-The_Changing_Role_of_the_CIO.pdf[Accessed 1st January 2016].

Demski, S. J., Lewis, T. R., Yao, D. & Yildirim, H., 2010. THE USE OF INFORMATION FLOW ANALYSIS FOR BUILDING AN EFFECTIVE ORGANIZATION.

DeWalt, K. M. & DeWalt, B. R., 2002. Participant observation: a guide for fieldworkers. Sixth ed. Chicago: AltaMira Press.

Durrheim, K., 2002. Quantitative Analysis. In: Research in practice: Applied Methods for the Social Sciences. 2nd ed. Capetown: University of Cape Town Press.haraf, K., 2012. Qualitative Data Collection Techniques:Training course in Sexual reproduction Health research, Geneva: University of Medical Sciences & Technology.

Elmusharaf, K. 2012. Qualitative Data Collection Techniques. Training Course in Sexual and Reproductive Health Research. Geneva 2012. University of Medical Science & Technology

Eubanks, V. E., 2007. Trapped in the Digital Divide: The Distributive Paradigm in Community Informatics. The journal of community informatics, 3(2).

European Federation for Welding, 2014. ORGANIZATION. [Online] Available at : http://www.ewf.be/about/about1/organization.aspx.[Accessed October 30 2015]

Fadhel, A.B, Bianculli, D & Briand, L. 2015. A comprehensive modeling framework for role-based access control policie. The Journal of Systems and Software 107 (2015) 110 - 126

Faust, G., 2012. The Roles of Management. [Online]
Available at: : https://www.youtube.com/watch?v=beHGczKkre4[Accessed 22 February 2015].

Fergusson, S., 2013. Employee Engagement - The Role of Senior Managers, describe the roles and responsibilities. [Online] Available at: https://www.youtube.com/watch?v=IFLvwgZS2LM[Accessed 28 May 2015].

FFIEC, 2015. Board and Senior Management Responsibilities. [Online]
Available at: http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/board-and-senior-management-responsibilities.aspx
[Accessed 15 May 2015].

Frenzel , W. C. & Frenzel, J. C., 2004. Management of Information Systems. Fourth ed. Canada: s.n.

Fuchs, C. & Horak, E., 2008. Africa and the digital divide. Telematics and Informatics , 25(2), p. 99–116.

Fuchs, L., Pernul, G. & Sandhu, R., 2011. Roles in information security - A survey and classification of the research area.. Computers & security , Volume 30, pp. 748 -769.

Garcia, M. T., 2015. [Online] Available at: http://www.irca.org/en-gb/resources/INform/archive/issue32/Features/Security-information-planning[Accessed 25 2015].

GCSE Business studies , 2., 2004. Types of Business Organisation. [Online] Available at: http://www.tutor2u.net/business/gcse/presentations/sample_pdf_orgtypes.pdf[Accessed 25 March 2015].

Goh, R., 2003. Information Security: The Importance of the Human Element, Singapore: Preston University.

Goksen, Y., Cevik, E. & Avunduk, H., 2015. A Case Analysis On The Focus On The Maturity Models And Information Technologies. Procedia Economics and Finance , Vol 19, pp. 208-216.

Granneman, J., 2013. IT security frameworks and standards: Choosing the right one. [Online] Availabe at: http://searchsecurity.techtarget.com/tip/IT-securityframeworks-and-standards-Choosing-the-right-one (Accessed February 20 2016)

Hancock, B., Windridge, K., & Ockleford, E. 2007. An Introduction to Qualitative Research. The NIHR RDS EM / YH

Hardcastle, E., 2008. Business Information Systems. s.l.:Elizabeth Hardcastle & Ventus publishing APS.

Hatala, P. J. & Lutta, G. J., 2009. Managing Information Sharing Within an Organizational Setting: A Social Network Perspective. Performance improvement quarterly, 21(4), pp. 5-33.

Holme, D. & Thomas , O., 2008. Managing and Maintaining a Microsoft® Windows Server(TM) 2008 Environment. Second ed. s.l.:Microsoft Press Publisher.

Holt, V., Ramage , M., Kear , K. & Heap , N., 2015. The usage of best practices and procedures in the database community. Computer Systems, Vol 49, p. 163–181.

Huang, M. S. et al., 2009. A business process gap detecting mechanism between information system process flow and internal control flow. Decision Support Systems. Decision Support Systems, 47(4), p. 436–454.

Humphreys, E., 2008. Information security management standards: Compliance, governance and risk management. Information Security Technical Report, 13(4), p. 247–255.

Jefrey, A.H. 2006. Modern Database Management. 8th Edition. Prentice-Hall, Inc. Upper Saddle River, NJ, USA.

Joppe, M. 2000). The Research Process. [Online] Available at; from http://www.ryerson.ca/~mjoppe/rp.htm [Accessed 26 August 2016]

Illinois State University, 2010. Organisation and the System Concept. [Online] Available at: http://communication.illinoisstate.edu/lwlong/COM495/downloads

/Katz%20Chap%202.pdf[Accessed 17 September 2016].

Microsoft Inc, 2015. Security Threats. [Online] Available at: https://msdn.microsoft.com/en-us/library/cc723507.aspx[Accessed 2nd April 2015].

ISACA, 2008. Aligning CobiT® 4.1, ITIL® V3 and ISO/IEC 27002 for Business Benefit. [Online] Available at: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf[Accessed 21 July 2015].

ISACA, 2011. Cobit 5 - Isaca. [Online] Available at: http://www.isaca.org/chapters2/New-York-Metropolitan/membership/Documents/2012-04-30%20Spring%20Conference-Meeting/3%20Barnier%20VBA%20COBIT5.pdf[Accessed 1 November 2015].

Jack, P. E. & Raturi, S. A., 2006. Lessons learned from methodological triangulation in management research. Management Research News , 29(6), pp. 345-357.

Jaquith, A., 2007. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Reading: Addison Wesley.

Jarvelainen, J., 2013. IT incidents and business impacts: Validating a framework for continuity management in information systems. International Journal of Information Management , Vol 33, p. 583– 590.

Joseph, V. & Schneider, C., 2010. Information Systems Today: Managing in the Digital World. 4th ed. New Jersey: Prentice-Hall.

Jouinia, M., Rabaia , L. B. & Aissab, A. B., 2014. Classification of security threats in information systems. Procedia Computer Science , Volume 32, p. 489 – 496.

Jurnal, K., 2007. Case study as a research method. Jurnal Kemanusiaan , Volume 9, pp. 1-2.

Kaptein, M. & Avelino, S., 2005. Measuring corporate integrity: a survey-based approach. Corporate Governance, 5(1), pp. 45-54.

Kaspersky, 2016. How Social Engineering works. [Online] Available at: https://usa.kaspersky.com/internet-security-center/threats/malware-social-engineering#.WAX8E4VOLIU[Accessed 25 July 2015]

Kavanagh, J., 2016. Computer Weekly.com. [Online] Available at: http://www.computerweekly.com/feature/Security-special-report-The-internal-threat[Accessed 23 Decemeber 2015].

Kaya, L., 2012. ISO 27001 Information Security Management System (ISMS) Certification Overview. [Online]
Available at: http://slideplayer.com/slide/1514902/[Accessed 20 December 2015].

Kerrigan, M., 2013. A capability maturity model for digital investigations. Digital Investigation: The International Journal of Digital Forensics & Incident Response , 10(1), p. 19–33.

Kitchenham, B. & Pfleeger, L. S., 2002. Principles of Survey Research Part 5: Populations and Samples. Software Engineering, 27(5), pp. 17-20..

Kraemer, S., Carayo, P. & Clem, J., 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security , 28(7), p. 509 – 520.

Kumta , G. A. & Shah, M. D., 2002. CAPABILITY MATURITY MODEL A HUMAN PERSPECTIVE. Delhi Business Review , 3(1).

Layton, T. P., 2009. Information Security .Design, Implementation, Measurement, and Compliance. s.l.:Auarbach publications.

Lawry, R., Wadell, D., & Singh, M., 2007. Roles, Responsibilities and Futures of Chief Information Officers (CIOs) in the Public Sector. Proceedings of European and Mediterranean Conference on Information Systems 200, Spain: Polytechnic University of Valencia

Limoncelli, T. A., Hogan, C. J. & Chalup, S. R., 2007. The Practice of System and Network Administration. 2nd ed. Indianapolis: Addison-Wesley.

Locke, G. & Gallagher, P. D., 2010. Guide for Applying the Risk Management Framework to Federal Information Systems, Gaithersburg: NIST .

Locke, L. F., Silverman, S. J. & Spriduso, W. W., 2010. Reading and understanding research. 3rd ed. Texas: Sage.

Logan, P. Y. & Clarkson, A.C., 2005. Enhancing Information Security: A Qualitative Risk Analysis Method for Overcoming the Insider Threat. Modern Organizations Through Information Technology

Lunenburg, F.C., 2010. Formal Communication Channels: Upward, Downward, Horizontal, and External. FOCUS ON COLLEGES, UNIVERSITIES, AND SCHOOL., 4(1) , p. 1-7

Marshall, C. & Rossman, G. B., 1999. Designing Qualitative Research. 3rd ed. London: Sage Publications.

Macnamara, J. 2015, ‘Creating an “architecture of listening” in organizations: The basis of engagement, trust, healthy democracy, social equity, and business sustainability’, University of Technology Sydney.

Meskovska, A., 2008. Most common Threats to Information Security. Strumica, ILSA.

Mind Tools, 2015. Plan-Do-Check-Act (PDCA). [Online]
Available at: https://www.mindtools.com/pages/article/newPPM_89.htm
[Accessed 16 March 2015].

Mirror, 2011. 25 million Sony gamers' details stolen in second PlayStation Network security breach. [Online] Available at: http://www.mirror.co.uk/news/technology-science/technology/25-million-sony-gamers-details-126334[Accessed 7 June 2015]

Monette, D. R., Sullivan, T. J. & DeJong, C. R., 2002. Applied Social Research. 5th ed. Orlando: Harcourt Press.

Nikolakopoulos, T., 2009. Evaluating the Human Factor in Information Security. Network and System Administration, Oslo: Oslo University College.

NIST, 2010. Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach. Information Security, (1) p. 1-38

Nurse-Family Partnership, 2009. Implementation Overview & Planning. A guide for prospective Nurse-Family Partnership Implementing Agencies.[Online] Available at: https://atlantawomen.org/wp-content/uploads/2012/11/NFP_Overview_Planning.pdf(Accessed 20 January, 2015)

OECD, 2003.Organisation for Economic co-operation & Development. E-Government Studies: Finland

Oates, J. B., 2006. Researching Information Systems and Computing. London: Sage.

Oira, 2013. Analyzing and Interpreting Data. [Online]
Available at: https://oira.syr.edu/assessment/assesspp/Analyze.htm [Accessed 1st October 2013].

Padmapriya, A., & Subhasri, P., 2013. “Cloud Computing: Security Challenges & Encryption Practices”. International Journal of Advanced Research in Computer Science and Software Engineering. Vol 3(3), pp. 257

Pardo, T. A., Cresswell, A. M., Dawes, S. S. & Burke, G. B., 2004. Hawaii International Conference on System Sciences (HICSS-37). Hawaii, s.n.

Pardo, T. A., Cresswell, A. M., Thompson, F. & Zhang, J., 2006. Knowledge sharing in cross-boundary information system development in the public sector. Information Technology and Management, 7(4), p. 293−313.

Partridge, H., 2005. Establishing the human dimension of the digital divide. Information Security and Ethics: Social and Organizational Issues, pp. 23-47.

Patil, J., 2008. Information Security Framework. Case study of a manufacturing orgaisation, New York: Mercy College

Petrauskas, V., 2006. The use of information flow analysis for building an effective organisation. 124X INFORMATION TECHNOLOGY AND CONTROL, 35(4), pp. 50-215.

Petrauskas, V., 2006. THE USE OF INFORMATION FLOW ANALYSIS FOR BUILDING AN EFFECTIVE ORGANIZATION. INFORMATION TECHNOLOGY AND CONTROL, 35(4), pp. 1-8.

Pfleeger , C. P., 2007. . Reflections on the Insider Threat. Birmingham, University of Birmingham .

Pfleeger, C. P. & Pfleeger, S. L., 2007. Security in Computing. 4th ed. New Jersey: , Prentice Hall.

Pickard, A. J., 2007. Research Methods in Information.. 2nd ed. s.l.: Facet Publishing.

Pooley, R. & Wilcox, P., 2004. Applying UML - Advanced application. 1st ed. Burlington: s.n.

Post, G. V. & Kagan, A., 2007. Evaluating information security trade-offs: Restricting access can interfere with user tasks. Computers & Security, 27(3), p. 229 – 237.

Prenhall, 2015. 4chapterManaging the Information Systems Infrastructure. [Online] Available at: http://www.prenhall.com/behindthebook/0132335069/pdf/Jessup_CH04.pdf[Accessed 15 October 2015].

Rao, S. S., 2005. Bridging digital divide: Efforts in India. Telematics and Informatics , Volume 22, p. 361–375.

Rishipal, D., 2014. Analytical Comparison of Flat and Vertical Organizational Structures. European Journal of Business and Management. 6(36), p. 56 - 65

Reuters, 2015. Bitcoing exchange Bitstamp says to resume trading with 24 hours. [Online] Available at: http://www.reuters.com/article/us-bitstamp-cybersecurity-idUSKBN0KG0S420150107[Accessed 3rd October 2015]

Rhee, H., Ryu, Y. U. & Kim, C., 2012. Unrealistic optimism on information security management. Computers & Security , Volume 31, p. 221 – 232.

Roberts, P., Priest, H. & Traynor, M., 2006. Reliability and validity in research. Nursing Standard, 44(20), pp. 41- 45.

Salaski, P., 2013. Capability Maturity Assessment - Trissential. [Online] Available at: http://www.trissential.com/PDF/Training-Workshops/TCBAF/2013/01-15-2013/tcbaf-presentation-01-15-2013.pdf[Accessed 9 August 2016].

Saleh, M. F., 2011. Information Security Maturity Model. International Journal of Computer Science and Security (IJCSS), 5(3), pp. 316-337.

Saleh, M. S. & Alfantookh, A., 2011. A new comprehensive framework for enterprise information security risk management. Applied Computing and Informatics, 9 (2), p. 107–118.

Sandhu, H. & Zhang, X., 2006. An Effective Role Administration Model. ACM Transactions on Information and System Security, 9(2), pp. 114-137.

Santouridis, L & Trivellas, P. 2010. Investigating the impact of service quality and customer satisfaction on customer loyalty in mobile telephony in Greece", The TQM Journal, Vol. 22 Issue: 3, pp.330-343,

Saunders, M., Lewis, P. & Thornhill, A., 2009. Research methods for business students. 5th ed. Harlow: Pearson Education.

Schach, S. R., 2011. Object-Oriented and Classical Software Engineering. 8th ed. New York: McGraw-Hill Companies,Inc.

Schleicher, A. & Saito, M., 2005. Quantitative research methods in educational planning. [Online] Available at: http://www.unesco.org/iiep/PDF/TR_Mods/Qu_Mod10.pdf [Accessed 17 September 2014].

Scholar Banks, 2010. Research Method.Chapter 7. [Online] Available at: http://scholarbank.nus.edu.sg/termsofuse;jsessionid=6E36DDDD26C732A90C336D1308BA6218[Accessed 20 May 2016].

Schulze, S. 2003. Views on the Combination of Quantitative and Qualitative Research Approaches. University of South Africa. Progression 25(2):8-20

Shipsey, R., 2010. Information systems: foundations of e-business Volume 1 , London: University of London.

Simpson, S., 2011. Issues in Data Protection and Individual Privacy.Herriot Watt University, Edinburg: Herriot Watt University.

Singh, D., 2015f. Framework to develop Master Sample Frame for Agriculture. [Online] Available at: http://www.unsiap.or.jp/e-learning/el_material/Agri/rap4_dec2014/1_3_Framework%20to%20develop%20MSF%20for%20Agriculture.pdf[Accessed April 30 2015].

Siponen, M. & Willison, R., 2009. Information security management standards: Problems and solutions. Information & Management , 46(5), p. 267–270.

Smirnova, M. M., Kouchta, S. P. & Podmetina, P. V., 2009. Key Stakeholders Interaction as a Factor of Innovativeness in Transitional. [Online] Available at: https://www.researchgate.net/profile/Daria_Podmetina/publication/228896793_Key_Stakeholders_Interaction_as_a_Factor_of_Innovativeness_in_Transitional_Economies_the_case_of_Russia/links/0912f513443e92e625000000.pdf [Accessed 17 May 2015].

Smit, S., 2014. Organisational Structure Presentation – Human Resource. [Online] Available at: https://www.youtube.com/watch?v=eU55cdqHv44 [Accessed 6th April 2016].

Spruit, M. & Roeling, M., 2014. ISFAM: THE INFORMATION SECURITY FOCUS AREA MATURITY MODEL, Utrecht: Utrecht University.

Stair, G., 2012. Fundementals of Information systems. 6th ed. Boston: Joe Sabatino.

Starman, A. B., 2013. The Case study as a type of qualitative research. Journal of contemporary educational studies , Volume 1, pp. 28 -29..

Tashakkori, A. & Teddlie, C., 2003. Handbook of mixed methods in social & behavioral research. 2nd ed. Louisiana: Sage.

Teddlie, C. & Yu, F., 2007. Mixed Methods Sampling. Journal of Mixed Methods Research January , Vol 1, pp. 77-100 .

Terre Blanche, M. & Durrheim, K., 2002. Research In Practice: Applied Methods for the Social Sciences. Capetown: University of Cape Town Press.

The Open University, 2011. Understanding Operations Management. [Online] Available at: http://www.open.edu/openlearn/money-management/management/leadership-and-management/understanding-operationsmanagement/ content-section-0[Accessed 27 March 2015].

The Oxford Dictionary , 2015. framework. [Online]
Available at: http://www.oxforddictionaries.com/definition/english/framework [Accessed 13 March 2015].

Thomas, R. M., 2003. Blending qualitative and quantitative research methods in thesis and dissertations. s.l.:Thousand Oaks, CA.

Tøndel, I. A., Line, M. B. & Jaatun, M. G., 2014. Information security incident management: Current practice as reported in the literature. Computers & Security , Volume 45, pp. 42-75 .

Trend Micro, 2015. Phishing. [Online]
Available at: http://www.trendmicro.com/vinfo/us/security/definition/phishing
[Accessed 4 April 2015].

Trinity College Dublin, 2007. Information Security Policy. [Online]
Available at: https://www.tcd.ie/ITSecurity/policies/Information%20Security %20Supporting%20Policies.pdf[Accessed 27 December 2015].

United States International Trade Commission, 2010. [Online] Available at: https://www.usitc.gov/publications/332/pub4125.pdf (Accessed 14 October 2015)

van Dijk, J. A., 2006. Digital divide research, achievements and shortcomings. Poetics, 34(4), pp. 221-235.

Vicka, T. E., Naganoa, M. S. & Popadiuk, S., 2015. Information culture and its influences in knowledge creation: Evidence from university teams engaged in collaborative innovation projects.. International Journal of Information Management, 35(1), pp. 292-298.

Von Solms, R, van de haar, H, von solms,S.H and W.J. Caelli.1994. A framework for information security evaluation. Journal of Information and Management. Volume 26 Issue 3, March 1994. pp 143-153

Walsham, G. 2006. Doing interpretive research. European Journal of Information Systems, 15(3), 320330.

Ward, P. & Smith, C. L., 2002. The Development of Access Control Policies for Information Technology Systems. Computers & Security , 21(4), pp. 356-371.

Warkentin, M. & Willison, R., 2009. Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems , 8(4), p. 101–105..

Warschauer, M., 2002. Reconceptualizing the digital divide.The theory of risk homeostasis: implications for safety and health. First Monday, 2(4), p. 209–25.

Westrum, R., 2014. The study of information flow: A personal journey. Safety Science, Vol 67, p. 58–63.

Whitman, M. E., & Mattord, H. J., 2008. Management of Information Security, Course Technology. 2nd ed. Boston: Course Technology.

Whitman, M. E., & Mattord, H. J., 2012. .Principles of Information Security. 4th ed. Boston: Course Technology.

Whitteker, W., 2014. Point of Sale (POS) Systems and Security. [Online] Available at: https://www.sans.org/reading-room/whitepapers/bestprac/point-sale-pos-systems-security-35357[Accessed 21 August 2015].

Whitten, J.L, Bentley, L.D., Dittman, K, Whitten, J, & Bentley, L. 2004. Systems Analysis and Design Methods. Sixth edition. Toledo: McGraw-Hill.

Williams, P. A., 2008. In a ‘trusting’ environment, everyone is responsible for information security. Information security technical report , 13(4), pp. 207-215.

Wright, N. & Losekoo, E., 2010. Interpretative Research Paradigms: Points of Difference. [Online] Available at: http://aut.researchgateway.ac.nz/bitstream/handle/10292/4523/ECRM2012BoltonWrightLosekootRE.pdf?sequence=2[Accessed 26 August 2016].

Xiao-yan, G., Yu-qing, Y. & Li-leic, L., 2011. An Information Security Maturity Evaluation Mode. Procedia Engineering , Vol 24, p. 335 – 339. .

Yang, T. M. & Maxwell, T. A., 2011. Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. Government Information Quarterly, 28(3), p. 164–175.

Yazici, H. J., 2002. The role of communication in organizational change: An empirical investigation. Information and Management, 39(7), p. 539–552.

Yin, R. K., 2009. Case Study Research: Design and Methods. 4th ed. Thousand Oaks: SAGE Publications Inc.

Yin, R.K., 2003. Case study research, design and methods. 3rd ed. Thousand Oaks: Sage

Zainal, Z. 2007. Case study as a research method. Jurnal Kemanusiaan 9, p. 1-4

Zhang, Y. et al., 2015. Towards more pro-active access control in computer systems and networks. Computers & Security , Vol 49, p. 132 – 146. .

Zikmund, W. G., 2003. Basic Data Analysis:Descriptive Statistics. [Online] Available at: http://pioneer.netserv.chula.ac.th/~ppongsa/2900600/LMRM02.pdf [Accessed 17 May 2016].

Zissis, D. & Lekkas, D., 2012 . Addressing cloud computing security issues. Future Generation Computer Systems , 28 (3), p. 583–592.

Appendices

Appendix A – Ethical Clearance Form

ETHICAL CLEARANCE APPLICATION FORM

Please Note That The Form Must Be Completed In Typed Script. Handwritten Applications Will Not Be Considered.

SECTION 1: PERSONAL DETAILS

1	**Details of Applicant**	
1.1 Full Name and Surname: Emmanuel Chisanga		
1.2	Title (Ms/ **Mr**/ Mrs/ Dr/ Professor/etc.):	
1.3	Student Number (where applicable):48123412	
	Staff Number (where applicable):	
1.4	School: Computing	
1.5	College:Science,Engineering & Technology	
1.6	Campus: Florida Park,Roodepoort	
1.7	Existing Qualifications: Bachelor's Honours degree Business Informatics	
1.8	Proposed Qualification for Project: Master of Science - Computing	
	(In the case of research of degree purposes)	
2.	**Contact Details**	
	Telephone Number	+264.81.23.41.305
	Cell. Number	+264.81.23.41.305
	e-Mail	:48123412@mylife.unisa.ac.za
Postal address (in the case of students and external applicants)		

P. O. Box 20238, Windhoek, Namibia. Postal code 9000

3. SUPERVISOR/ PROJECT LEADER DETAILS

NAME	TELEPHONE NO.	EMAIL	SCHOOL / INSTITUTION	QUALIFICATIONS
3.1 Prof. Ernest Ngassam	+27823552519	eketcha@gmail.com	UNISA	Professor
3.2				
3.3				

SECTION 2: PROJECT DESCRIPTION

Please do *not* provide your full research proposal here: what is required is a short project description of not more than two pages that gives, under the following headings, a brief overview spelling out the background to the study, the key questions to be addressed, the participants (or subjects) and research site, including a full description of the sample, and the research approach/ methods

2.1 Project title : Towards a conceptual Framework For Benchmarking Information Security Digital Divide

Background

The motivation for this research was driven by first-hand experience on the devastating impact information security breach may inflict on organisations. During years of IT experience, there was an observation that most organisations do not institute methods to demarcate corporate data access and use according to its relevance. Thus, in this research, critical success factors which will be vital in creating a security capability maturity model called information security digital divide maturity Framework (ISDDMF) have been identified. This proposed model strives to divide end-users, business partners, and other stakeholders into "*specific information haves and have-nots*", digitally. The idea is to carve out a model that helps organisations to appraise their information security and based on the outcome help them to tailor-design a security architecture that only avails information to individuals on the basis of their functionality, roles and responsibilities in accordance with the organisational structure while at the same time enforcing the traditional security standpoint of maintaining the confidentiality, integrity, and availability of corporate data.

Key questions

How can we develop a framework for assessing the maturity of ISSD in organizations for further improvements?

Sub-questions

- What are the current information security organizational practices and how is success measured in such context??
- How can the concept of digital divide be leveraged positively in the context of information security at organization level?
- How can a framework for assessing ISDD be developed and validated in a real-world context?

Participants (or subjects) and research site

Participants will be mostly selected strategic employees in case organisations such as the HR, IT manager, CIO, data entry clerk including external professionals independent from these organisations but ICT experts in the industry. The research sites will be mostly the IT departments and applicable relevant personnel to this study.

Full description of sample

Chapter 6 of this study will involve testing the developed framework in the real-world context by performing three case studies at the following target organisations in three vital sectors:

- Government sector (Laboratory)
- Information Communication and Technology sector (ICT)
- None Profit Making (Humanitarian)

In each organisation, certain metrics of ISDD are benchmarked as follows:

1. Government sector (Laboratory). How are the different departments, personnel, etc. allocated rights, e.g. towards results to diagnosis of animals that die mysteriously as brought in by farmers and outbreak of any animal disease)

2. ICT sector (Standard practice and permission levels among IT professionals when addressing resources, e.g. Can an IT professional requested to correct an e-mail failure on the CEO’s laptop view sensitive data or manipulate it when they log on to that machine using their account?)

3. Non Profit Making – Humanitarian – How information access is handled on and off the field

Data collection

For each of the identified case study organisations above, there will be structured questionnaires and interviews towards selected personnel relevant to the research, e.g. IT manager, HR, system administrators, and data entry clerks. Also, random IT professionals who are not part of the organisations will be consulted through structured interview questionnaires for the purpose of improving the framework. Review of documents such as IT security policy will be used as well as observation.

SECTION 3: ETHICAL ISSUES

The UNISA Ethics Policy[1] applies to all members of staff, graduate and undergraduate students who are involved in research on or off the campuses of UNISA. In addition, any person not affiliated with UNISA who wishes to conduct research with UNISA students and/or staff is bound by the same ethics framework. Each member of the University community is responsible for implementing this Policy in relation to scholarly work with which she or he is associated and to avoid any activity which might be considered to be in violation of this Policy.

All students and members of staff must familiarise themselves with AND sign an undertaking to comply with the University's "Code of Conduct for Research" (the policy can be accessed at the following URL: http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf)

[1] The URL for this is: http://cm.unisa.ac.za/contents/departments/res_policies/docs/ResearchEthicsPolicy_apprvCounc_21Sept07.pdf

SECTION 4: FORMALISATION OF THE APPLICATION

APPLICANT **Chisanga Emmanuel**

I **Chisanga Emmanuel** have familiarised myself with the UNISA Ethics policy, the form completed and undertake to comply with it. I hereby declare the following with regard to my research project:

(1) No human participants are involved in my research project;
(2) No animals are involved in my research project;
(3) No personal data stored in any way is used for this project;
(4) No materials harmful to humans are in any way used in this project;
(5) No external parties or organisations are involved in this project;
(6) No external resources are needed for the project for which permission needs to be sought from any parties;
(7) The research is not supported by funding that is likely to inform or impact in any way on the design, outcome, and dissemination of the research.

The information supplied above is correct to the best of my knowledge. I have read the policy for research ethics of UNISA, and the contents of my application as presented to the CREC of CSET is a true and accurate reflection of the methodological and ethical implications of my proposed study. I shall carry out the study in strict accordance with the approved proposal and the ethics policy of Unisa. I shall maintain the confidentiality of all data collected from or about research participants, and maintain security procedures for the protection of privacy. I shall record the way in which the ethical guidelines as suggested in the proposal has been implemented in my research. I shall notify URERC in writing immediately if any change to the study is proposed or if any adverse event occurs or when injury or harm is experienced by the participants attributable to their participation in the study.

NB: PLEASE ENSURE THAT THE ATTACHED CHECK SHEET IS COMPLETED

SIGNATURE OF APPLICANT ……… …………… DATE …26-01-2016…..

SUPERVISOR/DIRECTOR OF SCHOOL

NB: PLEASE ENSURE THAT THE APPLICANT HAS COMPLETED THE ATTACHED CHECK SHEET AND THAT THE FORM IS FORWARDED TO YOUR COLLEGE RESEARCH COMMITTEE FOR FURTHER ATTENTION

DATE: …10-02-2016………………….

SIGNATURE OF SUPERVISOR/ PROJECT LEADER :___ ___

RECOMMENDATION OF COLLEGE RESEARCH AND ETHICS COMMITTEE

RECOMMENDATION OF SENATE RESEARCH AND ETHICS COMMITTEE

NAME OF CHAIRPERSON:________________________SIGNATURE____________________

DATE...

UNISA

CSET – CREC

ETHICAL CLEARANCE APPLICATION FORM

CHECK SHEET FOR APPLICATION

PLEASE TICK (✓)

1. Form has been fully completed and all questions have been answered	
2. Signature of Supervisor / project leader	
3. Application forwarded to College Research Committee for recommendation	

APPLICATION: UNISA ETHICS REVIEW COMMITTEE

GENERAL GUIDELINES

Two copies each in English of the following must be submitted to the ERC:

(i) Complete research proposal. The proposal which is submitted for scientific or technical review must be the same as that submitted for ethics review.

(ii) Completed application for review form.

(iii) Proposal summary sheet.

(iv) Documents related to the proposal.

APPLICATION (as per 10.2)

(i) Researchers' names, affiliations, addresses and contact numbers.

(ii) Organisation(s) or institution(s) involved in the study.

(iii) Sponsors or funders.

(iv) Other pertinent information such a conflict of interests. There is conflict of interest when the researcher has an interest in the research that may jeopardise his/her ability to undertake the research in a scientific and ethical manner.

PROPOSAL SUMMARY SHEET (as per 10.3)

(i) Title of the proposal.

(ii) List and definitions of acronyms and abbreviations.

(iii) Name(s) of principal investigator(s)/researcher(s). If this is a student, a letter of confirmation from Unisa must be included.

(iv) Names and addresses of all sponsor(s) or funder(s).

(v) Abstract of the proposal in nontechnical language.

(vi) Research objectives.

(vii) Anticipated outcomes.

(viii) Inclusion or exclusion criteria (if applicable).

(ix) Withdrawal or discontinuation criteria (if applicable).

(x) Methodology or research design.

(xi) Activity plan or timeline.

(xii) Safety procedures and criteria (if applicable).

(xiii) Description of procedure of reporting to Unisa Research Ethics Review Committee

(xiv) Description of how participants will be informed of the findings or results and consulted on potential or actual benefits of such findings or results to them and others.

(xv) Description of the risks of the procedures which participants may/will suffer (e.g. no

risk, discomfort, pain, stigmatisation, negative labelling/other potential risks) as well as the level of risk (as per paragraph 10.10).

Paragraph 10.10 stipulates the following:

10.10.1 It is the duty of reviewers to identify whether or not the research will involve vulnerable persons or groups and to ensure that adequate protective measures are provided for.

10.10.2 Special attention should be given to evaluating the risks of participants in relation to benefits.

10.10.3 Research can be classified on the basis of the degree of risk:

'Category 1' Research involving negligible or minimal risk

'Category 2' Research involving greater than minimal risk but presenting the prospect of direct benefit to participants

'Category 3' Research involving a minor increase in minimum risk and presenting no prospect of direct benefit to participants

'Category 4' Research that does not fit the above categories

10.10.4 While all research involving human subjects should be approved by an ERC and subjected to scrutiny, research involving reviews of administrative records which contain names of people may require a lower level of scrutiny, while research involving solely aggregated data and literature reviews needs the lowest scrutiny (if any).

PROPOSAL-RELATED DOCUMENTS (as per 10.4)

(i) Participant information sheet (if applicable).

(ii) Description of the process for obtaining informed consent.

(iii) Informed consent form in English and in the language of the potential participants.

The language should be understandable to a lay person.

(iv) Description and/or amounts of compensation including reimbursements, gifts or services to be provided to participants (if applicable).

(v) Description for arrangement for indemnity (if applicable.)

(vi) Description of any financial costs to participants (if applicable).

(vii) Description of provision of insurance coverage to participants (if applicable).

(viii) Description of steps to be undertaken in case of adverse event or when injury or harm is experienced by the participants attributable to their participation in the study.

(ix) Statement agreeing to comply with ethical principles set out in the Unisa Policy on

Research Ethics.

Applicant’s statement agreeing to comply with ethical principles set out in the Unisa policy on research ethics:

I …**Chisanga Emmanuel....** (Full names of applicant) declare that I have read the Policy on Research Ethics of Unisa and that the contents of my application as presented to URERC are a true and accurate reflection of the methodological and ethical implications of my proposed study. I shall carry out the study in strict accordance with the approved proposal and the Research Ethics Policy of Unisa. I shall maintain the confidentiality of all data collected from or about research participants, and maintain security procedures for the protection of privacy. I shall record the way in which the ethical guidelines as suggested in the proposal has been implemented in my research. I shall notify URERC in writing immediately if any change to the study is proposed or if any adverse event occurs or when injury or harm is experienced by the participants attributable to their participation in the study.

. ...

(Signature)................01-01-2016..

(Date)

(x) Disclosure of any previous ethics review action by other ethics review bodies (if applicable).

(xi) Research instruments such as questionnaires, interview guides and similar documents. (Indicate the language that will be used for questionnaires and interview guides. Where this is different from the language of the intended research participants/respondents, provide details on translation).

(xii) Research budget.

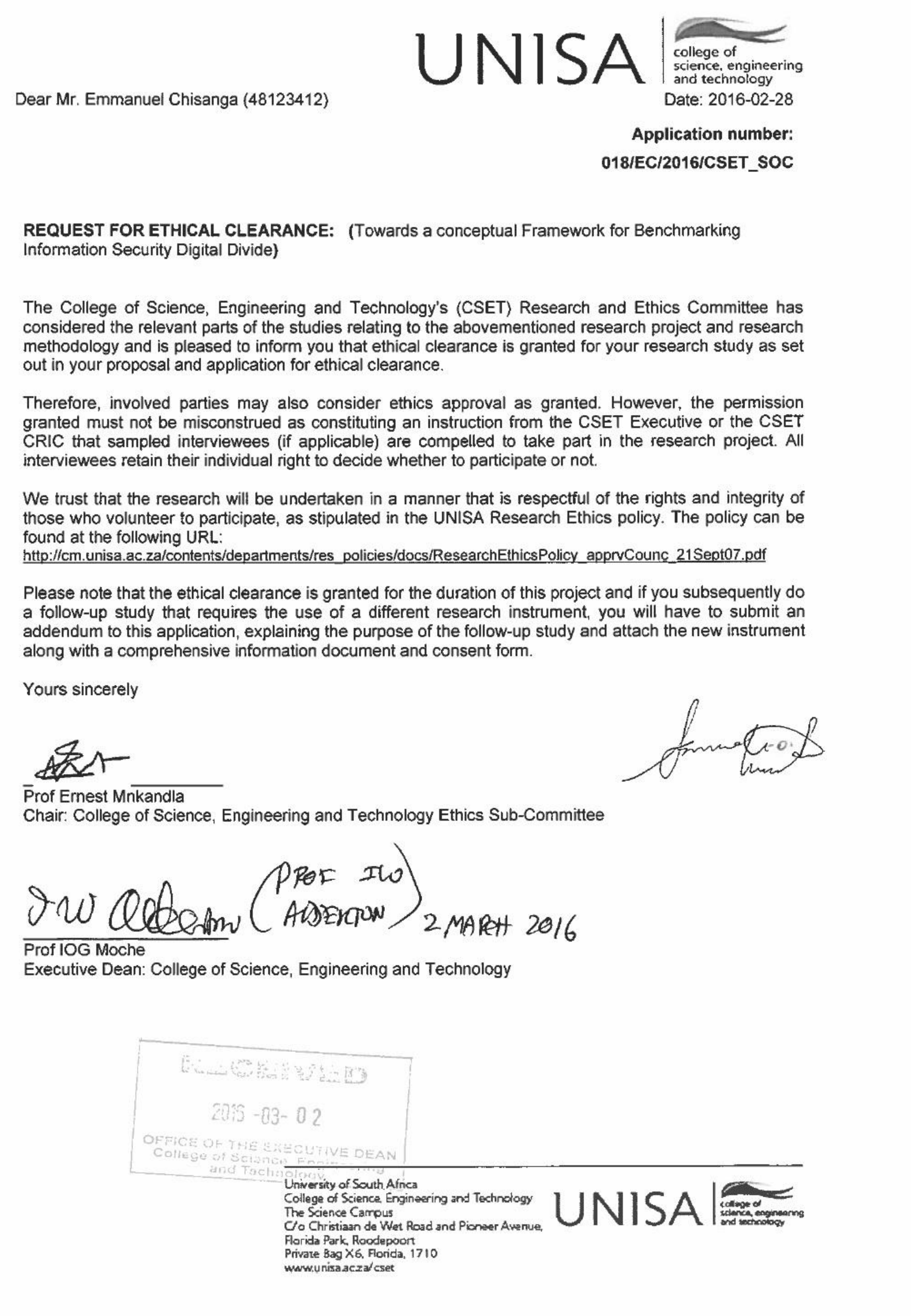
(xiii) Project agreement (e.g. MOA).

(xiv) CVs of principal investigators

(xv) Letter(s) of permission from relevant bodies. (If the research study involves

collaborative, multi-institutional or multi-country research, this must be explained in detail. See in this regard, paragraph 6 of the Unisa Policy on Research

Appendix B – Letter of Approval



UNISA college of science, engineering and technology

Dear Mr. Emmanuel Chisanga (48123412)

Date: 2016-02-28

Application number:
018/EC/2016/CSET_SOC

REQUEST FOR ETHICAL CLEARANCE: (Towards a conceptual Framework for Benchmarking Information Security Digital Divide)

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

IW Alderton (PROF IW ADDERTON) 2 MARCH 2016

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 C – Questionnaires

IS Expert Questions

5. Information Security Management

The main objective of this section is to assess the quality of information security digital divide (ISDD) framework by engaging with information ICT experts in the industry. The outcome of the analysis of these questions will help us define a broadly consensual framework for ISDD.

Section1: Demography

5.1.1 Which sector or industry do you represent?

Government □ Banking □ Information, Communication and Technology □
Manufacturing □ Not for Gain □ Other, please specify

…………………………………………………………………………………………….

5.1.2 Please inform us on years of experience in ICT and/or information security

Less than 2 □ 2-3 □ 3-5 □ 5-10 □ More than 10 □

5.1.3 Please indicate your occupation in the industry [tick off option]

Software developer □ System Analyst □ Chief Information security Officer □
IT manager □ Chief Information officer □ IT consultant □

System administrator □ Other, specify

…………………………………………………………………………………………….

Section 2 – Importance of Information Security to an Organisation

5.1.4 On a scale of 1 - 5, how critical is information security to the operations of an organisation? 1. Not critical □ 2. Slightly □ 3. Fairly □ 4.Critical □

5. Very critical □

5.1.5 The use of a security model in an organisation is mandatory?

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.6 Which of the listed options below are the most influential when managing information security? [You can select more than one option]

A clearly outlined security policy □ Management support □

A budget for IT □ An IT department with highly skilled staff □

Other, please specify

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

Section 3 – Information System Access Management

Please provide your assessment with the following statements and questions concerning access to information within an organisation.

5.1.7 The flow of information plays an important role in designing access control to information systems

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.8 The flow of reporting structures in an organisation must form part of the basis on which access control to systems should be designed

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.9 The structure of the organisation ought to be considered when assigning credentials to end-users

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.10 The degree of accessing information in an organisation depends on your role and its complexity

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.11 For external stakeholders who need services from the back-end office, through various access channels available, what do you think is the best authentication method to be followed?

Through front-office only □ Through Front, Middle and Back-end offices □

Through Middle and Back-end offices □ Directly through to the Backend □ All the above-listed options □ Other, please specify

……………………………………………………………………………………………

……………………………………………………………………………………………

5.1.12 Information Systems in an organisation should be accessed based on business roles

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.13 Personnel responsibilities must also be strongly considered when deciding access levels to an Information System

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.14 Should information systems in an organisation be accessed based on experience?

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.15 The more you are senior in an organisation, the more wide is your degree for accessing information

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.16 The more you are junior in an organisation, the more you are prevented from accessing information

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.17 Which of the options listed below are relevant when determining the ability of an individual to access information resources among employees in an organisation?

Roles □ Responsibilities □ Business function □ Position □ Seniority □ Experience □ Other, please specify

……………………………………………………………………………………………

……………………………………………………………………………………………

5.1.18 Is access control to Information Systems generally significant to business operations in your industry?

Strongly disagree □ Disagree □ Agree □ Strongly Agree □

5.1.19 For external end-users such as partners, suppliers, customers and other stakeholder that require access to a system mostly from outside, suggest which options are the most viable for accessing the system [Select all that apply]

Internet □ Remote Desktop Protocol (RDP) □ Telephone □

Face-to-face (F2F) □ VPN □ Others, specify ……………………………………………………………………………………………..

Section 4 – Policy Formation, Standard Practice and Compliance

5.1.20 An organisation must have a clearly defined access control mechanism to its systems. Based on this statement, which of the following must be enforced to that effect?

Standard security practice □ Enforce policy & regulation □

Role-based access control according to Hierarchy □ Security Training & Awareness □ Employee Self-assessment tool □ Other, please specify

………………………………………………………………………………………………

……………………………………………………………………………………………….

5.1.21 For internal Information System end-users or stakeholders, which of the access options below do you suggest are applicable? [Select all that apply]

Intranet □ Remote Desktop Protocol (RDP) □ Telephone □ Face-to-face (F2F) □ VPN Other, specify

……………………………………………………………………………………………..

5.1.22 Which security measures do you think are the most appropriate when accessing the system through the channels indicated below? [Tick the options]

	Security methods					
Access channel	**Authentication**	**Encryption**	**Antivirus Software**	**Access Card**	**Firewall**	**Policy & Regulation**
VPN						
Intranet						
Internet						
Telephone						
RDP						
F2F						

Other, specify

……………………………………………………………………………………………

……………………………………………………………………………………………

5.1.23 A system should be able to temporarily allow the work scope of a business role such as a middle manager or general staff to be upscaled or downscaled in an event where they require to perform a duty below or above their work scope?

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

Section 5 – Structure of an Organisation and Flow of Information

5.1.24 For a standard enterprise, the structure of the business function should compose of? [Tick off options]

Front-end office □ Middle office □ Back-end office □

Other, specify

……………………………………………………………………………………………

5.1.25 Suggest business roles which must be considered when planning ISDD management in an enterprise

CEO □ Upper management □ Lower management □ General staff □

IT support □ Other, specify

……………………………………………………………………………………………

5.1.26 Authentication to the system must be determined according to the business function end-user reports into and/or which parts of the system they wish to get a service from

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

5.1.27 Suggest the most commonly used front-end applications from the list below

Internal front-end applications □ Customer facing front-end applications □
Enterprise front-end applications □ Engineering and development applications □

Other, please specify
……………………………………………………………………………………..…………
……………………………………………………………………………………………..

5.1.28 From the list below, mark the most common software consumed as a service in your sector?

Enterprise resource planning (ERP) □ Enterprise Service Bus (ESB) □

Enterprise Integrated Bus (EIB) □ Other, please specify
…………………………………………………………………………………………………
…………………………………………………………………………………………………

5.1.29 On a scale of 1 – 5, how applicable is the core and context of this framework to your organisational environment?

1. Not applicable □ 2. Slightly □ 3. Moderately□ 4. Fairly □ 5. Very applicable □

5.1.30 Access to an Information System must be audited as a requirement to track and counteract security breach

Strongly disagree □ Disagree □ Agree □

Neutral □ Strongly Agree □

System End-user and other Stakeholders Questionnaire

ISDD General Staff Questionnaire

The purpose of this section is to assess the information security digital divide (ISDD) level of an organisation. To do so, we will identify a range of Information System end-users and stakeholders both internal and external

5.2 Information security digital divide among general staff

Section 1 – Demography

5.2.1 Please state your business role/or where you fall within the organisation

CEO □ Upper Management □ Middle Management □

Lower Management □ General staff □ IT □ Other, Please specify

………………………….…………………………………………………………………

5.2.2 State how long you have been in your current occupation at this organisation

Below 2 years □ 2-5 years □ 5-7 years □ 8-10 years □

Beyond 10 years □

5.2.3 Which business function do you report into? [Select all applicable options if possible] Front-end office □ Middle office □ Back-end office □ Other, please specify

…………………………………………………………………………………………………

Section 2 – Information System Access Management

5.2.4 Does your business role or position require you to access the system from outside the organisation, e.g. from home after hours or other places while you work?
Not at all □ Sometimes □ Occasionally □ All the time □

5.2.5 Does your business role or position require you to interact with external stakeholders such as suppliers, investors, customers or contractors, etc?

Not at all □ Sometimes □ All the time □ I am an external stakeholder □

5.2.6 Which access channel(s) do you use to access the system when you are outside the organisation? [Select all options that apply]

Internet □ VPN □ Remote Desktop Protocol (RDP) □ Telephone □

Face-to-Face (F2F) □ Other, please specify

…………………………………………………………………………………………

5.2.7 Which access channel(s) do you use to access the system when you are inside the organisation?

Internet □ VPN □ Remote Desktop Protocol (RDP) □ Telephone □

Intranet □ Face-to-Face (F2F) □ Other, please specify

…………………………………………………………………………………………

5.2.8 In accordance with the access channel(s) available to you, which authentication method do you use when accessing the system? [Tick or cross out applicable options]

	Authentication Method				**Other, Specify**
Access channel	**Password**	**Biometric (Fingerprint)**	**Interactive voice recognition**	**Smart card**	
VPN	Yes / No	Yes / No	Yes / No	Yes / No	
Internet	Yes / No	Yes / No	Yes / No	Yes / No	
Telephone	Yes / No	Yes / No	Yes / No	Yes / No	
RDP	Yes / No	Yes / No	Yes / No	Yes / No	
Intranet	Yes / No	Yes / No	Yes / No	Yes / No	

	Authentication Method				**Other, Specify**
F2F	Yes / No	Yes / No	Yes / No	Yes / No	

5.2.9 In your opinion, does the organisation's Information System limit your access to what is relevant for you to perform your duties?

Strongly Disagree □ Disagree □ Not sure □ Agree □

Strongly Agree □

5.2.10 I am not given the right access level to the system to freely go on with my work

Disagree □ Not sure □ Agree □

5.2.11 I am free to explore a lot of resources on the system including some items which are not relevant to my work scope

Strongly Disagree □ Disagree □ Neutral □ Agree □

Strongly Agree □

5.2.12 Do you know and understand the meaning of business functions in an organisation?

Not at all □ I have an idea □ It is unclear □ Strongly know □

5.2.13 Which physical access restriction method to information resources do you use in your business function?

Biometric (Fingerprint) □ Keys □ Access cards □ No restriction; it is an open office policy □ Other, please specify

……………………………………………………………………………………………………
……………………………………………………………………………………………………

Section 3 – Computer Skills, Security Awareness and Training

5.2.14 Do you have any formal computer literacy training?

Not at all □ Yes, by an accredited institution □ Yes, from inside, on-the-job training □ Other, please specify

……………………………………………………………………………………………….

……………………………………………………………………………………………….

5.2.15 Where would you rate your computer skill set level?

Beginner □ Intermediate □ Advanced □ Professional □

5.2.16 I fully understand the consequences of my actions while interacting with/or accessing the Information System

Strongly Disagree □ Disagree □ Not sure □ Agree □

Strongly Agree □

5.2.17 Have you ever received information security training and awareness within the organisation before, e.g. through presentation, lectures, etc?

Not at all □ Once □ Periodically □ Frequently □

It is a routine □

5.2.18 While working on your computer and you encounter a security incident that you think might compromise the security of the system such as a potential virus attack or irregular behaviour, what action do you take? [Select all that apply]

Do nothing □ Send an e-mail to IT and continue working □ Consult a friend □ Shut down the computer immediately and inform IT □ Other, specify

………………………………………………………………………………………………

………………………………………………………………………………………………

5.2.19 When being interviewed during the recruitment process, were you screened for your computer use skill set?

Yes □ No □ I don't remember □

Section 4 – Procedure and standard practice

5.2.20 In your organisation, where can you find Information System regulation regarding standard practice, access, and acceptable use?

Information security policy template □ Workplace policies and procedures □
Brochures provided by IT □ Job description □ Other, please specify

…………………………………………………………………………………………………
……………………………………………………………………………………………..

5.2.21 If there is a reference document present with information on system access, use and standard practice, in your opinion, is it comprehensively written to make it easy for you to understand and get guidance on how to use the system to reduce the risk of compromising it?

Strongly Disagree □ Disagree □ Neutral □ Agree □

Strongly Agree □

15.2.22 If you selected **strongly disagree** or **disagree** in the previous question (5.2.21), how would you prefer the security policy template to be written to make it easy to understand?

Less technical, using layman terms □ Less words more images □

More words less images □ Other, specify

…………………………………………………………………………………………………

15.2.23 Do you understand the need for standard practice and acceptable use when interacting with the system during your day-to-day activities?

Not at all □ Slightly □ Neutral □ I understand □

Strongly understand □

15.2.24 I have signed a non-disclosure agreement in this organisation

Disagree □ Not sure □ Agree □

Section 5 – Application Use and know-how

15.2.25 Which front-end application programs do you use the most in your business role? [Select options which apply]

Internal front-end applications □ Customer facing front-end applications □
Enterprise front-end applications□ Engineering and development applications □
Not sure □ I don't know □ Other, please specify

……………………………………………………………………………………………..…………

………………………………………………………………………………………………………..

15.2.26 I am able to view and access any website through the Internet from my computer

Disagree □ Sometimes □ Agree □

15.2.27 I can download and upload any content through the Internet from my computer and transfer to my colleagues easily

Disagree □ Sometimes □ Agree □

15.2.28 Do you use instant messaging applications such as Skype for business or social media?

Not at all □ Sometimes □ Occasionally □ Always □

It is part of my business role □

15.2.29 If you use instant messaging, are you able to interact with external contacts and also exchange documents and other data?

Not at all □ Sometimes □ Partially able □ Fully able □

15.2.30 Do you think your business role is empowered Information System-wise according to the organisational structure?

Strongly Disagree □ Disagree □ Neutral □ Agree □

Strongly Agree □

15.2.31 For what purpose do you access your organisation's Information System? [You can select more than one if necessary]

To attend to clients queries □ To provide service to external stakeholders □

To make an internal query with other departments □ To undertake my daily duties □ Instant messaging □ Social media □ Other, please specify

………………………………………………………………………………………………………
………………………………………………………………………………………………………

Section 6 – Culture of Protecting Information

15.2.32. On a scale of 1-5, what is your security awareness knowledge on the latest threat and risk trends such as viruses, spyware and hacking methods? [Circle option]

1. Very little □ 2. Little □ 3. Average □ 4. Good □ 5. Very good □

15.2.30. Do you know what the name of the antivirus your organisation is using?

Not at all □ I have an idea □ I know □

15.2.33. I know how to correctly use the antivirus to scan a computer and other external storage devices to ensure secure access during use

Strongly Disagree □ Disagree □ Neutral □ Agree □

Strongly Agree □

15.2.34. On a scale of 1-5, how concerned are you about information sharing, privacy, and protection according to your work scope?

1. Not concerned at all □ 2. Slightly □ 3. Average □ 4. Concerned □

5. Very concerned □

Appendix D – Informed Consent

for the Master’s study entitled:
Towards a Conceptual Framework for Benchmarking Information Security Digital Divide
Conducted by Chisanga Emmanuel in Namibia at three target organisations

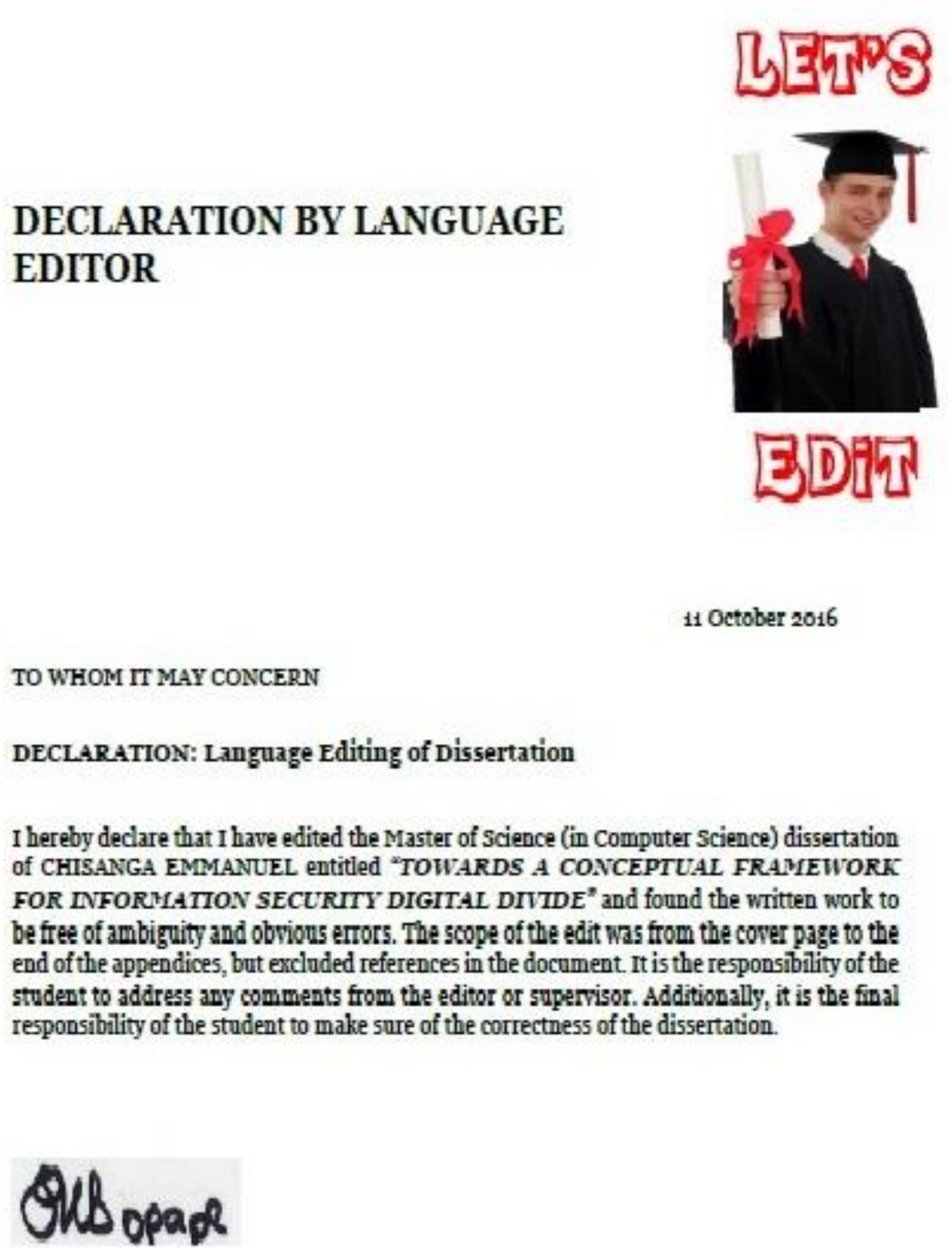
This study is conducted for the purposes of developing a self-appraisal framework for evaluation information access control within an information system and the general effectiveness of the system

I offer to take part in this information security research voluntarily
I understand that:

- ✓ My views and opinions will be recorded
- ✓ Data and information I share today will be handled confidentially and anonymously
- ✓ I can withdraw from this study at any time and have the information provided in my questionnaires removed in entirety from this study
- ✓ My personal data will be protected to the extent provided by law and all references to information about my data will be kept anonymous to the extent provided by law

Signature: ……………………………….
Name: Contact details (Cell Phone #) …………………………………………………..
(Please print*)*
Date:…………………………………

Appenidx E – Technical editing declaration



LET'S

EDiT

DECLARATION BY LANGUAGE EDITOR

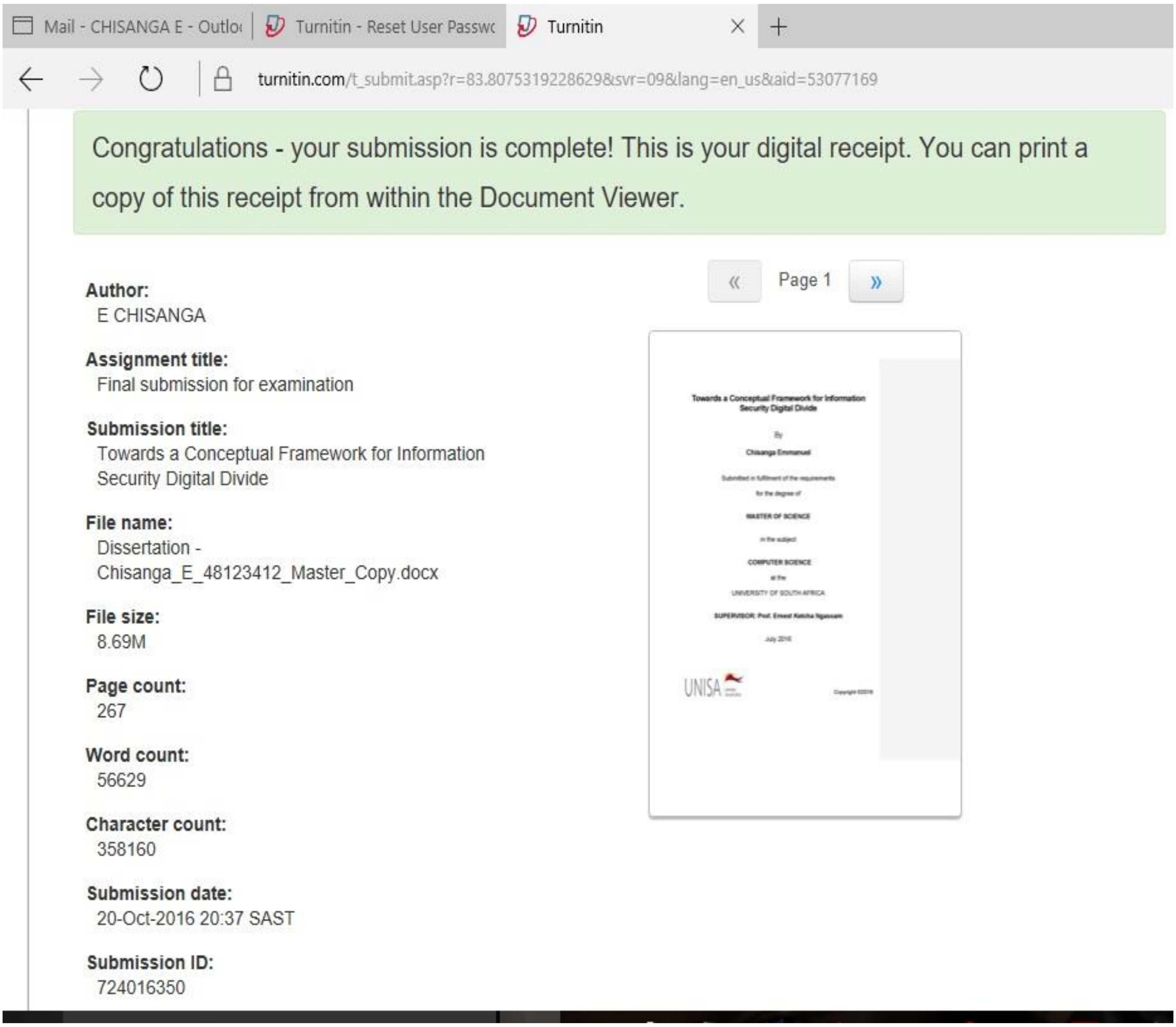
11 October 2016

TO WHOM IT MAY CONCERN

DECLARATION: Language Editing of Dissertation

I hereby declare that I have edited the Master of Science (in Computer Science) dissertation of CHISANGA EMMANUEL entitled *"TOWARDS A CONCEPTUAL FRAMEWORK FOR INFORMATION SECURITY DIGITAL DIVIDE"* and found the written work to be free of ambiguity and obvious errors. The scope of the edit was from the cover page to the end of the appendices, but excluded references in the document. It is the responsibility of the student to address any comments from the editor or supervisor. Additionally, it is the final responsibility of the student to make sure of the correctness of the dissertation.

Appendix F - Turn –it-in Digital Certificate


Mail - CHISANGA E - Outlo
Turnitin - Reset User Passwc
Turnitin
turnitin.com/t_submit.asp?r=83.8075319228629&svr=09&lang=en_us&aid=53077169
« Page 1 »

Congratulations - your submission is complete! This is your digital receipt. You can print a copy of this receipt from within the Document Viewer.

Author:
E CHISANGA

Assignment title:
Final submission for examination

Submission title:
Towards a Conceptual Framework for Information Security Digital Divide

File name:
Dissertation - Chisanga_E_48123412_Master_Copy.docx

File size:
8.69M

Page count:
267

Word count:
56629

Character count:
358160

Submission date:
20-Oct-2016 20:37 SAST

Submission ID:
724016350

Towards a Conceptual Framework for Information Security Digital Divide

By

Chisanga Emmanuel

Submitted in fulfilment of the requirements
for the degree of

MASTER OF SCIENCE

in the subject

COMPUTER SCIENCE

at the

UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: Prof. Ernest Ketcha Ngassam

July 2016

UNISA

Copyright ©2016

Appendix G - COBIT Information Technology Maturity Metrics

Phase	Awareness & Communication	Policies, Procedures & Standards	Tools & Automation	User Management	Responsibility and Accountability	Goal Setting and Measurement
1	Recognition of the need for process is eminent, and so is irregular communication of issues	Approach to process and practice is unstructured	Tools are present, but use is basic and limited to desktop tools. Tool use is not planned	Required skills for process are not identified. Training is non-existent	Accountability and responsibility are not defined. People rely on their own discretion	Goals are not clear, and no measurement takes place
2	There is acknowledgement for the need to act; thus, management communicates overall issues	While process may arise, it is mainly instinctive. Individual expertise creates informal policy and procedure understanding	Approach to use of tools is common but is centred on solutions developed by key individuals. Tools may be present but not used	Minimum skills are identified for critical areas. Training is reactive, not proactive, leading to on-the-job training	Pro-activeness exists. Individuals know their roles are held responsible even if there is no formal agreement. Accountability is confusing, leading to shift of blame	Some goals are set. Financial measures may be established but do not span the entire organisation. Monitoring may exist in a few areas

3	Communication by management is now organised because of the understanding of the need to act	Good conduct develops. Policies and process are documented and are processes of key activities	Tools are standardised to automate processes. There is use of tools but not in alignment with the plan	The need for skills is clear and documented. Training is planned but is not mandatory	Process responsibility and accountability are clear. Process owners are known and take ownership	Performance measurement is possible but poorly communicated. A link to business goals exists. Process measurement is present but inconsistent
4	There is understanding of the full requirements. Mature communication techniques are applied, and standard communication tools are in place	Process is complete and internal best practices are deployed. Documentation processes are advanced and supported by management	Implementation of tools is standard. Automated tools now manage, control, and monitor critical activities	Need for skill is routinely updated. Training techniques are applied according to plan. Knowledge is well shared	There is complete accountability for process, such that process owners are now able to execute their roles as a culture	Performance is measurable and communicated and linked to business objectives and IT strategic plan. Continuous improvement is emerging

5	Communication techniques, trends, and pro-activeness are at their ultimate best	External best practices and standards are commonplace. Processes, policies, and procedures are completely documented and recognised thoroughly	Standardised toolsets are used across the enterprise. Tools are fully integrated with other related tools to enable support of the process and continuous improvement of process	Knowledge sharing is now an enterprise culture. Continuous improvement of skills is primary through training and awareness to support external best practices used for guidance	Process owners are empowered to make decisions and take actions. Process management is strong and consistent throughout the enterprise	Performance is highly integrated and measureable, linking IT strongly to business goals. Continuous improvement is a part of the enterprise culture

Source: ISACA (2011)