Towards a Cybersecurity Skills Framework for South Africa

M. Kruger

2023

Towards a Cybersecurity Skills Framework for South Africa

by

Madri Kruger

Dissertation

Submitted in fulfilment of the requirements

for the degree

Master of Information Technology

in the

Faculty of Engineering, the Built Environment and Technology

of the

Nelson Mandela University

April 2023

Supervisor: Prof. Lynn Futcher

Co-supervisor: Prof. Kerry-Lynn Thomson

Permission to Submit

NELSON MANDELA UNIVERSITY

PERMISSION TO SUBMIT FINAL COPIES OF TREATISE/DISSERTATION/THESIS TO THE EXAMINATION OFFICE

Please type or complete in black ink

FACULTY: Faculty of Engineering, the Built Environment and Technology

SCHOOL/DEPARTMENT: School of Information Technology

I, (surname and initials of supervisor) Futcher L

and (surname and initials of co-supervisor) Thomson KL

the supervisor and co-supervisor respectively for (surname and initials of candidate) Kruger M

(student number) s216638305 a candidate for the (full description of qualification)

Master of Information Technology

with a treatise/dissertation/thesis entitled (full title of treatise/dissertation/thesis):

Towards a Cybersecurity Skills Framework for South Africa

It is hereby certified that the proposed amendments to the treatise/dissertation/thesis have been effected and that **permission is granted to the candidate to submit** the final bound copies of his/her treatise/dissertation/thesis to the examination office.

15/03/2023

SUPERVISOR **DATE**

And

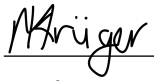
15/03/2023

CO-SUPERVISOR **DATE**

Declaration

I, Madri Kruger, hereby declare that:

- The work in this dissertation is my own work.
- All sources used or referred to have been documented and recognised.
- This dissertation has not been previously submitted in full or partial fulfilment of the requirements for an equivalent or higher qualification at any other recognised educational institute.



Madri Kruger

15/03/2023

Date

Abstract

Cybersecurity is an ever-growing area of concern both globally and in South Africa. The increasing number of cyberattacks daily has had a large effect on individuals, organisations, governments, and society at large. The growing need to combat cybercrime is accompanied by the increased need for skilled IT professionals to assist in protecting against cybercrime. Currently, there is a worldwide cybersecurity skills gap and a lack of IT professionals with the requisite cybersecurity skills. Many countries have developed their own taxonomies and common lexicons for IT and cybersecurity work, specifically for their context. This type of common lexicon is important to help assist in the development of skills. However, South Africa does not yet have its own cybersecurity skills framework to serve as a common lexicon for the South African context. Hence, the problem defined for this study is that, without a common lexicon of the cybersecurity knowledge, skills, abilities, and tasks (KSATs) required of IT professionals as they relate to specific IT job roles in South Africa, the cybersecurity skills gap cannot be sufficiently addressed. Such a lexicon could help drive the development of skills in South Africa and, in so doing assist in alleviating the cybersecurity skills gap. This study therefore presents a common lexicon by collecting job postings over a four-month period from 1 October 2020 to 31 January 2021. These job postings were analysed using a thematic content analysis. The results identified 20 common IT job roles, together with the specific KSATs relating to each job role identified. As a result, these job roles form part of a proposed cybersecurity skills framework for South Africa (CSFwSA) which could help and guide South Africa towards more targeted cybersecurity skills development. The proposed framework could also be useful in guiding tertiary educational facilities in the creation of cybersecurity curricula that represent the real-world expectations. This, in turn, could help South Africa to address the cybersecurity skills gap by better preparing IT professionals and ensuring that they are trained and skilled in cybersecurity.

Acknowledgements

First, I would like to express my gratitude towards my supervisors, Prof. Lynn Futcher and Prof. Kerry-Lynn Thomson for their continuous support, guidance, and sound advice during my master's studies. I do not believe it would have been possible to find better supervisors. Their constant motivation, enthusiasm and massive knowledge base has kept me motivated to complete this study.

I would also like to thank the Post Graduate Research Scholarship (PGRS) for funding my studies.

Lastly, I would like to thank my parents, my grandparents as well as my best friend, Michael de Jager, for their ongoing support during this journey. Without their care this would not have been possible.

Table of Contents

List of Tables

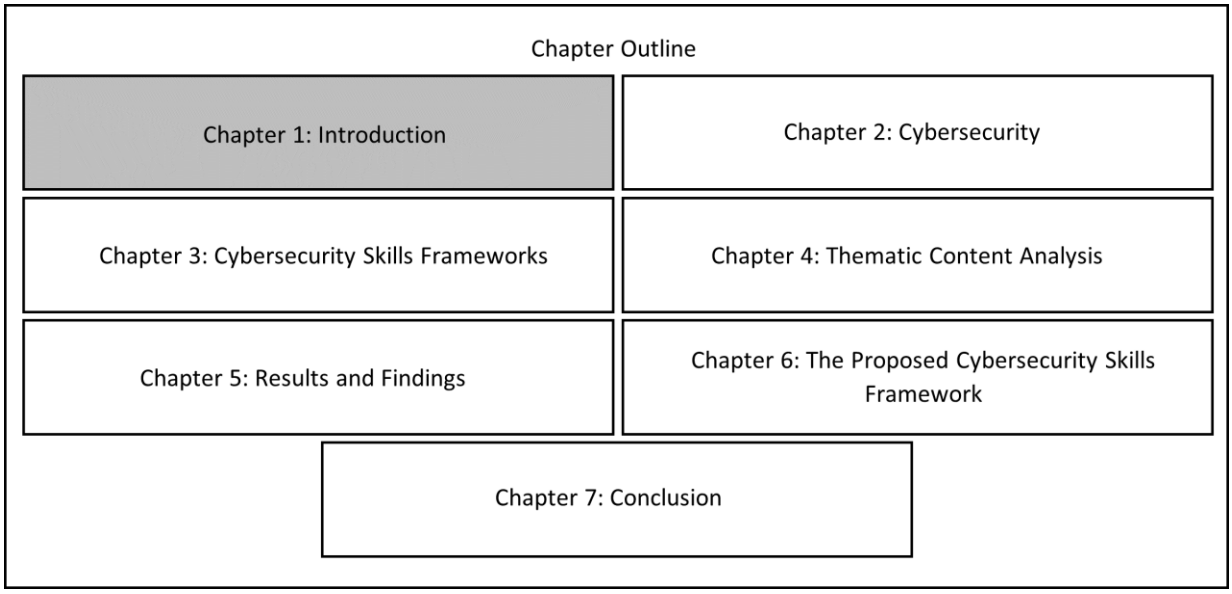
List of Figures

List of Abbreviations

ASD	Australian Signals Directorate
CCNA	Cisco Certified Network Associate
CEH	Certified Ethical Hacker
CEI	Cyber Exposure Index
CIA	Confidentiality, Integrity, and Availability
CIISEC	Chartered Institute of Information Security
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CS	Cybersecurity
CSA	Cybersecurity Agency of Singapore
CSFwSA	Cybersecurity Skills Framework for South Africa
CSIRT	Computer Security Incident Response Teams
CSJ	Cybersecurity Job
CSK	Cybersecurity Knowledge
CST	Cybersecurity Task
DA	Data and Artificial Intelligence
DAJ	Data and Artificial Intelligence Job
DAK	Data and Artificial Intelligence Knowledge
DAT	Data and Artificial Intelligence Task
DoS	Denial of Service
ECSF	European Cybersecurity Skills Framework
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EU	European Union
IMDA	Infocomm Media Development Authority
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KSAs	Knowledge, Skills and Abilities
KSATs	Knowledge, Skills, Abilities, and Tasks
MCSE	Microsoft Certified Solutions Expert
MI	Maharishi Institute
NCPF	National Cybersecurity Policy Framework
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NTA	Non-Technical Ability
NTS	Non-Technical Skill
OS	Operations and Support
OSJ	Operations and Support Job
OSK	Operations and Support Knowledge
OST	Operations and Support Task
POPIA	The Protection of Personal Information Act
PII	Personally Identifiable Information

QCA	Qualitative Comparative Analysis
SA	Software and Application Development
SAJ	Software and Applications Development Job
SAK	Software and Applications Development Knowledge
SAT	Software and Application Development Task
SFIA	Skills Framework for the Information Age
SFw for ICT	Skills Framework for Infocomm Technology
SG	Strategy and Governance
SGJ	Strategy and Governance Job
SGK	Strategy and Governance Knowledge
SGT	Strategy and Governance Task
SSG	Skills Future Singapore
TA	Technical Ability
TS	Technical Skill
UK	United Kingdom
USA	United States of America
WSG	Workforce Singapore
XSS	Cross-site Scripting

Chapter 1 - Introduction



1.1. Introduction

Ted Schlein, a leading investor in cybersecurity and enterprise technology, states: "*I firmly believe that there are only two kinds of companies in the world, those that have been breached and know it and those that have been breached and don't know it"* (Schlein, 2014). Cybersecurity is a crucial part of ensuring that data is kept confidential, has integrity and is available to those who have authorisation to access it.

This chapter provides a clear perspective of the necessity of cybersecurity skills and the current threats that all industries are facing in terms of cybercrime. The research problem has also been defined, together with the research objectives to address the identified problem. In addition, it highlights the research methods used to meet the research objectives and describes the research process of this study.

The structure of the chapter is as follows: Section 1.2 provides a brief overview, followed by a description of the problem area in Section 1.3. Thereafter, the problem statement is presented in Section 1.4, followed by the research objectives in Section 1.5. Section 1.6 delineates the study while Section 1.7 describes the research process followed during this study. Section 1.8 highlights the ethical considerations of the study and Section 1.9 provides a chapter outline. Section 1.10 concludes this chapter.

1.2. Brief Overview

According to Cisco (2021), cybersecurity is seen as the practice of defending systems, networks and programs from cyberattacks. Cybersecurity is important because without it our networks and devices would be vulnerable to attacks. There are many threats to cybersecurity, such as phishing, malware, trojans, ransomware, worms and Denial of Service attacks (DoS), amongst others (Tunggal, 2020). The personal information stored on devices like computers and mobile phones could be used for identity theft, financial gain, blackmail and for gaining access to highly confidential information. A large number of attacks rely on human error so that cyberattacks can be initiated. Human error is the cause of 95 percent of cybersecurity breaches (Usecure, 2019). Through advances in the technological tools used in information and network security, the large majority of threat detection and monitoring has been automated. However, some tasks cannot be automated and require human intervention to effectively secure information and networks (Parker & Brown, 2018).

Technology is developing rapidly and is being implemented in almost all aspects of human life. Cyberattacks are growing alongside this increase in technology usage. In the first six months of 2022, a total of 1980 breaches were reported globally (Risk Based Security, 2022). According to ISACA (2022), in 2022, 43 percent of employees globally indicated that they are experiencing more cyberattacks in their organisation than at the same time in 2021, with 36 percent having indicated that their organisation is experiencing the same number of attacks as in 2021. Furthermore, in 2022, it was estimated that globally, data breaches cost companies on average $4.35 million, which is an all-time high, with an overall increase of 2.6 percent compared to 2021 (IBM, 2022). Cybersecurity is the only line of defence against such cyberattacks and, based on the global statistics pertaining to cyberattacks, it is undeniable that cybersecurity should be a top priority for all organisations, government departments and society at large.

In 2015, Tamarkin (2015) stated that "*most African states are lagging behind in strengthening cybersecurity and fighting cybercrime; cybercriminals have recognised this vulnerability and are targeting the continent".* According to the Kaspersky laboratory, malware attacks in South Africa increased by 22 percent in the first quarter of 2019 compared to the same time in 2018. This equates to about 13842 attempted cyberattacks daily, or just over 9 attacks per second (Smith, 2019).

Furthermore, in 2020, the global Cyber Exposure Index ranked South Africa sixth on the list of most-targeted countries for cyberattacks (Cyber Exposure Index, 2020). Due to this growth in cyberattacks in South Africa, cybersecurity needs to grow in response to prevent such attacks.

In December 2015, the South African government approved a policy called the National Cybersecurity Policy Framework (NCPF), which is their attempt at protecting against cyberattacks. The NCPF states three objectives that have to be implemented for the policy to be successful, namely the establishment of a Cybersecurity Hub; the rolling out of a Cybersecurity Awareness Programme; and assisting in the development of Sector Computer Security Incident Response Teams (CSIRT). However, according to Gwala (2016), there have been multiple barriers identified that have made it difficult to implement the NCPF. Barriers were identified, such as the lack of catering for all South African languages in cybersecurity awareness programs, and the lack of skilled cybersecurity professionals for the Cybersecurity Hub, amongst others (Gwala, 2016).

1.3. Description of Problem Area

The growing cybersecurity needs globally are creating what is known as the cybersecurity skills gap. This means that there is a shortage of Information Technology (IT) professionals in the field of cybersecurity that have the required knowledge, skills and abilities (KSAs), as well as soft skills, to effectively fill the growing need for cybersecurity professionals. According to Oltsik (2020), 20 percent of employers globally reported that their organisation has been negatively impacted by the cybersecurity skills shortage, and 93 percent of employees believe the skills shortage has either stayed the same or become worse in the last few years.

Annually ISACA conducts survey to better understand the current state of cybersecurity globally. According to ISACA (2022), 63 percent of their respondents stated that they have unfilled cybersecurity positions in their organisations, which is an 8 percent increase from 2021. The study also indicated that 30 percent of positions within organisations take between 3 to 6 months to fill, with 29 percent of positions taking longer than 6 months to fill. Technically skilled cybersecurity professionals are hard to find, thus contributing to the struggle to fill open cybersecurity positions.

According to Burning Glass Technologies (2019), the number of cybersecurity job postings globally had grown 94 percent since 2013. Although IT jobs can be acquired without the need for extensive training, cybersecurity requires specific KSAs, some of which can only be gained through specialised training.

There are several different types of certifications that a cybersecurity professional can obtain, such as Certified Information Systems Security Professional (CISSP), CompTIA Security+ and Certified Ethical Hacker (CEH), to name just a few. All of these certifications have different purposes in industry, and all of them are recognised globally. When taking into consideration that, in order to apply for a CISSP certification, applicants require at least five years of relevant experience, one can understand why there is such a dire need for skilled and trained cybersecurity employees (Burning Glass Technologies, 2019). Due to these high education and experience requirements for cybersecurity jobs, the cybersecurity skills gap will not be addressed easily in the near future. Burning Glass Technologies (2019) states, that although cybersecurity is considered a specialist area, most of the people practising cybersecurity in the workplace are not cybersecurity specialists. Some IT job roles, such as a Network Administrator, have tasks associated with the job role that are considered cybersecurity-related. These types of IT job roles make up 56 percent of all cybersecurity-related job postings (Burning Glass Technologies, 2019). With this in mind, this research considers cybersecurity knowledge, skills and abilities as essential to all IT professionals.

South Africa has also been affected by the worldwide shortage of cybersecurity skills. In 2019, Communications Deputy Minister, Pinky Kekana, indicated that cybersecurity skills are not in abundance across the world, let alone in South Africa (Rogers, 2019). Professor Elmarie Bierman from the Cyber Security Institute stated that there is a lack of cost-effective local cybersecurity training being offered to South Africans (Doyle, 2016). Most cybersecurity courses are offered by international organisations and this is often too expensive for most South Africans, due to them being billed in US dollars (Doyle, 2016). In recent years, there have been various attempts to provide South Africans with cost-effective cybersecurity training. For example, one of South Africa's largest banks, Absa, collaborated with the Maharishi Institute (MI), to set up the Absa Cybersecurity Academy as an attempt to address South Africa's cybersecurity skills shortage (Bucchianeri, 2019). This programme is aimed at empowering marginalised South African youth, who would otherwise not have had access to a tertiary education. The students who participate

in the programme become certified cybersecurity analysts. The programme offers students accredited cybersecurity training and bridging courses. It also includes financial support, including bursaries and work experience at MI's call centres. In order to effectively address the cybersecurity skills gap in South Africa, many more such programmes will be needed in the future.

An earlier study conducted by Kortjan (2013) investigated developed countries, including the United States of America (USA), the United Kingdom (UK), Australia, and Canada, and their respective cybersecurity policies as they relate to cybersecurity education, training and awareness. Kortjan (2013) concluded that the rationale behind pursuing cybersecurity education, training and awareness varies from country to country, and that it can be argued that each country should consider cybersecurity education, training and awareness in its own context.

The National Institute of Standards and Technology (NIST), a United States-based institute, has developed the National Initiative for Cybersecurity Education (NICE) framework. The NICE framework attempts to create a better understanding of what cybersecurity positions entail and what knowledge, skills, and abilities (KSAs) are needed to complete certain tasks based on job roles. This is a useful tool for organisations seeking guidance on their cybersecurity workforce development. Frameworks such as NICE are important in terms of creating a taxonomy and common lexicon for individuals, businesses and training providers (Skills Future, 2016). These types of frameworks aid in the standardisation of KSATs and the development of training programmes and, as such, play an important role in skills development (Skills Future, 2016). However, it was stated at a recent NIST webinar that the NICE framework is good at defining job descriptions, but due to there being over 1600 KSAs and more than 50 job roles, it is rather unmanageable; also some KSAs are vague and not well defined (NIST, 2020). The NICE framework is considered to be overly complicated in certain aspects and therefore could be improved upon (NIST, 2020). Furthermore, in November 2020 a revision of the NICE framework was developed and released. This revision had some changes to the overall layout of the NICE framework including a shift from KSAs to Tasks, Knowledge and Skills (TKS)(Petersen et al., 2020). However, this study chose to remain focused on KSATs as per the earlier version of the NICE framework as the thematic content analysis started prior to the 2020 revision.

When investigating frameworks such as the NICE framework that uses KSAs to define tasks related to certain job roles, it is clear that cybersecurity professionals should have certain skills, knowledge, and abilities to effectively protect against cyberattacks. Just as cybersecurity professionals have a need for certain KSAs in order to work effectively, it is argued that cybersecurity KSAs are required to some extent by all IT professionals. In South Africa, it is important to understand what IT job roles require in terms of KSATs, in the same way that the NICE framework was established for this purpose in the USA.

Lacking in robust cybersecurity measures, laws and regulations, South Africa currently is one of the largest targets for hackers and cyber terrorists. Furthermore, many IT job postings in South Africa neglect to explicitly state the requirements for cybersecurity KSATs to sufficiently implement the security measures required to protect South African organisations from cyberattacks.

There is very little academic research regarding the cybersecurity skills gap in South Africa. However, a fairly recent study by Parker and Brown (2018) provides some insight into various cybersecurity jobs advertised in South Africa, together with the typical skills required by such cybersecurity professionals. Parker and Brown (2018) consider their work as an initial exploratory study that can be used as the basis for more specific studies in the future.

The lack of research in this area indicates an opportunity for more research into the South African cybersecurity skills gap, and the need for a taxonomy and common lexicon within the South African context.

1.4. Problem Statement

Based on the discussion in Section 1.3, the problem identified for this study is as follows:

Without a common lexicon of the cybersecurity knowledge, skills, abilities, and tasks (KSATs) required of IT professionals, as they relate to specific IT job roles in South Africa, the cybersecurity skills gap cannot be sufficiently addressed.

1.5. Research Objectives

In order to address the identified problem, the following primary research objective was established:

- **PRO:** To develop a cybersecurity skills framework by determining the cybersecurity knowledge, skills, abilities, and tasks (KSATs) required for specific IT job roles in South Africa.

For the purpose of achieving the primary objective of this study, the following secondary objectives were identified:

- **SRO1:** To position the cybersecurity threat landscape as it relates to the cybersecurity skills gap both globally and in South Africa.
- **SRO2:** To compare existing global cybersecurity skills frameworks according to their key characteristics.
- **SRO3:** To determine the cybersecurity KSATs required of IT professionals within South Africa, and how they relate to specific IT job roles.

1.6. Delineation

This study proposes a cybersecurity skills framework specifically for IT professionals in the South African context.

1.7. Research Process

Creswell (2018) stated that research designs provide specific direction for procedures in a research study. As such, research design can be seen as an overall strategy or framework for the research process and includes the procedure of carrying out certain tasks/methods to achieve the research objectives of the study (Somasundaram, 2022). Research design dictates the value of the conclusions from the research objectives and their respective outcomes (Bordens & Abbot, 2017).

According to Creswell (2014), qualitative research involves emerging questions and procedures, where data analysis builds inductively from particulars to general themes, with the researcher making interpretations of the meaning of the data or general themes. Qualitative research typically follows a subjective type of reasoning and, as such, often makes use of induction.

However, there are cases where qualitative research follows a deductive approach. Sarker et al. (2018), for example, demonstrate that qualitative research can be both inductive and deductive. Quantitative research, on the other hand, is a technique for putting theories about the relationships between variables to the test. To enable analysis of numbered data, these variables can be measured, often using instruments (Creswell, 2014). In contrast to qualitative research, quantitative research most often makes use of a deductive approach, but similarly to qualitative research, quantitative research can also be inductive. This is the case with a study by Iivari and Huisman (2007).

Qualitative research typically focuses on textual, visual or audio-based data (Phair & Warren, 2021). Hence, this study can be seen as qualitative due to the use of textual data in the form of job postings that were collected from LinkedIn. Along with the qualitative research comes the inductive approach used in this study. Induction generally requires critical thinking/reasoning which most often aligns with qualitative research (Burney & Saleem, 2008). This study developed the proposed framework through an inductive approach using literature reviews, critical reasoning and a thematic content analysis of job postings collected over a four-month period.

Figure 1.1 shows the research process, highlighting the research objectives to address the identified problem statement. In addition, it indicates the research methods employed in achieving each of the objectives and the associated outputs.

The research process started with the identification of the problem statement for this study. In order to address the problem identified, a Primary Research Objective (PRO) and three Secondary Research Objectives (SROs) were determined.

SRO1's aims to position cybersecurity in terms of the cybersecurity threat landscape as it relates to the cybersecurity skills gap both globally and in South Africa. SRO2 deals with the existing cybersecurity skills frameworks found globally and compares them to one another in terms of their key characteristics such as the target audience, KSATs, job roles and focus. Both SRO1 and SRO2 were achieved through a literature review.

Researchers undertake literature reviews for numerous reasons, including to determine what has and what has not been investigated to date, to identify possible data sources that others

have used for similar topics, or to provide evidence that could help to support one's own findings.

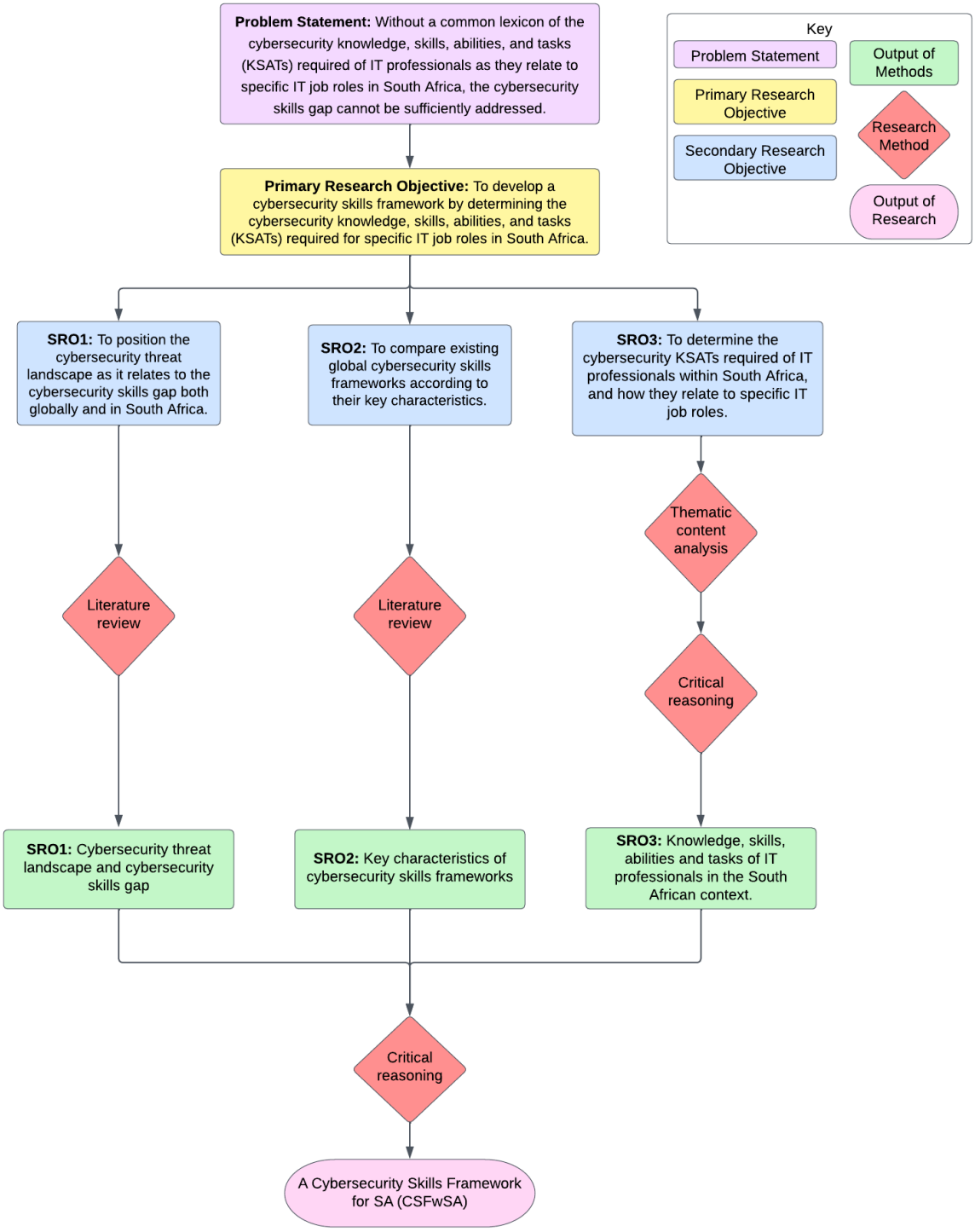


Figure 1.1: Research Process Overview

Walliman (2011) states that "*a literature review is to go through all the available information sources in order to track down the latest knowledge, and to assess it for relevance, quality, controversy and gaps*".

Various search engines were used to gather literature relating to this study, including Google, Google Scholar, IEEE, and Science Direct. SRO1 made use of all of the above mentioned search engines. Some examples of the search terms used for this objective included 'Cybersecurity', 'Cybersecurity skills gap', 'Cybersecurity threats' and 'Cybersecurity statistics'. SRO2 primarily made use of Google and Google Scholar, and some examples of the terms used to search for cybersecurity skills frameworks included 'Cybersecurity skills frameworks' and 'Most used cybersecurity skills frameworks globally'.

Upon completion of the literature reviews for both SRO1 and SRO2, the output of both research objectives was achieved. The output for SRO1 is the cybersecurity threat landscape and cybersecurity skills gap (Chapter 2), while the output of SRO2 is the key characteristics of various cybersecurity skills frameworks identified as relevant to this study (Chapter 3).

SRO3 aims to determine the cybersecurity KSATs required of IT professionals within South Africa, and how they relate to specific IT job roles. This was achieved by the collection of job postings from a popular job posting website named LinkedIn. These job postings were analysed through a thematic content analysis using the software tool called ATLAS.ti.

A thematic content analysis is a research method used to identify patterns in a set of data (Luo, 2019). A researcher will collect data either as written text, orally or visually. This can be via books, newspapers, speeches, interviews, web pages or even photos or films. Content can be both qualitative and quantitative. The researcher typically 'codes' words, themes or concepts within the data and analyses the results (Luo, 2019). This approach has been used in many studies in many different areas of research. For example, Meyer (2019) made use of a thematic content analysis of job postings related to Data Scientists; Li (2021) conducted a thematic content analysis on job postings to identify in-demand qualifications and competencies for translation curricula; and a study by Brannon et al. (2022) also used a thematic content analysis of job postings to identify the roles and responsibilities of Cataloging Managers.

This study comprised of multiple steps in the data collection and analysis process, as presented in Figure 1.2. The three-phased approach to the thematic content analysis was adapted from the three-phased approach identified by Soratto et al. (2020).

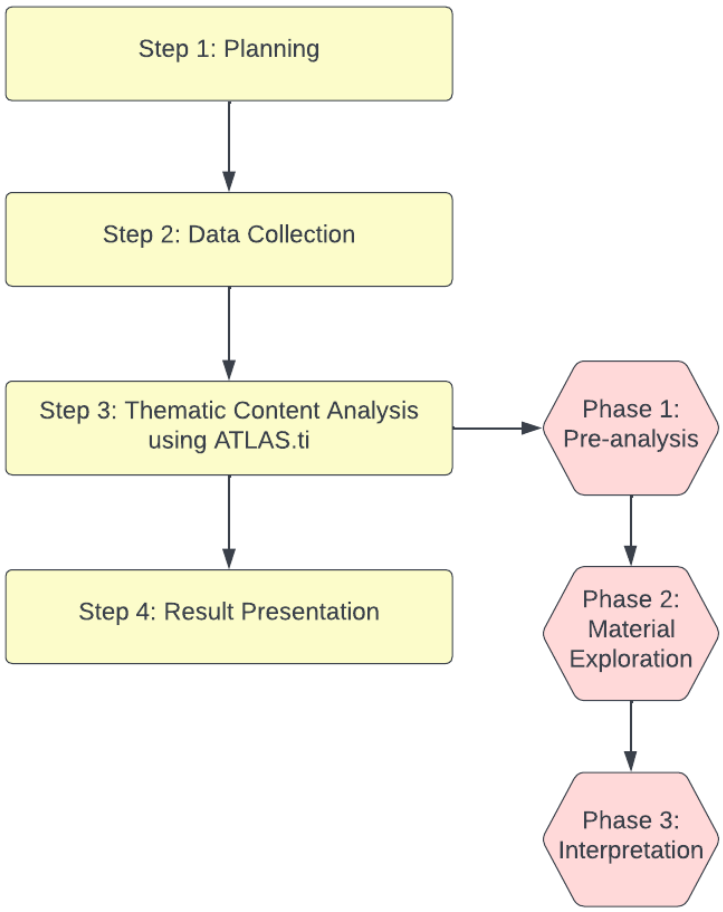


Figure 1.2: Data Collection and Analysis Process

During **Step 1**, a data collection pilot study was conducted. This pilot study was conducted for a month in September of 2020. During this time job postings were collected from three job posting websites namely, LinkedIn, Careers24 and Career Junction. The search term used on all three websites was 'Information Technology' and the results from this search term were filtered by week. A detailed discussion of the pilot study can be found in Chapter 4, Section 4.4.1. During this planning step, an investigation was also conducted into possible software tools to use for the data analysis. Various software analysis tools were identified and compared based on specific features, including:

- NVivo
- ATLAS.ti
- Provalis Research Text Analytics Software

- Quirkos
- MAXQDA
- Dedoose

After the comparison of these software analysis tools, ATLAS.ti was identified as the most appropriate one to use for this study, as it had all of the required features needed for the thematic content analysis. The detailed comparison can be found in Chapter 4, Section 4.3, Table 4.1.

After the month-long pilot study, **Step 2** followed where the actual data collection took place over a four-month period from the beginning of October 2020 until the end of January 2021. Various changes to the data collection process were made based on the results of the pilot study conducted. Instead of using three job posting websites, it was decided to only make use of LinkedIn. This was due to LinkedIn including most of the IT job postings on the other two websites, in addition to its own unique postings. Furthermore, instead of only using the single search term 'Information Technology', it was decided to broaden the range of search terms to include Computer Science, Information security, Cybersecurity/Cyber security, and Network security. In total 313 job postings were collected over the four-month period.

Step 3 followed the data collection phase, where ATLAS.ti was used as the data analysis tool for the thematic content analysis. The thematic content analysis made use of a three-phased approach, as shown in Figure 1.2. It started with the *pre-analysis* phase, where the job postings collected were added to ATLAS.ti in their respective word documents and grouped according to the week and month of collection. The second phase, *material exploration* was then started. During this phase the IT job postings were coded, and each code was categorised and grouped. In total, this phase identified 552 codes. In the final phase, *interpretation,* each IT job role that was coded was individually assessed, according to their associated knowledge, skills, abilities, tasks (KSATs) together with the required certifications which were all noted in a comment associated with the specific IT job role. To determine whether the identified IT job roles were similar, KSATs were compared. With the completion of this phase, the thematic content analysis was finalised. A more detailed discussion regarding the thematic content analysis can be found in Chapter 4, Section 4.5.

Step 4 presented the results of the thematic content analysis which were derived by using critical reasoning. Critical reasoning is a deeper kind of thinking in which a researcher must analyse and evaluate what they read, hear, say or write (Monash University, 2019). It seeks to identify reliable information and to make reliable judgements based on the information. Critical reasoning can be used to prove a point if it is backed up with credible data and statements to support the point. Through critical reasoning, the KSATs for 20 IT job roles were identified and, in so doing, completing the output of SRO3. These KSATs are detailed in Chapter 5.

Upon completion of the secondary research objectives, the outputs of each of the objectives were used, along with critical reasoning, to complete the PRO of this research study which was to develop a Cybersecurity Skills Framework for South Africa (CSFwSA), as presented in Chapter 6. The output of SR01 was used to better understand the current threat landscape both globally and in South Africa, as well as understanding the cybersecurity skills gap and how a cybersecurity skills framework can help to alleviate the current cybersecurity skills gap in South Africa. The output of SRO2 was used to better understand the existing cybersecurity skills frameworks globally, which helped to inform the structure of the proposed cybersecurity skills framework for the South African context. The output of SRO3 was a list of KSATs relating to specific IT job roles that was used to develop the proposed cybersecurity skills framework for the South African context. Achieving the secondary objectives allowed for the understanding of the context, structure and required KSATs to achieve the PRO.

1.8. Ethical Considerations

This study did not require ethical clearance since it used readily available data found online via a popular global employment website called LinkedIn.

1.9. Chapter Outline

Table 1.1 presents the chapter outline of this dissertation, providing a brief description of the seven chapters comprising this document.

Table 1.1: Chapter Outline

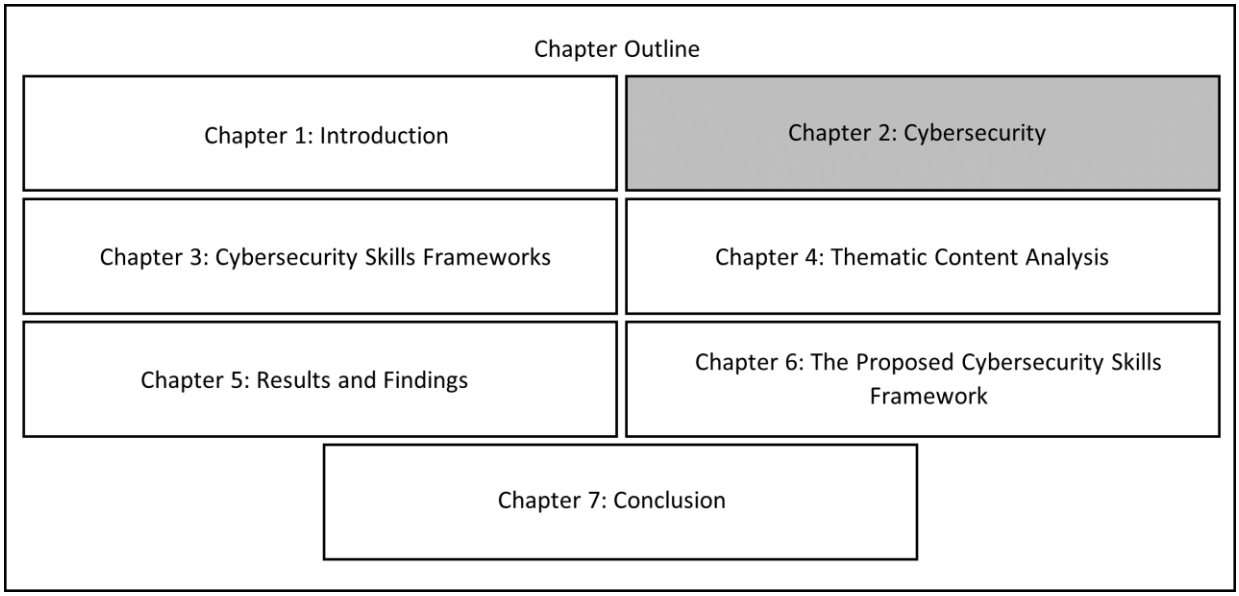
Chapter	Description
Chapter 1: Introduction	The purpose of this chapter is to introduce the research problem, research questions and objectives for this study. The research process is discussed as well as the ethical considerations and delineation of the study.
Chapter 2: Cybersecurity	This chapter focuses on cybersecurity: what cybersecurity is, the cybersecurity skills gap as well as the importance of these topics both globally and in the context of South Africa. This chapter positions the cybersecurity threat landscape as it relates to the cybersecurity skills gap.
Chapter 3: Cybersecurity Skills Frameworks	This chapter introduces various skills frameworks that are currently in development or used globally. It highlights how the identified skills frameworks compare to one another in terms of focus, usage, and KSATs. These key characteristics are used to inform the proposed framework.
Chapter 4: Thematic Content Analysis	The purpose of this chapter is to define and describe the process followed in conducting the thematic content analysis, detailing specifically the data collection process and the thematic content analysis based on the three-phased approach.
Chapter 5: Results and Findings	This chapter focuses on the results and findings of the thematic content analysis discussed in Chapter 4, by providing a detailed discussion of the results. The interpretation of the results are also discussed in this chapter.
Chapter 6: The Proposed Cybersecurity Skills Framework	This chapter details the structure of the proposed framework as well as its alignment with the Skills Framework for Infocomm Technology. Furthermore, the proposed framework is contextualised, and the potential role of this proposed framework is highlighted.
Chapter 7: Conclusion	This chapter concludes this dissertation and presents the contribution of this research, namely the proposed Cybersecurity Skills Framework for South Africa (CSFwSA), the achievement of the research objectives, the limitations of the study, proposed future research and the publication associated with this study.

1.10. Conclusion

The research area and research problem were introduced in this chapter, which led to the identification of a set of objectives that must be satisfied in order for the research problem to be addressed. Furthermore, this chapter provides an overview of the research process and the research methods used to meet the defined objectives. Three secondary objectives have been identified and, as such, the achievement of these secondary objectives will follow in the coming chapters.

Chapter 2 positions cybersecurity by discussing the threats that are prevalent globally as well as in South Africa. This is important when considering the cybersecurity skills required to protect organisations from such threats.

Chapter 2 – Cybersecurity



2.1. Introduction

Chapter 1 introduced the problem area, as well as the research objectives and overall aim of this study. This chapter focuses on cybersecurity: what cybersecurity is, and why it is important both globally but also specifically in the context of South Africa. The chapter helps to provide an understanding of the cybersecurity landscape that individuals and organisations face every day.

The structure of this chapter is as follows: Section 2.2 positions cybersecurity, while Section 2.3 details cyber threats and vulnerabilities. Section 2.4 highlights the prevalence of cyberattacks globally followed by Section 2.5 detailing the prevalence of cyberattacks in South Africa. Section 2.6 discusses South African Laws and Regulations as they relate to cybersecurity, followed by Section 2.7, which covers the McCumber model and how cybersecurity skills are required to mitigate cyberattacks. Section 2.8 focuses on the impact of the cybersecurity skills gap both globally and in South Africa, leading into Section 2.9 with the discussion of Cybersecurity Education, Training and Awareness. The conclusion to this chapter is provided in Section 2.10.

2.2. Positioning Cybersecurity

Concerns about cybersecurity are rising globally, driven by headlines of increasingly big data breaches and a scarcity of qualified cybersecurity personnel (Van Niekerk, 2017). To attempt to address cybersecurity issues found worldwide, it is important to understand the cybersecurity landscape. Without knowledge of the cybersecurity landscape, one cannot effectively address the cybersecurity issues that are arising.

The author of the Cybersecurity Body of Knowledge, Abu-Taieh (2018), defines cybersecurity as the protection of information systems, including the data on such information systems, against unauthorised access, harm, or misuse via the system operator, intentionally, accidentally, or through not following security procedures. Cisco (2021) defines cybersecurity more succinctly as "*the practice of protecting systems, networks, and programs from digital attacks*". The definition provided by Abu-Taieh (2018) is more focused on the protection of information systems, compared to the definition by Cisco (2021), which states that cybersecurity is more than just the protection of Information systems, as the protection of networks and programs are also relevant when considering cybersecurity.

The International Organisation for Standardization (ISO) is a globally recognised body that develops and publishes worldwide standards. According to the ISO (2012), cybersecurity relies on Information Security, Application Security, Network Security, and Internet Security to effectively protect devices connected to cyberspace from attack. The International Organization for Standardization ISO (2012) defines these security domains as follows:

- **Information Security** sets out to ensure the confidentiality, integrity, and availability (CIA) of information;
- **Application Security** is the protection of applications by applying certain controls and measures to manage the risk of applications in use by the general public, as well as by organisations;
- **Network Security** is concerned with the design, implementation, and operation of networks to protect information within and between organisations and users; and

- **Internet Security** protects all internet-related services and functions as an extension of Network Security in organisations and at home. Internet security also aims to ensure that internet services are available and reliable.

Figure 2.1 shows the relationship between cybersecurity and these security domains as critical building blocks of cybersecurity. These all need to co-exist to ensure the protection of the Critical Information Infrastructure (CII), such as telecommunications network infrastructure. If not properly managed, any of these security domains could lead to the unavailability of services which, in turn, could have a direct negative impact on national security.

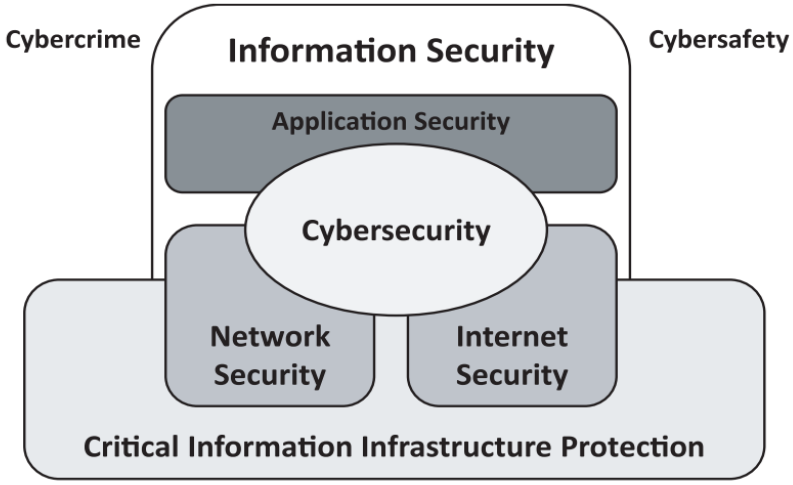


Figure 2.1: Relationship between Cybersecurity and other Security Domains (ISO, 2012)

Cybersecurity has a unique scope that necessitates active participation from various stakeholders in order to preserve and increase the reliability of cyberspace (ISO, 2012). Even though these security domains are interrelated, the focus of this study is specifically on cybersecurity.

Cybersecurity is important for preventing and protecting against a wide range of cyber threats and cybercrimes, including identity theft, financial fraud or theft and political hacktivism. According to the Joint Task Force on Cybersecurity Education (2017) "*the growing threat of cyberattacks has made governments and companies more aware of the need to defend the computerised control systems of utilities and other critical infrastructure.*"

Often these cyberattacks are intended to inflict damage or to harm a business or a person's reputation. Theft of valuable data can also be used as a means of financial gain, since this

information can be sold on the dark web for substantial amounts of money. Nobody is immune to cyberattacks due to them targeting individuals, groups, organisations, and governments (Symanovich, 2020).

2.3. Cyber Threats and Vulnerabilities

According to Hewitt (2021), a cybersecurity vulnerability is a flaw in an organisation's information systems of which cyber terrorists can take advantage. Ross et al. (2018), in a NIST special publication, states more broadly that a cybersecurity vulnerability is a weakness in a system, system security procedure, internal control, or implementation that could be exploited or triggered by a threat. Cyber terrorists can use these flaws and weaknesses to gain access to information systems and to collect data. Cyber vulnerabilities are rarely triggered by the acts of cybercriminals; instead, they are frequently caused by operating system faults or network misconfigurations. There are many different types of cybersecurity vulnerabilities (Hewitt, 2021), including:

- **System misconfigurations:** These occur because of network assets having vulnerable settings, for example, a router using the default usernames and passwords.
- **Unpatched software:** Older or unpatched versions of software may contain security vulnerabilities that can be exploited by cybercriminals; software updates contain security fixes where vulnerabilities have been identified.
- **Malicious insider threats:** Employees with access to vital systems can disclose information that allows cybercriminals to enter a network. Insider threats are difficult to detect because all actions taken by employees will appear genuine, raising few to no red flags.
- **Weak authorisation credentials:** Cybercriminals can brute force their way into a network by guessing employee credentials. Employees must be educated on cybersecurity best practices for their login information not to be misused easily, for example, passwords that are too simple, such as ‘12345’.
- **Poor data encryption:** Poor encryption of critical information can aid cybercriminals in accessing systems, for example, databases with no encryption on passwords.
- **Zero-day vulnerabilities:** Specific software vulnerabilities that are known to the attacker but have not yet been uncovered by an organisation are known as zero-day threats. To

reduce the risk of a zero-day attack, it is critical to stay vigilant and to monitor systems constantly for vulnerabilities.

Just as there are many vulnerabilities, there are many different types of cyber threats, each of which has different methods of execution, and each requires different means of protection and prevention. Table 2.1 identifies and defines some of the most common types of cyber threats, including malware, cross-site scripting (XSS), brute force, SQL injection, ransomware, phishing, and denial-of-service (DoS) attacks.

Table 2.1: Types of Cyber Threats (Fortinet, 2020)

Cyber Threats	Definition
Malware	Malware infects a computer and alters its behaviour, destroys data, or eavesdrops on user or network activity as it passes by.
XSS	XSS, or cross-site scripting, is a technique in which an attacker sends malicious scripts to a target's browser via clickable content. The script is run when the victim clicks on the content.
Brute force	The attacker simply tries to guess the login credentials of someone with access to the target system. They will gain access once they guess correctly. While this may appear to be a time-consuming and tough task, attackers frequently utilise bots to guess passwords.
SQL injection	An SQL attack involves an SQL query sent from the client to a database on the server. Clients are machines that retrieve information from servers. The instruction is injected into a data field in place of something else that would ordinarily be there, such as a password. The command is then executed on the database server, and the system is breached.
Ransomware	The victim's computer is held captive by ransomware until the victim agrees to pay the attacker a ransom. After the payment has been received, the attacker gives the recipient instructions on how to take control of their machine again.
Phishing	Phishing occurs when a malicious person sends emails that appear to be from trustworthy, reputable sources to obtain sensitive information from the recipient.
DoS	The target site is overwhelmed with fraudulent requests during a DoS attack. Because the site must react to each request, all the responses utilise the site's resources. This makes it difficult for the site to serve users as it should, and it frequently leads to the site's complete closure.

Cyber threats are more difficult to execute where proper vulnerability detection is in place and where information systems are constantly being monitored for new vulnerabilities. However, this is easier said than done. Even now in 2022, cyberattacks are increasing as organisations are not securing their information systems nor ensuring that vulnerabilities do not leave a gateway for cyberattacks.

2.4. Prevalence of Cyberattacks Globally

The most common motive for cyberattacks is financial gain (Verizon, 2021), where cyber terrorists stand to gain financially. Consequently, the organisations they target lose large amounts of money when they are attacked. According to a study conducted annually by Risk Based Security (2020), the number of leaked records have been increasing progressively over the past decade. Figure 2.2 represents the number of records leaked each year since 2013.

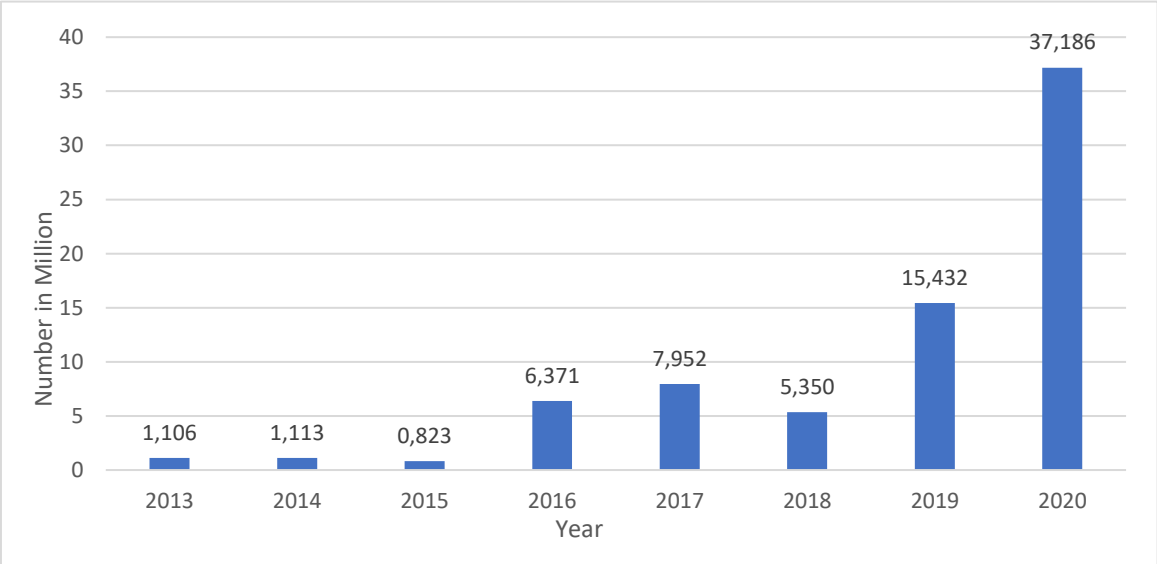


Figure 2.2: Number of Records Lost per year Since 2013 (In Millions)(Risk Based Security, 2020)

From Figure 2.2 it is evident that there has been a growth in data leaks annually since 2013. Of great concern is the significant increase in 2020 when compared to 2019, with 2020 having 21,754 million more records leaked than in 2019. Risk Based Security (2020) suggests that this is one of the many effects that the global Covid-19 pandemic has had on cybersecurity. In addition, Risk Based Security (2020) found that 77 percent of reported data breaches are from external actors, with 23 percent of reported data breaches being internal to the organisation. Of the 23 percent of internal data breaches, 69 percent are deemed to be as a result of employee mistakes, errors, or oversights.

Risk Based Security (2020) further identified the healthcare sector as the sector with the most breaches, followed by the information and financial sectors, respectively. In 2018 and 2019 the healthcare sector was a large target for cyberattacks and ranked as the sector with the second most breaches in both years. The increase that the healthcare sector experienced in 2019 to 2020 is most likely because cyber terrorists capitalised on the stress that the pandemic placed

on the healthcare sector (Risk Based Security, 2020). The healthcare sector has also had the highest average number of breaches over the past eleven years (IBM, 2021).

Figure 2.3 shows the average cost of a data breach each year since 2015, with the average cost in 2021 being the highest since 2016.

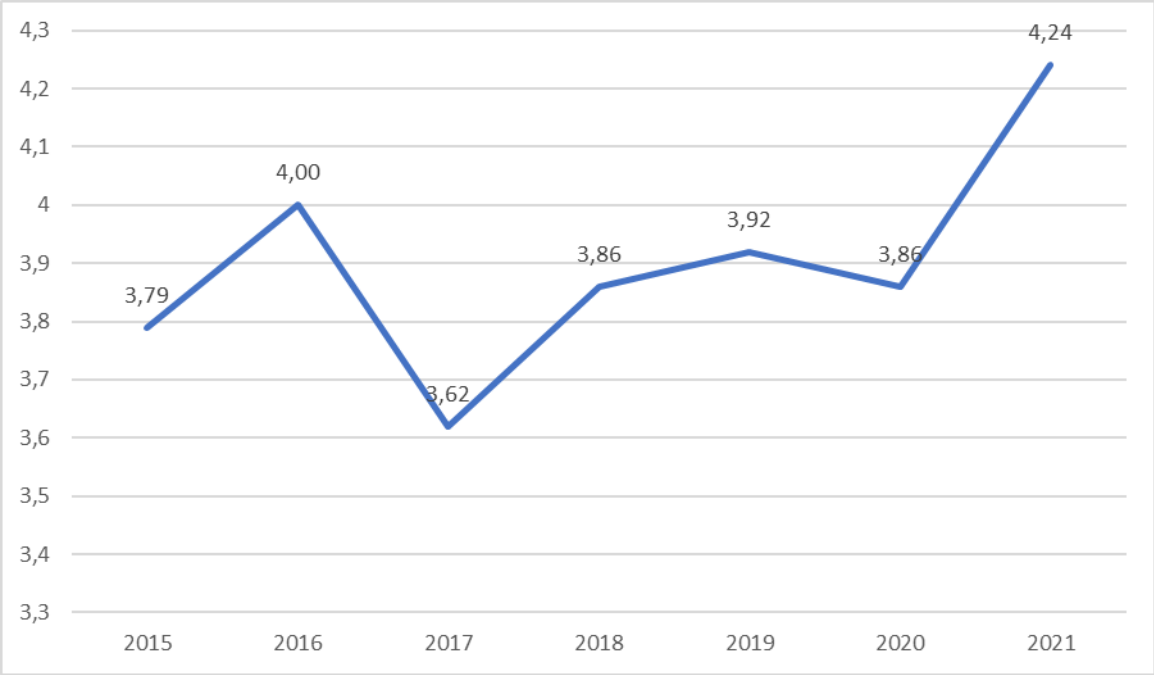


Figure 2.3: Data Breach Average Cost from 2015 until 2021 (IBM, 2021)

IBM (2021) found that from 2020 to 2021 there was a 10 percent increase in the average cost of a data breach, the largest increase in the past seven years. In addition, IBM (2021) identified customer personally identifiable information (PII) as the most common type of data loss being included in 44 percent of all breaches. PII loss is also the costliest to recover from, costing approximately $180 per lost or stolen record. On average in 2021, it took 287 days for a data breach to be identified and contained. This is seven days more than the average in 2020. This means that if a breach occurred on 1 January 2021, the breach would only be contained by 14 October 2021 (IBM, 2021).

With the worldwide state of the pandemic, most of the world's workforce was shifted from office to home-based work. In cases where remote working was a factor in causing a breach of data, the cost of the reported breach was $1.07 million more per remote breach, than that of a breach where remote working was not a factor (IBM, 2021).

Since the start of the pandemic there has been a massive surge in email threats (Mimecast, 2021). During 2020, email threats rose by more than 64 percent globally. It has been found that employees are three times more likely to click on a suspicious email than before the pandemic. Mimecast (2021) conducted a global survey in 2021 and concluded that 43 percent of the participants worldwide believe that the naivete of employees regarding cybersecurity is one of the biggest vulnerabilities. These concerns regarding employee naivete are significant globally, but four countries were identified as being more concerned, namely the UK, Netherlands, South Africa, and the United Arab Emirates.

2.5. Prevalence of Cyberattacks in South Africa

A study conducted in 2017 analysed cyber incidents in South Africa and concluded that, as internet connectivity in Africa improves and a larger percentage of the population gets access to the internet, we may expect a rise in cybercrime, which will target newcomers who are not yet completely aware of the security risks (Van Niekerk, 2017). This statement is true since South Africa has been seeing a large increase in cyberattacks year on year. According to Mcanyana et al. (2020), authors for Accenture, South Africa has the third most cybercrime victims worldwide and is losing R2.2 billion a year due to these cyberattacks. South Africa has the second-highest GDP and the second-fastest internet in Africa, but its internet users are less experienced with technology than those in other countries (Mcanyana et al., 2020). In 2019, there were multiple major incidents that affected the critical infrastructure in South Africa. In February 2019, a South African energy supplier had two security breaches in quick succession. Furthermore, in July 2019, a ransomware infection left South Africans without electricity when one of its prepaid electricity providers was attacked. More recently, in September 2021, the South African Department of Justice network was infected by ransomware. This left all of the Department's information and backups encrypted and unavailable, with a ransom of 50 bitcoins, about R33 million, demanded (Mybroadband, 2021).

IBM (2021) reported that South Africa had the second highest average data breach cost increase from 2020 to 2021, with the average cost increasing by 50 percent. As discussed in Section 2.4, Mimecast (2021) conducted a survey and found that there was a concern surrounding employee naivete. Of South Africa's respondents, 52 percent are concerned with employee naivete, being the highest of all countries. News24 (2020) confirmed this by stating that email

threats have risen by 56 percent in South Africa since the start of the pandemic. Mcanyana et al. (2020) stated that very few Dark Web threat actors mentioned South Africa between 2010 and 2014. However, between 2014 and 2016, mentions increased somewhat. Since 2016, the criminal underground has increased the focus on South Africa. This can be seen in the Figure 2.4 below.

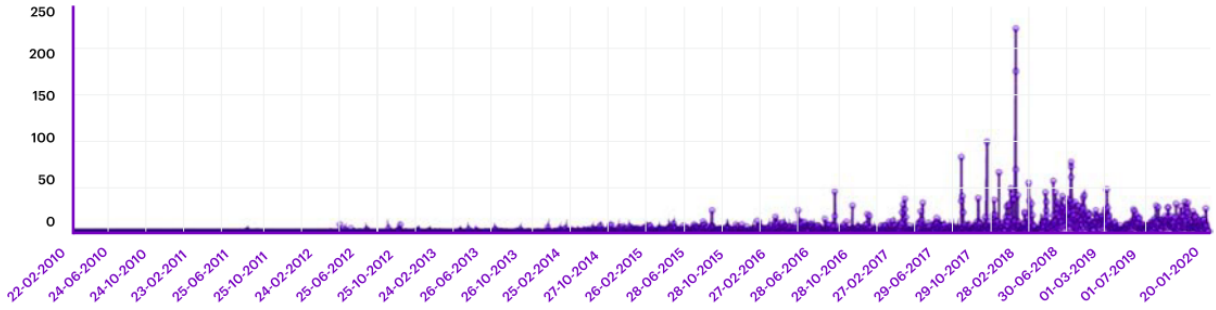


Figure 2.4: Dark Web Mentions of South Africa from 2010 to 2020 (Mcanyana et al., 2020)

South Africa currently is one of the largest targets for hackers and cyber terrorists. Lacking in robust cybersecurity measures, laws and regulations, South Africa is considered a good testing ground for malware and other forms of cyberattacks.

2.6. Cybersecurity Laws and Regulations in South Africa

South Africa has been slow to adopt legislation to address cybercrime. In December 2015, the South African government approved a policy called the National Cybersecurity Policy Framework (NCPF), which is their attempt at protecting against cyberattacks (Mahlobo, 2015). The national assembly only recently, in January 2020, adopted the Cybercrimes Act, which was officially signed into law by the president on 26 May 2021 (Business Insider SA, 2020). In addition, the Protection of Personal Information Act (POPIA) became effective on 1 July 2020.

The Cybercrimes Act creates multiple new offences with regard to cybercrime (Government Gazette, 2020), including:

- **Unlawful interception of data:** The acquisition, viewing, capturing, or copying of data of a non-public nature using a hardware or software tool.
- **Cyber forgery:** Any person who, unlawfully and with the intention to defraud, creates false data or a false computer program to the actual or potential prejudice of another person.

- **Cyber extortion:** Any person who unlawfully and intentionally commits, or threatens to commit, any offence for the purpose of obtaining any advantage from another person; or compelling another person to perform or to abstain from performing any act.

Previously it was difficult to prosecute those who committed crimes on the internet as there was no real definition of what is considered to be cybercrimes. However, now that the Cybercrimes Act has defined these crimes, it can be used in the prosecution of cyberterrorists. The Cybercrimes Act also gives the police service the ability to investigate, access or seize anything they find relevant to their investigation, should they have a warrant.

The Cybercrimes Act creates an opportunity for people to submit evidence of cybercrimes and even punishes those who intend to deceive by not submitting cybercrime evidence. Even though the Cybercrimes Act is a step in the right direction, cybersecurity is largely absent from the Cybercrimes Act. Cybersecurity was removed from the original document due to concerns such as privacy, amongst others. A dedicated Cybersecurity Bill is needed, although it could be years before such a Bill is adopted (ISS Africa, 2021).

The NCPF is another of South Africa's attempts to ensure cybersecurity. The NCPF states three objectives that have to be implemented for the policy to be successful, namely the establishment of a Cybersecurity Hub; the rolling out of a Cybersecurity Awareness Programme; and assisting in the development of Sector Computer Security Incident Response Teams (CSIRT). However, according to Gwala (2016), there have been multiple barriers identified that have made it difficult to implement the NCPF. Barriers were identified, such as the lack of catering for all South African languages in cybersecurity awareness programmes and the lack of skilled cybersecurity professionals for the Cybersecurity Hub, amongst others.

The POPIA came into effect on 1 July 2020 and businesses had to ensure compliance with the POPIA by 30 June 2021. The POPIA is seen as a data protection legislation. A stated by Mohamed (2021), "*POPIA applies to the processing of personal information entered into a record by or for a responsible party by making use of automated or non-automated means, where the responsible party is domiciled in South Africa.*"

The Cybercrimes Act, in combination with the POPIA, is a large step in the right direction for South Africa. The NCPF is also helping in certain aspects, even if its implementation is not

flawless. Critically, cybersecurity specifically is still not being addressed due to the lack of a Cybersecurity Bill.

2.7. Cybersecurity Skills in Mitigating Cyberattacks

The McCumber Cube is a model framework developed by John McCumber in 1991 to assist companies in establishing and evaluating information security initiatives by taking into consideration all of the relevant aspects that impact them (McCumber, 1991). Since information security is a critical building block and domain of cybersecurity, this model is also applicable in the context of cybersecurity. Figure 2.5 visually represents the McCumber model.

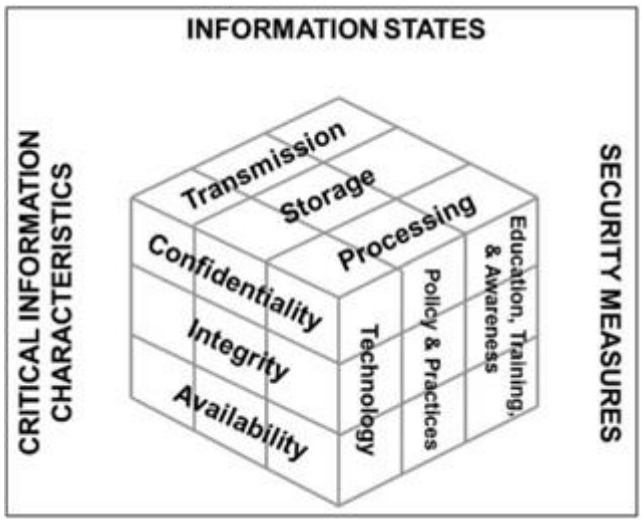


Figure 2.5: McCumber Model (McCumber, 1991)

Based on Figure 2.5, the McCumber Model has three dimensions, namely:

1. Critical Information Characteristics (confidentiality, integrity, availability)
2. Information States (transmission, storage, processing)
3. Security Measures (technology, policy and practices, education, training and awareness)

Each of these dimensions have sub-dimensions. The sub-dimensions of Critical Information Characteristics include:

- **Confidentiality** is a set of guidelines that prevents sensitive data from being shared with unauthorised persons, resources, or processes. Data encryption, identity proofing, and two-factor authentication are all methods for ensuring confidentiality.
- **Integrity** ensures that system information or processes are not manipulated, either intentionally or unintentionally. A hash function or checksum is one technique to assure integrity.

- **Availability** means that only authorised users have access to systems and data when and where they are needed, while those who do not fulfil the requirements are denied access. Maintaining equipment, doing hardware repairs, keeping operating systems and software up to date, and creating backups are all ways to achieve this.

The sub-dimensions of Information States are:

- **Transmission** refers to the movement of data between information systems (data in transit).
- **Storage** refers to data stored in memory or on a permanent storage device such as a hard drive, solid-state drive, or USB drive (data at rest).
- **Processing** refers to information or data that is used to perform a specific task, such as editing a database entry (data in process).

The sub-dimensions of Security Measures are:

- **Technology** refers to software and hardware-based solutions for protecting information systems, such as firewalls, which constantly monitor a network for potential malicious incidents.
- **Policy and practices** refer to administrative controls, such as incident response plans and best practice guidelines, that provide a basis for how an organisation implements information assurance.
- **Education, Training and Awareness** are the safeguards put in place by an organisation to ensure that users are aware of potential security dangers, and the steps they can take to safeguard information systems.

Of the three dimensions that exist within the McCumber model, the Security Measures dimension is most relevant to this study. The three sub-dimensions of security measures are not only information security specific but can also apply to cybersecurity. Just as there is education, training and awareness needed for information security, there is also a need for it in cybersecurity. The same can be said for technology, policies and practices.

All three of the Security Measures sub-dimensions require input from humans in order to work efficiently. There is a human factor involved in ensuring that people are educated, trained and aware of cybersecurity risks. Furthermore, software and hardware-based technologies are used to ensure cybersecurity, and these technologies are created and maintained by humans. In

addition, policies and procedures require humans to create said policies and practices as well as to enforce them. Where there is a need for the human factor there will be a need for skills, and in this case a need for cybersecurity skills.

2.8. The Cybersecurity Skills Gap

As discussed in Sections 2.4 and 2.5, cybercrime is growing at a rapid rate both globally and in South Africa. According to Oltsik (2017), one of the key contributing factors is the lack of skilled cybersecurity professionals. As of 2019, there were 800 000 active cybersecurity workers in the United States, 289 000 in the United Kingdom, and 133 000 in Germany. The Asia Pacific area has the biggest demand for cybersecurity specialists with an estimated 2.6 million trained cybersecurity workers required. With over 1 million cybersecurity workers needed, North and South America are in a close second place, while Europe has a demand of approximately 300 000 cybersecurity professionals (International Information System Security Certification Consortium, 2019). Based on the International Information System Security Certification Consortium (2019), in 2019 more than 4 million trained cybersecurity professionals were needed worldwide.

Oltsik (2017) conducted a global survey in 2017 to better understand the current cybersecurity skills gap. A number of elements were identified by this survey that provide some indication as to why this cybersecurity skills gap exists. Firstly, 77 percent of the survey participants previously worked in an Information Technology (IT) field outside of the cybersecurity domain. This points to an opportunity to better understand the cybersecurity knowledge, skills, abilities, and tasks (KSATs) of these IT professionals, since they are responsible for a large number of cybersecurity professionals. Secondly, the study found that most cybersecurity professionals were not happy in their current position. This could lead to high attrition rates in the near future causing the already large skills gap to grow. In addition, Beltrami (2020) found that more than 70 percent of cybersecurity professionals are under severe stress, which could also add to the possibility of high attrition rates. Thirdly, 62 percent of respondents indicated that they believe their organisation is not providing adequate cybersecurity training to keep up to date with the latest cybersecurity threats. It was also noted that, due to the skills gap, cybersecurity professionals are continuously being approached by other companies to consider other cybersecurity jobs.

Oltsik's 2020 global report shows little improvement (Oltsik, 2020). The 2020 report found that 70 percent of cybersecurity professionals believe that their organisation is being impacted negatively by the cybersecurity skills shortage, and 45 percent of these professionals also believe that the cybersecurity skills shortage and its effects are getting worse.

Just as the cybersecurity skills shortage has been increasing globally, it has also influenced South Africa. The shortage of experienced IT professionals with a broad understanding of the cybersecurity area has created a challenging situation for organisations in South Africa. Securing a company's IT infrastructure is one place where this influence is apparent. Mr Barry Kemp, the Head of Managed IT at Vox in South Africa states: "*South African companies are extremely vulnerable when it comes to IT security, especially because IT security is the field with the fewest skilled personnel. It's no surprise that South Africa is the third most vulnerable to cyber-attacks"* (Vox, 2019). Furthermore, the cybersecurity skills gap in South Africa is being exacerbated by the fact that the majority of trained and skilled cybersecurity specialists are being headhunted by other global corporations (Bucchianeri, 2019).

2.9. Cybersecurity Education, Training and Awareness

Cybersecurity education is one of the solutions to the growing cybersecurity skills gap. As stated by Humphreys (2021), a convenor at ISO: "*The more information we have about our strengths and weaknesses, and those of our enemy, the better prepared we are. We need to gain information about who the enemy is, why, when, how and what they might attack and what they want to gain from it. If we know ourselves and our enemy well, we have a high chance of winning the battle".* In other words, we would be in a strong position if we had a cyber-aware workforce with trained IT professionals and well-informed people. This entails investing time and resources into cybersecurity education, awareness, and training.

One way of addressing the cybersecurity skills gap is through professional certifications. There are multiple cybersecurity certifications that can be attained. The top five certifications, as identified by Oltsik (2020) are:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)

- CompTIA Security+
- Certified Ethical Hacker (CEH)

CISSP is considered the most important to cybersecurity professionals. CISSP has a cybersecurity work experience requirement, so unless someone fulfils this requirement, they cannot get the CISSP certification. This means that most people will have to work in a highly skilled profession while not being properly certified. Luckily, although all these certifications are important, they are mostly considered as a way into the field of cybersecurity, rather than a must-have in order to do the job effectively. This is proven true as 52 percent of the respondents in Oltsik (2020) study indicated that hands-on experience is more important that attaining professional cybersecurity certifications.

A further means to address the cybersecurity skills gap is through formal education at universities. Although universities offer formal qualifications, very few currently offer qualifications related to cybersecurity, and those offering IT-related qualifications typically neglect to integrate cybersecurity into their curricula. Only 42 percent of the top 50 Computer Science programmes in the United States provide three or more information security-specific undergraduate courses (Mickos, 2019). Universities need to revise their IT-related qualifications to include dedicated cybersecurity courses not just at an undergraduate level, but also at postgraduate level.

2.10. Conclusion

This chapter discussed many different aspects relating to cybersecurity. Cybersecurity was discussed in order to better understand how it relates to this study. Multiple cyber threats and vulnerabilities were discussed and the prevalence of cyberattacks was explored both globally and in South Africa in order to highlight the growing need for effective cybersecurity worldwide.

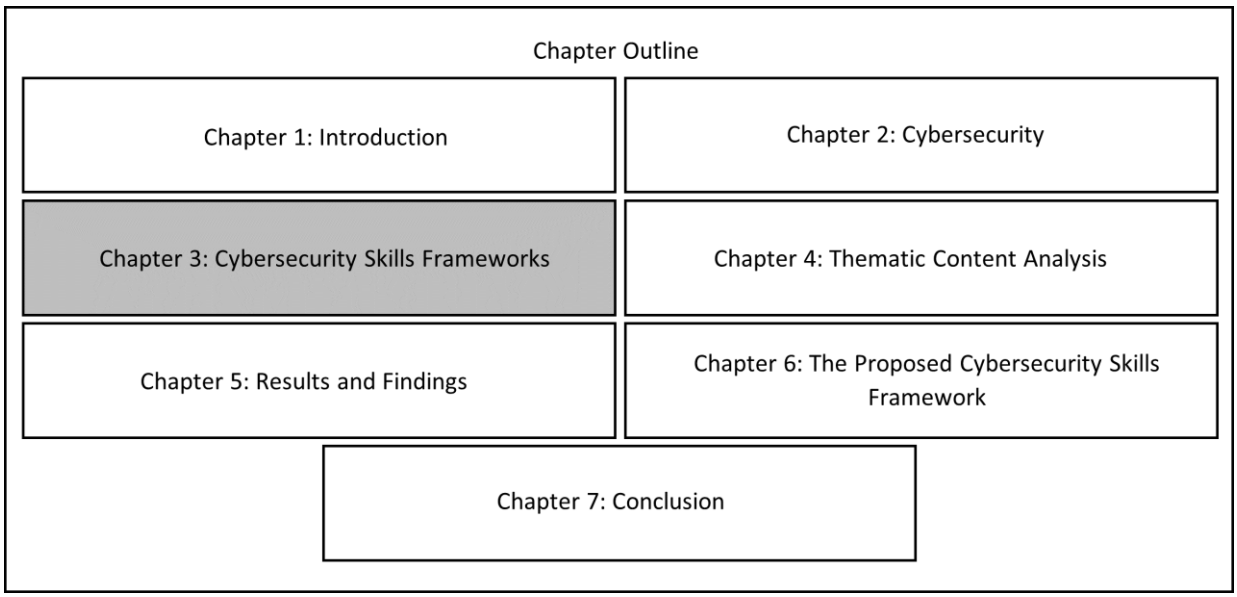
South Africa was highlighted as one of the countries that is most often attacked due to most cybersecurity-related policies and laws still being in their infancy. Cybersecurity laws and legislation in South Africa were explored in order to understand what measures South Africa has taken or intends to take with regards to cybersecurity.

The McCumber model was discussed and how it can be used, not only for its original purpose of establishing and evaluating information security initiatives, but also to help mitigate cyberattacks and to ensure cybersecurity through the effective use of its Security Measures dimension that specifies technology, policy and practices, education, training and awareness as its sub-dimensions. All of this has an impact on the cybersecurity skills gap that is continuously growing. Human intervention is needed in all of the sub-dimensions of the Security Measures dimension of the McCumber model; therefore, to effectively implement these Security Measures, human resources are needed.

Currently, there is a lack of human resources with the required skills to effectively secure cyberspace. This cybersecurity skills gap is growing and is an issue both globally and in South Africa. This study aims to help alleviate this gap by taking a step towards creating a taxonomy and common lexicon for cybersecurity skills for IT professionals.

Many of these taxonomies and common lexicons are already in existence or in development with many countries implementing their own skills and workforce frameworks. These workforce and skills frameworks are discussed in Chapter 3.

Chapter 3 – Cybersecurity Skills Frameworks



3.1. Introduction

Chapter 2 discussed cybersecurity as the overarching field of interest of this study. Chapter 3 introduces various skills frameworks that are currently in development or used globally. This chapter highlights how the identified skills frameworks compare to each other in terms of focus, usage, and other key characteristics.

This chapter is structured as follows. Section 3.2 discusses global IT Skills Frameworks while Section 3.3 focuses more specifically on global Cybersecurity Skills Frameworks. Section 3.4 compares the frameworks highlighted in Sections 3.2 and 3.3 against one another in terms of their focus, usage, and key characteristics. The conclusion for this chapter follows in Section 3.5.

3.2. Global IT Skills Frameworks

Skills frameworks aim to establish a taxonomy and common lexicon for skills. Individuals, companies, and training providers are able to communicate in a common language owing to the existence of these skills frameworks (Skills Future, 2016). Such frameworks also aid in the recognition of skills, and the establishment of training programmes for skills and career development globally.

Since the terms job roles, knowledge, skills, abilities and tasks are used frequently in this chapter and throughout this study, it is important to define these terms. NIST (2017) defines them as follows:

- **Job role** refers to a part played by an employee as per their key responsibility areas. Each Job Role has defined KSATs in which the employee should be competent, e.g., a cybersecurity specialist is a job role, and it has defined KSATs.
- **Knowledge** refers to a body of information applied directly to the performance of a job role, e.g., knowledge regarding security vulnerabilities and exploits are required for cybersecurity specialists.
- **Skill** refers to the ability to do something that comes from training, experience, or practice, e.g., technical writing skills.
- **Ability** refers to the competence to perform an observable behaviour, e.g., ability to investigate malware, intrusion attempts and vulnerabilities.
- **Task** refers to a specific defined piece of work that, combined with other identified tasks, comprises the work in a specific job role.

The skills frameworks discussed in this section include the Skills Framework for Infocomm Technology (SFw for ICT) and the Skills Framework for the Information Age (SFIA) as two of the most used and widely known skills frameworks.

These frameworks are considered general IT frameworks as they do not have a specific focus on cybersecurity.

3.2.1. Skills Framework for Infocomm Technology

The Skills Framework for Infocomm Technology (SFw for ICT) is a skills framework that does not focus solely on cybersecurity, but on Information Technology as a whole (IMDA, 2017). This framework was jointly developed by the Infocomm Media Development Authority (IMDA), Skills Future Singapore (SSG), Workforce Singapore (WSG) and the Cybersecurity Agency of Singapore (CSA). SFw for ICT aims to provide information on career paths, existing and emerging skills as well as occupations and job roles and their respective knowledge, skills, abilities and tasks (KSATs). It is therefore useful for employers and educational facilities, as well as for individuals who are job seeking or planning their careers.

The SFw for ICT provides a very user-friendly approach by using visuals to represent the information on their website. This framework is considered to be a general IT skills framework. Although this framework does not focus specifically on cybersecurity, it does have some cybersecurity aspects that are highlighted in this section.

Figure 3.1 provides a visual overview of SFw for ICT indicating the seven high-level categories and their associated sub-categories.

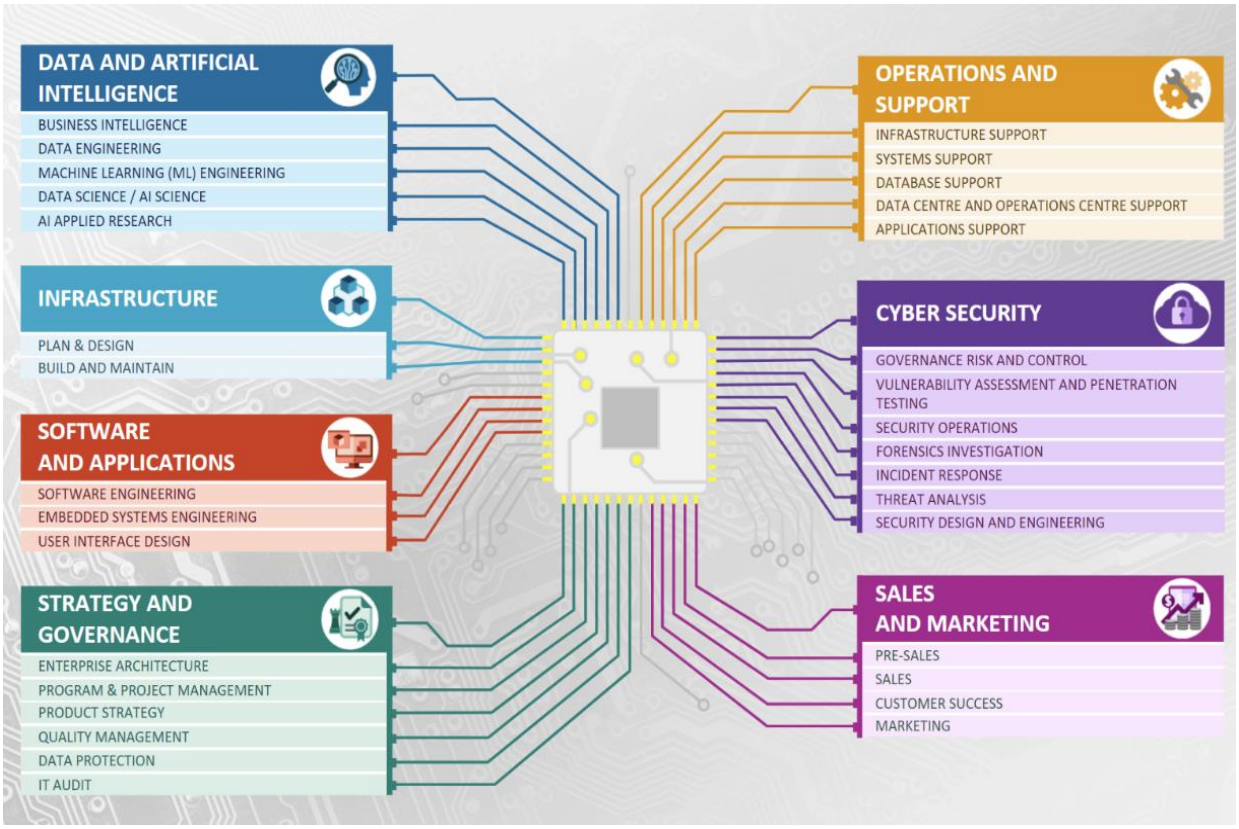


Figure 3.1: Overview of SFw for ICT (IMDA, 2017)

The seven high-level categories comprising the SFw for ICT include:

1. Data and Artificial Intelligence (five sub-categories)
2. Infrastructure (two sub-categories)
3. Software and Applications (three sub-categories)
4. Strategy and Governance (six sub-categories)
5. Operations and Support (five sub-categories)
6. Cybersecurity (seven sub-categories)
7. Sales and Marketing (four sub-categories)

Each of the sub-categories is further broken down into multiple job roles, as shown in Figure 3.2. In Figure 3.2, each of the red blocks identifies a job role in the Software Engineering sub-category, which lies within the main Software and Applications category. Each of these job roles is expanded upon. Figures 3.3 and 3.4 show the 'Software Engineer' job role as presented by SFw for ICT (IMDA, 2017).

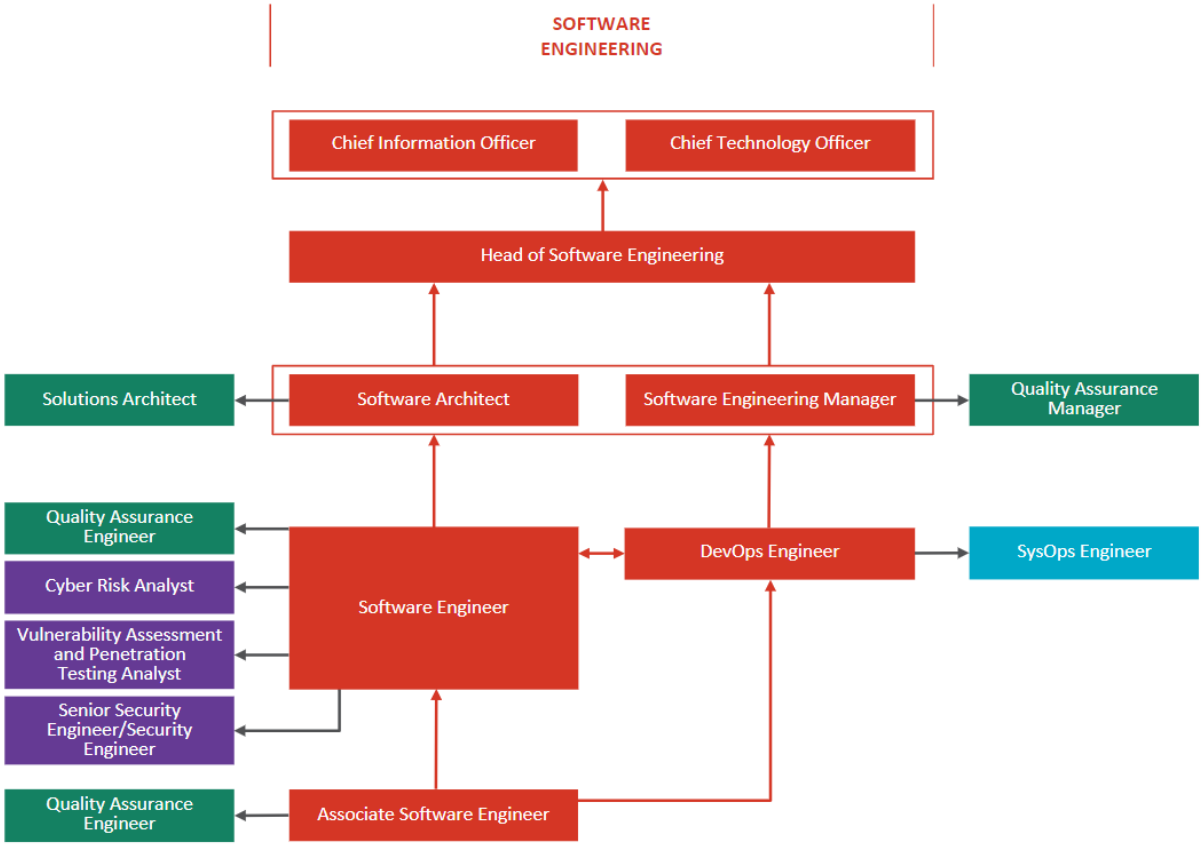
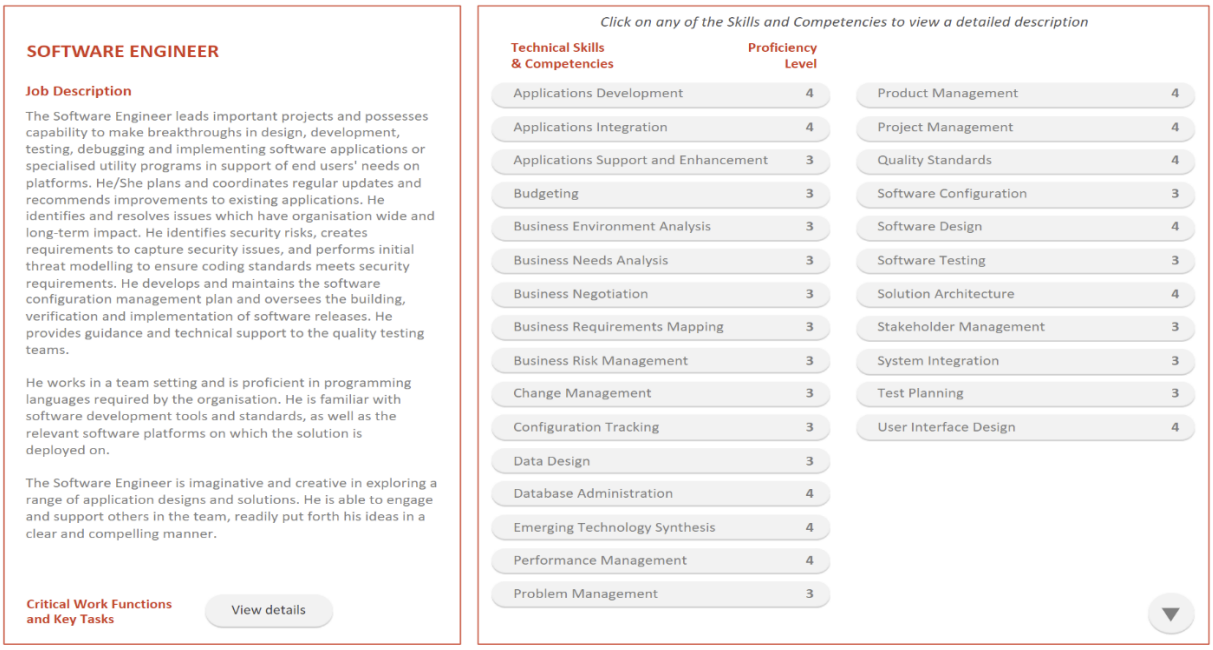


Figure 3.2: Software Engineer Sub-category (IMDA, 2017)

Figure 3.3 provides further detail regarding the Software Engineer job role, including a description of the job role, as well as the technical competencies required by the job role, and the required proficiency level for each of the technical competencies indicated by the number to the right of each competency.

Each skill is assigned multiple proficiency levels from 1 to 6, with 1 being the lowest level of understanding and 6 being the highest. Each of these proficiency levels is unique to the assigned

skill and indicates the level of understanding that the employee is required to have for that specific skill.



SOFTWARE ENGINEER

Job Description

The Software Engineer leads important projects and possesses capability to make breakthroughs in design, development, testing, debugging and implementing software applications or specialised utility programs in support of end users' needs on platforms. He/She plans and coordinates regular updates and recommends improvements to existing applications. He identifies and resolves issues which have organisation wide and long-term impact. He identifies security risks, creates requirements to capture security issues, and performs initial threat modelling to ensure coding standards meets security requirements. He develops and maintains the software configuration management plan and oversees the building, verification and implementation of software releases. He provides guidance and technical support to the quality testing teams.

He works in a team setting and is proficient in programming languages required by the organisation. He is familiar with software development tools and standards, as well as the relevant software platforms on which the solution is deployed on.

The Software Engineer is imaginative and creative in exploring a range of application designs and solutions. He is able to engage and support others in the team, readily put forth his ideas in a clear and compelling manner.

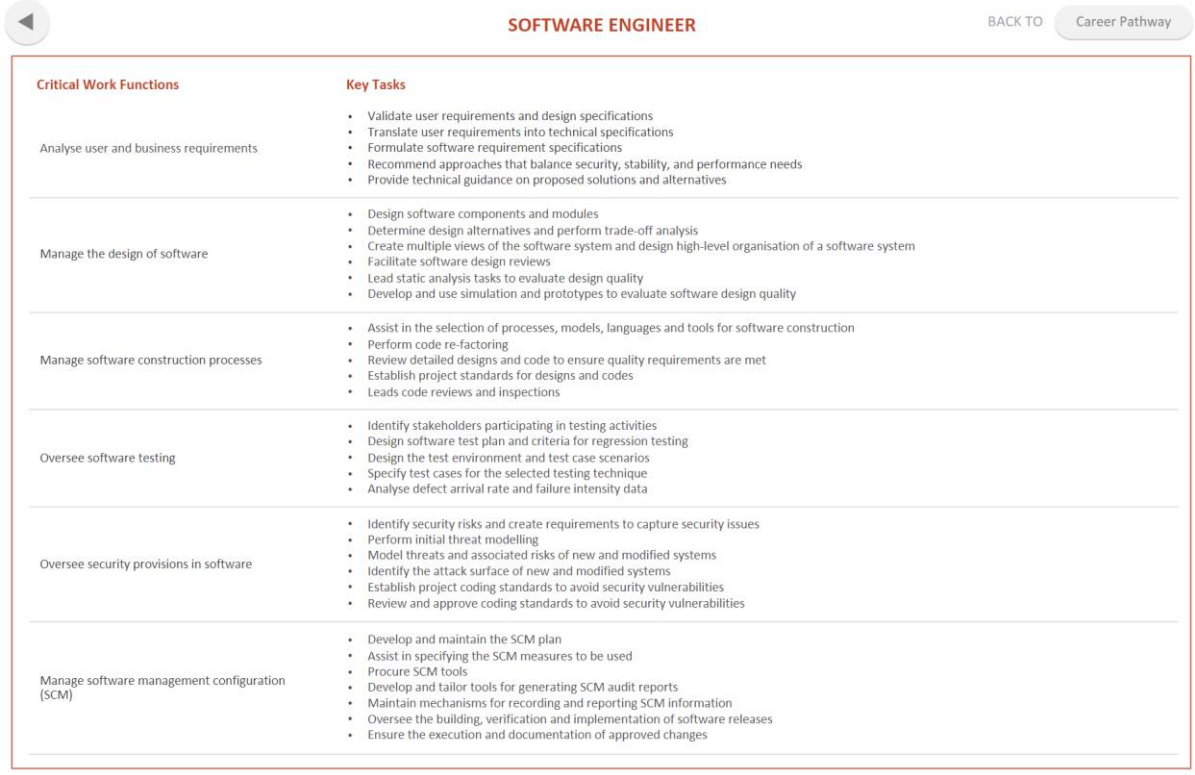
Critical Work Functions and Key Tasks | View details

Click on any of the Skills and Competencies to view a detailed description

Technical Skills & Competencies	Proficiency Level
Applications Development	4
Applications Integration	4
Applications Support and Enhancement	3
Budgeting	3
Business Environment Analysis	3
Business Needs Analysis	3
Business Negotiation	3
Business Requirements Mapping	3
Business Risk Management	3
Change Management	3
Configuration Tracking	3
Data Design	3
Database Administration	4
Emerging Technology Synthesis	4
Performance Management	4
Problem Management	3
Product Management	4
Project Management	4
Quality Standards	4
Software Configuration	3
Software Design	4
Software Testing	3
Solution Architecture	4
Stakeholder Management	3
System Integration	3
Test Planning	3
User Interface Design	4

Figure 3.3: Software Engineer Skills (IMDA, 2017)

Figure 3.4 provides a further level of detail highlighting the work functions and each of the key tasks associated with each work function for the Software Engineer job role. Based on Figures 3.3 and 3.4, one can clearly see what KSATs are required for the job role of Software Engineer.



SOFTWARE ENGINEER

BACK TO Career Pathway

Critical Work Functions	Key Tasks
Analyse user and business requirements	• Validate user requirements and design specifications • Translate user requirements into technical specifications • Formulate software requirement specifications • Recommend approaches that balance security, stability, and performance needs • Provide technical guidance on proposed solutions and alternatives
Manage the design of software	• Design software components and modules • Determine design alternatives and perform trade-off analysis • Create multiple views of the software system and design high-level organisation of a software system • Facilitate software design reviews • Lead static analysis tasks to evaluate design quality • Develop and use simulation and prototypes to evaluate software design quality
Manage software construction processes	• Assist in the selection of processes, models, languages and tools for software construction • Perform code re-factoring • Review detailed designs and code to ensure quality requirements are met • Establish project standards for designs and codes • Leads code reviews and inspections
Oversee software testing	• Identify stakeholders participating in testing activities • Design software test plan and criteria for regression testing • Design the test environment and test case scenarios • Specify test cases for the selected testing technique • Analyse defect arrival rate and failure intensity data
Oversee security provisions in software	• Identify security risks and create requirements to capture security issues • Perform initial threat modelling • Model threats and associated risks of new and modified systems • Identify the attack surface of new and modified systems • Establish project coding standards to avoid security vulnerabilities • Review and approve coding standards to avoid security vulnerabilities
Manage software management configuration (SCM)	• Develop and maintain the SCM plan • Assist in specifying the SCM measures to be used • Procure SCM tools • Develop and tailor tools for generating SCM audit reports • Maintain mechanisms for recording and reporting SCM information • Oversee the building, verification and implementation of software releases • Ensure the execution and documentation of approved changes

Figure 3.4: Software Engineer Key Tasks(IMDA, 2017)

As depicted in Figure 3.1, the Skills Framework for Infocomm Technology has a total of seven categories, each with their respective sub-categories. Cybersecurity is one of the aforementioned categories. There are seven sub-categories in the cybersecurity category, namely:

1. Governance Risk and Control
2. Vulnerability Assessment and Penetration Testing
3. Security Operations
4. Forensics Investigation
5. Incident Response
6. Threat Analysis
7. Security Design and Engineering

Figure 3.5 depicts each of the sub-categories in the cybersecurity category as well as all the related job roles associated with cybersecurity. In total, there were 15 cybersecurity-specific job roles identified by this framework. One can also see the job hierarchy in Figure 3.5. Each of these job roles identified has specific KSATs assigned to it.

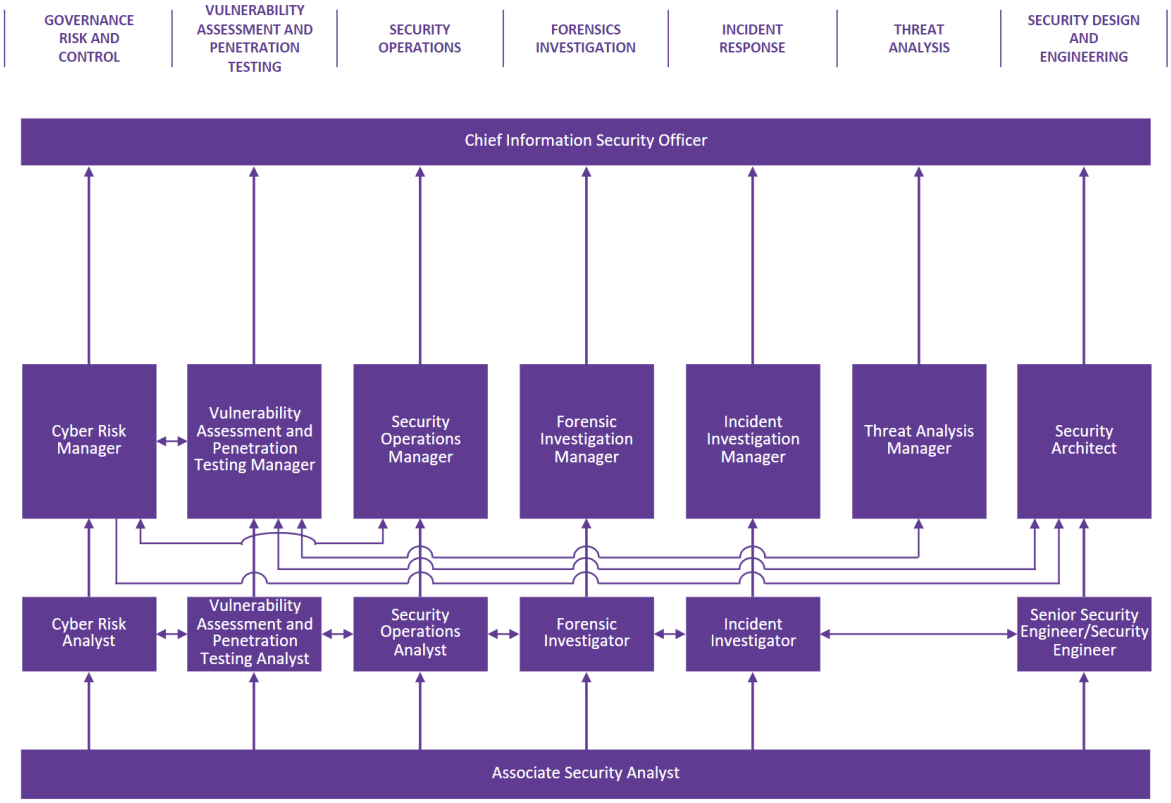


Figure 3.5: Cybersecurity Category (IMDA, 2017)

Figures 3.6 and 3.7 illustrate the skills and key tasks needed by a forensics investigator job role.

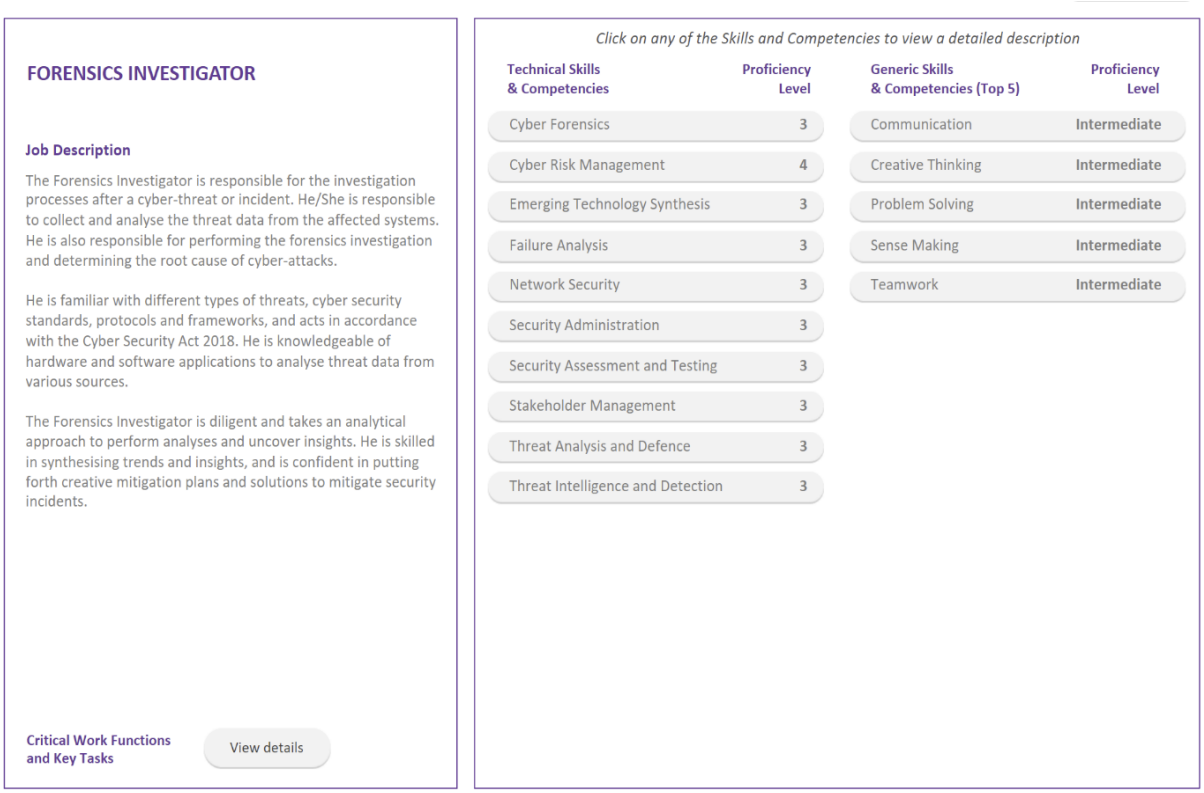


Figure 3.6: Forensic Investigator Skills (IMDA, 2017)

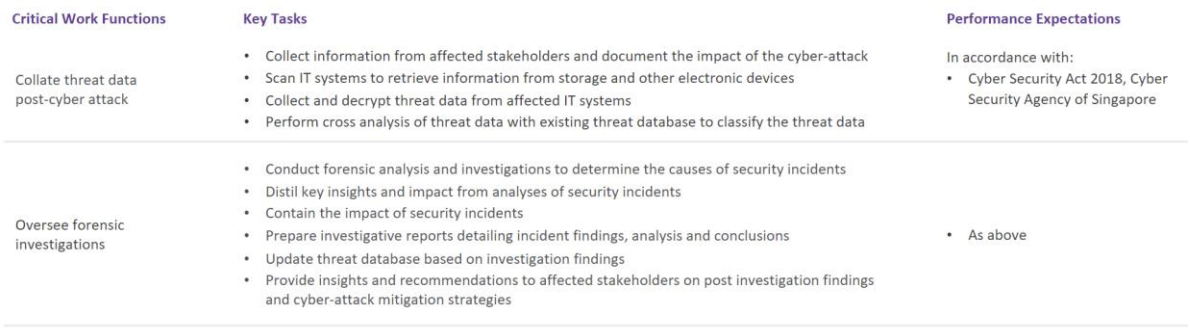


Figure 3.7: Key Tasks for a Forensics Investigator (IMDA, 2017)

The Forensics Investigator job role, similar to the Software Engineer job role, has proficiency levels associated with the identified skills. The Skills Framework for Infocomm Technology follows the same level of detail in all its categories and job roles.

3.2.2. Skills Framework for the Information Age (SFIA)

The Skills Framework for the Information Age (SFIA) was first published in the year 2000 but has since had multiple updates. The current version of SFIA is SFIA 8. SFIA was created by many organisations but spearheaded by the British Computer Society (BCS) (SFIA Foundation, 2018).

SFIA is targeted at a large audience including individuals seeking jobs, organisational leaders and education providers. SFIA makes use of proficiency levels for each skill within the seven levels defined by SFIA, as depicted in Table 3.1. Each of these proficiency levels is of a varying difficulty, and therefore changes how the skill is applied by the user. Level 1 is the lowest level, described as 'Follow', while Level 7 is the highest level, described as 'Set strategy, inspire and mobilise'.

Table 3.1: SFIA Proficiency Levels (SFIA Foundation, 2018)

Proficiency Level	Description
Level 1	Follow
Level 2	Assist
Level 3	Apply
Level 4	Enable
Level 5	Ensure, advise
Level 6	Initiate, influence
Level 7	Set strategy, inspire, mobilise

Similar, to other frameworks, SFIA is divided into six categories, each with its own sub-categories, as shown in Table 3.2. In addition, each sub-category has multiple skills assigned to it.

Table 3.2: SFIA Categories and Sub-categories (SFIA Foundation, 2018)

Category	Sub-categories
Strategy and Architecture	1. Information Strategy 2. Advice and Guidance 3. Business Strategy and Planning 4. Technical Strategy and Planning
Change and Transformation	1. Business Change Implementation 2. Business Change Management
Development and Implementation	1. Systems Development 2. User Experience 3. Installation and Integration
Delivery and Operation	1. Service Design 2. Service Transition 3. Service Operation
Skills and Quality	1. Skills Management 2. People Management 3. Quality and Conformance
Relationships and Engagement	1. Stakeholder Management 2. Sales and Marketing

Each of the sub-categories has skills that are associated with it. Table 3.3 provides an example of the Digital Forensics skills as defined by SFIA. The Digital Forensics skill is associated with the quality and conformance sub-category found in the skills and quality category. As shown in this

example, each skill is assigned a skill code - in this example the skill code for Digital Forensics is DGFS. A brief description for each skill is also provided, followed by the relevant proficiency levels. In the case of the Digital Forensics skill, it has three proficiency levels, namely Levels 4, 5 and 6, as described in Table 3.3.

Table 3.3: Digital Forensics Skill according to SFIA (SFIA Foundation, 2018)

Skill name:	Digital forensics
Skill code:	DGFS
Skill description:	The collection, processing, preserving, analysis, and presentation of forensic evidence based on the totality of findings including computer-related evidence in counterintelligence, or law enforcement investigations.
Level description:	Level 6: Sets policies and standards and guidelines for how the organisation conducts digital forensic investigations, Leads and manages complex investigations engaging additional specialists if required. Authorises the release of formal forensic reports. Level 5: Conducts investigations to correctly gather, analyse and present the totality of findings including digital evidence to both business and legal audiences. Collates conclusions and recommendations and presents forensics findings to stakeholders. Contributes to the development of policies, standards, and guidelines. Level 4: Contributes to digital forensic investigations. Process and analyses evidence in line with policy, standards and guidelines and supports production of forensics findings and reports.

SFIA also focuses on skills that are considered cybersecurity skills such as Security Administration and Penetration Testing. According to SFIA, Penetration Testing falls into three proficiently levels namely, Levels 4, 5 and 6. All three of these levels occur towards the higher end of the SFIA proficiently scale, meaning they require higher levels of knowledge and that there is an increased level of difficulty in applying the skill of Penetration Testing.

Since SFIA focuses specifically on IT skills, this makes it less relevant to this research than other frameworks that focus on job roles, and the specific KSATs for such job roles. However, SFIA can still be used as a reference to compare skills identified during this study.

Having considered two global IT skills frameworks and their particular structures, the following section presents some well-known global cybersecurity frameworks.

3.3. Global Cybersecurity Skills Frameworks

In order to identify the most well-known global cybersecurity skills frameworks, a high-level Google and Google Scholar search was conducted, using search terms “Cybersecurity skills framework” and “Most used cybersecurity skills frameworks globally”. This resulted in the identification of the following well-known cybersecurity skills frameworks:

- The National Initiative for Cybersecurity Education (NICE)
- SPARTA Cybersecurity Skills Framework
- CIISEC Framework
- ASD Cyberskills Framework
- European Cybersecurity Skills Framework (ECSF)
- Canadian Cybersecurity Skills Framework

These are discussed in more detail in the following sub-sections.

3.3.1. The National Initiative for Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE) Framework is a workforce framework for cybersecurity that was published by the National Institute of Standards and Technology (NIST) in the United States (NIST, 2017). The NICE framework is mostly used in the United States and the framework describes the knowledge, skills, abilities, and tasks (KSATs) that are required for cybersecurity job roles and is therefore considered to be a common lexicon that categorises and describes cybersecurity work in the United States.

Although NICE is mainly targeted at employers, it can also assist educational institutions, as well as graduates and job seekers to better understand what is required of certain cybersecurity job roles. The NICE framework has over 52 defined job roles, and over 1600 defined KSATs relating to these job roles. According to NIST (2017), having defined so many job roles and KSATs is not only one of the benefits of the NICE framework, but also one of its largest limitations. NIST (2017) acknowledges that NICE is very difficult to manage with so many job roles and KSATs, and with some of the KSATs also not being well defined

Figure 3.8 depicts the structure of the NICE framework (NIST, 2017). Categories appear at the highest level of the structure, with each category broken down into specialty areas.

These specialty areas are further broken down into job roles, with specific KSATs related to each job role. Figure 3.8 below uses the terms work roles, but in the case of this study the term work roles and job roles are used interchangeably and have the same meaning.

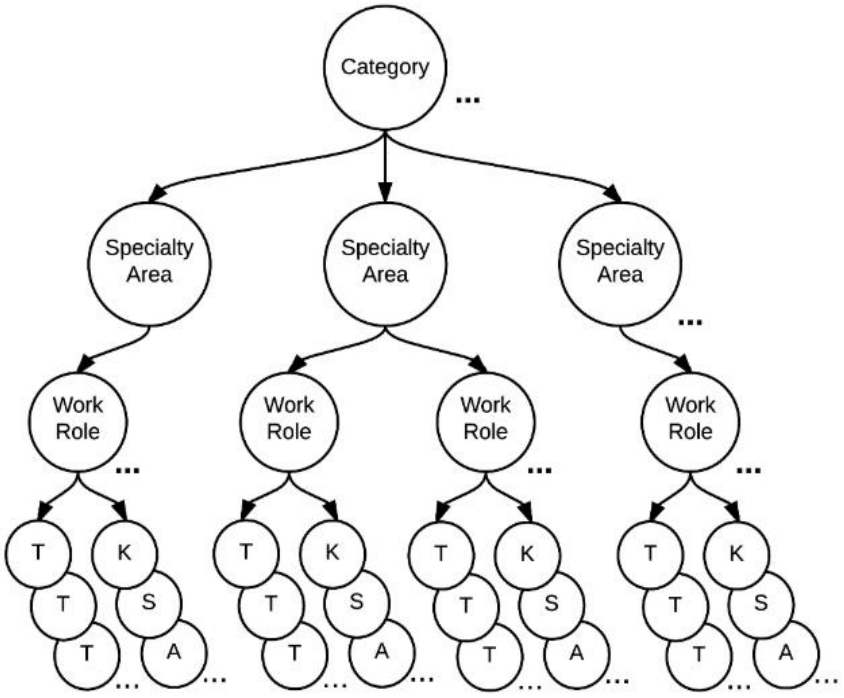


Figure 3.8: High level Overview of the NICE Framework (NIST, 2017)

The seven categories defined by NICE are listed and described in Table 3.4.

Table 3.4: NICE Framework Categories (NIST, 2017)

Categories	Descriptions
Securely provision (SP)	Conceptualises, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so that the organisation may conduct cybersecurity work effectively.
Protect and defend (PR)	Identifies, analyses, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyse (AN)	Performs highly specialised review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and operate (CO)	Provides specialised denial and deception operations and collection of cybersecurity information that may be used to develop intelligence
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Each of the categories presented in Table 3.4 is further divided into multiple Speciality Areas. As an example, the seven Speciality Areas for the Securely Provision (SP) category are highlighted in Table 3.5.

Table 3.5: NICE Framework Speciality Areas (NIST, 2017)

Speciality Areas	Speciality Area Descriptions
Risk management (RSK)	Oversees, evaluates, and supports the documentation, validation, assessment, and authorisation processes necessary to assure that existing and new information technology (IT) systems meet the organisation's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.
Software development (DEV)	Develops and writes/codes new (or modifies existing) computer applications, software, or specialised utility programs following software assurance best practices.
Systems architecture (ARC)	Develops system concepts and works on the capabilities phases of the system's development life cycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.
Technology Research and Development (TRD)	Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.
Systems Requirement Planning (SRP)	Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.
Test and evaluation (TST)	Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating IT.
Systems development (SYS)	Works on the development phases of the system's development life cycle.

Furthermore, each of these Speciality Areas have multiple job roles assigned to them. As an example, Software Development (DEV) has two job roles assigned to it, namely Software Developer (SP-DEV-001) and Secure Software Assessor (SP-DEV-002). These job roles also each have various KSATs assigned to them.

Although the NICE framework specifies that it is a cybersecurity workforce framework, it does not only describe cybersecurity job roles. NIST (2017) states that "cybersecurity workforce" is shorthand for a workforce with job roles that have an impact on an organisation's ability to protect its data, systems, and operations; hence, the inclusion of job roles such as Software

Developer. Even though their primary role is not to ensure cybersecurity, they have a substantial impact on the organisation's ability to ensure cybersecurity.

Table 3.6 presents the Software Developer job role, according to the NICE framework, including the job role name, ID, speciality area, category as well as a brief description of the job role and each of the KSATs associated with the job role. Each job role within the NICE framework is structured and presented in a similar way to that of the Software Developer job role shown in Table 3.6.

Table 3.6: Software Developer Job Role according to NICE (NIST, 2017)

Work Role Name	**Software Developer**
Work Role ID	**SP-DEV-001**
Speciality Area	**Software Development (DEV)**
Category	**Securely Provision (SP)**
Work Role Description	Develops, creates, maintains, and write/codes new (or modifies existing) computer applications, software, or specialised utility programs.
Tasks	T0009, T0011, T0013, T0014, T0022, T0026, T0034, T0040, T0046, T0057, T0077, T0100, T0111, T0117, T0118, T0171, T0176, T0181, T0189, T0217, T0228, T0236, T0267, T0303, T0311, T0324, T0337, T0416, T0417, T0436, T0455, T0500, T0553, T0554
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0027, K0028, K0039, K0044, K0050, K0051, K0060, K0066, K0068, K0070, K0073, K0079, K0080, K0081, K0082, K0084, K0086, K0105, K0139, K0140, K0152, K0153, K0154, K0170, K0179, K0199, K0202, K0260, K0261, K0262, K0263, K0322, K0332, K0342, K0343, K0624
Skills	S0001, S0014, S0017, S0019, S0022, S0031, S0034, S0060, S0135, S0138, S0149, S0174, S0175, S0367
Abilities	A0007, A0021, A0047, A0123, A0170

However, from Table 3.6 it is very difficult to determine what the actual KSATs are for the Software Developer job role due to the KSATs only being referred to by their ID number instead of by name. To understand each set of KSATs, it is required that the reader look through the lists of KSATs to find the specific ones related to each job role. This makes the NICE framework extremely difficult to read and very challenging for the reader to understand.

3.3.2. SPARTA Cybersecurity Skills Framework

The SPARTA Cybersecurity Skills framework uses a very different approach. Where most other skills frameworks target multiple audiences, such as employers, job seekers and educational facilities, SPARTA has a direct focus on educational facilities and cybersecurity curricula (Hajny et al., 2020). The framework aims to help universities with the creation of their cybersecurity study programmes.

The development of cybersecurity curricula, as suggested by SPARTA, is tightly related to the activity of key European Union (EU) institutions like the European Union Agency for Cybersecurity (ENISA) and the European Cyber Security Organisation (ECSO). The NICE Framework has also had a significant impact on the creation of the SPARTA Framework.

The SPARTA Framework connects KSATs to job roles, defining essential topics for students interested in working in the cybersecurity field. They use the core principles of job roles and competencies to create the curricula, identifying the typical roles on the labour market, and categorising the key technical skills and soft skills required for work in specific cybersecurity job roles.

When using the SPARTA framework, it is easy to determine which technical and soft skills are required for specific job roles and should thus be included in study programmes. The clearly defined job roles also make it easier to focus study programs on specific areas of cybersecurity and to create tailored curricula based on a university's profile and particular demands.

Table 3.7 illustrates how the Software Developer job role is defined according to the SPARTA Cybersecurity Skills framework. Based on Table 3.7, it is clear that SPARTA uses a different approach to most other cybersecurity skills frameworks as it includes the degree level needed for a Software Developer job role. In addition, it specifies the field of the degree and the certifications and experience levels. SPARTA also indicates both the technical and soft skills required for each specified job role.

Table 3.7: Software Developer Job Roles according to SPARTA (Hajny et al., 2020)

Degree Level	Bachelor's degree; grad degree for some positions
Degree Field	Computer or information science
Certification	Voluntary certifications available
Experience	Varies depending on the position
Key Technical Skills	Programming and testing Analytical and communication skills Proficiency in variety of computing languages and environments (containers, virtual machines, Operating systems (OSs))
Key Soft Skills	Adaptability Team Spirit Time management Ability to deliver Methodology and rigour

Similarly to NICE, SPARTA states that although some job roles, such as that of a Software Developer, are not specifically a cybersecurity job role, it is still a requirement for people in these job roles to have a certain level of cybersecurity knowledge; hence, the inclusion of these types of job roles in the framework.

3.3.3. Chartered Institute of Information Security Skills Framework (CIISec)

The Chartered Institute of Information Security (CIISec) Skills Framework outlines the set of skills that Information Security and Information Assurance professionals are expected to possess to do their jobs effectively (CIISec, 2019). This framework was created as a result of collaboration between business and public sector organisations, as well as with internationally known academics and security experts. It not only assesses security professionals' knowledge, but also outlines the skills and capabilities expected of them in practice.

CIISec uses six levels, as indicated in Figure 3.9, to show proficiency of skills. Levels 1 and 2 are for those with basic knowledge of the skill, but who lack the real-world experience in the area, and therefore would require significant guidance. Skills Levels 3 and 4 refer to those who can operate at a practical level, with some guidance if needed, while Levels 5 and 6 function at a Senior, Principal or Lead Practitioner level and require little to no guidance.

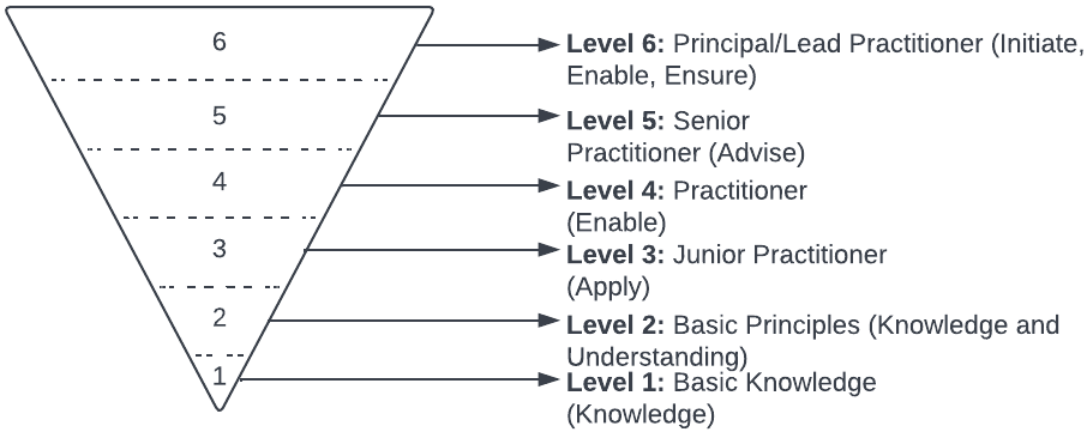


Figure 3.9: Skills Levels used in CIISec Skills Framework (CIISec, 2019)

CIISec has multiple skills areas that were identified by their study, with each skill area having multiple skills. Each of these skills is then divided into the six proficiency levels mentioned above. CIISec has eleven skill areas namely:

A. Information Security Governance and Management
B. Threat Assessment and Information Risk Management
C. Implementing Secure Systems
D. Assurance: Audit, Compliance, and Testing
E. Operational Security Management
F. Incident Management, Investigation and Digital Forensics
G. Data Protection, Privacy, and Identity Management.
H. Business Resilience.
I. Information Security Research.
J. Management, Leadership, Business, and communications.
K. Contributions to the Information Security Profession and Professional Development.

Table 3.8 presents seven of the skills associated with skill area A: information security governance and management. These are numbered A1 - A7.

Table 3.8: Information Security Governance and Management Skill Area Sub-sections (CIISec, 2019)

Section A	Security Discipline – Information Security Governance and Management
A1	Governance
A2	Policy and Standards
A3	Information Security Strategy
A4	Innovation and Business Improvement
A5	Behavioural Change
A6	Legal and Regulatory Environment and Compliance
A7	Third Party Management

Table 3.9 further expands on this by presenting a brief description of skill A1 - governance (which belongs to skill area A - information security governance and management) and examples of the skills associated with each of the six proficiency levels.

Table 3.9: Governance Skill according to CIISec Skills Framework (CIISec, 2019)

Section A	Security Discipline – Information Security Governance and Management	
Skills Group	**Principles**	**Example Skills**
A1 - Governance	Directs, oversees, designs, implements or operates within the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage Cyber and Information Security at an enterprise level, supporting an organisation's immediate and future regulatory, legal, risk, environment and operational requirements and ensuring compliance with those requirements.	**Level 1:** Can describe the principles of Information Security Governance. Can list the possible impacts that occur where poor Information Governance has been observed.
		Level 2: Can explain the basic principles of Information Security Governance and how it applies within an organisation.
		Level 3: Understands local (organisation or project) Information Security Governance processes. Undertakes Information Security Governance tasks under supervision. Recognises and addresses non-compliance and makes recommendations for change.
		Level 4: Leads the development, revision and implementation of Information Security Governance processes.
		Level 5: Responsible for the development, revision and implementation of Information Security Governance processes across a range of clients or within a large corporate organisation.

Unlike other frameworks like NICE, CIISec focuses mainly on cybersecurity skills and not on actual job roles.

3.3.4. Australian Signals Directorate Cyber Skills Framework

The Australian Signals Directorate (ASD) launched the ASD Cyber Skills Framework version 1.0 in July 2019 as an iterative framework to assess, maintain, and monitor the ASD cyber workforce's cybersecurity skills, knowledge, and attributes (Australian Signals Directorate, 2020). Version 2.0 of the framework was released in 2020. The ASD Cyber Skills Framework is supported by other reputable skills frameworks, such as the CIISec Framework (Section 3.3.3), and SFIA (Section 3.2.2). It also takes some inspiration from the NICE Framework (Section 3.3.1).

When compared to other frameworks, the ASD Cyber Skills Framework focuses not only on job roles, but also on the skills and capabilities relevant to the job roles, similar to the NICE framework. The key difference between the job roles in the NICE framework compared to the ASD Cyber Skills Framework is that the ASD Cyber Skills Framework focuses solely on cybersecurity-related job roles compared to the more general IT job roles that also impact the cybersecurity of an organisation, as used by NICE.

Figure 3.10 depicts the four main disciplines and cyber job roles, as defined by the ASD Cyber Skills Framework. These include the following:

1. Cybersecurity Analysis (Job roles: Cyber Threat Analyst, Intrusion Analyst and Malware Analyst)
2. Cybersecurity Operations (Job roles: Incident Response, Operations Coordinator)
3. Cybersecurity Architecture (Job roles: Cybersecurity Advice and Assessment, Vulnerability Researcher)
4. Cybersecurity Testing (Job roles: Penetration Tester, Vulnerability Assessor)

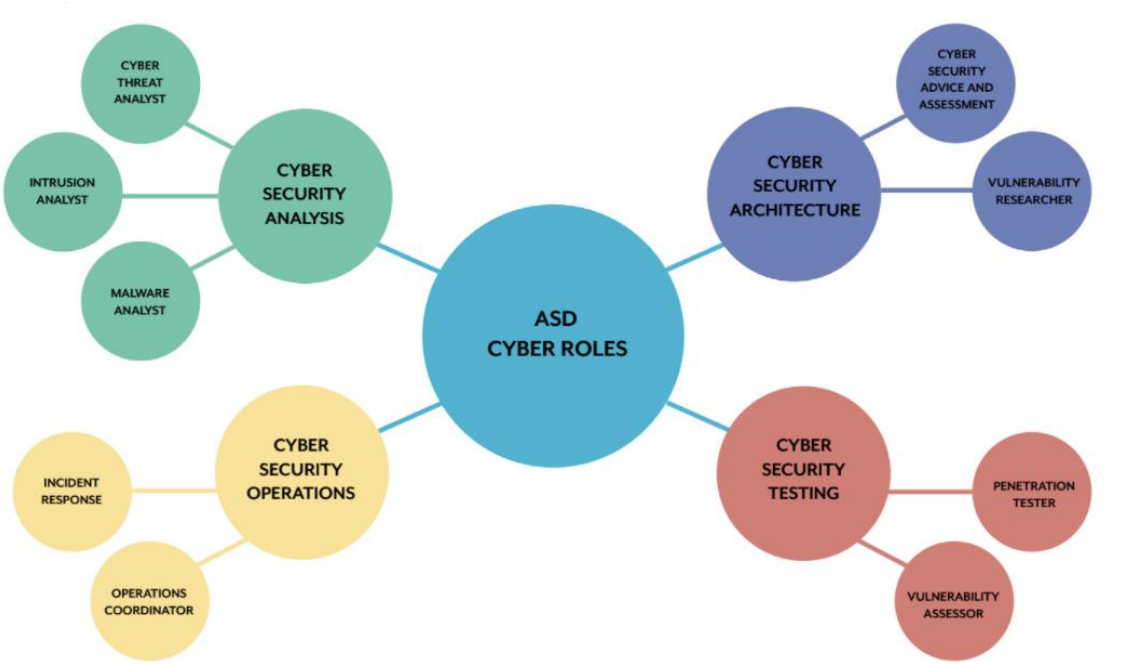


Figure 3.10: ASD Cyber Skills Framework Job Roles (Australian Signals Directorate, 2020)

As with SFIA and CIISec, this framework uses proficiency levels to illustrate the level of skills understanding. Figure 3.11 shows the proficiency levels for CIISec, SFIA and ASD Cyber Skills Framework. Both CIISec and the ASD Cyber Skills Framework have six proficiency levels, whilst SFIA has seven. The ASD Cyber Skills Framework uses these proficiency levels to show the proficiency levels for all the skills associated with the job roles they identified.

CIISec SKILLS FRAMEWORK	SFIA	NEW: ASD CYBER SKILLS FRAMEWORK
Level 1 (Knowledge)	Level 1 (Follow)	Level 1 (Learner)
Level 2 (Knowledge and Understanding)	Level 2 (Assist)	Level 2 (Novice)
Level 3 (Apply)	Level 3 (Apply)	Level 3 (Practitioner)
Level 4 (Enable)	Level 4 (Enable)	Level 4 (Senior Practitioner)
Level 5 (Advise)	Level 5 (Advise, Ensure)	Level 5 (Principal Practitioner)
Level 6 (Expert)	Level 6 (Initiate, Influence)	Level 6 (Expert Practitioner)
	Level 7 (Set Strategy, Inspire, Mobilise)	

Figure 3.11: Proficiency Levels for CIISec, SFIA and ASD (Australian Signals Directorate, 2020)

As an example, Figure 3.12 shows the job role of an Intrusion Analyst which lies within the Cybersecurity Analysis discipline. The Intrusion Analysis job role has multiple capabilities associated it, with each capability having many skills that are required to effectively perform the capability they are associated with. These skills are each ranked based on the proficiency levels, as depicted in Figure 3.11. Figure 3.12 shows that the Information Security Strategy skill requires both Level 1 and Level 4 proficiency and the Legal and Regulatory Environment skill requires Level 2 proficiency.

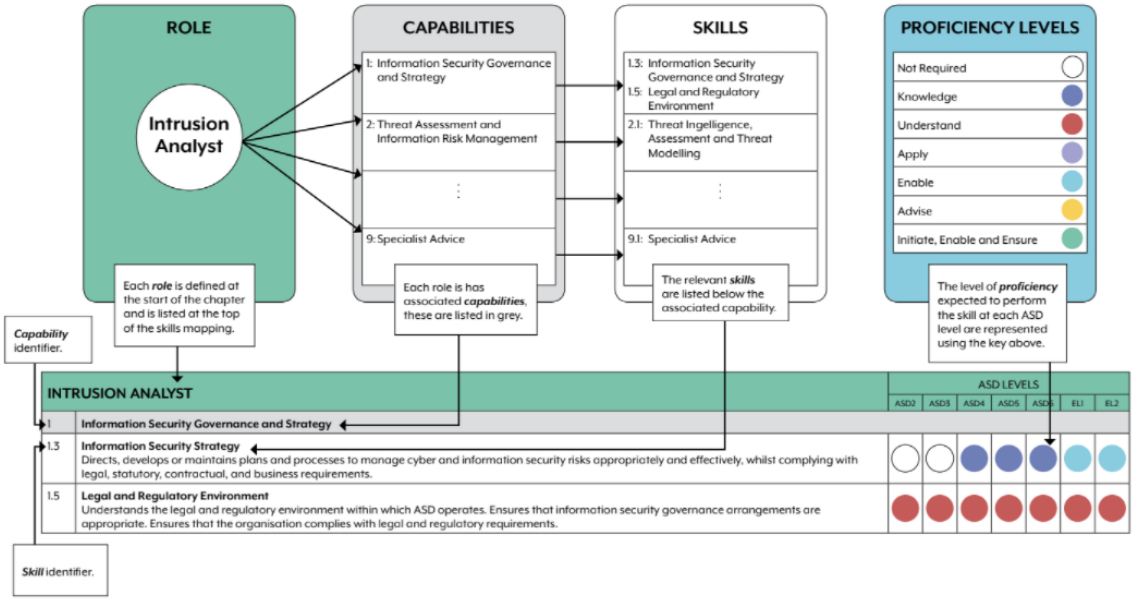


Figure 3.12: Intrusion Analyst according to ASD Cyber Skills Framework (Australian Signals Directorate, 2020)

This framework takes the proficiency level system, a key aspect from both CIISec and SFIA, and modifies it to fit its context. Overall, this framework is detailed and focusses on the proficiency levels required for skills related to cybersecurity job roles.

3.3.5. European Cybersecurity Skills Framework (ECSF)

The European Cybersecurity Skills Framework is an upcoming skills framework that has only recently (in November 2020) established an expert working group (ENISA, 2020). The goal of this working group was to advise and assist ENISA in building a European Cybersecurity Skills Framework that allows individuals, businesses, and training providers across the EU Member States to have a common understanding of the roles, competencies, skills, and knowledge they use. It might also raise awareness by identifying cybersecurity skills gaps that could be addressed through the adoption of a uniform European Cybersecurity Skills Framework.

The European Cybersecurity Skills Framework's major goal is to encourage harmonisation in the cybersecurity education, training, and workforce development ecosystem, as well as the establishment of a common European language in the cybersecurity skills context.

In April 2022, the European Cybersecurity Skills Framework released a draft version of the skills framework at a webinar (ENISA, 2022a). The final version of the framework was published in September 2022.

The European Cybersecurity Skills Framework identified 12 cybersecurity-specific job roles. Each of the job roles has defined knowledge areas, skills and tasks, including other details such as deliverables and missions (ENISA, 2022b). The 12 identified job roles are as follows:

1. Chief Information Security Officer (CISO)
2. Cyber Incident Responder
3. Cyber Legal, Policy and Compliance Officer
4. Cyber Threat and Intelligence Specialist
5. Cybersecurity Architect
6. Cybersecurity Auditor
7. Cybersecurity Educator
8. Cybersecurity Implementer
9. Cybersecurity Researcher
10. Cybersecurity Risk Manager
11. Digital Forensics Investigator
12. Penetration Tester

Table 3.10 shows the Digital Forensics Investigator job role in ECSF.

Table 3.10: Digital Forensics Investigator according to ECSF (ENISA, 2022b)

Profile Title	Digital Forensics Investigator	
Alternative Title(s)	Digital Forensics Analyst Cybersecurity & Forensic Specialist Computer Forensics Consultant	
Summary statement	Ensure the cybercriminal investigation reveals all digital evidence to prove the malicious activity.	
Mission	Connects artefacts to natural persons, captures, recovers, identifies and preserves data, including manifestations, inputs, outputs and processes of digital systems under investigation. Provides analysis, reconstruction and interpretation of the digital evidence based on a qualitative opinion. Presents an unbiased qualitative view without interpreting the resultant findings.	
Deliverable(s)	• Digital Forensics Analysis Results • Electronic Evidence	
Main task(s)	• Develop digital forensics investigation policy, plans and procedures • Identify, recover, extract, document and analyse digital evidence • Preserve and protect digital evidence and make it available to authorised stakeholders • Inspect environments for evidence of unauthorised and unlawful actions • Systematically and deterministic document, report and present digital forensic analysis findings and results • Select and customise forensics testing, analysing and reporting techniques	
Key skill(s)	• Work ethically and independently; not influenced and biased by internal or external actors • Collect information while preserving its integrity • Identify, analyse and correlate cybersecurity events • Explain and present digital evidence in a simple, straightforward and easy to understand way • Develop and communicate, detailed and reasoned investigation reports	
Key knowledge	• Digital forensics recommendations and best practices • Digital forensics standards, methodologies and frameworks • Digital forensics analysis procedures • Testing procedures • Criminal investigation procedures, standards, methodologies and frameworks • Cybersecurity related laws, regulations and legislations • Malware analysis tools • Cyber threats • Computer systems vulnerabilities • Cybersecurity attack procedures • Operating systems security • Computer networks security • Cybersecurity-related certifications	
e-Competences (from e-CF)	A.7. Technology Trend Monitoring B.3. Testing B.5. Documentation Production E.3. Risk Management	Level 3 Level 4 Level 3 Level 3

Alternative titles for this job role are shown, including Digital Forensics Analyst, Cybersecurity and Forensic Specialist and Computer Forensics Consultant. The Digital Forensics Investigator has a defined mission, deliverables, tasks, skills and knowledge.

This framework focuses on cybersecurity job roles only; hence, it does not consider other non-cybersecurity related job roles.

3.3.6. Canadian Cybersecurity Skills Framework

Canada has developed its very own Cybersecurity Skills Framework to address the unique needs of the Canadian labour market. This framework aims to guide cybersecurity workforce

development efforts that will support business and industry (Technation, 2020). The Canadian Cybersecurity Skills Framework is based on the NICE framework.

Figure 3.13 shows an overview of the Canadian Cybersecurity Skills Framework in which one can see that the framework has four categories, namely: Oversee and Govern, Design and Develop, Operate and Maintain, Protect and Defend. Each of these categories has different business-oriented job roles associated with them, some being technical roles, and others non-technical.

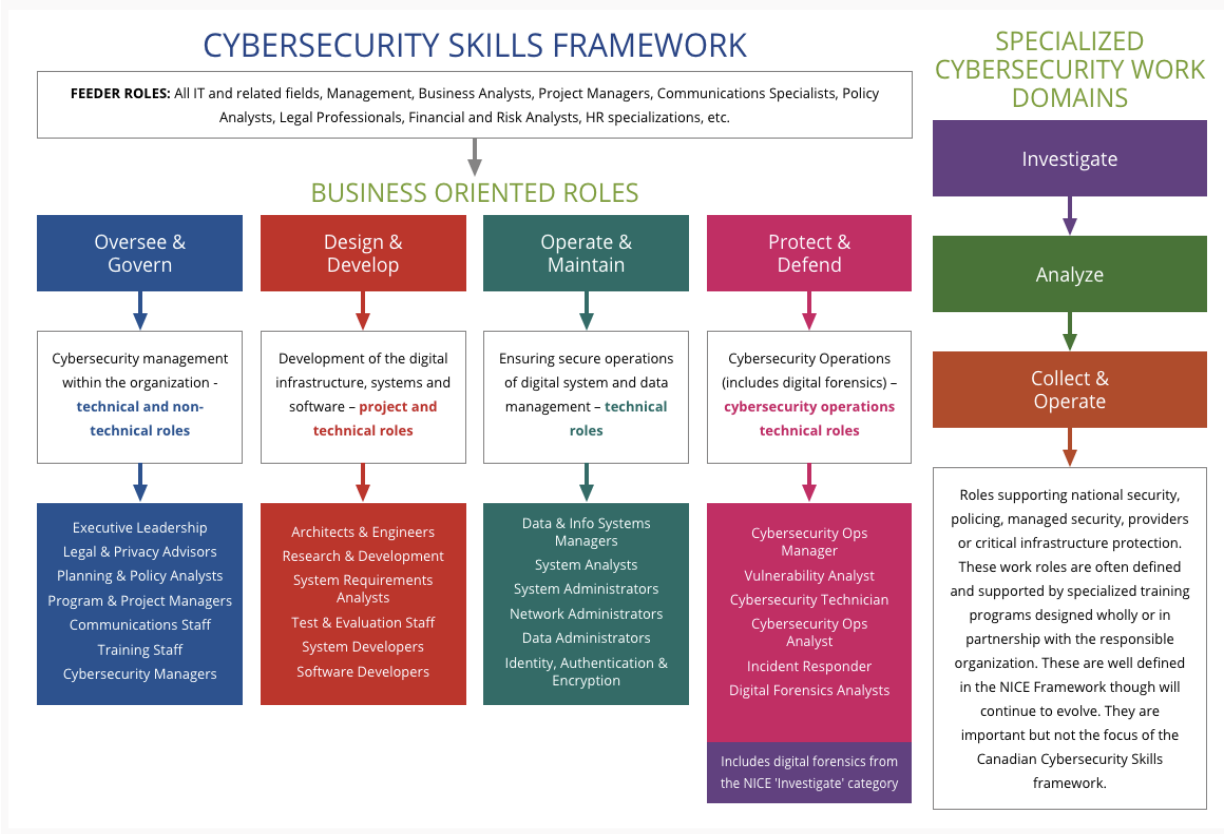


Figure 3.13: Canadian Cybersecurity Skills Framework Overview (Technation, 2022)

This framework does not focus solely on cybersecurity job roles, but also considers the cybersecurity-related KSATs required of non-cybersecurity workers (Adjacent Roles).

The business-oriented roles associated with the Operate and Maintain category are as follows (Technation, 2022):

Core Cybersecurity Roles:

- Identity Management and Authentication Support Specialist
- Encryption/Key Management Support Specialist
- Data Privacy Specialist/Privacy Officer

Adjacent Roles:

- Database Administrator
- Data Analyst
- Information Manager (NICE Knowledge Manager)
- Technical Support Specialist
- Network Operations Specialist
- System Administrator
- Data Systems Analyst
- Systems Manager (Includes system, software and data systems manager roles)

Each of these roles has defined KSATs and various other key aspects as can be seen in Table 3.11.

Table 3.11: Identity Management and Authentication Support Specialist in the Canadian Cybersecurity Skills Framework (Technation, 2022)

NICE Framework Role	None
Functional Description	Provides ongoing support to identity, credentials, access, and authentication management in support of organizational IT security.
Consequence of error or risk	Error, neglect, outdated information, lack of attention to detail or poor judgment could result in compromise of the system which, depending on the type of compromise, may have a significant impact on organizational IT systems, capabilities, or functions.
Development pathway	This is an often an entry-level job to the security domain after gained experience with network or system administration access management and credentials. With additional training and experience there is potential for more technically or operationally focused roles as well as management opportunities.
Other titles	• Access management analyst • System analyst • Identity, credentials, and access management (ICAM) specialist
Related NOCs	2171 Information systems analysts and consultants 2281 Computer network technicians

<table>
<tr><td></td><td colspan="2">2282 User support technicians</td></tr>
<tr><td>Tasks</td><td colspan="2">• Identify client requirements and propose technical solutions
• Model and map users to resources (e.g., role based)
• Install, configure, operate, maintain, and monitor related applications
• Deploy, configure, and manage user provisioning including identity synchronization, auto provisioning and automatic access deactivation, self-service security request approvals workflow and consolidated reporting
• Configure and manage enterprise and web-based access management solutions (single sign on, password management, authentication and authorization, delegated administration)
• Analyse patterns or trends in incidents for further resolution
• Manage identity change-request approval processes
• Audit, log, and report user life-cycle management steps against access control list on managed platforms
• Configure and manage federated identity, credentials, access management tools in compliance with security policy, standards, and procedures
• Complete tasks related to authorization and authentication in physical and logical environments
• Develop, deliver, and oversee related cybersecurity training material and educational efforts related to role</td></tr>
<tr><td rowspan="3">Required qualifications</td><td>Education</td><td>College diploma in IT field.</td></tr>
<tr><td>Training</td><td>• Training in relevant identity, credentials, access management and authentication policies, protocols, tools, and procedures.
• Developing and applying user credential management system</td></tr>
<tr><td>Work experience</td><td>Experience in managing directory services and working in a security environment.</td></tr>
<tr><td>Tools & Technology</td><td colspan="2">• Identity and access management systems
• Directory services
• Authentication tools and services
• Security event and incident management systems and/or incident reporting systems and networks</td></tr>
<tr><td>Competencies</td><td colspan="2">KSAs applied at the basic level:

• Identity, credential and access management architectures and standards
• Related application life-cycle processes
• Mapping and modelling credentials
• Policy-based and risk-adaptive access controls
• Developing and applying user credential management system
• Organizational analysis of user and business trends
• Client consultation and problem resolution

KSAs applied at an advanced level:</td></tr>
</table>

	• Network access, identity, and access management protocols, tools, and procedures • Authentication, authorization, and access control methods • Install, configure, operate, maintain, and monitor related applications • Developing and applying security system access controls. • Maintaining directory services • Organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)
Future Trends Affecting Key Competencies	• The increased reliance on virtualized and/or 'cloud-based' services will require knowledge of responsibilities of the services provider including their responsibilities for cybersecurity systems management. • If practiced within the organization, there will be a requirement to fully understand the implications of 'bring your own device' (BYOD) policies. This means that regardless of the device capabilities, there will need to be an assessment of the risks posed to the organization, mitigations to account for potential compromise through a personal device, and what actions will be required by the SOC in the event of an incident. • Increased use of automated tools, aided by artificial intelligence, will require understanding of how the tools will be integrated into identity and access management processes and the related technical and process changes. • Mechanisms to support the required level of trust and organizational risk will need to be in place to support monitoring and reporting of results from automated tools. Consequently, there will need to be increased understanding of organizational risks posed and potential responses within the dynamic threat environment. • The emergence and use of quantum technologies by threat actors will fundamentally change encryption security. This will require knowledge and skills related to implementing a quantum safe strategy as well as a deep understanding of the implications to authentication protocols and how to defend against potential quantum computing threats.

With the Canadian Cybersecurity Skills Framework having been discussed in detail the next section will compare each of the identified frameworks based on their key characteristics.

3.4. Comparative Analysis of Global Skills Frameworks

Having discussed the most common global IT skills frameworks and global cybersecurity skills frameworks it is important to compare these according to their target audience namely, Employees (EMP), Job Seekers (JS) and Educational Facilities (EF) as well as KSATs, job roles and focus. Table 3.12 provides a summary of this comparative analysis.

Table 3.12: Comparative Analysis of Global IT and Cybersecurity Skills Frameworks

Framework name	Target Audience			KSATs				Job roles	Focus
	EMP	JS	EF	K	S	A	T		
Skills Framework for Infocomm Technology	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	**Main:** General IT **Secondary:** Cybersecurity
Skills Framework for the Information Age (SFIA)	Yes	Yes	Yes	No	Yes	No	No	No	**Main:** General IT **Secondary:** Cybersecurity
The National Initiative for Cybersecurity Education (NICE)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	**Main:** Cybersecurity **Secondary:** General IT
SPARTA Cybersecurity Skills Framework	No	No	Yes	Yes	Yes	Yes	No	Yes	**Main:** Cybersecurity **Secondary:** General IT
CIISec Framework	No	Yes	No	Yes	Yes	Yes	No	No	**Main:** Cybersecurity
ASD Cyberskills Framework	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	**Main:** Cybersecurity
European Cybersecurity Skills Framework (ECSF)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	**Main:** Cybersecurity
Canadian Cybersecurity Skills Framework	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	**Main:** Cybersecurity **Secondary:** General IT

Each of the eight skills frameworks has key differences but also many similarities due to many of them being based on one or more of the other identified frameworks. The frameworks are each unique in their approach, with some specifically focusing on cybersecurity job roles and some focusing specifically on general IT job roles.

Based on Table 3.12, three main target audiences were identified, namely employers, job seekers and educational facilities. Employers can use these frameworks to better understand the job roles in their organisation and to improve existing job roles. Job seekers can use these frameworks to better understand what is required of the job role that they are interested in pursuing. Educational facilities can use these frameworks to improve their IT-related curricula to ensure that it aligns with the needs of the industry and prepares graduates for future IT job roles. Five out of the eight identified frameworks cater for all three target audiences. Frameworks such as the SPARTA Cybersecurity Skills Framework and the CIISec Framework only cater for a single target audience, that is, educational facilities and job seekers, respectively. The Canadian Cybersecurity Skills Framework caters for both employers and job seekers.

Of the identified skills frameworks, four of the eight make use of knowledge, skills, abilities and tasks (KSATs). SFIA is the only framework that focuses solely on skills. SPARTA, CIISec and ASD all make use of knowledge, skills and abilities, but do not specify tasks.

SFIA and CIISec are the only frameworks that do not accommodate for job roles; this means that six of the eight frameworks identified have a definite focus on job roles.

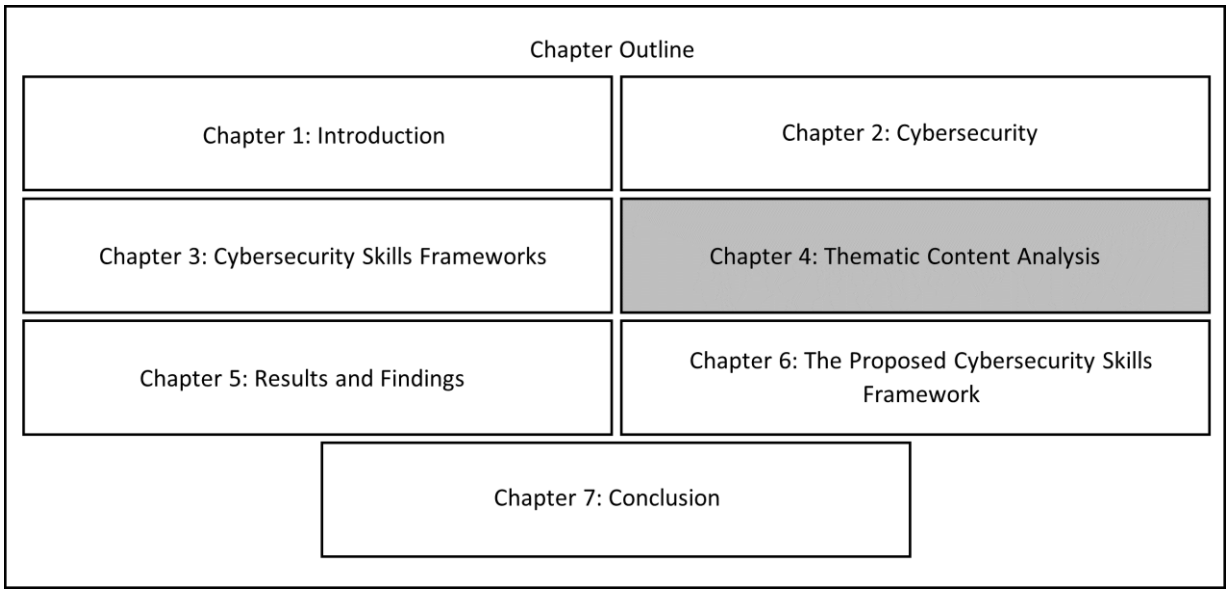
Three of the identified frameworks have a specific focus on cybersecurity. All the other frameworks do not focus specifically on cybersecurity but focus on both general IT as well as cybersecurity. Although some of them might have a stronger focus either on general IT or on cybersecurity, they do not exclude the other.

3.5. Conclusion

This chapter introduced some of the skills frameworks that are currently in development, as well as those already in use. The characteristics and structure of these frameworks helps inform the structure and detail of the proposed framework in Chapter 6.

This chapter assists in understanding the context of other countries skills frameworks and provides valuable input to the proposed cybersecurity framework for South Africa. To develop the proposed framework the detail used to define job roles and their KSATs in this chapter are used in conjunction with the data gathered from the job postings found on LinkedIn that were analysed using a thematic content analysis. The data collection process, as well as the thematic content analysis is discussed in Chapter 4. In addition, Chapter 4 compares and motivates the use of ATLAS.ti as the preferred software analysis tool to be used during the thematic content analysis.

Chapter 4 – Thematic Content Analysis



4.1. Introduction

Chapter 3 discussed the details regarding existing cybersecurity skills frameworks that are currently in use by other countries and their relevance to this study. This chapter provides a discussion of the data collection process and the thematic content analysis conducted during this study. In addition, this chapter motivates the use of ATLAS.ti as the preferred software tool for conducting the content analysis. The purpose of this chapter is therefore to define and describe the process followed in conducting the thematic content analysis.

The structure of this chapter is as follows: Section 4.2 discussed a related study in South Africa. Section 4.3 provides a detailed comparison of the data analysis software tools considered for the content analysis, while Section 4.4 describes the data collection process. Section 4.5 discusses the step-by-step phased approach used in conjunction with ATLAS.ti to conduct the thematic content analysis. The conclusion to this chapter is provided in Section 4.6.

4.2. Related Study in South Africa

The study by Parker and Brown (2018) entitled “Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa” is considered very relevant and important to this research and was used as a baseline for the data collection process of this study. Parker and Brown (2018) had a dataset of 196 job postings that had been collected over

a period of two months. Parker and Brown (2018) used five job posting websites for their study. Parker and Brown (2018) mostly made us of LinkedIn since it contributed 54.1 percent of their data sample, making it the website with the most job postings in their data sample. They also stated that the advertisements on LinkedIn provided a greater depth of information compared to other job posting websites.

Parker and Brown (2018) used the search terms 'cybersecurity' and 'IT security' on the job posting websites. In the description and title of postings they specifically looked for the word 'security'. Many job postings that would have been relevant to their study may not have been captured in their dataset since they only looked for the word 'security'. In most cases, the word 'security' is rarely mentioned explicitly; rather, a relevant security certification would be mentioned. Therefore, in moving forward with the data collection process of this study, it was decided not to only consider the term 'security', but also to look for possible certifications relevant to security as determining search terms for finding further relevant job postings. Parker and Brown (2018) also focused only on cybersecurity professionals. In contrast, this study focuses on IT professionals; as such, uses a broader range of search terms.

4.3. Data Analysis Software Tool Comparison

In this section it will be established which software tool was considered best used for the purpose of this research and for the effective conducting of the thematic content analysis. Multiple popular software analysis tools are compared against one another based on their features, and their relevance to this research.

The following software analysis tools were identified and compared according to the specific features required for this study:

- NVivo (Link)
- ATLAS.ti (Link)
- Provalis Research Text Analytics Software (Link)
- Quirkos (Link)
- MAXQDA (Link)
- Dedoose (Link)

The above-mentioned software tools were chosen as they are regarded as the top qualitative software analysis tools, according to Predictive Analytics Today (2021).

Before discussing each of the features and their relevance to the study, certain terms need to be defined and explained. According to Soratto et al. (2020) these are as follows:

- **Project:** A project is the file that contains all the relevant information for the content analysis.
- **Document:** represents all the empirical data added to the project for example, Word documents, images, video files.
- **Quotations and Codes:** These two are closely related since quotations are selected segments that are important to make note of and each of the quotations can be coded or assigned a code. Codes synthesise the meaning contained in a set of similar quotations.

See Figure 4.1, where the highlighted text is the quotation, and the associated code is the tag "Formal Education" located at the right-hand side of the highlighted quotation.

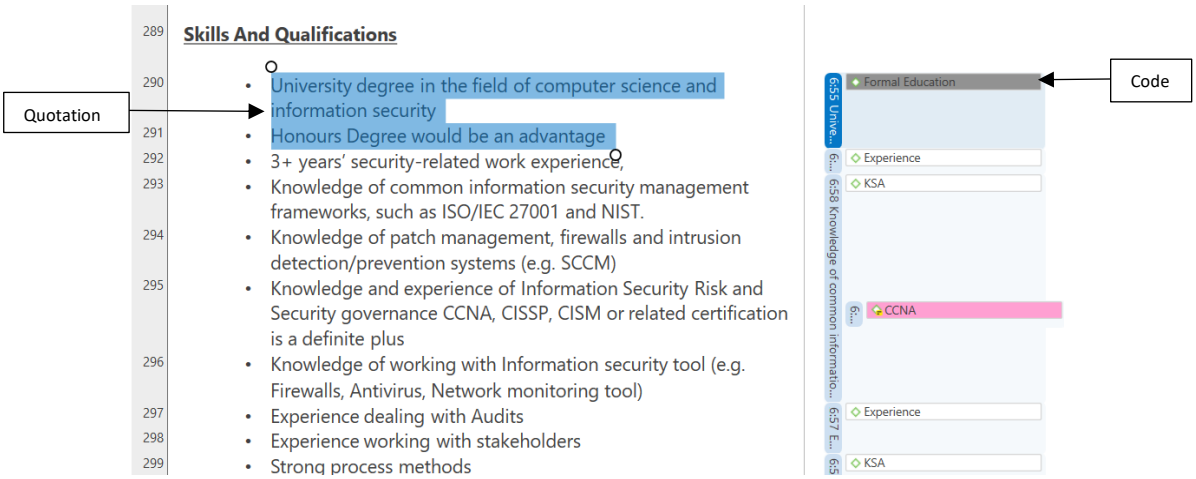


Figure 4.1: Example of Codes and Quotations in ATLAS.ti

- **Data segments:** Refers to sections of information that need to be captured or made note of. These data segments are what is used to create Quotations and Codes.
- **Comments and memos:** Comments can be written for all kinds of objects (for example, codes and quotations) in a project, whereas memos are useful for a variety of purposes. They can be used as purely technical devices to generate a list of codes, reminders or research diary entries.

The following were deemed to be relevant features that the chosen tool should have:

- **Annotation support.** Annotation is achieved by labelling data segments with a code and, if required, adding comments to the segment (Wijngaarden, 2019). Annotations are required to code a data set; hence, a requirement for this study.
- **Data import/export.** *Data import* is the ability to import documents, video files, pictures, or any other required media into the software analysis tool. *Data export* is the ability to generate reports based on the coding done in a project. It was deemed necessary to be able to import documents into the software tool and to have the ability to generate reports for the study.
- **Tagging**, in this scenario, tagging is a synonym for coding (Atlas Ti, 2019). Tagging/coding was a requirement for this study as it was deemed necessary to be able to tag or code certain data segments with a relevant code to make the process of data analysis easier.
- **Text analysis** is the process of using unstructured text and creating facts (On To Text, 2017). The software tool needed to support *Text analysis* for the researcher to make use of the unstructured text, in this case the job postings, and then to analyse this unstructured text and create facts surrounding these job postings.
- **Data visualisation** is the representation of information in graphical manner. Some examples of this include graphs, charts and maps (Tableau, 2018). Graphical representation of information was considered highly important for this study as it simplified the delivery of information to relevant parties and, due to this, it was considered to be a requirement for the selected data analysis software tool.
- **Search/filter.** *Searching* is the process by which a term is used to find relevant information. This is typically done with the use of a search engine such as Google (BDC, 2016). *Filtering* is used to refine a specific search with the use of filters such as date ranges (Dynamic Yield, 2017). To search and filter effectively for specific codes or quotations or any other items, a good search and filtering system was a necessary feature for the selected software tool.

Based on the above-mentioned features, Table 4.1, compares each software tool identified against the predetermined set of required features, as well as whether an Nelson Mandela University (NMU) Licence was available for use. The list of features per software analysis tool used to create Table 4.1 can be found at Capterra (n.d.).

Table 4.1: Comparison of Software Analysis Tools

Name	NMU Licence	Annotations	Data Import /Export	Tagging	Text Analysis	Data Visualization	Search/ Filter
NVivo	No	Yes	Yes	Yes	Yes	Yes	No
ATLAS.ti	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Provalis	No	Yes	No	No	Yes	No	No
Quirkos	No	Yes	No	No	Yes	Yes	Yes
MAXQDA	No	Yes	No	No	Yes	Yes	No
Dedoose	No	No	Yes	No	No	Yes	Yes

Based on Table 4.1, it is evident that ATLAS.ti is the software that has all the required features and therefore it was chosen as the software analysis tool that will be used to conduct the thematic content analysis.

NVivo could also have been a good option, but it lacked the support for *searching and filtering*, which is one of the most important required features. ATLAS.ti is also available through The Nelson Mandela University, which means there was no need for the purchasing of a licence.

4.4. Data Collection Process

Data collection is a systematic process of gathering observations or measurements, which allows researchers to gain first-hand knowledge and original insights into their research problem (Bhandari, 2020). The research problem defined for this study is stated as follows: "*Without a common lexicon of the cybersecurity knowledge, skills, abilities, and tasks (KSATs) required of IT professionals, as they relate to specific IT job roles in South Africa, the cybersecurity skills gap cannot be sufficiently addressed"*. This chapter aimed to gather the relevant data needed to define the KSATs needed of IT professionals by collecting job postings. This data was then further explored in the chapters to follow.

4.4.1. Data Collection Pilot Study

Before starting the formal data collection process, it was decided to conduct a pilot study to gain a better understanding of the data to be collected for this study. In September 2020, the pilot study began. Data was collected weekly on three job posting websites, namely: LinkedIn, Careers24 and Career Junction. Figure 4.2 illustrates the process followed during the pilot study.

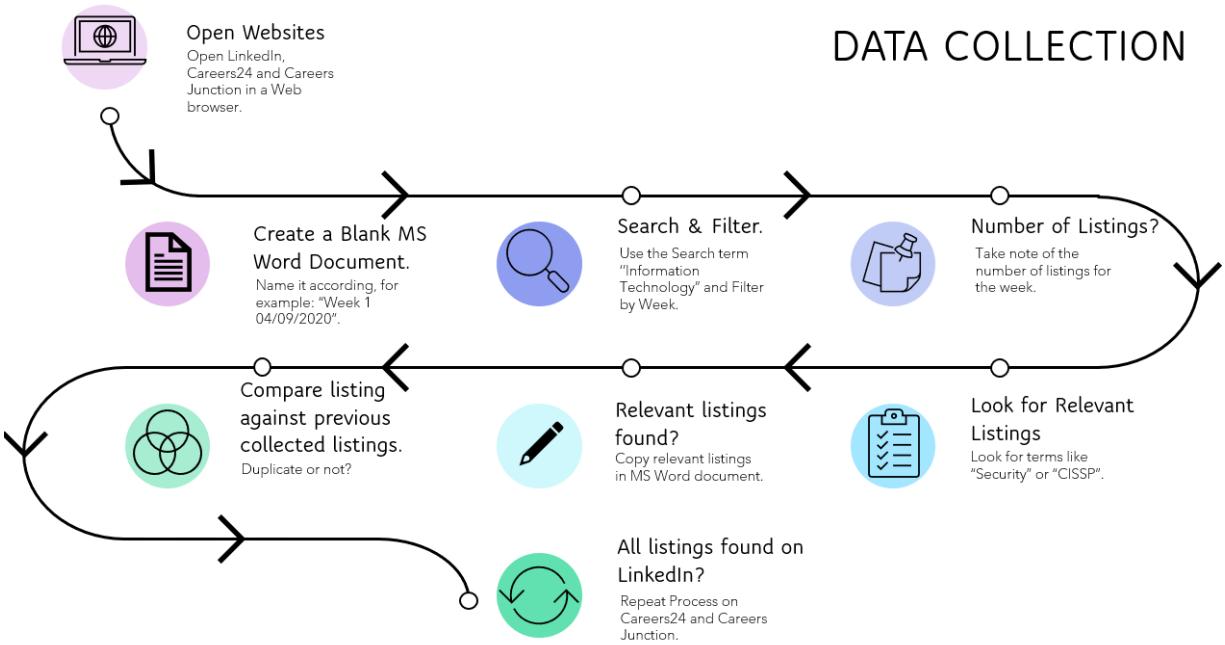


Figure 4.2: Pilot Study Data Collection Process

On the Friday of each week in September 2020 (4, 11, 18 and 25 September), the data for that week was collected. All three websites (LinkedIn, Careers24, and Career Junction) were opened in a web browser tab of their own. A blank MS-Word document was created and named according to the week of the month and date of collection, for example 'Week 1 04/09/2020'. Focusing on one website at a time, the search feature was used with the search term 'Information Technology' to search for relevant job postings.

The search results were further filtered by week using the search filters provided and set to be South African-based job posting only. This resulted in job postings being displayed for each specified week in South Africa. A note was then made about the number of job postings for that week. All displayed job postings were read and scanned for terms relating to 'security' or certifications relating to security, such as 'CISSP'. All job postings containing any of these terms were considered relevant to the study, and their titles were noted, together with the organisation posting the advertisement and the location of the position. The entire job posting

was then copied from the website and pasted into the corresponding MS Word document created for that week. The title of the job posting was then searched for on the other websites to check for duplications on those websites. If the advertisement was found on the other two websites, a note was made regarding this. The title and location, as well as the organisation posting the advertisement, were compared to previously collected postings noted. Job postings that already existed in the dataset were removed as they were deemed to be duplicates. Table 4.2 illustrates an example of the job postings found on LinkedIn.

Table 4.2: An Example of a Job Posting on LinkedIn.

Desktop Support Technician
Company Name: Vox Telecom
Company Location: Durban, KwaZulu-Natal, South Africa
Support and maintain organizational computer systems, desktops, and peripherals. That includes installing, diagnosing, repairing, maintaining, and upgrading all organizational hardware and equipment while ensuring optimal workstation performance.
Job Objectives:
To provide immediate first line support and daily assistance of all IT related issues. Assisting the regional IT Managers and the Head of IT with all IT related functions.Troubleshooting and problem solving of user issues (Local and remote). Maintaining company IT standards and procedures, network security and confidentiality of information. Hardware and Software - setup, repair, configure, troubleshoot. Assisting with general tasks and administration or Ad-hoc tasks and problems. Improving helpdesk turnaround time and escalation of any issues and calls. Ensure prompt feedback to all calls assigned and do follow ups with users. Assisting with uptime and monitoring of the IT infrastructure. Assisting with the Helpdesk function – logging and maintaining all support calls. End user support queries. Maintaining company hardware assets using asset management tools and processes. Setup hardware devices for users. (PC's laptops, Tablets, Mobile devices). Repair laptops – diagnose for hardware faults and provide assessment. Repair laptops –upgrade, install or swop internal components or parts.
Minimum Requirements:
Matric. CompTIA A+ Essential. CompTIA N+ or IT Diploma, MCITP or MSCE 2012 (Desktop Engineer).

Job Skills:
Willingness to learn and follow through on operations. Handle stress very well and work under lots of pressure – Deadline orientated. Troubleshooting ability & quick learner for recurring problems. Flexible with working hours availability to work afterhours – occasional overtime may be required. Must have a good telephonic manner and communication skills.
Seniority Level: Entry level
Industry
Information Technology & Services Computer Software Telecommunications
Employment Type: Full-time

The data collection process discussed above was repeated until all postings had been collected on the job posting website focused on. Thereafter, the focus was shifted to the next job posting website and the process repeated. LinkedIn was always focused on first, followed by Careers24 and lastly, Career Junction.

During the pilot study, certain findings became evident. On average, 522 job postings were posted on LinkedIn weekly in South Africa, when using only the search term 'Information Technology', as depicted in Figure 4.3.

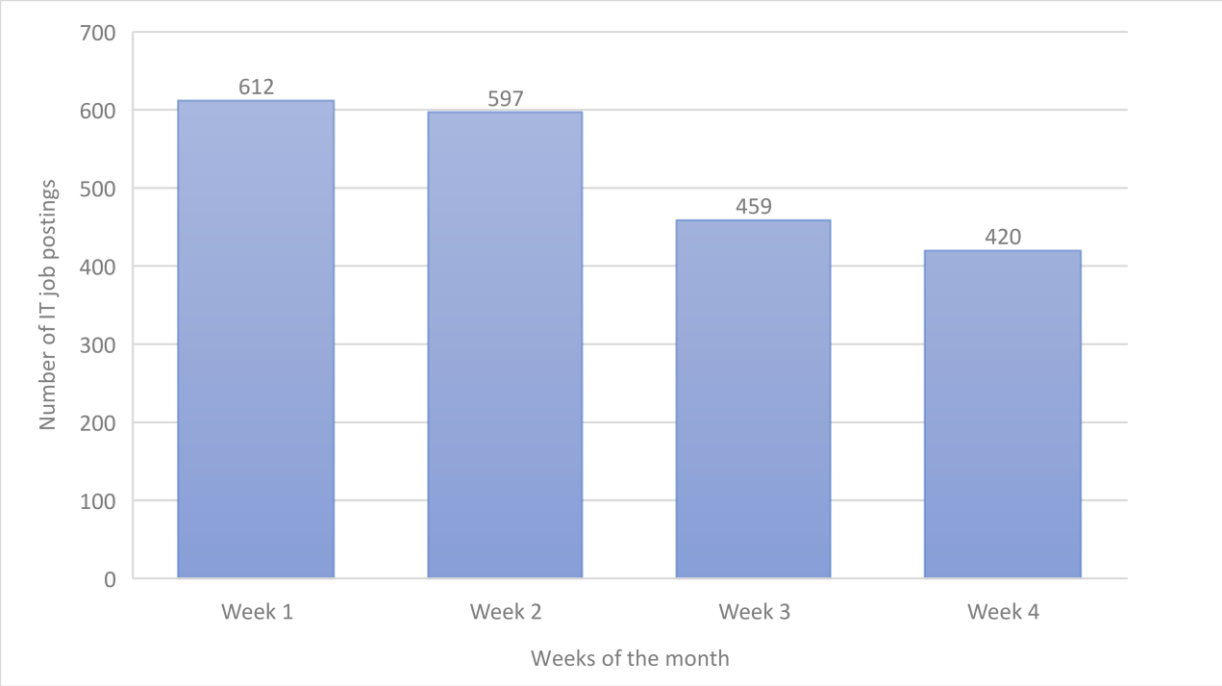


Figure 4.3: Number of Postings per week in September 2020 on LinkedIn Only (Pilot Study)

Week 1 provided the highest number of IT job postings with 612, followed by Week 2 with 597 related IT job postings. There was a significant drop in IT job postings during Week 3 (459) and Week 4 (420).

This did not include the IT job postings on the other two websites, namely Careers24 and Career Junction. LinkedIn by itself had, on average, 522 IT job postings per week, while the other two career websites added another 500 job postings. Due to the number of daily job postings across the three websites, the data collection became too overwhelming to handle on a single day each week as this required the manual reading of about 1000 IT job postings in a single day. Because of this, it only allowed for a small sample of the available IT job postings to be collected, resulting in possibly missing other relevant job postings. This led to the decision to conduct data collection three times per week to capture as many relevant job postings as possible. It was decided to use the 24-hours filtering option due to the limited filtering options in LinkedIn. LinkedIn only allows the following filtering options: '*All Time*', '*Past Month*', '*Past Week'* and '*Past 24 hours'*. Ideally, an option for the past 48 hours would have been more effective, but unfortunately this was not available; hence, the decision to use the '*Past 24 hours'* filter. It also allowed for the use of more search terms to widen the range of possible IT job postings. During the pilot study, it also became evident that the two most important collection days are Tuesdays and Thursdays, since the most postings occur on these days. There was found to be an average of 100 job postings daily using the search term 'Information Technology'. The third collection day was either on Wednesdays or Fridays. In the event that data collection could not take place on the Wednesday, Fridays were used as a backup data collection day. It must also be noted that there was a downward trend in terms of the number of IT job postings per week as the month progressed, as evident in Figure 4.3.

When conducting the pilot study, it also became evident that Careers24 had very few postings compared to LinkedIn (55 job postings weekly using the search term 'Information Technology') and that many of these IT job postings were duplications posted by the same organisations/people (spam postings). The job postings on Careers24 and Career Junction also lacked detail compared to those on LinkedIn. For most job postings on Careers24 and Career Junction, the advertisement could also be found on LinkedIn. From the pilot study, it was evident that LinkedIn contained most of the IT job postings on Careers24 and Career Junction, in addition to its own unique IT job postings that could not be found on either of the other

career websites. This led to the decision to use LinkedIn solely for the data collection for this study. Furthermore, LinkedIn contained more detail in IT job postings, contained fewer spam postings, and had more job postings posted daily.

To broaden the possible range of job postings relating to IT professionals, it was necessary to consider further search terms. Although most job postings could be found using only the term 'Information Technology', there were some job postings that only appeared when using other search terms, for example, 'information security', 'computer science', 'cyber security', 'cybersecurity', and 'network security'.

Due to the findings of the pilot study the final set of search terms selected for the actual job posting data collection phase of this study included the following:

- Information Technology
- Computer Science
- Information security
- Cybersecurity/Cyber security (Both spelling variations)
- Network security

In summary, the data collection process was refined using a pilot study and the necessary changes in the way the data was collected were documented. Instead of only once weekly, data was collected three times weekly based on the most active days, Tuesdays, Thursdays and one other day of the week. In addition, only LinkedIn.com was used over the four-month period from October 2020 to January 2021.

4.4.2. Data Collection (October 2020 - January 2021)

Based on the findings during the pilot study, the data collection process involved with the actual data collected from October 2020 until January 2021, was refined. Certain changes were made to make the data collection process easier and more accurate. Table 4.3 shows the changes implemented as a result of the pilot study.

Table 4.3: Comparison between Pilot Study and Refined Data Collection Process

Original Data Collection Process (Pilot Study)	Refined Data Collection Process
Data collected once a week	Data to be collected on Tuesdays, Thursdays and Wednesdays or Fridays resulting in data being collected on three days per week.
Three websites used, namely LinkedIn, Careers24 and Career Junction	LinkedIn was the only career website used to collect the data.
Search location was set to South Africa. Search filter used was for the past week	Search location was set to South Africa. Search filter was changed to the past 24 hours to capture all postings for the past 24 hours.
Only two search terms used, i.e., 'Information Technology' and 'Computer Science'	Search terms used: Information Technology Computer Science Information security Cybersecurity/Cyber security Network security

Besides these changes, the overall step-by-step process of collecting data was kept the same as the process used in the pilot study. Figure 4.4 depicts of the updated data collection process.

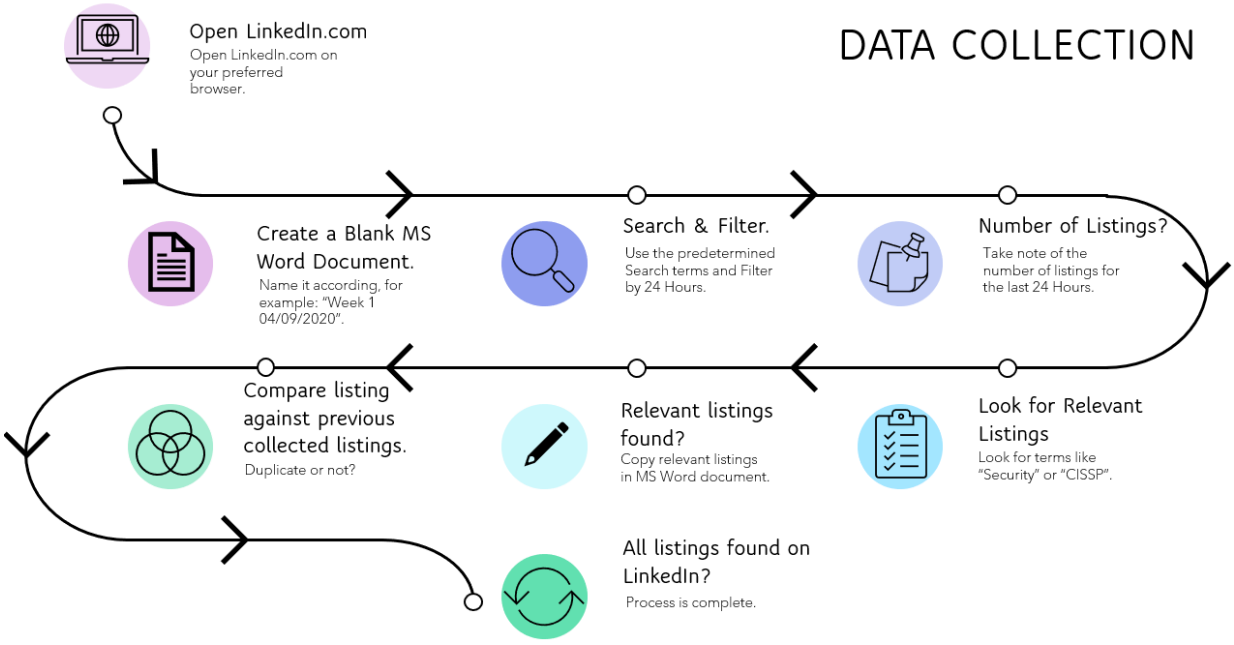


Figure 4.4: Revised Data Collection Process

Over the four-month period of data collection from October 2020 to January 2021, a total of 313 IT-related job postings were collected. A steady decline was evident in the number of job postings collected from October to December of 2020, as depicted in Figure 4.5.

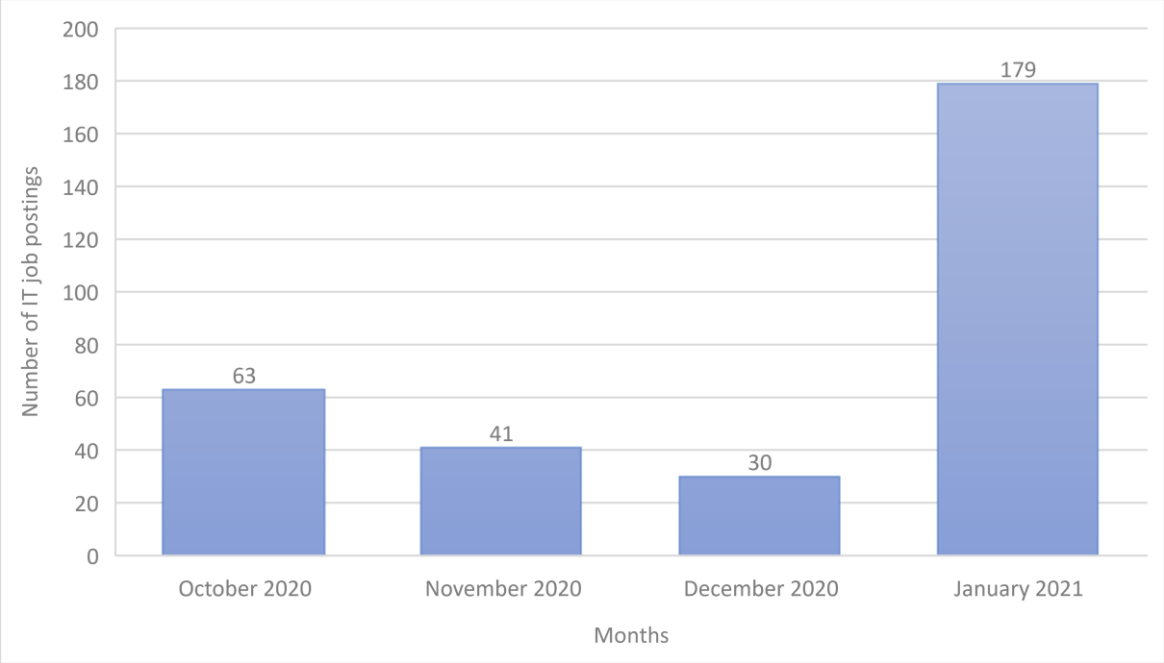


Figure 4.5: Number of Job Postings Monthly (Oct 2020 – Jan 2021)

In January 2021, the number of job postings grew substantially, leading to January 2021 contributing 57 percent of the total job postings in the dataset. This increase is believed to be due to many companies wanting to hire newly graduated students early in the new year and due to many employees resigning at the end of the year. This data was then analysed using the software tool, ATLAS.ti, discussed in Section 4.3. The following section explains how the data was analysed.

4.5. Thematic Content Analysis Using ATLAS.ti

Data collection for this study finished at the end of January 2021 after having collected a total of 313 job postings. These job postings were then analysed by conducting a thematic content analysis in ATLAS.ti.

In order to effectively analyse the data collected, a three-phased approach was used, similar to the approach used by Soratto et al. (2020). Soratto et al. (2020) explains in detail how using ATLAS.ti, in combination with the proposed three-phased approach, provides a promising strategy for conducting a thematic content analysis. Table 4.4 presents the three phases of the thematic content analysis and the associated steps taken in ATLAS.ti.

Table 4.4: Three-Phased Approach to ATLAS.ti Content Analysis (Soratto et al. ,2020)

Phases of thematic content analysis	**Steps in ATLAS.ti**
First Phase: Pre-analysis	Creating the project. Adding documents. Grouping documents into document groups. Writing first memos on overall project aim including research questions.
Second Phase: Material Exploration	Reading the data, selecting data segments, and creating quotations. Creating and applying codes. Writing memos and comments. Grouping codes and memos.
Third Phase: Interpretation	Exploring the coded data using various analysis tools. Linking quotations, codes, and memos on the conceptual level. Continuing memo writing. Generating network views. Extracting reports.

First Phase: Pre-analysis

To start the first phase, a new project was created in ATLAS.ti. The project was titled 'Job Analysis'. All the data collected for the months of October 2020, November 2020, December 2020, and January 2021 were added to this project. The next step was to import the MS Word documents containing the job postings for each month into the project. Once imported, these documents were grouped according to month, resulting in four groups named 'OCT', 'NOV', 'DEC' and 'JAN'. Each monthly group contained four MS Word documents, one for each week of the month, as shown in Figure 4.6. The number indicated in brackets for each week, as shown in Figure 4.6, is the number of quotations in the document for that week.

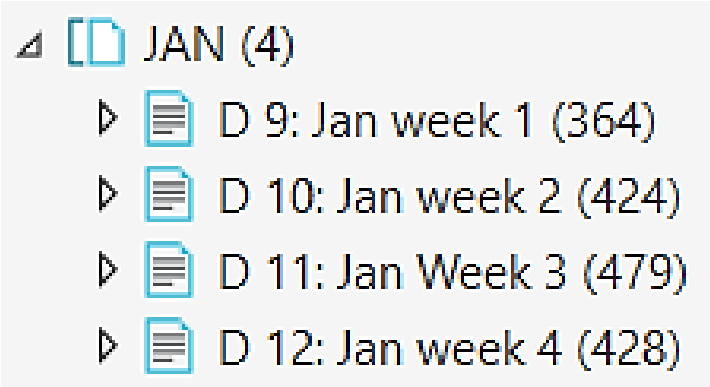


Figure 4.6: Example of a Document Group

Once the documents were grouped, memos were written containing the research objectives/questions and the overall aim of the project so that it could be accessed easily in ATLAS.ti. The specific research objective that is relevant to this chapter is SRO3 which is: "*To*

determine the cybersecurity KSATs required of IT professionals within South Africa, and how they relate to specific IT job roles".

Second Phase: Material Exploration

To start the second phase of the thematic content analysis, a document group was opened, and a document was analysed. This phase started with the document group called '*OCT*', and the document for the first week of October (Week 1 Oct) was selected. This document was then read, important data segments were selected, and quotations were created for these data segments. Each of the quotations was then assigned a code. Thereafter, the next document in the group was selected which, in this case, was called 'Week 2 Oct'. After it had been completed, the same process was followed for the documents 'Week 3 Oct' and 'Week 4 Oct'. Once the document group '*OCT*' was completed, the next group was selected, that being the document group '*NOV*', and the documents for each week in document group '*NOV*' were completed. The same process was followed for document groups 'DEC' and '*JAN*' as well as for their respective weekly documents. At this stage there were a total of 640 codes and 3580 quotations after completion of the coding for all four of the document groups (*OCT, NOV, DEC, JAN*). Table 4.5 contains a list of important data segments as well as examples of some identified quotations, codes, and code groups associated with each data segment.

Table 4.5: Example of Data Segments Identified in Study

Data segment	Example of possible quotations	Code assigned	Code group
The title of the job posting.	Cybersecurity Software Developer	Software developer	Job Roles
The company who posted the job posting.	Cisco	Cisco	Companies
The region in which it was posted.	Gauteng, Western Cape, Eastern Cape.	Gauteng	Regions
Any knowledge, skills, or abilities (KSAs) required for the job posting.	Able to work in teams and have good communication skills.	KSA	KSATs
The tasks associated with the job posting.	Fix UI issues on webpages. Ensure Security of Website.	Tasks	KSATs
Formal education required.	NDip Software Development	Formal Education	Education
Any certifications required.	CCNA	CCNA	Certifications

The industry the position is in.	Healthcare	Healthcare	Industries
Whether the position is full-time/part-time or contracted.	Full-time	Full-time	Type of job
The level of the position.	Entry level	Entry level	Job levels

These were the only data segments identified that were deemed relevant to the study and each quotation is linked to only one data segment. Each quotation was assigned a single code.

When all job postings had been coded, these codes needed to be organised. To do this, a similar process was followed to that with the document groups, called code groups. Assigned codes could only belong to one code group. Each of the different codes assigned was grouped according to their type. For example, all certifications were grouped into a code group called *Certifications*. The same was done for all the other assigned codes. A total of nine code groups were identified. Figure 4.7 contains the full list of the code groups identified for this study.

Figure 4.7: List of Code Groups

Once all codes had been grouped, each group was inspected individually looking for possible duplications. For example, in the case of the *Certifications* group, it contained multiple occurrences of the same certifications due to them often being referred to in various ways by different employers. One such case was the certification Security+. It was referred to as S+ in some cases and as Security+ in others. In this case, the two codes were merged into a single code, named Security+.

Figure 4.8 depicts the 32 codes within the *Certifications* Code Group.

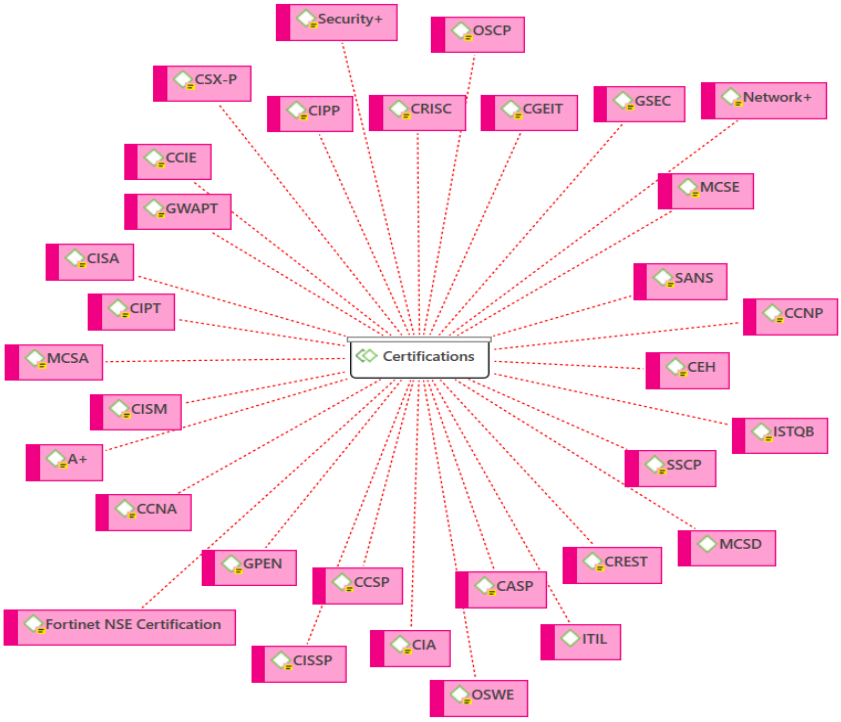


Figure 4.8: Certifications Code Group

Once the codes had been grouped and checked for duplicates, there were a total of 552 codes in the project; thus a reduction of 88 from the original 640 codes.

Even though steps were taken during the data collection process to mitigate the number of duplicate job postings, there was always still a chance that duplicate job postings could exist in the data set. Due to this, another check for duplicates was done before moving to the final phase of the thematic content analysis. This was done by focusing on the code group called "Companies". This code group contains all the company names that have job postings in the dataset. Each job posting from a company would be compared to see whether there were duplicate job listings for that company. If duplicates were found, the coding done on that job posting was removed; thus, effectively removing the job posting from the dataset. There were 33 identified duplicates at this stage, bringing the total number of job postings down from 313 postings to 280 postings.

Third Phase: Interpretation

In this phase of the thematic content analysis, the primary focus was on the code group called "Job Roles". At the start of this phase there were a total of 280 job roles in the "Job Roles" code group. Some of these job roles were the same type of job, but were named differently due to

some companies having different names for the same job role. For example, a job role named '*Software Developer*' and a job role named '*Application Developer*' would be merged into a single job role named '*Software Developer*' since they refer to the same job role. Each job role was individually assessed, and their knowledge, skills, abilities, tasks (KSATs) and required certifications were noted in a comment associated with the job role. To determine whether job roles are the same, KSATs were compared. If they had the same KSATs and the job roles seemed to be the same the job role, the job roles were merged into one. After the completion of this phase, there were a total of 20 unique job roles, each having defined KSATs as well as various certifications associated with them. Appendix A depicts the 20 identified job roles as well as the job role codes that have been merged with each identified job role.

This was a substantial decrease from the original 280 job roles at the beginning of this phase. Once the thematic content analysis process had been completed, the total number of codes was reduced to 351, from the initial number in the second phase of 552. This large reduction in codes is mainly due to the merging of job roles.

Figure 4.9 depicts the changes in the number of job roles, codes and job postings during each phase of the process.

Figure 4.9: Graph Depicting the Three-Phased Approach

The last process in this third phase was generating reports and visual representations of the final data. This can be done through multiple methods such as exporting reports to an Excel

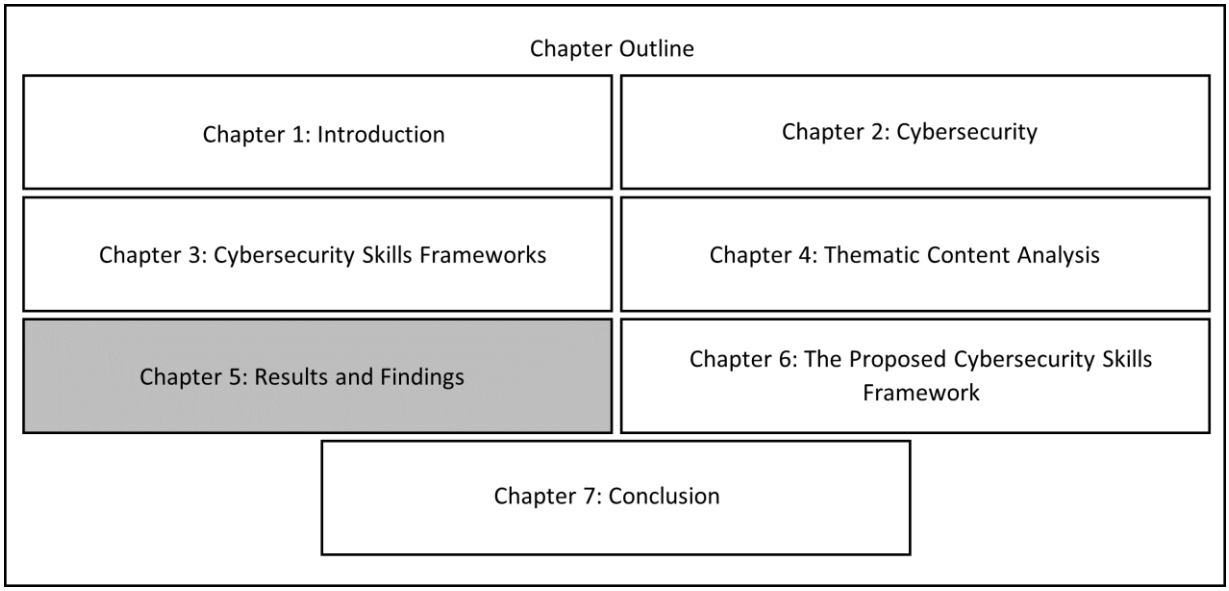
spreadsheet or creating a network view of the codes and quotations and how they link to one another or creating tables to illustrate the data. This study mainly made use of reports in the form of tables based on the information in ATLAS.ti. These tables are discussed and shown in Chapter 5.

4.6. Conclusion

This chapter discussed the thematic content analysis and all the processes required to complete thematic content analysis effectively. It was determined which software tool would be used for the thematic content analysis by comparing multiple software tools and their feature sets in terms of a predefined set of requirements. The two main topics discussed are the data collection pilot study (Sept 2020) and the actual data collection (October 2020 - January 2021). This included changes made to the process of data collection based on findings of the pilot study. Next the thematic content analysis using ATLAS.ti was discussed in detail. Three phases were identified and used to analyse the data gathered from LinkedIn during the data collection process. These three phases are pre-analysis, material exploration, and interpretation. During the thematic content analysis 20 unique job roles were identified.

These job roles are used to develop the proposed cybersecurity framework for South Africa. As such, the information gained from this chapter was used to inform the proposed framework along with the identified global skills frameworks identified in Chapter 3.The next chapter, Chapter 5, presents the results findings of the thematic content analysis.

Chapter 5 – Results and Findings



5.1. Introduction

Chapter 4 provided a discussion of the data collection process and the thematic content analysis conducted during this study. In addition, it motivated the use of ATLAS.ti as the preferred software tool for conducting the content analysis. This chapter presents the results and findings of the thematic content analysis discussed in Chapter 4. The interpretation of these results and findings informs the proposed cybersecurity skills framework presented in Chapter 6. As indicated in Chapter 4, this study collected job postings on LinkedIn from 1 October 2020 to 31 January 2021.

The structure of Chapter 5 is as follows: Section 5.2 and its related sub-sections present various categories of the results, such as the identified industries and the most common locations for the job postings analysed. Section 5.3 provides an interpretation of the results and findings within the context of this study. Lastly, Section 5.4 concludes this chapter.

5.2. Results and Findings by Category

During the thematic content analysis process, as discussed in Chapter 4, various key categories were identified as being relevant to this study and were therefore defined and coded for further analysis.

The key categories identified include the following for the job postings analysed:

- the industry (where five main industries were identified)
- the job location (this was indicated by province)
- the job level (ranging from entry level to executive level)
- the minimum qualifications and certifications
- the job roles (where 20 job roles were identified)
- the knowledge, skills, abilities and tasks (KSATs) identified.

These key categories are further analysed in their respective sub-sections. Approximately 90 percent of the job postings were for full-time positions.

5.2.1. Identified Industries

From the thematic content analysis conducted, it was found that most of the job postings indicated the specific industry of the job advertised.

Table 5.1 presents the various industries that were advertising to recruit IT professionals with cybersecurity knowledge on LinkedIn from 1 October 2020 to 31 January 2021. In total, there were 43 industries identified by the 280 job postings analysed. Job postings, in some cases, specified more than one industry, meaning that a single job posting could belong to more than one industry, for example, a 'Systems Administrator' forms part of both the 'Information Technology and Services' industry as well as the 'Computer Software' industry. Job postings, however, specified only a maximum of three industries per job posting. Specific industries for the job postings were referred to 561 times in total. 'Information Technology and Services' was mentioned the most, 140 times (25.0%), while Financial Services followed being referred to 122 times (21.7%). Computer Software and Telecommunications have frequency percentages of 15.0% and 4.5% respectively. Insurance, Retail, Computer and Network Security, Accounting, and Internet each have a frequency percentage of less than 3% with 2.9%, 2.7%, 2.3%, 2.1% and 2.1% respectively. The remaining 34 industries combined make up 21.7%. Each of these industries has a frequency percentage of less than 2%.

Table 5.1: Job Postings Classified by Industry

Industry	Frequency	Frequency Percentage
Information Technology and Services	140	25.0%
Financial Services	122	21.7%
Computer Software	84	15.0%
Telecommunications	25	4.5%
Insurance	16	2.9%
Retail	15	2.7%
Computer and Network Security	13	2.3%
Accounting	12	2.1%
Internet	12	2.1%
Other (34 Industries)	122	21.7%
TOTAL	**561**	**100%**

The Financial industry is the industry with the second highest requirement for IT professionals with cybersecurity KSATs. This is most likely due to the financial industry being a large target for cyberattacks.

5.2.2. Job Locations

South Africa has a total of nine provinces, eight of which had job listings during the four-month data collection period from 1 October 2020 to 31 January 2021. The Northern Cape was the only province with no job listings from the job postings analysed.

Table 5.2 presents the number of job postings per province in South Africa. In cases where the province was not listed, job postings are indicated under South Africa. Where the city name was provided instead of the province, the researcher determined the respective province and made the appropriate classification. Gauteng accounted for most of the job postings (178 postings, 63.6%), followed by the Western Cape (67 postings, 23.9%). These two provinces accounted for 87.5% of the total job postings with the rest of the provinces each making up less than 5%.

Table 5.2: Job Postings Classified by Province

Locations	Number of Job Postings	Frequency Percentage
Gauteng	178	63.6%
Western Cape	67	23.9%
Kwazulu-Natal	12	4.3%
South Africa (No Province Specified)	8	2.9%
Eastern Cape	7	2.5%
Mpumalanga	3	1.1%
Limpopo	2	0.7%
Northwest	2	0.7%
Free State	1	0.3%
TOTAL	**280**	**100%**

5.2.3. Job levels

Many of the job postings collected over the four-month period had a job level assigned to it. Each job posting was therefore classified according to whether it was Entry Level, Mid-level, Senior Level or Executive Level. Those that did not specify the job level were classified under 'Not Specified'.

As can be seen in Table 5.3, Entry Level jobs made up 36.1% (101 postings) followed by Mid-level (87 postings, 31.1%) and Senior Level (65 postings, 23.2%). Executive level only made up 3.5% of the total job postings, while 6.1% did not specify a job level.

Table 5.3: Job Postings Classified by Job Level

Job Level Name	Number of Job Postings	Frequency Percentage
Entry Level	101	36.1%
Mid-Level	87	31.1%
Senior Level	65	23.2%
Not Specified	17	6.1%
Executive Level	10	3.5%
TOTAL	**280**	**100%**

5.2.4. Qualifications and Certifications

This section discusses the minimum required qualifications and most common certifications listed in the job postings analysed. Of the 280 job postings analysed, 231 job postings listed a specific requirement in terms of formal tertiary education. This gives an idea of the strong emphasis on meeting specific academic requirements to enter the IT industry.

Table 5.4 shows that more than half of the job postings (65.8%, 152 job postings) specified that it requires a degree in either Computer Science, Information Systems or Information Technology, as a minimum qualification. This indicates that there is a demand for academic qualifications needed for most of the job postings and that a diploma would not suffice in the majority of cases. A diploma was specified as a requirement for 69 (29.9%) of the job postings, with 10 (4.3%) requiring either a Master's degree or some form of postgraduate qualification.

Table 5.4: Job Postings Classified by Minimum Qualifications Required

Qualification Type	Number of Mentions	Frequency Percentage
Degree	152	65.8%
Diploma	69	29.9%
Master's Degree/Postgraduate Qualification	10	4.3%
No qualification specified	49	17.5%
TOTAL	**280**	**100%**

In addition to formal qualifications, many of the job postings recommended specific certifications. Most job postings specified at least one or more of these certifications. However, some job postings did not specify certifications at all.

Figure 5.1 shows the top 10 certifications mentioned as recommendations in the 280 job postings analysed.

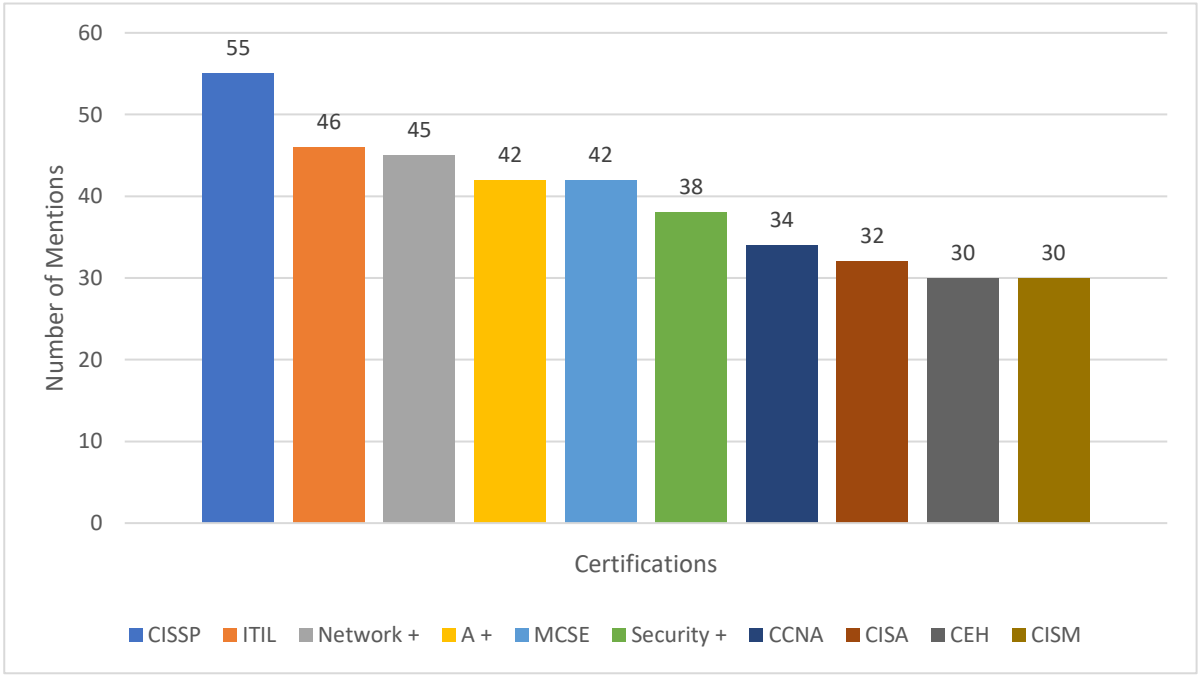


Figure 5.1: Top 10 Certifications Specified

Certified Information Systems Security Professional (CISSP) was the most mentioned certification. This was followed by Information Technology Infrastructure Library (ITIL) and many of the certifications provided by COMPTIA, such as Network+, Security+ and A+. Microsoft's MCSE certification, and Cisco's CCNA were also mentioned multiple times. Other certifications mentioned frequently included Certified Systems Auditor (CISA), Certified Information Security Manager (CISM) and Certified Ethical Hacker (CEH).

5.2.5. Job Roles

During the thematic content analysis, many job roles were identified and analysed. Figure 5.2 depicts a word cloud that visually shows recurring words found in the job roles of the job postings analysed. The larger the text of a word, the more frequently it was specified. Based on the word cloud, it is clear that the most frequently used words were 'Security' and 'Engineer'. One of the most common job roles identified was 'Network Engineer', which aligns with the fact that 'Engineer' was one of the most used words. It is also evident that 'Manager', 'Specialist', 'Administrator' and 'Technician' are also words that were frequently mentioned. These words were mostly used in job roles such as 'IT Manager', 'Cybersecurity Specialist', 'Compliance Specialist', 'IT Technician' and 'Systems Administrator'.

Figure 5.2: Job Role Word Cloud

In total, 20 unique job roles were identified from the 280 job postings analysed. In Chapter 4, Section 4.5, it was mentioned how some of these job roles had the same KSATs but different naming conventions, for example, a job role named 'Software Developer' and a job role named 'Application Developer'. These two job roles are considered to be the same and therefor they

were merged into a single job role namely 'Software Developer'. This process was followed throughout all identified job roles and led to the outcome shown in Table 5.5. Each of these job roles have defined KSATs that are discussed in detail in Chapter 6. Table 5.5 shows the 20 job roles identified as well as their frequency percentage within the data set.

Table 5.5: Job Roles Identified

Job Role	Number of Job Postings	Frequency Percentage
IT Technician	43	15.4%
Cybersecurity Specialist	43	15.4%
Systems Administrator	37	13.2%
Software Developer	26	9.3%
Network Engineer	20	7.1%
Information Technology Manager	17	6.1%
Digital Forensics Analyst	16	5.7%
Compliance Specialist	14	5.0%
Information Technology Auditor	11	3.9%
DevOps Engineer	9	3.2%
Quality Assurance Analyst	9	3.2%
Project Manager	7	2.5%
Security Engineer	6	2.1%
Data Privacy and Protection Specialist	5	1.8%
Application Security Specialist	4	1.4%
Chief Information Officer	3	1.1%
Cybersecurity Manager	3	1.1%
Data Warehousing Engineer	3	1.1%
Cloud Architect	2	0.7%
Penetration Tester	2	0.7%
TOTAL	**280**	**100%**

The job roles, knowledge areas and tasks identified during the thematic content analysis were divided into job categories according to their relevance to each of the following:

- Cybersecurity [CS]
- Operations and Support [OS]

- Data and Artificial Intelligence [DA]
- Strategy and Governance [SG]
- Software and Application Development [SA]

All of the above job categories were defined in the Skills Framework for Infocomm Technology, as discussed in Chapter 3, Figure 3.1. Due to the similarity between this study and the Skills Framework for Infocomm Technology, these job categories were deemed relevant to this research and, as such, all job categories but Software and Applications Development have been directly incorporated into the categorisation of the job roles, knowledge areas and tasks identified through this research. Software and Applications Development was originally called Software and Applications in SFw for ICT, the addition of the word Development has been added in this study to better fit the contents of the job category as it pertains to this study. Tables 5.6 contains the categorised job roles as well as their respective job role codes.

Table 5.6 presents the 20 job roles categorised according to the five job categories listed above. Cybersecurity had seven related job roles (CSJ01 to CSJ07), followed by Strategy and Governance with six (SGJ01 to SGJ06), and Data and Artificial Intelligence with three (DAJ01 to DAJ03). Operations and Support (OSJ01 and OSJ02) and Software and Application Development (SAJ01 and SAJ02) each had two related job roles identified.

Table 5.6: Job Roles Identified by Job Category

Cybersecurity [CS]		**Strategy and Governance [SG]**	
Code	**Description**	**Code**	**Description**
CSJ01	Cybersecurity Specialist	SGJ01	Information Technology Manager
CSJ02	Digital Forensics Analyst	SGJ02	Information Technology Auditor
CSJ03	Security Engineer	SGJ03	Compliance Specialist
CSJ04	Data Privacy and Protection Specialist	SGJ04	Project Manager
CSJ05	Cybersecurity Manager	SGJ05	Quality Assurance Analyst
CSJ06	Application Security Specialist	SGJ06	Chief Information Officer
CSJ07	Penetration Tester		
Operations and Support [OS]		**Data and Artificial Intelligence [DA]**	
Code	**Description**	**Code**	**Description**
OSJ01	IT Technician	DAJ01	Systems Administrator
OSJ02	Network Engineer	DAJ02	Data Warehousing Engineer
Software and Application Development [SA]		DAJ03	Cloud Architect

Code	Description	
SAJ01	Software Developer	
SAJ02	DevOps Engineer	

The following presents the identified knowledge, skills and abilities and their alignment with the identified job categories.

5.2.6. Knowledge, Skills, Abilities and Tasks

During the analysis of the job postings, using the thematic content analysis discussed in Chapter 4, multiple knowledge, skills, and abilities, and tasks (KSATs) were identified. In this section the identified KSATs are categorised and discussed.

Knowledge Areas

Knowledge areas, similar to job roles, have been categorised according to the job categories found in the Skills Framework of Infocomm Technology. Table 5.7 presents the categorisation of the identified knowledge areas, as well as their knowledge area codes. In total, 54 knowledge areas were identified and categorised as follows:

- Cybersecurity (9)
- Operations and Support (13)
- Data and Artificial Intelligence (6)
- Strategy and Governance (15)
- Software and Application Development (11)

Table 5.7 presents the 54 knowledge areas identified and categorised. Most of the knowledge areas fall within the Strategy and Governance job category (SGK01 to SGK15), followed by Operations and Support (OSK01 to OSK13).

Table 5.7: Knowledge Areas Identified by Job Category

Cybersecurity [CS]		**Strategy and Governance [SG]**		**Software and Application Development [SA]**	
Code	**Description**	**Code**	**Description**	**Code**	**Description**
CSK01	Security Proxies	SGK01	Project Management	SAK01	SDLC
CSK02	Security Frameworks	SGK02	IT Risk	SAK02	Secure Coding
CSK03	Anti-Virus Software	SGK03	NIST	SAK03	Application Security
CSK04	Security Best Practices	SGK04	ISO	SAK04	SQL
CSK05	Penetrating Testing	SGK05	COBIT	SAK05	Coding Languages
CSK06	Security Vulnerabilities and Exploits	SGK06	Business Operations	SAK06	Functions
CSK07	Firewalls	SGK07	King IV	SAK07	Databases
CSK08	SSL	SGK08	Problem Management	SAK08	Stored Procedures
CSK09	IPS/IDS	SGK09	Incident Management	SAK09	Database Design
Operations and Support [OS]		SGK10	Access Management	SAK10	API Management Tools
Code	**Description**	SGK11	Compliance	SAK11	Version Control
OSK01	Operating Systems	SGK12	Change Management		
OSK02	PC Hardware and Software	SGK13	IT Governance		
OSK03	Backups	SGK14	ITIL		
OSK04	VMWare	SGK15	IT Security Policies		
OSK05	Active Directory	**Data and Artificial Intelligence [DA]**			
OSK06	VPN	**Code**	**Description**		
OSK07	IIS	DAK01	Data Warehousing		
OSK08	OWASP	DAK02	Data Analysis		
OSK09	Routers	DAK03	Data Modelling		
OSK10	Switches	DAK04	Machine Learning		
OSK11	IP/VOIP/TCP	DAK05	Cloud Services		
OSK12	Network Security	DAK06	Automation		
OSK13	Network Monitoring Tools				

Skills

The skills identified during the thematic content analysis were divided into technical and non-technical skills.

Table 5.8 presents the 23 skills identified and categorised according to their technical or non-technical nature. Seventeen skills were identified as non-technical (NTS01 to NTS17), while six were identified as technical (TS01 to TS06).

Table 5.8: Non-Technical and Technical Skills Identified

Non-Technical Skills		**Technical Skills**	
Code	**Description**	**Code**	**Description**
NTS01	Planning Skills	TS01	Troubleshooting Skills
NTS02	Leadership Skills	TS02	Technical Writing Skills
NTS03	Presentation Skills	TS03	Diagnostic Skills
NTS04	Analytical Thinking Skills	TS04	General Programming Skills
NTS05	Communication Skills	TS05	Administration Skills
NTS06	Adaptability Skills	TS06	Problem Solving Skills
NTS07	Fast Learner Skills		
NTS08	Organisational Skills		
NTS09	Time Management Skills		
NTS10	Attention to Detail Skills		
NTS11	Conflict Management Skills		
NTS12	Collaboration Skills		
NTS13	Customer Service Skills		
NTS14	Strategic Thinking Skills		
NTS15	Negotiation Skills		
NTS16	Decision Making Skills		
NTS17	Logical Thinking Skills		

Table 5.9 presents the mapping of technical skills according to the previously identified job categories. Notable technical skills shown in Table 5.9 are TS01 (Troubleshooting Skills) and TS06 (Problem Solving Skills). TS01 is present in all job categories identified and TS06 was identified in all but one job category, Software and Application Development [SA]. In addition, Cybersecurity [CS] required all but one of the technical skills identified.

Table 5.9: Technical Skills Mapped according to Job Category

	Technical Skills						
Job Category	**TS01**	**TS02**	**TS03**	**TS04**	**TS05**	**TS06**	**TOTAL**
CS							5
OS							4
DA							3
SG							4
SA							4
TOTAL	**5**	**3**	**3**	**3**	**2**	**4**	

Similar to the technical skills, the non-technical skills have also been mapped according to the identified job categories as can be seen in Table 5.10. Table 5.10 highlights the four most relevant non-technical skills, namely: NTS04 (Analytical Thinking Skills), NTS05 (Communication Skills), NTS10 (Attention to Detail Skills), as well as NTS17 (Logical Thinking Skills). NTS04, NTS05, NTS10 and NTS17 are required by all job categories. Furthermore, both Cybersecurity [CS] and Strategy and Governance [SG] require 15 of the 17 identified non-technical skills.

Table 5.10: Non-Technical Skills Mapped according to Job Category

	Non- Technical Skills																	
Job Category	**NTS 01**	**NTS 02**	**NTS 03**	**NTS 04**	**NTS 05**	**NTS 06**	**NTS 07**	**NTS 08**	**NTS 09**	**NTS 10**	**NTS 11**	**NTS 12**	**NTS 13**	**NTS 14**	**NTS 15**	**NTS 16**	**NTS 17**	**TOTAL**
CS																		**15**
OS																		**8**
DA																		**8**
SG																		**15**
SA																		**9**
TOTAL	**2**	**3**	**2**	**5**	**5**	**4**	**3**	**4**	**3**	**5**	**2**	**3**	**1**	**2**	**2**	**4**	**5**	

Abilities

Similar, to the skills identified in this study, the abilities identified during the thematic content analysis were also divided into two categories, namely technical and non-technical abilities.

Table 5.11 presents the 16 non-technical abilities (NTA01 to NTA16) and 11 technical abilities (TA01 to TA11) that were identified.

Table 5.11: Non-Technical and Technical Abilities Identified

Non-Technical Abilities		**Technical Abilities**	
Code	**Description**	**Code**	**Description**
NTA01	Ability to manage human resources	TA01	Ability to solve technical problems
NTA02	Ability to lead teams	TA02	Ability to write reports
NTA03	Ability to work with leadership	TA03	Ability to obtain forensic evidence
NTA04	Ability to work in teams	TA04	Ability to provide technical assistance
NTA05	Ability to maintain confidentiality	TA05	Ability to troubleshoot
NTA06	Ability to research	TA06	Ability to maintain hardware and software
NTA07	Ability to manage many priorities concurrently	TA07	Ability to analyse data
NTA08	Ability to engage and contribute	TA08	Ability to investigate malware, intrusion attempts and vulnerabilities
NTA09	Ability to execute instructions	TA09	Ability to learn new technology independently
NTA10	Ability to be proactive and efficient	TA10	Ability to create network diagrams and related documentation
NTA11	Ability to work under pressure	TA11	Ability to write secure code
NTA12	Ability to adapt to changing environments		
NTA13	Ability to stay organised		
NTA14	Ability to communicate effectively and efficiently		
NTA15	Ability to prioritise		
NTA16	Ability to work independently		

Table 5.12 present the mapping of the technical abilities to the identified job categories. It can be seen in Table 5.12 that TA01 (Ability to solve technical problems) and TA05 (Ability to troubleshoot) have been identified as required for all the identified job categories. Cybersecurity [CS], Operations and Support [OS] as well as Data and Artificial Intelligence [DA] mapped against 7 of the 11 technical abilities.

Table 5.12: Technical Abilities Mapped according to Job Category

	Technical Abilities											
Job	**TA01**	**TA02**	**TA03**	**TA04**	**TA05**	**TA06**	**TA07**	**TA08**	**TA09**	**TA10**	**TA11**	**TOTAL**
CS												**7**
OS												**7**
DA												**7**
SG												**5**
SA												**5**
TOTAL	**5**	**2**	**1**	**4**	**5**	**2**	**4**	**1**	**3**	**2**	**2**	

Table 5.13 depicts the mapping of the non-technical abilities to the previously identified job categories. As seen in Table 5.13, both NTA04 (Ability to work in teams) and NTA09 (Ability to

execute instructions) are required by all identified job categories. Furthermore, Cybersecurity [CS] and Strategy and Governance [SG] both required 13 of the 17 non-technical abilities identified.

Table 5.13: Non-Technical Abilities Mapped according to Job Category

	Non-Technical Abilities																
Job Category	**NTA 01**	**NTA 02**	**NTA 03**	**NTA 04**	**NTA 05**	**NTA 06**	**NTA 07**	**NTA 08**	**NTA 09**	**NTA 10**	**NTA 11**	**NTA 12**	**NTA 13**	**NTA 14**	**NTA 15**	**NTA 16**	**TOTAL**
CS																	**13**
OS																	**7**
DA																	**10**
SG																	**13**
SA																	**6**
TOTAL	**1**	**3**	**2**	**5**	**3**	**3**	**4**	**3**	**5**	**3**	**3**	**4**	**2**	**4**	**1**	**3**	

Tasks

The tasks identified during the thematic content analysis follow the same categorisation as the job roles and knowledge areas. These tasks were categorised into each of the following job categories:

- Cybersecurity (19)
- Operations and Support (15)
- Strategy and Governance (21)
- Software and Application Development (8)
- Data and Artificial Intelligence (5)

Table 5.14 presents the codes associated with the 19 identified Cybersecurity [CS] Tasks. These codes all start with CST and have been numbered sequentially from 01 to 19.

Table 5.14: Cybersecurity Tasks Identified

Task Code	Cybersecurity Tasks
CST01	Identify cyber threats.
CST02	Respond to cybersecurity incidents.
CST03	Develop and maintain security policies and standards.
CST04	Implement security policies and standards.
CST05	Design, implement and monitor controls.
CST06	Implement security solutions.
CST07	Manage or perform security config reviews on network devices, databases, and operating systems.
CST08	Perform penetration testing.
CST09	Implement security best practices.
CST10	Monitor network software for proper security procedures.
CST11	Align enterprise data to ensure that it supports information security.
CST12	Conduct forensic investigations.
CST13	Provide support to forensic investigational teams.
CST14	Develop and improve security posture and threat surfaces through scoping and shaping of information security programs.
CST15	Ensure information is kept protected.
CST16	Train and raise awareness regarding security.
CST17	Guide teams through the design and implementation of cyber solutions.
CST18	Assist with prototypes and pilot runs of proposed security solutions.
CST19	Identify, assess and manage cyber risk.

Table 5.15 presents the codes associated with the fifteen identified Operations and Support [OS] Tasks. These codes all start with OST and have been numbered sequentially from 01 to 15.

Table 5.15: Operations and Support Tasks Identified

Task Code	Operations and Support Tasks
OST01	Do preventative maintenance.
OST02	Provide IT support to users.
OST03	Manage server services.
OST04	Provide hardware and software support.
OST05	Perform and maintain backups.
OST06	Install and configure hardware and software.
OST07	Keep systems up to date.
OST08	Manage networks and network devices.
OST09	Troubleshoot networks.
OST10	Monitor network activity.
OST11	Design and implement network solutions.
OST12	Assist clients with improving their security on their networks by performing security assessments.
OST13	Assign network access (Access Management).
OST14	Manage internet resources.
OST15	Manage firewalls.

Table 5.16 presents the codes associated with the 21 identified Strategy and Governance [SG] Tasks. These codes all start with SGT and have been numbered sequentially from 01 to 21.

Table 5.16: Strategy and Governance Tasks Identified

Task Code	Strategy and Governance Tasks
SGT01	Direct and organise IT related projects.
SGT02	Maintain IT compliance/risk management frameworks.
SGT03	Define, assess, maintain, and advise on IT Regulatory universe.
SGT04	Develop, facilitate compilation of and review IT compliance risk management plans.
SGT05	Conduct IT compliance monitoring.
SGT06	Handle all customer escalations ensuring compliance with Service Level Agreements (SLAs).
SGT07	Manage and ensure compliance with internal policies and procedures.
SGT08	Assist in the development and maintenance of policies, procedures, and technical standards.
SGT09	Assist in the Incident Management process.
SGT10	Assist in the Problem Management process.
SGT11	Assist in the Access Management process.
SGT12	Assist in the Change Management process.
SGT13	Advise the business on its data protection obligations in respect of the policies, processes, and technology that supports the products and services and solutions.
SGT14	Monitor and evaluate the effectiveness of data privacy and protection programs.
SGT15	Design internal audit procedures and programs.
SGT16	Assist in audit engagement, planning and reporting activities.
SGT17	Present and compile reports.
SGT18	Develop strategic plans, set timelines of evaluation, development, and deployment of technology resources.
SGT19	Ensure adherence to project budgets.
SGT20	Ensuring that project objectives, customer acceptance criteria and internal performance metrics are achieved.
SGT21	Draft project proposals and cost estimates.

Table 5.17 presents the codes associated with the eight identified Software and Application Development Tasks [SA]. These codes all start with SAT and have been numbered sequentially from 01 to 08.

Table 5.17: Software and Application Development Tasks Identified

Task Code	Software and Application Development Tasks
SAT01	Develop secure applications.
SAT02	Develop applications to monitor networks for cyberthreats.
SAT03	Develop applications to automate tasks performed by security analysts.
SAT04	Contribute to the design, development, testing and evaluation of systems and infrastructure.
SAT05	Lead Software Development Life Cycle.
SAT06	Design, develop, test and implement new features and changes to current functionality to applications as per requirements.
SAT07	Develop and monitor the integration, creation and maintenance of coding standards.
SAT08	Create test plans with the relevant test scenarios.

Table 5.18 presents the codes associated with the five identified Data and Artificial Intelligence [DA] Tasks. These codes all start with DAT and have been numbered sequentially from 01 to 05.

Table 5.18: Data and Artificial Intelligence Tasks Identified

Task Code	Data and Artificial Intelligence Tasks
DAT01	Design the architecture of cloud systems and infrastructure.
DAT02	Partner with others to deploy cloud services and automation.
DAT03	Design, develop, and manage data warehousing environments.
DAT04	Define and continuously improve the data engineering architecture framework and modelling standards.
DAT05	Deploy authentication solutions and increase the degree of automation of the solutions provided.

With all of the identified KSATs being discussed the next section will further detail the results and findings of this chapter.

5.3. Discussion of Results and Findings

The results of this study were compared those of the study conducted by Parker and Brown (2018). In most cases, the results of this study and that of Parker and Brown (2018) are very closely aligned. Parker and Brown (2018) identified 20 industries based on the 196 adverts they collected, compared to the 43 industries identified by this study. In terms of how these industries compared, in Parker and Brown (2018) the Financial Services industry had the highest frequency percentage with 27%, followed by Information Technology and Services with 24%. In this study, Information Technology and Services had 25% frequency compared to Financial Services with 21.7%.

Job postings by location were very similar with Gauteng having a 64.8% in the Parker and Brown (2018) study compared to 63.6% in this study, the Western Cape was in second place for both studies, with 22.5% for Parker and Brown (2018) study, and 23.9% for this study.

Where the two studies differed is in terms of job level. Parker and Brown (2018) found that most job postings were listed as either mid-level or senior level, whereas in this study most job postings were either entry level or mid-level. In addition, Parker and Brown (2018) noted that, of their job postings analysed, most required at least a degree. This finding is true for this study as well.

From this study it is evident that IT professionals with cybersecurity KSAs are required for IT jobs in various industries in South Africa. Many job postings specified the position as an entry-

level position, despite there being a need for security knowledge, and in some cases, certifications related to cybersecurity for these entry-level positions. CISSP was the most mentioned certification, yet it requires a minimum of five years' cybersecurity experience to qualify for the certification. In 65.8% of the job postings analysed in this study, the employers expect the ideal candidate to have a degree in either Computer Science, Information Systems or Information Technology. In addition, cybersecurity-related certifications were considered an advantage, if not a requirement, for many of the 280 job postings analysed. It was interesting to note that there were some cases where an entry-level job required a CISSP certification, as well as a relevant degree, further indicating the high level of experience and academic requirements for IT professionals with cybersecurity KSAs. Skills and abilities relating to the Cybersecurity [CS] job category is by far the most in demand based on the job postings analysed.

Several trends were identified from this study. Table 5.7 presents the knowledge areas found in the 280 job postings analysed. However, many of the knowledge areas could be considered to be technical skills rather than knowledge areas. For example, Penetration Testing (CSK05) and Secure Coding (SAK02) are often considered to be technical skills. However, employers seem to focus more on knowledge requirements and non-technical skills, with the technical skills mentioned being less specific and more generalised, for example Problem Solving skills (TS06). This is also evident in Table 5.8, when comparing the number of technical (6) and non-technical (17) skills. It is interesting to note the emphasis on non-technical skills and abilities, especially in the Cybersecurity [CS] and Strategy and Governance [SG] job categories.

Based on this study, one can more clearly determine what is required in terms of KSAs when employing IT professionals in the five identified job categories. This information was used to inform the proposed cybersecurity skills framework for South Africa, which may contribute to improving the South African cyber-security posture.

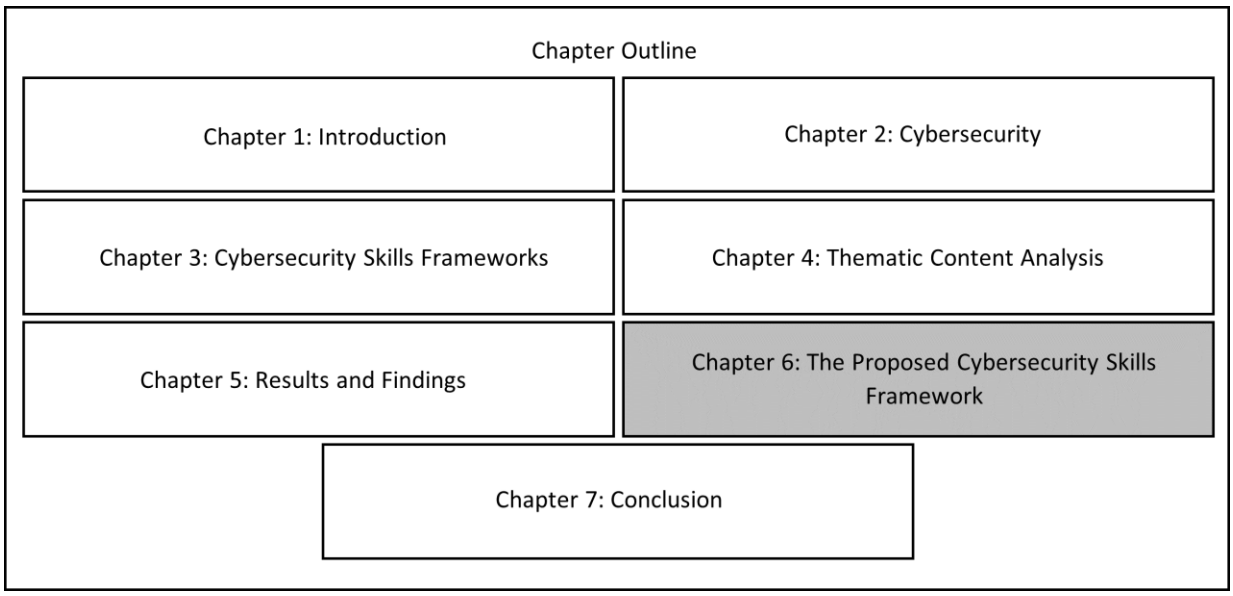
5.4. Conclusion

In this chapter the results and findings of the thematic content analysis discribed in Chapter 4 were discussed. The results were analysed according to the industry (where five main industries were identified), the job location (this was indicated by province), the job level (ranging from entry level to executive level), the minimum qualifications and certifications, the job roles

(where 20 job roles were identified) and the knowledge, skills, abilities and tasks (KSATs) identified.

The KSAs identified in this study closely align with the Skills Framework for Infocomm Technology (SFw for ICT), sharing many knowledge areas, skills and abilities. Due to this study's alignment with SFw for ICT, it could provide a good baseline for a cybersecurity skills framework for South Africa. This could be used to better inform employers and future employees, as well as to assist in the further development of cybersecurity curricula in the education sector. Most countries are developing their own workforce and skills frameworks for IT professionals. Australia, Canada, the United Kingdom and Singapore are among those who have developed, or are in the process of developing, their own frameworks. South Africa has a need for a similar framework that identifies the cybersecurity knowledge, skills, abilities and tasks for different IT job roles in the South African context. This chapter presents the many KSATs and job roles that has been identified in Chapter 4. These KSATs along with the guidance from existing global skills frameworks such as NICE and SFw for ICT informs the proposed cybersecurity skills framework for South Africa. In Chapter 6 the proposed framework will be discussed in detail.

Chapter 6 – The Proposed Cybersecurity Skills Framework



6.1. Introduction

In Chapter 5, the results and findings of this study were presented. Based on the thematic content analysis conducted, key groupings were identified, namely the industry; the job location; the job level; the minimum qualifications and certifications; the job roles; the knowledge, skills, abilities and tasks (KSATs).

These key groupings were each discussed in detail. This chapter focuses on the proposed framework, called the Cybersecurity Skills Framework for South Africa (CSFwSA), thereby addressing the primary objective of this research, which is to develop a cybersecurity skills framework by determining the cybersecurity knowledge, skills, abilities, and tasks (KSATs) required for specific IT job roles in South Africa.

This chapter starts by detailing the high-level structure of CSFwSA (Section 6.2), followed by a discussion of the alignment of the Skills Framework for Infocomm Technology (Section 6.3) to this study. Thereafter, the CSFwSA is presented (Section 6.4) followed by a contextualisation of the proposed framework (Section 6.5). This then leads to a discussion of the potential role of the proposed framework (Section 6.6) and the conclusion to the chapter (Section 6.7).

6.2. High-Level Structure of the Proposed Framework

In determining the high-level structure for the proposed framework, this study considered many of the existing IT and cybersecurity skills and workforce frameworks that are currently in use or being developed globally, as discussed in Chapter 3.

Figure 6.1 shows the high-level structure of the proposed framework. Job roles each have defined knowledge and tasks, but the knowledge and tasks do not solely belong to a single job category. For example, a job role can have tasks and knowledge from the Cybersecurity [CS] and Strategy and Governance [SG] job categories as well as from any of the other identified job categories. This is illustrated by the dotted lines and boxes in Figure 6.1. Skills and abilities are not categorised according to the five defined job categories, but instead are categorised based on their technical or non-technical nature. As such, each job role can make use of a pool of possible skills and abilities that were identified. Through the thematic content analysis, it was found that the breakdown of job roles shares many similarities with the NICE framework in terms of the general layout/structure. The NICE framework (NIST, 2017) also makes use of KSATs to define their job roles.

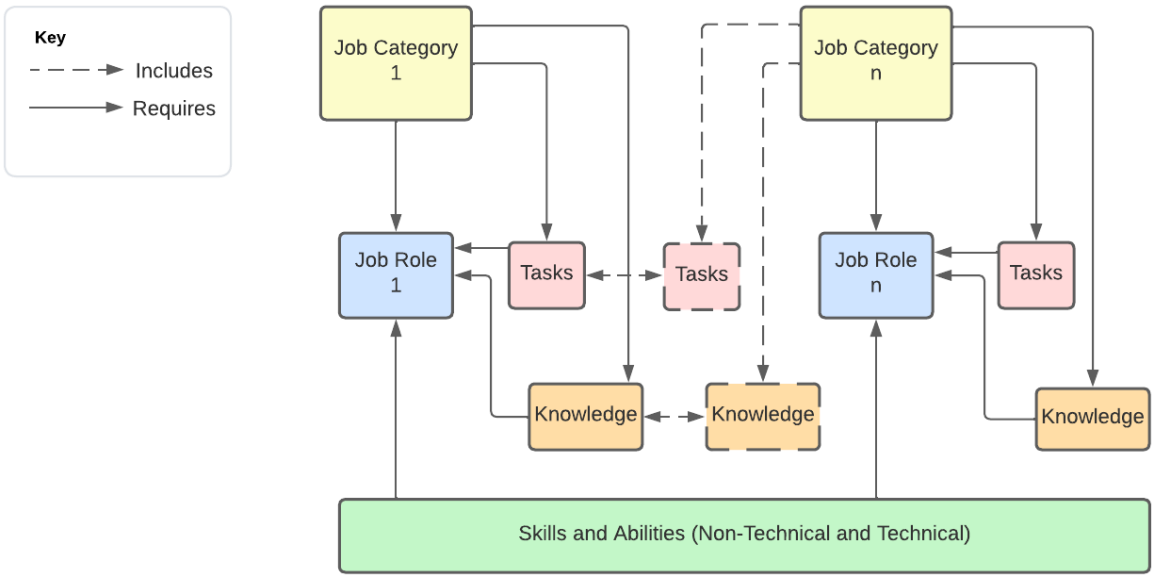


Figure 6.1: High-Level Structure of Proposed Framework

From the thematic content analysis conducted, five main job categories were identified in Chapter 5, namely:

- Cybersecurity [CS]
- Operations and Support [OS]
- Strategy and Governance [SG]
- Software and Application Development [SA]
- Data and Artificial Intelligence [DA]

These five job categories are based on the job categories found in the Skills Framework for Infocomm Technology (SFw for ICT) (IMDA, 2017), as well as being clearly identifiable based on the results of the thematic content analysis conducted during this study. The NICE framework (NIST, 2017) has divided its job roles into seven job categories, namely Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyse (AN), Collect and Operate (CO), and Investigate (IN). Table 6.1 shows how the job categories identified from this study, Software and Applications Development [SA], Operations and Support [OS], and Strategy and Governance [SG], align with Securely Provision (SP), Operate and Maintain (OM), and Oversee and Govern (OV), respectively.

Table 6.1: Alignment of this Study to NICE Framework

Overarching Job Category	**Job Categories from NICE Framework**	**Job Categories identified in this study**
Cybersecurity [CS]	Securely Provision (SP)	Software and Applications Development [SA]
	Operate and Maintain (OM)	Operations and Support [OS]
	Oversee and Govern (OV)	Strategy and Governance [SG]
	Protect and Defend (PR)	Cybersecurity [CS]
	Analyse (AN)	Cybersecurity [CS]
	Collect and Operate (CO)	Cybersecurity [CS]
	Investigate (IN)	Cybersecurity [CS]

In addition, all four of the NICE job categories, Protect and Defend (PR), Analyse (AN), Collect and Operate (CO), and Investigate (IN) relate to cybersecurity work. Therefore, in this study, these NICE job categories align with the Cybersecurity [CS] job category. However, cybersecurity is fundamental to all seven of the NICE job categories, and as such, the Cybersecurity [CS] job category in this study is considered to be the overarching job category represented in all of the NICE job categories. One job category that is not explicitly represented in the NICE framework but has been identified in this study is Data and Artificial Intelligence [DA].

As discussed in Section 5.2.5, in total, there were 20 job roles identified during the thematic content analysis conducted on the job postings collected from 1 October 2020 until 31 January 2021. As can be seen in Figure 6.1, each of the identified job roles has defined tasks associated with it. These tasks were also identified during the thematic content analysis, as discussed in Section 5.2.6. To effectively complete the assigned tasks, certain knowledge, skills, and abilities are needed. All the knowledge, skills and abilities (KSATs) included in CSFwSA were identified during the thematic content analysis. In total, 68 tasks, 54 knowledge areas, 23 skills, and 27 abilities were identified, as highlighted in Section 5.2.6.

Although similarities and alignment with the NICE framework is evident, the actual KSATs identified during the thematic content analysis of this study align more closely with the Skills Framework for Infocomm Technology (SFw for ICT).

6.3. Alignment with the Skills Framework for Infocomm Technology

Due to the nature of the job postings analysed, it was decided to compare the identified skills and abilities with the SFw for ICT to gain an understanding of possible gaps in the identified job roles. For example, when considering a job role such as an Information Technology Manager it seems logical that a skill like Leadership would be fundamental to such a job role. However, when analysing the job postings collected, this skill was not highlighted as being required for the job role. Hence, there was a need to further analyse the skills and abilities identified in comparison with the job roles to understand where there had been possible gaps in the job postings and then, in turn, to fill these gaps where needed.

Table 6.2 shows the skills identified in this study compared to their counterparts in SFw for ICT, as well as the job roles where there was a gap identified in terms of the specific skills identified.

Table 6.2: Skills Identified in this Study Compared to SFw for ICT

SFw for ICT	Skills identified in this study	Job roles identified with missing skills
Leadership	**NTS02:** Leadership skills	Information Technology Manager
Creative Thinking	**NTS04:** Analytical thinking skills	Penetration Tester, Systems Administrator, Information Technology Auditor
Interpersonal skills	**NTS05:** Communication skills	Cybersecurity Manager, Systems Administrator, Cloud Architect, Information Technology Manager, Information Technology Auditor, Chief Information Officer
Decision Making	**NTS16:** Decision making skills	Information Technology Manager, Compliance Specialist
Infrastructure Support	**TS01:** Troubleshooting skills	DevOps Engineer
Sense Making	**TS03:** Diagnostic skills	Cloud Architect
Problem Solving	**TS06:** Problem solving skills	Cybersecurity Specialist, Data Privacy and Protection Specialist, Cybersecurity Manager, Penetration Tester, Cloud Architect

Similar to Table 6.2, Table 6.3 highlights the abilities identified in this study compared to their counterparts in SFw for ICT, as well as to which job roles these abilities had been added.

Table 6.3: Abilities Identified in this Study Compared to SFw for ICT

SFw for ICT	Abilities identified in this study	Job roles identified with missing abilities
Resource Management	**NTA01:** Ability to manage human resources	Information Technology Manager, Compliance Specialist
Teamwork	**NTA04:** Ability to work in teams	Network Engineer, Systems Administrator, Project Manager, DevOps Engineer
Communication	**NTA14:** Ability to communicate effectively and efficiently.	Cybersecurity Manager, IT Technician
Applications Support and Enhancement	**TA01:** Ability to solve technical problems	DevOps Engineer
Threat Intelligence and Detection	**TA03:** Ability to obtain forensic evidence	Data Privacy and Protection Specialist
Applications Support and Enhancement	**TA04:** Ability to provide technical assistance	Systems Administrator, DevOps Engineer

Infrastructure Support	**TA05:** Ability to troubleshoot	Cybersecurity Manager, Systems Administrator, Software Developer, DevOps Engineer
Network Administration and Maintenance	**TA06:** Ability to maintain hardware and software	Network Engineer, Systems Administrator
Data Analytics	**TA07:** Ability to analyse data	Digital Forensics Analyst, Data Warehousing Engineer, Information Technology Manager, Compliance Specialist, Project Manager
Threat Analysis and Defence	**TA08:** Ability to investigate malware, intrusion attempts and vulnerabilities.	Cybersecurity Manager, Penetration Tester
Applications Development	**TA11:** Ability to write secure code	Software Developer, DevOps Engineer

Tables 6.2 and 6.3 indicate how the skills and abilities in SFw for ICT helped identify the gaps in this study. In some instances, skills and abilities were added to the proposed framework to address the missing skills and abilities identified.

6.4. The Proposed Framework

As discussed in Section 6.2, the proposed framework is structured according to the KSATs relating to various job roles within specific job categories. Table 6.4 presents the detailed structure of the CSFwSA, indicating clearly the specific tables linking to SFw for ICT and the results of the thematic content analysis conducted. This structure is used for all job roles identified in this study.

In Table 6.4, the job category (Table 5.6) is clearly indicated in the top row, followed by the job role (Table 5.5) in the next row. Each of the job roles identified by this study (see Table 5.5) is structured according to Table 6.4 and can be found in Appendix B.

The tasks were derived from the thematic content analysis and were categorised based on the identified job categories. Tables 5.14, 5.15, 5.16, 5.17 and 5.18 show all of the identified tasks according to their assigned job categories.

The knowledge areas identified for each job role were determined through the thematic content analysis. Table 5.7 lists all the knowledge areas identified during the thematic content analysis and used within the proposed framework.

All the skills identified during the thematic content analysis are depicted in Table 5.8, with Tables 5.9 and 5.10 depicting their mappings to the identified job categories. Similarly, the abilities identified during the thematic content analysis can be found in Table 5.11, with their relevant job category mappings in Tables 5.12 and 5.13.

Furthermore, possible certifications were also derived from the thematic content analysis according to each job role. The top 10 certifications identified during this study are listed in Figure 5.1.

Table 6.4: Detailed Structure of the Proposed Framework (CSFwSA)

<table>
<tr><th colspan="3">JOB CATEGORY (TABLE 5.6)</th></tr>
<tr><th colspan="3">JOB ROLE (TABLE 5.5)</th></tr>
<tr><th colspan="3">TASKS</th></tr>
<tr><td colspan="3">Thematic Content Analysis:
Table 5.14 [Cybersecurity tasks]
Table 5.15 [Operations and Support tasks]
Table 5.16 [Strategy and Governance tasks]
Table 5.17 [Software and Application Development tasks]
Table 5.18 [Data and Artificial Intelligence tasks]</td></tr>
<tr><th>KNOWLEDGE</th><th>SKILLS</th><th>ABILITIES</th></tr>
<tr><td>Thematic Content Analysis
Table 5.7</td><td>Thematic Content Analysis
Table 5.8
Table 5.9
Table 5.10
Skills Framework for Infocomm Technology (Table 6.2)</td><td>Thematic Content Analysis
Table 5.11
Table 5.12
Table 5.13
Skills Framework for Infocomm Technology (Table 6.3)</td></tr>
<tr><th colspan="3">CERTIFICATIONS</th></tr>
<tr><td colspan="3">Thematic Content Analysis:
Figure 5.1</td></tr>
</table>

The complete proposed framework, including all 20 job roles identified during this study, is provided in Appendix B.

6.5. Contextualising the Proposed Framework

As an example, this section contextualises the proposed framework for the Cybersecurity Specialist (CSJ01) within the Cybersecurity [CS] job category. A total of seven of job roles were identified to be relevant to the Cybersecurity [CS] job category, each of which has their own KSATs assigned to them and a list of related certifications.

As depicted in Table 6.5, the Cybersecurity Specialist (CSJ01) job role has 15 possible specific tasks relating to it, as well as six general tasks, all of which require specialised knowledge.

Specific tasks are the tasks identified to be needed for the job role purely based on the job postings for this type of job role. General tasks are tasks that have been identified by the researcher, after further analysis, to be relevant to the job role even though it was not explicitly stated in the relevant job postings. The general tasks have been derived from the tasks associated with the job category that the job role falls within; hence, only general cybersecurity tasks have been added to the cybersecurity specialist job role.

Table 6.5: Cybersecurity Specialist Tasks

JOB CATEGORY	**CYBERSECURITY [CS]**
JOB ROLE	**CSJ01: CYBERSECURITY SPECIALIST**
TASKS	
SPECIFIC TASKS	
Cybersecurity [CS] **CST02:** Respond to cybersecurity incidents. **CST04:** Implement security policies and standards. **CST06:** Implement security solutions. **CST09:** Implement security best practices **CST10:** Monitor network software for proper security procedures. **CST14:** Develop and improve security posture and threat surfaces through scoping and shaping of information security program **CST15:** Ensure information is kept protected. **Software and Application Development [SA]** **SAT02:** Develop applications to monitor networks for cyberthreats. **SAT03:** Develop applications to automatise tasks performed by security analysts. **Strategy and Governance [SG]** **SGT08:** Assist in the development and maintenance of policies, procedures, and technical standards. **SGT09:** Assist in the incident management process. **SGT10:** Assist in the problem management process. **SGT11:** Assist in the access management process. **SGT12:** Assist in the change management process. **SGT17:** Present and compile reports.	
GENERAL TASKS	
CST01: Identify cyber threats **CST03:** Develop and maintain security policies and standards **CST05:** Design, implement and monitor controls **CST11:** Align enterprise data to ensure that it supports information security. **CST13:** Provide support to forensic investigational teams. **CST19:** Identify, assess, and manage cyber risk.	

Although this job role is cybersecurity specific, it does not mean that all the specific tasks form part of the Cybersecurity [CS] job category. Even though the Cybersecurity Specialist (CSJ01) job role falls within the cybersecurity job category, some of the related specific tasks do not fall directly within the cybersecurity job category. Examples include SAT02 and SAT03 within

Software and Application Development [SA] and SGT08, SGT09, SGT10, SGT11, SGT12 and SGT17 within Strategy and Governance [SG].

Similar to that of specific tasks, a Cybersecurity Specialist (CSJ01) requires knowledge that falls within multiple knowledge areas as identified during the thematic content analysis, such as Cybersecurity [CS], Operation and Support [OS] and Strategy and Governance [SG] as can be seen below in Table 6.6. As an example, the Cybersecurity Specialist (CSJ01) should have knowledge in Cybersecurity [CS], specifically regarding anti-virus software, IPS/IDS, security proxies, security vulnerabilities and exploits as well as Operations and Support [OS] knowledge areas like operating systems and backups and lastly Strategy and Governance [SG] knowledge is also needed in terms of concepts like project management and ISO to name a few.

A Cybersecurity Specialist (CSJ01) also requires certain technical and non-technical skills and abilities. These can be seen in their respective columns in Table 6.6. It was identified that a Cybersecurity Specialist needs the technical skill problem-solving and the non-technical skills communication skills, organisation skills, collaboration skills and customer service skills. Some skills and abilities such as the problem solving skill (TS06) were not highlighted in the job postings analysed as a required skill for a Cybersecurity Specialist (CSJ01). However, as discussed in Section 6.3, the SFw for ICT was used to determine gaps and as such problem solving skills are argued to be relevant for a Cybersecurity Specialist (CSJ01). Certain technical abilities are required by a Cybersecurity Specialist (CSJ01), namely ability to solve technical problems, to write reports, to investigate malware, intrusion attempts and vulnerabilities. The non-technical abilities identified for the Cybersecurity Specialist (CSJ01) are the ability to work in teams, maintain confidentiality, manage many priorities concurrently and to stay organised.

Table 6.6: Cybersecurity Specialist KSAs

CSJ01: Cybersecurity Specialist		
KNOWLEDGE	**SKILLS**	**ABILITIES**
Cybersecurity (CS) **CSK01:** Security proxies **CSK03:** Anti-virus software **CSK04:** Security best practices **CSK05:** Penetration testing **CSK06:** Security vulnerabilities and exploits **CSK07:** Firewalls **CSK08:** Secure Sockets Layer (SSL) **CSK09:** Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) **Operations and Support (OS)** **OSK01:** Operating systems **OSK03**: Backups **OSK05:** Active directory **OSK06:** Virtual Private Network (VPN) **OSK08:** Open Web Application Security Project (OWASP) **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **Strategy and Governance (SG)** **SGK01:** Project management **SGK02:** Information Technology Risk **SGK03:** National Institute of Standards and Technology (NIST) **SGK04:** International Organization for Standardization (ISO) **SGK05:** Control Objectives for Information and Related Technologies (COBIT) **SGK14:** Information Technology Infrastructure Library (ITIL)	**Technical Skills** **TS06:** Problem solving skills **Non-Technical Skills** **NTS05:** Communication skills **NTS08:** Organisation skills **NTS12:** Collaboration skills **NTS13:** Customer service skills	**Technical Abilities** **TA01:** Ability to solve technical problems **TA02:** Ability to write reports **TA08:** Ability to investigate malware, intrusion attempts and vulnerabilities **Non-Technical Abilities** **NTA04:** Able to work in teams **NTA05:** Ability to maintain confidentiality. **NTA07:** Ability to manage many priorities concurrently **NTA13:** Ability to stay organised.

Certain certifications are also noted in Table 6.7. These certifications could help an employee within the Cybersecurity Specialist (CSJ01) job role. A Cybersecurity Specialist (CSJ01) could benefit from having a CISSP or CEH certification or any of the other mentioned certifications.

Table 6.7: Possible Certifications for a Cybersecurity Specialist

CERTIFICATIONS
Certified Information Systems Security Professional (CIISP)
CompTIA Advanced Security Practitioner (CASP)
Certified Ethical Hacker (CEH)
Certified Information Security Manager (CISM)
Cisco Certified Network Associate (CCNA)
GIAC Security Essentials (GSEC)
Security +
Systems Security Certified Practitioner (SSCP)

The above structure can be followed throughout the framework as it is the same for each job role identified. Each of the job roles are setup in the same manner with the tasks, knowledge, skills, abilities and certifications as can be seen in Appendix B.

6.6. Potential Role of the Proposed Framework

The proposed Cybersecurity Skills Framework for South Africa (CSFwSA) could play a role in addressing the cybersecurity skills gap within the South African context. This is represented in Figure 6.2.

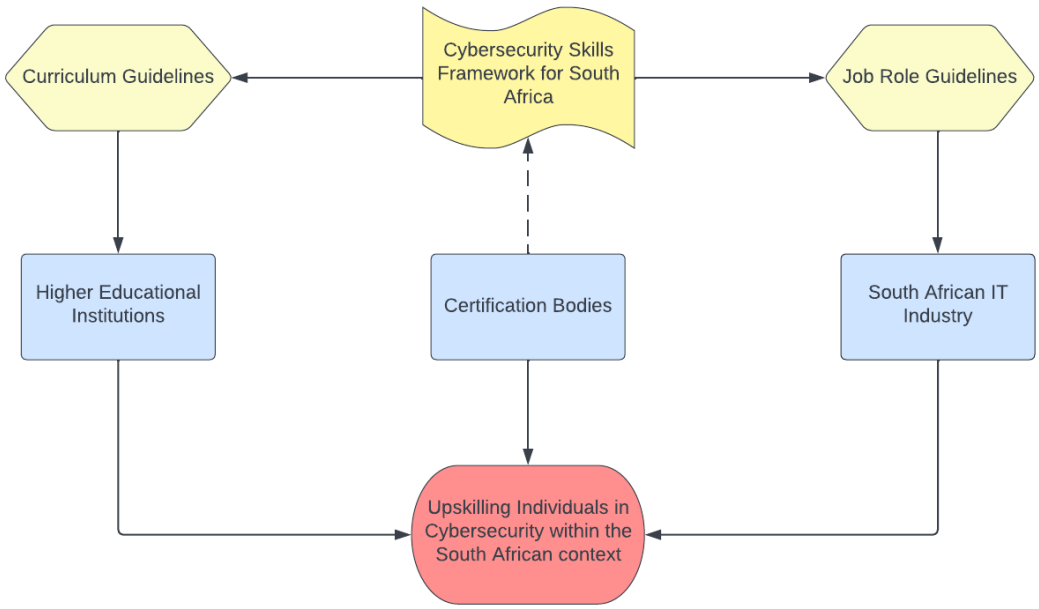


Figure 6.2: Potential Role of CSFwSA

Many higher educational institutions in South Africa are still in the process of developing curricula for cybersecurity qualifications and adapting existing curricula to integrate cybersecurity. Higher educational institutions could therefore use the CSFwSA to help guide them in their curriculum development. The KSATs identified in this study could assist in the

creation of cybersecurity curricula that are better aligned to real-world job requirements. Similarly, higher educational institutions could use the framework to revise their existing curricula, such as Information Systems and Information Technology. In so doing, learning outcomes could be better aligned to IT job roles requiring specific knowledge, skills and abilities.

The IT industry could also use the CSFwSA to train employees for specific IT job roles. Existing employees can be trained to better fit within their designated job role with the guidance of the CSFwSA based on the KSATs identified for their job role. In addition, the framework could be used to guide employers in defining and advertising specific IT job roles.

Students or future employees could also use the CSFwSA to help identify KSATs and certifications that they need for their future potential job role. For example, a student can study the framework to determine their preferred IT job roles. They can then develop themselves to fulfil the KSATs specified by the job roles of interest and in that way better prepare themselves for employment.

From the discussion above it is clear that the proposed CSFwSA could play a key role in developing a skilled workforce that matches the real-world expectations in the industry. This could assist in addressing the cybersecurity skills gap in South Africa by upskilling individuals in cybersecurity.

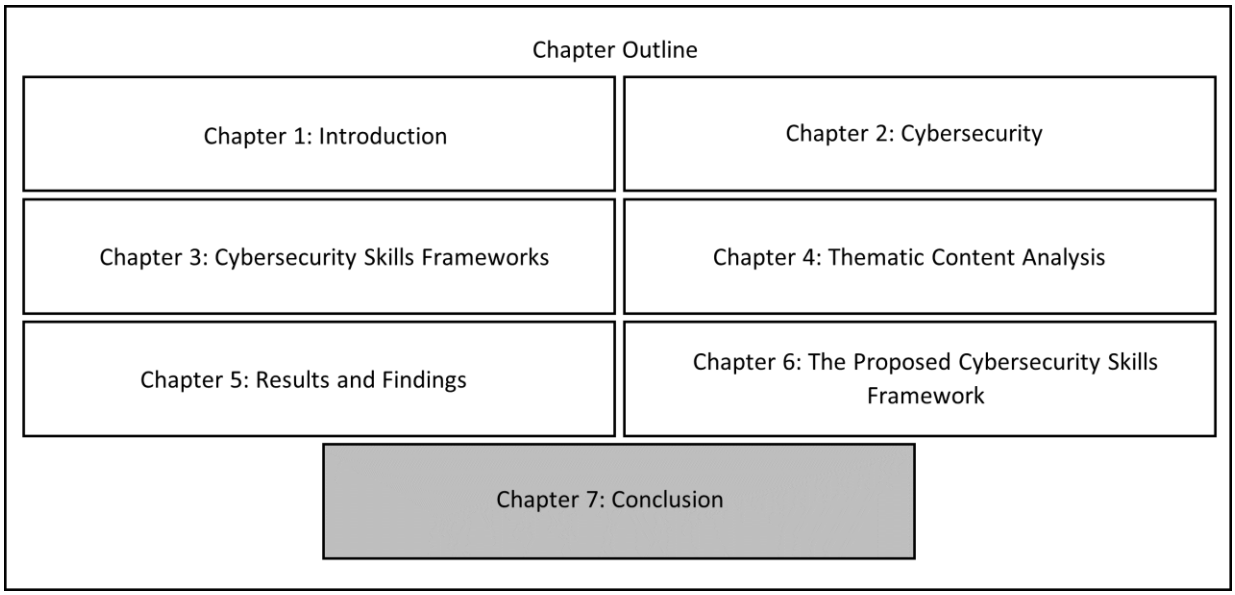
6.7. Conclusion

This chapter detailed the structure of the proposed framework, CSFwSA, as well as contextualised the CSFwSA. The potential role of the framework was also discussed.

The proposed framework resulted from the detailed thematic content analysis discussed in Chapter 4 as well as from the analysis of other existing skills and workforce frameworks as highlighted in Chapter 3. This proposed framework allows for a better understanding of the required KSATs for IT job roles within the South African context, and, as such, could assist in the improvement of South Africa's cybersecurity posture by providing guidance to the IT industry in South Africa.

The following chapter concludes this study by arguing how the research objectives were met, detailing the limitations of the study, as well as highlighting possible future work.

Chapter 7 – Conclusion



7.1. Introduction

The purpose of this chapter is to conclude this dissertation. Section 7.2 provides a chapter summary, while Section 7.3 restates the primary and secondary research objectives and argues how these objectives were met. Section 7.4 discusses the research contribution which, in this case, is the proposed framework. Section 7.5 highlights the research limitations of this research, and Section 7.6 lists suggestions for future research. Section 7.7 provides the publication stemming from this research

7.2. Summary of Chapters

This dissertation consists of seven chapters, as summarised below.

Chapter 1 introduced the problem area of this study, as well as highlighting the research problem and objectives for this study. This chapter includes the background of the study, the problem area and the research process and research approach used in this study.

Chapter 2 provided important background regarding cybersecurity as the main area of study for this research. This was achieved by reviewing multiple aspects of cybersecurity including cyber threats and vulnerabilities, South African laws and regulations, the cybersecurity skills gap, as well as education, training and awareness in the cybersecurity space.

Chapter 3 provided an overview of various global cybersecurity workforce and skills frameworks. These skills frameworks were discussed in detail and compared according to their key characteristics.

Chapter 4 described the thematic content analysis conducted during this study, including the data collection process, as well as details regarding the thematic content analysis using ATLAS.ti as an analysis tool.

Chapter 5 discussed the results of the thematic content analysis conducted during this study. It also provides an interpretation of the results and findings within the context of this study.

Chapter 6 presented the solution of this study by proposing the Cybersecurity Skills Framework for South Africa (CSFwSA). This chapter highlighted the structure of the framework, contextualising it to provide a clear understanding, and discussed the possible role of the framework.

Chapter 7 concludes the study by arguing towards the achievement of the research objectives identified in Chapter 1. This chapter also provides the limitations of this study, as well as suggesting possible future research.

7.3. Meeting the Research Objectives

This section highlights how the research objectives of this study were met. As indicated in Chapter 1, Section 1.5, the primary research objective of this study was as follows:
Primary Objective: *To develop a cybersecurity skills framework by determining the cybersecurity knowledge, skills, abilities, and tasks (KSATs) required for specific IT job roles in South Africa.*

To address the primary objective, the following secondary objectives were met:

Secondary Objective 1: *To position the cybersecurity threat landscape as it relates to the cybersecurity skills gap both globally and in South Africa.* The purpose of this objective was to provide a better understanding in terms of the cybersecurity landscape by discussing various key aspects of cybersecurity and how they relate to the cybersecurity skills gap. These key aspects include the positioning of cybersecurity and the related cyber threats and

vulnerabilities that result in the prevalence of cyberattacks both globally, and in South Africa. The mitigation of such attacks is addressed, as well as the various cybersecurity laws and legislations in South Africa. Furthermore, the cybersecurity skills gap is highlighted, and the importance of cybersecurity education, training and awareness in addressing this gap. During the discussion of these aspects, it was highlighted that South Africa is one of the countries that is most often attacked due to their cybersecurity policies still being in their infancy. It was also made clear that to implement security measures effectively, human resources are needed. However, there is a lack of human resources, especially IT professionals, with the required cybersecurity skills to secure cyberspace effectively. This objective was achieved in Chapter 2 through a literature review.

Secondary Objective 2: *To compare existing global cybersecurity skills frameworks according to their key characteristics.* The purpose of this objective was to identify and compare existing cybersecurity skills and workforce frameworks that are currently being used worldwide. This objective was intended to help guide this study in terms of the development of the proposed cybersecurity skills framework for South Africa. This objective was achieved through a literature review as discussed in Chapter 3. In total, eight frameworks were identified, discussed and compared. These frameworks were compared based on their target audience, KSATs, job roles and focus. After the comparison, two key skills frameworks were deemed to be the most relevant to the development of the proposed cybersecurity skills framework, namely NIST's NICE framework and the Skills Framework for Infocomm Technology (SFw for ICT). As discussed in Chapter 6, the NICE framework provided for a solid structure for the proposed framework, whereas the SFw for ICT was more suited to the content of the proposed framework and, as such, was useful for filling any gaps in the KSATs relating to the job roles identified through the thematic content analysis.

Secondary Objective 3: *To determine the cybersecurity KSATs required of IT professionals within South Africa, and how they relate to specific IT job roles.* This objective was achieved through the thematic content analysis described in Chapter 4, as well as through critical reasoning in Chapter 5. The thematic content analysis was used to code and analyse 280 job postings that were gathered over a four-month period from LinkedIn.com. From the thematic content analysis conducted, 20 IT job roles were identified, as well as 54 knowledge areas, 23 skills, 27

abilities, and 68 tasks. These KSATs serve as the output of this research objective, and contribute to the proposed solution of this study.

The **primary research objective** made use of the cybersecurity and skills gap understanding gained via the output of SRO1 to confirm the need for a cybersecurity skills framework for South Africa. The output of SRO2, namely the key characteristics of the identified skills frameworks, helped to provide the proposed framework with both a structure via the NICE framework and missing content identified using the SFw for ICT. The KSATs, which serve as the output of SR03, provided the proposed framework with 20 IT job roles which all have defined KSATs. The output from all three secondary objectives contributed to the development of the proposed framework leading to the meeting of the primary research objective of this study. The proposed framework is explained in Chapter 6 with the full framework being provided in Appendix B. The proposed framework is aptly called the Cybersecurity Skills Framework for South Africa and abbreviated to CSFwSA.

7.4. Research Contribution

The main contribution of this study is the proposed Cybersecurity Skills Framework for South Africa (CSFwSA), as explained in Chapter 6, and presented in full in Appendix B. The framework contributes valuable knowledge regarding IT job roles in South Africa. As such, it can benefit academia by guiding the development of IT curricula for both existing and new qualifications in higher educational institutions and providing the South African industry with KSATs relating to IT job roles. This could lead to the upskilling of IT professionals and graduates in South Africa with IT curricula better serving the cybersecurity needs of the South African industry. Furthermore, the proposed framework could guide organisations in South Africa to train their existing IT professionals to better fit the cybersecurity needs of their job roles.

The proposed framework could therefore help to build a more cybersecurity-capable workforce in all areas of the IT industry, as well as helping to provide the industry with new and highly skilled IT graduates. In the long term, this could help narrow the cybersecurity skills gap in South Africa.

7.5. Research Limitations

This study focused on IT job postings found on LinkedIn.com over a four-month period and these job postings were used to define the proposed framework. However, two main limitations must be acknowledged. Firstly, only one job postings website, LinkedIn, was included in the thematic content analysis, although others were considered as discussed in Chapter 4 Section 4.4.2. Secondly, the data collection only took place over a four-month period, which was also over the Covid-19 lockdown period in South Africa. It is therefore recommended that any future such studies in South Africa consider other job posting websites and that the data collection takes place over a longer period of time, for example, six to twelve months.

In addition, many of the IT job postings analysed lacked detail as they did not necessarily contain all of the relevant information for a particular IT job role. Although measures were taken to fill some of the identified gaps, this was not validated further.

During the course of this study, and specifically during the thematic content analysis where coding of data was performed, the researcher strived to be objective. However, often decisions had to be made regarding ambiguous data where some bias could have been introduced into the findings of the study. It is therefore recommended for future research to make use of more researchers to eliminate as much bias as possible.

Due to the NICE framework revision in November 2020, and the fact that the thematic content analysis had already been started, the researcher opted to use the NICE framework released in 2017 instead of the updated 2020 version. Although this is considered a further limitation of this study, it also creates the opportunity for future research and a revision of the proposed framework.

Despite the limitations of the study, this proposed framework provides a solid foundation for future research, and in so doing, will further contribute to the body of knowledge relating to the cybersecurity skills gap in South Africa.

7.6. Suggestions for Future Research

As stated in Section 7.5, this research focused solely on analysing IT job postings. This leads to the possible exploration of other methods of identification of IT job roles and their KSATs, such

as possible industry investigations through surveys or interviews. Industry input through the stated surveys or interviews, along with the results of this study, could provide for a very detailed framework. This study would also benefit from further validation through survey, interviews, or expert reviews.

7.7. Publication

The following publication stemmed directly from this research and is attached in Appendix C:

- Kruger, M., Futcher, L., Thomson, KL. (2022). A Thematic Content Analysis of the Cybersecurity Skills Demand in South Africa. In: Clarke, N., Furnell, S. (eds) Human Aspects of Information Security and Assurance. HAISA 2022. *IFIP Advances in Information and Communication Technology*, vol 658. Springer, Cham. https://doi.org/10.1007/978-3-031-12172-2_3.

References

Abu-Taieh, E. M. O. (2018). Cyber Security Body of Knowledge. *Proceedings - 2017 IEEE 7th International Symposium on Cloud and Service Computing, SC2 2017*, 104–110. https://doi.org/10.1109/SC2.2017.23

Atlas Ti. (2019). *Data Analysis - Analyzing Data in Qualitative Research | ATLAS.ti*. https://atlasti.com/analyzing-data-data-analysis/

Australian Signals Directorate. (2020). *ASD Cyber Skills Framework v2.0*. 64. https://www.cyber.gov.au/sites/default/files/2020-09/ASD-Cyber-Skills-Framework-v2.pdf

BDC. (2016). *What is a search engine*. https://www.bdc.ca/en/articles-tools/entrepreneur-toolkit/templates-business-guides/glossary/search-engine

Beltrami, S. (2020). *How to Minimize the Impact of the Cybersecuirty Skills Shortage*. *583*(7815), 195. https://www.vmware.com/learn/security/how-to-minimize-the-impact-of-the-cybersecurity-skills-shortage.html

Bhandari, P. (2020). *Data Collection: A Step-by-Step Guide with Methods and Examples*. https://www.scribbr.com/methodology/data-collection/

Bordens, K. S., & Abbot, B. B. (2017). *Research Design and Methods: A Process Approach* (10th ed.). McGraw Hill.

Brannon, S., Sassen, C., & Yanowski, K. (2022). Roles and Responsibilities of Cataloging Managers: An Updated Study of Job Advertisements. *Technical Services Quarterly*, *39*(1), 17–36. https://doi.org/10.1080/07317131.2021.2011144

Bucchianeri, S. (2019). *The cybersecurity skills gap offers SA an opportunity to lead in the 4IR*. https://www.absa.africa/world-economic-forum/africa/absa-at-wef/op-ed-piece-7/

Burney, S. M., & Saleem, H. (2008). *Inductive & Deductive Research Approach*. *March*. https://doi.org/10.13140/RG.2.2.31603.58406

Burning Glass Technologies. (2019). *The State of Cybersecurity Hiring* (Issue June).

Business Insider SA. (2020). *Hackers on the dark web love South Africa - here's why we suffer 577 attacks per hour*. https://www.businessinsider.co.za/sa-third-highest-number-of-cybercrime-victims-2020-6

Capterra. (n.d.). *Capterra: Find Business Software reviews, prices, and comparisons*. Retrieved July 29, 2021, from https://www.capterra.co.za/

CIISec. (2019). *CIISec Skills Framework*. *November*, 38. https://www.ciisec.org/CIISEC/News/CIISec_release_the_latest_version_of_the_Skills_Framework_V_2_4.aspx

Cisco. (2021). *What is Cyber Security?* https://www.cisco.com/c/en_uk/products/security/what-is-cybersecurity.html

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (4th ed.).

Creswell, J. W., & Creswell, D. J. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). Sage Publications.

Cyber Exposure Index. (2020). *Country statistics*. https://cyberexposureindex.com/country-statistics/

Doyle, K. (2016). Wanted: Cyber security expertise. *ITWeb's Corporate IT Training Guide*, *4th Issue*, Page 27. http://books.itweb.co.za/tg/

Dynamic Yield. (2017). *What is a Search Filter? Definition & Examples — Dynamic Yield*. https://www.dynamicyield.com/glossary/search-filter/

ENISA. (2020). *European Cybersecurity Skills Framework*. https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework

ENISA. (2022a). *ENISA Webinar: Using the European Cybersecurity Skills Framework to sustain cybersecurity workforce*. https://www.youtube.com/watch?v=yTuWWg_JG64

ENISA. (2022b). *European Cybersecurity Skills Framework Draft v0.5*. *April*, 0–26. https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

Fortinet. (2020). *Top 20 Most Common Types Of Cyber Attacks*. https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks

Government Gazette. (2020). *Cybercrimes Act 19 of 2020*. http://www.nsw.gov.au/sites/default/files/Government_Gazette_2_December.pdf#page=15

Gwala, S. (2016). Barriers To Implementation Of The National Cybersecurity Policy Framework. *Skripsi*, 1–111. https://core.ac.uk/download/pdf/188773121.pdf

Hajny, J., Ricci, S., Lieskovan, T., Janout, V., Proskurin, S., Ohm, M., Levillain, O., Stambiliyska, R., Galletta, L., De Nicola, R., Piesarskas, E., Bruze, E., Valutyte, R., Kaczmarek, K., & Adao, P. (2020). *SPARTA: Curricula Descriptions*. https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf

Hewitt, K. (2021). *What is a Cybersecurity Vulnerability?* https://securityscorecard.com/blog/what-is-a-cybersecurity-vulnerability

Humphreys, E. (2021). *ISO - The cybersecurity skills gap*. https://www.iso.org/news/ref2655.html

IBM. (2021). Cost of a Data Breach Report 2021. In *IBM Security*. https://www.ibm.com/security/data-breach

IBM. (2022). Cost of a Data Breach Report 2022. In *IBM Security*. https://www.ibm.com/security/data-breach

Iivari, J., & Huisman, M. (2007). The relationship between organizational culture and the deployment of systems development methodologies. *MIS Quarterly: Management Information Systems*, *31*(1), 35–58. https://doi.org/10.2307/25148780

IMDA. (2017). *Skills Framework For ICT*. https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html

International Information System Security Certification Consortium. (2019). Strategies for Building and Growing Strong Cybersecurity Teams. *(ISC)2 Cybersecurity Workforce Study*, *2019*, 1–37.

ISACA. (2022). *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations.* 1–39.

ISO. (2012). *ISO - ISO/IEC 27032:2012 - Information technology — Security techniques — Guidelines for cybersecurity*. *1*, 50. https://www.iso.org/standard/44375.html

ISS Africa. (2021). *Critical infrastructure attacks: why South Africa should worry*. https://issafrica.org/iss-today/critical-infrastructure-attacks-why-south-africa-should-worry

Joint Task Force on Cybersecurity Education. (2017). Cybersecurity Curricula 2017. In *Cybersecurity Curricula 2017* (Issue December). https://doi.org/10.1145/3422808

Kortjan, N. (2013). *A Cyber Security Awareness and Education Framework for South Africa* [Nelson Mandela University]. https://www.researchgate.net/publication/290139259_A_conceptual_framework_for_cyber_security_awareness_and_education_in_SA

Li, X. (2021). Identifying in-demand qualifications and competences for translation curriculum renewal: a content analysis of translation job ads. *The Interpreter and Translator Trainer*, *16*(2), 177–202. https://doi.org/10.1080/1750399X.2021.2017706

Luo, A. (2019). *Content Analysis: A Step by Step guide with examples*. Scribbr. https://www.scribbr.com/methodology/content-analysis/

Mahlobo, D. (2015). The National Cybersecurity Policy Framework (NCPF) For South Africa - 2015. *Government Gazette*, *39475*, 1–30. http://www.gov.za/sites/www.gov.za/files/39475_gon609.pdf

Mcanyana, W., Brindley, C., & Seedat, Y. (2020). *Insight into the cyberthreat landscape in South Africa*. 12. https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf

McCumber, J. (1991). Information Systems Security: A Comprehensive Model. *14th National Computer Security Conference*, 328–338.

Meyer, M. A. (2019). Healthcare data scientist qualifications, skills, and job focus: A content analysis of job postings. *Journal of the American Medical Informatics Association*, *26*(5), 383–391. https://doi.org/10.1093/jamia/ocy181

Mickos, M. (2019). *The Cybersecurity Skills Gap Won't Be Solved in a Classroom*. https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/?sh=1001e4dc1c30

Mimecast. (2021). *Securing the Enterprise in the Covid world: The state of Email Security*. https://www.mimecast.com/resources/webinars/the-state-of-email-security-securing-the-enterprise-in-the-covid-world/

Mohamed, Z. (2021). *Data protection and cybersecurity laws in South Africa | CMS*. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/south-africa

Monash University. (2019). *Critical thinking - Research & Learning Online*. https://www.monash.edu/rlo/research-writing-assignments/critical-thinking

Mybroadband. (2021). *Department of Justice hack — all backups gone and R33 million ransom demanded*. https://mybroadband.co.za/news/security/414902-department-of-justice-hack-all-backups-gone-and-r33-million-ransom-demanded.html

News24. (2020). *Cybercriminals change tack in SA, use more ransomware during lockdown*. https://www.news24.com/fin24/companies/ict/cybercriminals-change-tack-in-sa-use-more-ransomware-during-lockdown-20200613

NIST. (2017). *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-

resource-center

NIST. (2020). NICE Cybersecurity Workforce Framework Use Cases and Success Stories. *English Journal*, 1–21. https://www.nist.gov/news-events/events/2020/03/nice-webinar-nice-cybersecurity-workforce-framework-use-cases-and-success

Oltsik, J. (2017). *The Life and Times of Cybersecurity Professionals: A Cooperative Research Project by ESG and ISSA*. *November*, 9. http://www.esg-global.com/

Oltsik, J. (2020). *ESG Research Report: The Life and Times of Cybersecurity Professionals 2020* (Issue July). https://www.esg-global.com/research/esg-research-report-the-life-and-times-of-cybersecurity-professionals-2020

On To Text. (2017). *What is Text Analysis? | Ontotext Fundamentals Series*. https://www.ontotext.com/knowledgehub/fundamentals/text-analysis/

Parker, A., & Brown, I. (2018). Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. *International Information Security Conference ISSA 2018: Information Security*, Pages 176-192. https://link.springer.com/chapter/10.1007/978-3-030-11407-7_13

Petersen, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (2020). Workforce Framework for Cybersecurity (NICE Framework). *NIST Special Publication 800-181, Revision 1*, *3*, 27. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Phair, D., & Warren, K. (2021). *Saunders' Research Onion: Explained Simply*. https://gradcoach.com/saunders-research-onion/

Predictive Analytics Today. (2021). *Top 14 Qualitative Data Analysis Software in 2021 - Reviews, Features, Pricing, Comparison - PAT RESEARCH: B2B Reviews, Buying Guides & Best Practices*. https://www.predictiveanalyticstoday.com/top-qualitative-data-analysis-software/

Risk Based Security. (2020). *2020 Q3 Report Data Breach QuickView*. https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020 Q3 Data Breach QuickView Report.pdf

Risk Based Security. (2022). *The State of Data Breach Intelligence: 2022 Midyear Edition*. https://flashpoint.io/resources/thank-you-resource-the-state-of-data-breach-intelligence-2022-midyear-edition/

Rogers, P. (2019). *Plan to address the cybersecurity skills shortage in South Africa – Intelligent CIO Africa*. https://www.intelligentcio.com/africa/2019/03/28/plan-to-address-cybersecurity-skills-shortage-in-south-africa/

Ross, R., McEvilley, M., & Oren, J. C. (2018). NIST Special Publication 800-160 Volume 1 - Systems security engineering: considerations for a multidisciplinary approach in the engineering of trustworthy secure systems, volume 1. *NIST Special Publication*, *1*, 260.

Sarker, S., Xiao, X., Beaulieu, T., & Lee, A. S. (2018). Learning from first-generation qualitative approaches in the is discipline: An evolutionary view and some implications for authors and evaluators (part 1/2). *Journal of the Association for Information Systems*, *19*(8), 752–774. https://doi.org/10.17705/1jais.00508

Schlein, T. (2014). *Venture Capitalist Ted Schlein on the Future of Cybersecurity | Kleiner Perkins | Make History*. https://www.kleinerperkins.com/perspectives/venture-capitalist-ted-schlein-on-the-future-of-cybersecurity/

SFIA Foundation. (2018). *Sfia 7*. https://www.sfia-online.org/en

Skills Future. (2016). *SSG | Skills Framework*. https://www.skillsfuture.gov.sg/skills-framework

Smith, C. (2019, April 29). Major spike in SA cyber attacks, over 10 000 attempts a day. *News24*. https://www.fin24.com/Companies/ICT/major-spike-in-sa-cyber-attacks-over-10-000-attempts-a-day-security-company-20190429

Somasundaram, S. (2022). *Importance of Research Design for a Researcher*. https://www.ilovephd.com/why-research-design-is-important-for-a-researcher/

Soratto, J., Pires, D. E. P. de, & Friese, S. (2020). Thematic content analysis using ATLAS.ti software: Potentialities for researchs in health. *Revista Brasileira de Enfermagem*, *73*(3), e20190250. https://doi.org/10.1590/0034-7167-2019-0250

Symanovich, S. (2020). *Cyberattacks on the rise: What to do before and after a cyberattack or data breach*. NortonLifeLock. https://us.norton.com/internetsecurity-emerging-threats-cyberattacks-on-the-rise-what-to-do.html

Tableau. (2018). *What Is Data Visualization? Definition & Examples | Tableau*. https://www.tableau.com/learn/articles/data-visualization

Tamarkin, E. (2015). The AU's cybercrime response A positive start, but substantial challenges ahead. In *Institute for Security Studies* (Issue January 2015). https://issafrica.org/research/policy-brief/the-aus-cybercrime-response-a-positive-start-but-substantial-challenges-ahead

Technation. (2020). *Cybersecurity Skills Framework - TECHNATION*. https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-skills-framework/

Technation. (2022). *Operate & Maintain*. https://technationcanada.ca/en/future-workforce-development/cybersecurity/cybersecurity-skills-framework/operate-maintain/

Tunggal, A. T. (2020). *What is a Cyber Threat?* Upguard. https://www.upguard.com/blog/cyber-threat

Usecure. (2019). *The Role of Human Error in Successful Cyber Security Breaches*. Usecure. https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches

Van Niekerk, B. (2017). An Analysis of Cyber-Incidents in South Africa. *The African Journal of Information and Communication*, *20*, 113–132. https://doi.org/10.23962/10539/23573

Verizon. (2021). *2021 Data Breach Investigation Report.* https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report

Vox. (2019). *IT skills shortage in South Africa*. https://www.vox.co.za/content-hub/article/it-skills-shortage-in-south-africa?page=27465&category=5361

Walliman, N. (2011). *Research Methods: The Basics* (1st Ed). Routledge. https://www.researchgate.net/publication/308119180_Research_Methods_The_Basics

Wijngaarden, V. (2019). *The application of ATLAS.ti in different qualitative data analysis strategies by Dr. Vanessa Wijngaarden | ATLAS.ti*. https://atlasti.com/2019/05/23/the-application-of-atlas-ti-in-different-qualitative-data-analysis-strategies-by-dr-vanessa-wijngaarden/

Appendices

Appendix A: Identified Job Roles with the Merged Job Role Codes

CYBERSECURITY [CS] JOB CATEGORY	
Job Role	**Merged Job Role Codes**
CSJ01: Cybersecurity Specialist	Business Development Manager Cloud Security Engineer Crisis Management Coordinator Cryptography Specialist Cyber Technology Specialist Cybersecurity Engineer Cybersecurity Intelligence Centre Manager Head of Information Security ICT Security Specialist Information Officer information Security Administrator Information Security Analyst Information Security Architect Information Security Engineer Information Security Manager Information Security Officer Information Security Specialist Information Systems and Technology Manager IT Security Engineer IT Security Officer IT Security Specialist Senior Information Security Consultant Senior Specialist Senior Specialist: Cybersecurity SIEM Engineer Software Developer: Security
CSJ02: Digital Forensics Analyst	Cybersecurity Technician Digital Risk Analyst ICT Security Analyst Information Risk Analyst Information Security Threat Analyst Insider Trust Analyst IT Forensic Consultant IT Technical Support Security Analyst Senior Cyber Defence Analyst Senior Principal Security Analyst Threat Intelligence Analyst
CSJ03: Security Engineer	Cybersecurity Engineer Security Engineer Security Specialist
CSJ04: Data Privacy and Protection Specialist	Data Protection Manager Privacy Specialist

	Senior Cloud Data Engineer Senior Privacy and Technology Counsel
CSJ05: Cybersecurity Manager	Head of SOC SOC Services Manager
CSJ06: Application Security Specialist	Senior Specialist: Application and Endpoint Security Web Application Firewall Engineer
CSJ07: Penetration Tester	No other Job Role Codes

STRATEGY AND GOVERNANCE [SG] JOB CATEGORY	
Job Role	**Merged Job Role Codes**
SGJ01: Information Technology Manager	Head of Technical Head of Technology ICT Support Engineer ICT Team Lead Identity and Access Management Specialist Infrastructure Service Deliver Specialist Manager Senior Manager Technical Account Manager Technical Specialist
SGJ02: Information Technology Auditor	Auditor Cybersecurity Manager Head of Internal Audit Information Technology Audit Specialist Internal Audit Manager Internal Audit Supervisor IT Audit Manager IT Auditor IT Auditor Consultant IT Security Analyst IT Security Auditor
SGJ03: Compliance Specialist	Compliance Auditor Head of Technology Security Senior Specialist: IT Risk and Compliance Risk Advisory IT Compliance Information Security Specialist Risk Management Lead Information Governance Specialist Infrastructure Engineer: Security Head of IT Risk and Compliance IT Compliance Auditor
SGJ04: Project Manager	General Manager IT Security Program Manager Project Engineer
SGJ05: Quality Assurance Analyst	Analyst Automation Test Analyst Quality Assurance Engineer Quality Assurance Specialist Quality Assurance Tester

	Sales Engineer Software Quality Assurance Engineer Systems Analyst Test Analyst
SGJ06: Chief Information Officer	Customer Data and Analytics Solution Architect

OPERATIONS AND SUPPORT [OS] JOB CATEGORY	
Job Role	**Merged Job Role Codes**
OSJ01: IT Technician	Cloud Support Engineer Desktop Support Technician ICT Analyst ICT Support ICT Support Technician Infrastructure Architect IT Desktop Technician IT Engineer IT Field Technician IT Hardware and Support Technician IT Infrastructure Specialist IT Production Specialist IT Specialist IT Support Engineer IT Support Specialist IT Support Technician IT Technical Support IT Technician Managed Service Analyst Microsoft IT Technician Network Engineer PC Technician Senior Field Service Engineer Senior in IT Senior Infrastructure Specialist Service Desk Support Support Desk Engineer Support Technician Systems Engineer Technical Analyst Technical Support Technical Support Analyst Technical Support Engineer Technician
OSJ02: Network Engineer	Network Administrator Network and Security Lead Network Cable Technician Network Engineer Network Security Architect Network Security Engineer Network Specialist Network System Engineer

	Network Technician Security Administrator Transmission Engineer

DATA AND ARTIFICIAL INTELLIGENCE [DA] JOB CATEGORY	
Job Role	**Merged Job Role Codes**
DAJ01: System Administrator	Application Administrator Consultant Database Support Engineer Datacentre Engineer ICT Engineer ICT Server Administrator Information Technology Manager IT Administrator IT Infrastructure Manager Linus Engineer Network Administrator Server Engineer SQL Database Administrator System Administrator Systems Engineer Systems Engineer Specialist Technology Services Consultant
DAJ02: Cloud Architect	Senior Cloud Support Engineer
DAJ03: Data Warehousing Engineer	Business Intelligence Consultant Business Intelligence Developer Solution Architect

SOFTWARE AND APLICATION DEVELOPMENT [SA] JOB CATEGORY	
Job Role	**Merged Job Role Codes**
SAJ01: Software Developer	Application Developer Developer DevOps Engineer Full Stack Developer Full Stack Engineer Java Software Engineer Programmer Robotics Specialist Security Solution Software Developer Sharepoint Developer Software Engineer Software Security Engineer Team Lead
SAJ02: DevOps Engineer	Application Support Specialist DevOps Manager DevSecOps Engineer Integration Specialist Technical Business Analyst

Appendix B: The Cybersecurity Skills Framework for South Africa

JOB CATEGORY	CYBERSECURITY [CS]
JOB ROLE	CSJ01: CYBERSECURITY SPECIALIST

TASKS

SPECIFIC TASKS

Cybersecurity [CS]
CST02: Respond to cybersecurity incidents.
CST04: Implement security policies and standards.
CST06: Implement security solutions.
CST09: Implement security best practices
CST10: Monitor network software for proper security procedures.
CST14: Develop and improve security posture and threat surfaces through scoping and shaping of information security program
CST15: Ensure information is kept protected.

Software and Application Development [SA]
SAT02: Develop applications to monitor networks for cyberthreats.
SAT03: Develop applications to automatise tasks performed by security analysts.

Strategy and Governance [SG]
SGT08: Assist in the development and maintenance of policies, procedures, and technical standards.
SGT09: Assist in the incident management process.
SGT10: Assist in the problem management process.
SGT11: Assist in the access management process.
SGT12: Assist in the change management process.
SGT17: Present and compile reports.

GENERAL TASKS

CST01: Identify cyber threats
CST03: Develop and maintain security policies and standards
CST05: Design, implement and monitor controls
CST11: Align enterprise data to ensure that it supports information security.
CST13: Provide support to forensic investigational teams.
CST19: Identify, assess, and manage cyber risk.

KNOWLEDGE	SKILLS	ABILITIES
Cybersecurity [CS] **CSK01:** Security proxies **CSK03:** Anti-virus software **CSK04:** Security best practices **CSK05:** Penetration testing **CSK06:** Security vulnerabilities and exploits **CSK07:** Firewalls **CSK08:** Secure Sockets Layer (SSL) **CSK09:** Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) **Operations and Support [OS]** **OSK01:** Operating systems **OSK03**: Backups **OSK05:** Active directory	**Technical Skills** **TS06:** Problem solving skills **Non-Technical Skills** **NTS05:** Communication skills **NTS08:** Organisation skills **NTS12:** Collaboration skills **NTS13:** Customer service skills	**Technical Abilities** **TA01:** Ability to solve technical problems **TA02:** Ability to write reports **TA08:** Ability to investigate malware, intrusion attempts and vulnerabilities **Non-Technical Abilities** **NTA04:** Able to work in teams **NTA05:** Ability to maintain confidentiality. **NTA07:** Ability to manage many priorities concurrently

OSK06: Virtual Private Network (VPN) **OSK08:** Open Web Application Security Project (OWASP) **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **<u>Strategy and Governance [SG]</u>** **SGK01:** Project management **SGK02:** Information technology risk **SGK03:** National Institute of Standards and Technology (NIST) **SGK04:** International Organization for Standardization (ISO) **SGK05:** Control Objectives for Information and Related Technologies (COBIT) **SGK14:** Information Technology Infrastructure Library (ITIL)		**NTA13:** Ability to stay organised.
CERTIFICATIONS		
Certified Information Systems Security Professional (CIISP) CompTIA Advanced Security Practitioner (CASP) Certified Ethical Hacker (CEH) Certified Information Security Manager (CISM) Cisco Certified Network Associate (CCNA) GIAC Security Essentials (GSEC) Security + Systems Security Certified Practitioner (SSCP)		

JOB CATEGORY	CYBERSECURITY [CS]
JOB ROLE	CSJ02: DIGITAL FORENSICS ANALYST

TASKS

SPECIFIC TASKS

Cybersecurity [CS]
CST02: Respond to cyber security incidents.
CST12: Conduct forensic investigations.
CST13: Provide support to forensic investigational teams.

GENERAL TASKS

CST01: Identify cyber threats.
CST07: Manage or perform security config reviews on network devices, databases, and operating systems.
CST16: Train and raise awareness regarding security.
CST19: Identify, assess, and manage cyber risk.

KNOWLEDGE	SKILLS	ABILITIES
Cybersecurity [CS] **CSK04:** Security best practices **CSK06:** Security vulnerabilities and exploits **Strategy and Governance [SG]** **SGK03:** National Institute of Standards and Technology (NIST) **SGK08:** Problem management **SGK09:** Incident management **SGK11:** Compliance **SGK12:** Change management **SGK14:** Information Technology Infrastructure Library (ITIL) **Operations and Support [OS]** **OSK08:** Open Web Application Security Project (OWASP)	**Technical Skills** **TS01:** Troubleshooting skills **TS02:** Technical writing skills **TS06:** Problem solving skills **Non-Technical Skills** **NTS04:** Analytical thinking skills **NTS05:** Communication skills **NTS09:** Time management skills **NTS15:** Negotiation skills	**Technical Abilities** **TA02:** Ability to write reports **TA03:** Ability to obtain Forensic evidence **TA07:** Ability to analyse data **Non-Technical Abilities** **NTA04:** Ability to work in teams **NTA12:** Ability to adapt to changing environments

CERTIFICATIONS

A+
Certified Cloud Security Professional (CCSP)
Certified Ethical Hacker (CEH)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CIISP)
GIAC Security Essentials (GSEC)
Network+
Security+

JOB CATEGORY	CYBERSECURITY [CS]
JOB ROLE	CSJ03: SECURITY ENGINEER

TASKS

SPECIFIC TASKS

Cybersecurity [CS]
CST17: Guide teams through the design and implementation of cyber solutions.
CST18: Assist with prototypes and pilot runs of proposed security solutions

GENERAL TASKS

CST04: Implement security policies and standards.
CST05: Design, implement and monitor controls.
CST06: Implement security solutions.
CST09: Implement security best practices.
CST15: Ensure information is kept protected.

KNOWLEDGE	SKILLS	ABILITIES
Operations and Support [OS] **OSK01:** Operating systems **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **OSK12:** Network security **Strategy and Governance [SG]** **SGK04:** International Organization for Standardization (ISO) **SGK05:** Control Objectives for Information and Related Technologies (COBIT) **SGK11:** Compliance **SGK14:** Information Technology Infrastructure Library (ITIL) **Software and Application Development [SA]** **SAK07:** Databases	**Technical Skills** **TS06:** Problem solving skills **Non-Technical Skills** **NTS04:** Analytical thinking skills **NTS05:** Communication skills	**Technical Abilities** **TA01:** Ability to solve technical problems **Non-Technical Abilities** **NTA03:** Ability to work with leadership **NTA04:** Ability to work in teams **NTA16:** Ability to work independently

CERTIFICATIONS

A+
Certified Ethical Hacker (CEH)
Certified Information Security Manager (CISM)
Certified Information Systems Security Professional (CIISP)
GIAC Security Essentials (GSEC)
Network +

JOB CATEGORY	CYBERSECURITY [CS]
JOB ROLE	CSJ04: DATA PRIVACY AND PROTECTION SPECIALIST

TASKS

SPECIFIC TASKS

Strategy and Governance [SG]

SGT13: Advise the business on its data protection obligations in respect of the policies, processes, and technology that supports the products and services and solutions.

SGT14: Monitor and evaluate the effectiveness of data privacy and protection programs

GENERAL TASKS

CST03: Develop and maintain security policies and standards.

CST04: Implement security policies and standards.

CST11: Align enterprise data to ensure that it supports information security.

CST14: Develop and improve security posture and threat surfaces through scoping and shaping of information security programs.

KNOWLEDGE	SKILLS	ABILITIES
Cybersecurity [CS] **CSK04:** Security best practices **CSK06:** Security vulnerabilities and exploits **Data and Artificial Intelligence [DA]** **DAK04:** Machine learning **DAK05:** Cloud services	**Technical Skills** **TS02:** Technical writing skills **TS06:** Problem solving skills **Non-Technical Skills** **NTS02:** Leadership skills **NTS04:** Analytical thinking skills **NTS05:** Communication skills **NTS10:** Attention to detail skills	**Technical Abilities** **TA03:** Ability to obtain forensic evidence **Non-Technical Abilities** **NTA11:** Ability to work under pressure

CERTIFICATIONS

Certified in Risk and Information Systems Control (CRISC)
Certified Information Privacy Professional (CIPP)
Certified Information Privacy Technologist (CIPT)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)

JOB CATEGORY	CYBERSECURITY [CS]
JOB ROLE	CSJ05: CYBERSECURITY MANAGER

TASKS

SPECIFIC TASKS

Cybersecurity [CS]
CST07: Manage or perform security config reviews on network devices, databases, and operating systems
CST08: Perform penetration testing.

Strategy and Governance [SG]
SGT06: Handle all customer escalations ensuring compliance with Service Level Agreements (SLAs).
SGT07: Manage and ensure compliance with internal policies and procedures
SGT17: Present and compile reports.

GENERAL TASKS

CST01: Identify cyber threats.
CST02: Respond to cybersecurity incidents.
CST03: Develop and maintain security policies and standards.
CST04: Implement security policies and standards.
CST16: Train and raise awareness regarding security.
CST17: Guide teams through the design and implementation of cyber solutions.

KNOWLEDGE	SKILLS	ABILITIES
Operations and Support [OS] **OSK09:** Routers **OSK10:** Switches **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **OSK13:** Network monitoring tools **Cybersecurity [CS]** **CSK05:** Penetrating testing **CSK07:** Firewalls **CSK09:** Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS) **Strategy and Governance [SG]** **SGK03:** National Institute of Standards and Technology (NIST) **SGK04:** International Organization for Standardization (ISO) **SGK05:** Control Objectives for Information and Related Technologies (COBIT) **SGK14:** Information Technology Infrastructure Library (ITIL)	**Technical Skills** **TS06:** Problem solving skills **Non-Technical Skills** **NTS01:** Planning skills **NTS02:** Leadership skills **NTS03:** Presentation skills **NTS05:** Communication skills **NTS16:** Decision making skills **NTS17:** Logical thinking skills	**Technical Abilities** **TA05:** Ability to troubleshoot **TA08:** Ability to investigate malware, intrusion attempts and vulnerabilities. **Non-Technical Abilities** **NTA02:** Ability to lead teams **NTA14:** Ability to communicate effectively and efficiently.

CERTIFICATIONS

Certified Ethical Hacker (CEH)

Certified Information Systems Security Professional (CIISP) CompTIA Advanced Security Practitioner (CASP)

JOB CATEGORY	CYBERSECURITY [CS]
JOB ROLE	CSJ06: APPLICATION SECURITY SPECIALIST

TASKS

SPECIFIC TASKS

Cybersecurity [CS]
CST01: Identify cyber threats
CST02: Respond to cybersecurity incidents
CST04: Implement security policies and standards

Software and Application Development [SA]
SAT01: Develop secure apps

GENERAL TASKS

CST05: Design, implement and monitor controls.
CST07: Manage or perform security config reviews on network devices, databases, and operating systems.
CST14: Develop and improve security posture and threat surfaces through scoping and shaping of information security programs.

KNOWLEDGE	SKILLS	ABILITIES
Operations and Support [OS] **OSK08:** Open Web Application Security Project (OWASP) **Software and Application Development [SA]** **SAK02:** Secure coding **SAK03:** Application security **Cybersecurity [CS]** **CSK03:** Anti-virus software **CSK07:** Firewalls **Strategy and Governance [SG]** **SGK05:** Control Objectives for Information and Related Technologies (COBIT) **SGK14:** Information Technology Infrastructure Library (ITIL)	**Technical Skills** **TS01:** Troubleshooting skills **TS04:** General programming skills **TS06:** Problem solving skills **Non-Technical Skills** **NTS01:** Planning skills **NTS06:** Adaptability skills **NTS07:** Fast learner skills	**Technical Abilities** **TA01:** Ability to solve technical problems **TA05:** Ability to troubleshoot **TA08:** Ability to investigate malware, intrusion attempts and vulnerabilities **TA11:** Ability to write secure code **Non-Technical Abilities** **NTA07:** Ability to manage many priorities concurrently **NTA08:** Ability to engage and contribute **NTA09:** Ability to execute instructions **NTA12:** Ability to adapt to changing environments

CERTIFICATIONS

Certified Ethical Hacker (CEH)
Certified Information Systems Security Professional (CIISP)
CREST Certification
GIAC Security Essentials (GSEC)
Offensive Security Certified Professional (OSCP)
Offensive Security Web Expert (OSWE)

JOB CATEGORY	CYBERSECURITY [CS]
JOB ROLE	CSJ07: PENETRATION TESTER

TASKS

SPECIFIC TASKS

Cybersecurity [CS]
CST02: Respond to cybersecurity incidents.
CST16: Train and raise awareness regarding security

Operations and Support [OS]
OST12: Assist clients with improving their security on their networks by performing security assessments.

GENERAL TASKS

CST01: Identify cyber threats.
CST07: Manage or perform security config reviews on network devices, databases, and operating systems.
CST08: Perform penetration testing.
CST10: Monitor network software for proper security procedures.
CST19: Identify, assess and manage cyber risk.

KNOWLEDGE	SKILLS	ABILITIES
Cybersecurity [CS] **CSK04:** Security best practices **CSK05:** Penetrating testing **CSK06:** Security vulnerabilities and exploits **CSK07:** Firewalls **Software and Application Development [SA]** **SAK02:** Secure coding **SAK05:** Coding languages **Operations and Support [OS]** **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP)	**Technical Skills** **TS03:** Diagnostic skills **TS06:** Problem solving skills **Non-Technical Skills** **NTS01:** Planning skills **NTS04:** Analytical thinking skills **NTS05:** Communication skills **NTS06:** Adaptability skills **NTS08:** Organisational skills	**Technical Abilities** **TA01:** Ability to solve technical problems **TA08:** Ability to investigate malware, intrusion attempts and vulnerabilities **Non-Technical Abilities** **NTA08:** Ability to engage and contribute **NTA10:** Ability to be proactive and efficient **NTA12:** Ability to adapt to changing environments **NTA14:** Ability to communicate effectively and efficiently

CERTIFICATIONS

Certified Information Security Manager (CISM)
CREST Certification
GIAC Penetration Tester (GPEN)
GIAC Web Application Penetration Tester (GWAPT)
Offensive Security Certified Professional (OSCP)
Offensive Security Web Expert (OSWE)

JOB CATEGORY	OPERATIONS AND SUPPORT
JOB ROLE	OSJ01: IT TECHNICIAN

TASKS

SPECIFIC TASKS

Operations and Support [OS]
OST01: Do preventative maintenance
OST02: Provide information technology support to users
OST04: Provide hardware and software support

GENERAL TASKS

OST05: Perform and maintain backups.
OST06: Install and configure hardware and software.
OST07: Keep systems up to date.
OST13: Assign network access (Access Management).
OST14: Manage internet resources.
OST15: Manage firewalls.

KNOWLEDGE	SKILLS	ABILITIES
Operations and Support [OS] **OSK02:** PC hardware and software **OSK03:** Backups **OSK05:** Active directory **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **Strategy and Governance [SG]** **SGK08:** Problem management **SGK09:** Incident management **SGK10:** Access management **Cybersecurity [CS]** **CSK03:** Anti-virus software **CSK04:** Security best practices **CSK06:** Security vulnerabilities and exploits **CSK07:** Firewalls	**Technical Skills** **TS01:** Troubleshooting skills **TS03:** Diagnostic skills **TS06:** Problem solving skills **TS04:** General programming skills **Non-Technical Skills** **NTS04:** Analytical thinking skills **NTS05:** Communication skills **NTS09:** Time management skills **NTS10:** Attention to detail skills	**Technical Abilities** **TA01:** Ability to solve technical problems **TA04:** Ability to provide technical assistance **TA05:** Ability to troubleshoot **TA06:** Ability to maintain hardware and software **Non-Technical Abilities** **NTA04:** Ability to work in teams **NTA06:** Ability to research **NTA07:** Ability to manage many priorities concurrently **NTA09:** Ability to execute instructions **NTA14:** Ability to communicate effectively and efficiently

CERTIFICATIONS

Cisco Certified Network Associate (CCNA)
Cisco Certified Network Professional (CCNP)
Microsoft Certified Solutions Expert (MSCE)
Network +
Security +

JOB CATEGORY	OPERATIONS AND SUPPORT
JOB ROLE	OSJ02: NETWORK ENGINEER

TASKS

SPECIFIC TASKS

Operations and Support [OS]
OST08: Manage networks and network devices.
OST09: Troubleshooting networks
OST10: Monitor network activity
OST11: Design and implement network solutions

GENERAL TASKS

OST01: Do preventative maintenance.
OST13: Assign network access (Access Management).
OST15: Manage firewalls.

KNOWLEDGE	SKILLS	ABILITIES
Operations and Support [OS] **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **Cybersecurity [CS]** **CSK04:** Security best practices **CSK06:** Security vulnerabilities and exploits **CSK07:** Firewalls	**Technical Skills** **TS01:** Troubleshooting skills **TS06:** Problem solving skills **Non-Technical Skills** **NTS05:** Communication skills **NTS06:** Adaptability skills **NTS07:** Fast learner skills **NTS08:** Organisational skills **NTS17:** Logical thinking skills	**Technical Abilities** **TA01:** Ability to solve technical problems **TA06:** Ability to maintain hardware and software **TA07:** Ability to analyse data **TA09:** Ability to learn new technology independently. **TA10:** Ability to create network diagrams and related documentation **Non-Technical Abilities** **NTA04:** Ability to work in teams **NTA10:** Ability to be proactive and efficient. **NTA12:** Ability to adapt to changing environments

CERTIFICATIONS

Certified Information Systems Security Professional (CIISP)
Cisco Certified Internetwork Expert (CCIE)
Cisco Certified Network Associate (CCNA)
Cisco Certified Network Professional (CCNP)
Security +

JOB CATEGORY	DATA AND ARTIFICIAL INTELLIGENCE
JOB ROLE	DAJ01: SYSTEMS ADMINISTRATOR

TASKS

SPECIFIC TASKS

Cybersecurity [CS]
CST06: Implement security solutions

Operations and Support [OS]
OST03: Manage server services
OST04: Provide hardware and software support.
OST05: Perform and maintain backups
OST06: Install and configure hardware and software
OST07: Keep systems up to date
OST08: Manage networks and network devices.
OST10: Monitor network activity
OST13: Assign network access
OST14: Manage internet resources
OST15: Manage firewalls

Strategy and Governance [SG]
SGT09: Assist in the Incident management process.

GENERAL TASKS

DAT03: Design, develop, and manage data warehousing environments.
DAT05: Deploy authentication solutions and increase the degree of automation of the solutions provided.

KNOWLEDGE	SKILLS	ABILITIES
Operations and Support [OS] **OSK01:** Operating systems **OSK02:** PC hardware and software **OSK04:** VMWare **OSK05:** Active directory **OSK09:** Routers **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **OSK13:** Network monitoring tools **Strategy and Governance [SG]** **SGK14:** Information Technology Infrastructure Library (ITIL) **Cybersecurity [CS]** **CSK07:** Firewalls	**Technical Skills** **TS01:** Troubleshooting skills **TS06:** Problem solving skills **Non-Technical Skills** **NTS04:** Analytical thinking skills **NTS05:** Communication skills **NTS08:** Organisational skills **NTS16:** Decision making skills	**Technical Abilities** **TA01:** Ability to solve technical problems **TA04:** Ability to provide technical assistance **TA05:** Ability to troubleshoot **TA06:** Ability to maintain hardware and software **TA07:** Ability to analyse data **NTA09:** Ability to execute instructions **TA10:** Ability to create network diagrams and related documentation **Non-Technical Abilities** **NTA04:** Ability to work in teams **NTA05:** Ability to maintain confidentiality. **NTA14:** Ability to communicate effectively and efficiently **NTA16:** Ability to work independently

CERTIFICATIONS

A +

Certified Ethical Hacker (CEH)
Cisco Certified Network Associate (CCNA)
Microsoft Certified Solutions Associate (MCSA)
Microsoft Certified Solutions Expert (MSCE)
Network +
Security +

<table>
<tr><td>JOB CATEGORY</td><td colspan="2">DATA AND ARTIFICIAL INTELLIGENCE</td></tr>
<tr><td>JOB ROLE</td><td colspan="2">DAJ02: DATA WAREHOUSING ENGINEER</td></tr>
<tr><td colspan="3">TASKS</td></tr>
<tr><td colspan="3">SPECIFIC TASKS</td></tr>
<tr><td colspan="3"><u>Data and Artificial Intelligence [DA]</u>
DAT03: Design, develop, and manage data warehousing environments.
DAT04: Define and continuously improve the data engineering architecture framework and modelling standards.

<u>Cybersecurity [CS]</u>
CST11: Align enterprise data to ensure that it supports information security.</td></tr>
<tr><td colspan="3">GENERAL TASKS</td></tr>
<tr><td colspan="3">DAT01: Design the architecture of cloud systems and infrastructure.
DAT02: Partner with others to deploy cloud services and automation.</td></tr>
<tr><td>KNOWLEDGE</td><td>SKILLS</td><td>ABILITIES</td></tr>
<tr><td><u>Software and Application Development [SA]</u>
SAK01: Software Development Life Cycle (SDLC)
SAK04: Structured Query Language (SQL)

<u>Data and Artificial Intelligence [DA]</u>
DAK01: Data warehousing
DAK03: Data modelling</td><td><u>Technical Skills</u>
TS01: Technical writing skills
TS06: Problem solving skills

<u>Non-Technical Skills</u>
NTS05: Communication skills
NTS06: Adaptability skills
NTS11: Conflict management skills</td><td><u>Technical Abilities</u>
TA01: Ability to solve technical problems
TA07: Ability to analyse data

<u>Non-Technical Abilities</u>
NTA04: Ability to work in teams
NTA06: Ability to research
NTA08: Ability to engage and contribute</td></tr>
<tr><td colspan="3">CERTIFICATIONS</td></tr>
<tr><td colspan="3">Microsoft Certified Solutions Expert (MSCE)
Microsoft Certified Solutions Associate (MCSA)</td></tr>
</table>

JOB CATEGORY	DATA AND ARTIFICIAL INTELLIGENCE
JOB ROLE	DAJ03: CLOUD ARCHITECT

TASKS

SPECIFIC TASKS

Data and Artificial Intelligence [DA]
DAT01: Design the architecture of cloud systems and infrastructure.
DAT02: Partner with others to deploy cloud services and automation.

GENERAL TASKS

DAT04: Define and continuously improve the data engineering architecture framework and modelling standards.

KNOWLEDGE	SKILLS	ABILITIES
Data and Artificial Intelligence [DA] **DAK05:** Cloud services **DAK06:** Automation **Software and Application Development [SA]** **SAK05:** Coding languages **Cybersecurity [CS]** **CSK04:** Security best practices **CSK07:** Firewalls **Operations and Support [OS]** **OSK01:** Operating systems **OSK05:** Active directory **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **Strategy and Governance [SG]** **SGK01:** Project management	**Technical Skills** **TS03:** Diagnostic skills **TS06:** Problem solving skills **Non-Technical Skills** **NTS05:** Communication skills **NTS10:** Attention to detail skills **NTS17:** Logical thinking skills	**Technical Abilities** **TA09:** Ability to learn new technology independently **Non-Technical Abilities** **NTA03:** Ability to work with leadership **NTA10:** Ability to be proactive and efficient. **NTA12:** Ability to adapt to changing environments

CERTIFICATIONS

Certified Information Systems Security Professional (CIISP)
Certified Information Systems Auditor (CISA)
Certified Ethical Hacker (CEH)
Certified Information Security Manager (CISM)
Security +

JOB CATEGORY	STRATEGY AND GOVERNANCE
JOB ROLE	SGJ01: INFORMATION TECHNOLOGY MANAGER

TASKS

SPECIFIC TASKS

Strategy and Governance [SG]

SGT18: Develop strategic plans, set timelines of evaluation, development, and deployment of technology resources.

SGT19: Ensure adherence to project budgets.

GENERAL TASKS

SGT01: Direct and organise IT related projects.

SGT03: Define, assess, maintain, and advise on IT Regulatory universe.

SGT04: Develop, facilitate compilation of and review IT compliance risk management plans.

SGT06: Handle all customer escalations ensuring compliance with Service Level Agreements (SLAs).

SGT08: Assist in the development and maintenance of policies, procedures, and technical standards.

SGT12: Assist in the Change management process.

SGT17: Present and compile reports.

KNOWLEDGE	SKILLS	ABILITIES
Strategy and Governance [SG] **SGK01:** Project management **Operations and Support [OS]** **OSK01:** Operating systems **OSK03:** Backups **OSK05:** Active directory **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **Cybersecurity [CS]** **CSK04:** Security best practices **CSK05:** Penetrating testing **CSK06:** Security vulnerabilities and exploits **CSK07:** Firewalls	**Technical Skills** **TS01:** Troubleshooting skills **Non-Technical Skills** **NTS02:** Leadership skills **NTS05:** Communication skills **NTS06:** Adaptability skills **NTS11:** Conflict management skills **NTS14:** Strategic thinking skills **NTS16:** Decision making skills	**Technical Abilities** **TA04:** Ability to provide technical assistance **TA05:** Ability to troubleshoot **TA07:** Ability to analyse data **Non-Technical Abilities** **NTA01:** Ability to manage human resource **NTA02:** Ability to lead teams **NTA05:** Ability to maintain confidentiality. **NTA06:** Ability to research **NTA13:** Ability to stay organised. **NTA14:** Ability to communicate effectively and efficiently

CERTIFICATIONS

Certified Ethical Hacker (CEH)
Cisco Certified Network Associate (CCNA)
Fortinet Network Security Expert (NSE)
Security +

JOB CATEGORY	STRATEGY AND GOVERNANCE
JOB ROLE	SGJ02: INFORMATION TECHNOLOGY AUDITOR

TASKS

SPECIFIC TASKS

Strategy and Governance [SG]
SGT15: Design internal audit procedures and programs
SGT16: Assist in audit engagement, planning and reporting activities.

Cybersecurity [CS]
CST19: Identify, assess and manage cyber risk.

GENERAL TASKS

SGT03: Define, assess, maintain, and advise on IT Regulatory universe.
SGT04: Develop, facilitate compilation of and review IT compliance risk management plans.

KNOWLEDGE	SKILLS	ABILITIES
Strategy and Governance (SG) **SGK05:** Control Objectives for Information and Related Technologies (COBIT) **SGK11:** Compliance **SGK13:** Information technology governance **SGK14:** Information Technology Infrastructure Library (ITIL) **SGK15:** Information technology security policies **Operations and Support (OS)** **OSK01:** Operating systems **Cybersecurity (CS)** **CSK04:** Security best practices **CSK05:** Penetrating testing **CSK06:** Security vulnerabilities and exploits	**Technical Skills** **TS02:** Technical writing skills **Non-Technical Skills** **NTS04:** Analytical thinking skills **NTS05:** Communication skills **NTS08:** Organisational skills **NTS10:** Attention to detail skills	**Technical Abilities** **TA02:** Ability to write reports **Non-Technical Abilities** **NTA01:** Ability to manage human resources **NTA04:** Ability to work in teams **NTA08:** Ability to engage and contribute **NTA09:** Ability to execute instructions **NTA12:** Ability to adapt to changing environments

CERTIFICATIONS

Certified in Risk and Information Systems Control (CRISC)
Certified in the Governance of Enterprise IT (CGEIT)
Certified Information Systems Auditor (CISA)
Certified Internal Auditor (CIA)
Security +

JOB CATEGORY	STRATEGY AND GOVERNANCE
JOB ROLE	SGJ03: COMPLIANCE SPECIALIST

TASKS

SPECIFIC TASKS

Strategy and Governance [SG]
SGT02: Maintain IT compliance/risk management frameworks.
SGT03: Define, assess, maintain, and advise on IT regulatory universe
SGT04: Develop, facilitate compilation of and review IT compliance risk management plans
SGT05: Conduct IT compliance monitoring
SGT17: Present and compile reports.

Cybersecurity [CS]
CST17: Guide teams through the design and implementation of cyber solutions.
CST19: Identify, assess and manage cyber risk.

GENERAL TASKS

SGT07: Manage and ensure compliance with internal policies and procedures.
SGT08: Assist in the development and maintenance of policies, procedures, and technical standards.

KNOWLEDGE	SKILLS	ABILITIES
Strategy and Governance [SG] **SGK03:** National Institute of Standards and Technology (NIST) **SGK04:** International Organization for Standardization (ISO) **SGK05:** Control Objectives for Information and Related Technologies (COBIT) **SGK07:** King IV **SGK10:** Access management **SGK11:** Compliance **SGK14:** Information Technology Infrastructure Library (ITIL) **Data and Artificial Intelligence [DA]** **DAK05:** Cloud services	**Technical Skills** **TS02:** Technical writing skills **Non-Technical Skills** **NTS02:** Leadership skills **NTS05:** Communication skills **NTS12:** Collaboration skills **NTS16:** Decision making skills	**Technical Abilities** **TA02:** Ability to write reports **TA07:** Ability to analyse data **Non-Technical Abilities** **NTA01:** Ability to manage human resources **NTA02:** Ability to lead teams **NTA09:** Ability to execute instructions

CERTIFICATIONS

Certified Ethical Hacker (CEH)
Certified in Risk and Information Systems Control (CRISC)
Certified in the Governance of Enterprise IT (CGEIT)
Certified Information Privacy Professional (CIPP)
Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Certified Internal Auditor (CIA)
Certified Information Systems Security Professional (CISSP)
Certified Cloud Security Professional (CCSP)
Microsoft Certified Solutions Associate (MCSA)

JOB CATEGORY	STRATEGY AND GOVERNANCE
JOB ROLE	SGJ04: PROJECT MANAGER

TASKS

SPECIFIC TASKS

Strategy and Governance [SG]

SGT20: Ensuring that project objectives, customer acceptance criteria and internal performance metrics are achieved

SGT21: Draft project proposals and cost estimates

SAT05: Lead software development life cycle

GENERAL TASKS

SGT01: Direct and organise IT related projects.

SGT17: Present and compile reports.

SGT18: Develop strategic plans, set timelines of evaluation, development, and deployment of technology resources.

SGT19: Ensure adherence to project budgets.

KNOWLEDGE	SKILLS	ABILITIES
Cybersecurity (CS) **CSK04:** Security best practices **CSK06:** Security vulnerabilities and exploits **Strategy and Governance (SG)** **SGK01:** Project management **Software and Application Development (SA)** **SAK01:** Software development life cycle	**Technical Skills** **TS05:** Administration skills **Non-Technical Skills** **NTS02:** Leadership skills **NTS03:** Presentation skills **NTS04:** Analytical thinking skills **NTS15:** Negotiation skills **NTS16:** Decision making skills **NTS17:** Logical thinking skills	**Technical Abilities** **TA07:** Ability to analyse data **Non-Technical Abilities** **NTA01:** Ability to manage human resources **NTA02:** Ability to lead teams **NTA04:** Ability to work in teams **NTA11:** Ability to work under pressure **NTA15:** Ability to prioritise

CERTIFICATIONS

A +
Certified Associate in Project Management (CAPM)
Microsoft Certified Solutions Expert (MSCE)
Network +
PRINCE2
Project Management Professional (PMP)

<table>
<tr><td>JOB CATEGORY</td><td colspan="2">STRATEGY AND GOVERNANCE</td></tr>
<tr><td>JOB ROLE</td><td colspan="2">SGJ05: QUALITY ASSURANCE ANALYST</td></tr>
<tr><td colspan="3">TASKS</td></tr>
<tr><td colspan="3">SPECIFIC TASKS</td></tr>
<tr><td colspan="3"><u>Strategy and Governance [SG]</u>
SGT12: Assist in the change management process.

<u>Software and Application Development [SA]</u>
SAT08: Create test plans with the relevant test scenarios.
SAT07: Development and monitoring of integration, create and maintain coding standards.</td></tr>
<tr><td colspan="3">GENERAL TASKS</td></tr>
<tr><td colspan="3">SGT20: Ensuring that project objectives, customer acceptance criteria and internal performance metrics are achieved.</td></tr>
<tr><td>KNOWLEDGE</td><td>SKILLS</td><td>ABILITIES</td></tr>
<tr><td><u>Software and Application Development (SA)</u>
SAK04: Structured Query Language
SAK10: Application Programming Interface management tools

<u>Cybersecurity (CS)</u>
CSK04: Security best practices
CSK06: Security vulnerabilities and exploits

<u>Strategy and Governance (SG)</u>
SGK01: Project management
SGK04: International Organization for Standardization (ISO)
SGK11: Compliance</td><td><u>Technical Skills</u>
TS01: Troubleshooting skills
TS06: Problem solving skills

<u>Non-Technical Skills</u>
NTS01: Planning skills
NTS05: Communication skills
NTS09: Time management skills</td><td><u>Technical Abilities</u>
TA01: Ability to solve technical problems

<u>Non-Technical Abilities</u>
NTA04: Ability to work in teams</td></tr>
<tr><td colspan="3">CERTIFICATIONS</td></tr>
<tr><td colspan="3">ISTQB Certifications</td></tr>
</table>

JOB CATEGORY	STRATEGY AND GOVERNANCE
JOB ROLE	SGJ06: CHIEF INFORMATION OFFICER

TASKS

SPECIFIC TASKS

Strategy and Governance [SG]
SGT01: Direct and organise IT related projects.
SGT17: Present and compile reports.

Cybersecurity [CS]
CST03: Develop and maintain security policies
CST04: Implement security policies and standards.
CST05: Design, implement and monitor controls
CST06: Implement security solutions

GENERAL TASKS

SGT03: Define, assess, maintain, and advise on IT Regulatory universe.
SGT04: Develop, facilitate compilation of and review IT compliance risk management plans.
SGT07: Manage and ensure compliance with internal policies and procedures.
SGT08: Assist in the development and maintenance of policies, procedures, and technical standards.
SGT19: Ensure adherence to project budgets.
SGT20: Ensuring that project objectives, customer acceptance criteria and internal performance metrics are achieved.

KNOWLEDGE	SKILLS	ABILITIES
Operations and Support [OS] **OSK02:** PC hardware and software **Data and Artificial Intelligence [DA]** **DAK02:** Data analysis **Strategy and Governance [SG]** **SGK01:** Project management **SGK02:** Information technology risk **SGK06:** Business operations **SGK15:** Information Technology security policies **Cybersecurity [CS]** **CSK02:** Security frameworks	**Technical Skills** **TS05:** Administration skills **Non-Technical Skills** **NTS01:** Planning skills **NTS02:** Leadership skills **NTS05:** Communication skills **NTS14:** Strategic thinking skills	**Technical Abilities** **TA01:** Ability to solve technical problems **Non-Technical Abilities** **NTA01:** Ability to manage human resources **NTA02:** Ability to lead teams **NTA07:** Ability to manage many priorities concurrently

CERTIFICATIONS

Certified Information Security Manager (CISM)
Certified Information Systems Auditor (CISA)
Certified Information Systems Security Professional (CIISP)

JOB CATEGORY	SOFTWARE AND APPLICATION DEVELOPMENT
JOB ROLE	SAJ01: SOFTWARE DEVELOPER

TASKS

SPECIFIC TASKS

Software and Application Development [SA]

SAT06: Design, develop, test and implement new features and changes to current functionality to applications as per requirements.

SAT07: Develop and monitor the integration, creation and maintenance of coding standards.

Cybersecurity [CS]

CST09: Implement security best practices.

GENERAL TASKS

SAT01: Develop secure applications.

SAT02: Develop applications to monitor networks for cyberthreats.

SAT03: Develop applications to automate tasks performed by security analysts.

SAT04: Contribute to the design, development, testing and evaluation of systems and infrastructure.

KNOWLEDGE	SKILLS	ABILITIES
Operations and Support [OS] **OSK01:** Operating systems **OSK07:** Internet Information Services (IIS) **OSK11:** Internet Protocol (IP)/Voice Over Internet Protocol (VOIP)/ Transmission Control Protocol (TCP) **Strategy and Governance [SG]** **SGK01:** Project management **SGK05:** Control Objectives for Information and Related Technologies (COBIT) **SGK14:** Information Technology Infrastructure Library (ITIL) **Cybersecurity [CS]** **CSK04:** Security best practices **CSK06:** Security vulnerabilities and exploits **CSK07:** Firewalls **Software and Application Development [SA]** **SAK04:** Structured Query Language (SQL) **SAK06:** Functions **SAK08:** Stored procedures **SAK09:** Database design	**Technical Skills** **TS01:** Troubleshooting skills **TS02:** Technical writing skills **TS04:** General programming skills **Non-Technical Skills** **NTS04:** Analytical thinking skills **NTS05:** Communication skills **NTS10:** Attention to detail skills **NTS14:** Strategic thinking skills **NTS17:** Logical thinking skills	**Technical Abilities** **TA05:** Ability to troubleshoot **TA09:** Ability to learn new technology independently. **TA11:** Ability to write secure code **Non-Technical Abilities** **NTA04:** Ability to work in teams **NTA09:** Ability to execute instructions **NTA16:** Ability to work independently

CERTIFICATIONS

Certified Information Systems Security Professional (CIISP)
Microsoft Certified Solutions Expert (MSCE)

JOB CATEGORY	SOFTWARE AND APPLICATION DEVELOPMENT
JOB ROLE	SAJ02: DEVOPS ENGINEER

TASKS

SPECIFIC TASKS

Software and Application Development [SA]
SAT04: Contribute to the design, development, testing and evaluation of systems and infrastructure

Data and Artificial Intelligence [DA]
DAT05: Deploy authentication solutions and increase the degree of automation of the solutions provided.

GENERAL TASKS

SAT01: Develop secure applications.
SAT06: Design, develop, test and implement new features and changes to current functionality to applications as per requirements.
SAT07: Develop and monitor the integration, creation and maintenance of coding standards.

KNOWLEDGE	SKILLS	ABILITIES
Cybersecurity [CS] **CSK04:** Security best practices **CSK06:** Security vulnerabilities and exploits **CSK07:** Firewalls **Software and Application Development [SA]** **SAK11:** Version control **Data and Artificial Intelligence [DA]** **DAK05:** Cloud services **DAK06:** Automation **Operations and Support [OS]** **OSK01:** Operating systems **Strategy and Governance [SG]** **SGK03:** National Institute of Standards and Technology (NIST) **SGK14:** Information Technology Infrastructure Library (ITIL)	**Technical Skills** **TS01:** Troubleshooting skills **TS04:** General programming skills **TS05:** Administration skills **Non-Technical Skills** **NTS02:** Leadership skills **NTS05:** Communication skills **NTS07:** Fast learner skills **NTS12:** Collaboration skills **NTS16:** Decision making skills	**Technical Abilities** **TA01:** Ability to solve technical problems **TA04:** Ability to provide technical assistance **TA05:** Ability to troubleshoot **TA11:** Ability to write secure code **Non-Technical Abilities** **NTA02:** Ability to lead teams **NTA04:** Ability to work in teams **NTA07:** Ability to manage many priorities concurrently **NTA11:** Ability to work under pressure

CERTIFICATIONS

Certified Ethical Hacker (CEH)
Certified Information Systems Security Professional (CIISP)
Microsoft Certified Solutions Expert (MSCE)
Offensive Security Certified Professional (OSCP)

Appendix C: Publication

A Thematic Content Analysis of the Cybersecurity Skills Demand in South Africa

Madri Kruger [0000-0003-3400-8564],

Lynn Futcher [0000-0003-0406-8718], and

Kerry-Lynn Thomson [0000-0002-6456-9701]

Nelson Mandela University, Port Elizabeth, South Africa
{madri.kruger, lynn.futcher, kerry-lynn.thomson}@mandela.ac.za

Abstract. The cybersecurity skills demand is a growing concern both globally and in South Africa, creating what is known as the cybersecurity skills gap. This means that there is a shortage of Information Technology (IT) and cybersecurity professionals that have the required knowledge, skills and abilities, to effectively fill this gap. This study aims to provide a better understanding of the cybersecurity skills demand in South Africa having analysed job postings in South Africa over a 4-month period from 1st October 2020 to 31st January 2021. This was done by conducting a thematic content analysis of the 280 job postings identified during this period. Results indicate a condensed set of knowledge, skills and abilities (KSAs) categorised according to five main job categories, namely: Cybersecurity, Operations and Support, Data and Artificial Intelligence, Strategy and Governance, and Software and Application Development. These results can assist universities, training institutions and organisations to address the cybersecurity skills gap in South Africa.

Keywords: Cybersecurity – Skills Demand - Thematic Content Analysis

1 Introduction

The global Cyber Exposure Index ranks South Africa sixth on the list of most-targeted countries for cyberattacks [1]. According to the Kaspersky laboratory, malware attacks in South Africa increased by 22% in the first quarter of 2019 compared to the same time in 2018. This equates to about 13842 attempted cyberattacks daily, or just over 9 attacks per second [2]. Due to this growth in cyberattacks in South Africa, cybersecurity needs to grow in response in order to mitigate such attacks.

Cybersecurity is seen as the practice of defending systems, networks and programs from cyberattacks [3]. There are many threats to cybersecurity, such as phishing, malware, trojans, ransomware, worms and Denial of Service attacks (DoS), among others [4]. In addition, the personal information stored on devices like computers and mobile phones can be used for identity theft, financial gain, blackmail and for gaining access to highly confidential information.

Human error is the main cause of 95% of cybersecurity breaches [5]. Through advances in the technological tools used in information and network security, a large majority of threat detection and monitoring has been automated, However, some tasks cannot be automated and require human intervention to successfully secure information and networks [6].

In a global survey by Oltsik, 82% of respondents reported a shortage of cybersecurity skills, and 61% of companies believed that cybersecurity-related job applicants are not qualified for the job [7]. In a follow-up survey in 2020, 45% of the respondents believed that the skills shortage, as well as its impact, has gotten worse over the last few years [8].

The aim of this paper is to provide a better understanding of the cybersecurity skills demand in South Africa, by analysing job postings in South Africa over a 4-month period from 1st October 2020 to 31st January 2021. This was done by conducting a thematic content analysis of 280 relevant job postings identified during this period.

This paper is structured as follows. Section 2 provides related literature regarding the cybersecurity skills gap both globally and in South Africa. In addition, it highlights several skills frameworks that provide insight into various cybersecurity work roles and their related knowledge, skills and abilities (KSAs). Section 3 discusses the thematic content analysis conducted as a key research method of this study, and Section 4 presents the results and findings from the thematic content analysis. Section 5 provides a discussion before concluding the paper in Section 6.

2 Related Literature

In 2019, ISACA conducted a survey to better understand the current state of cybersecurity globally. 58% of their respondents indicated that they have unfilled cybersecurity positions within their organisations. The study also indicated an annual 6% increase in the waiting time of positions being filled, sometimes taking as long as six months to fill such positions. Technically skilled cybersecurity professionals were considered the hardest to find, further contributing to the struggle of filling open cybersecurity positions [9].

According to Burning Glass Technologies, job postings for cybersecurity openings have grown three times as fast as openings for IT jobs overall [10]. Although some IT jobs can be filled easily without the need for extensive training, most cybersecurity jobs require specific KSAs, some of which can only be gained through specialised training.

There are many accredited certifications that a cybersecurity professional can attain, including: Certified Information Systems Security Professional (CISSP), CompTIA Security + and Certified Ethical Hacker (CEH), to name just a few. Each certification targets a different need within industry and most of them are globally recognised. When taking into consideration that in order to apply for CISSP certification, applicants require at least 5 years of relevant experience, one can understand why there is such a huge need for skilled and trained cybersecurity employees [9]. Due to the high qualification and experience requirements for most cybersecurity-related jobs, the cybersecurity skills gap will not be easily addressed in the near future.

South Africa has also been affected by the worldwide shortage of cybersecurity skills. One of South Africa's largest banks, Absa, has collaborated with the Maharishi Institute (MI) to set up the Absa Cybersecurity Academy in an attempt to address its skills shortage [11]. Despite these kinds of targeted efforts, there is a lack of cost-effective local cybersecurity training offered to South Africans. Most cybersecurity courses offered by international organisations are often unaffordable for most South Africans due to them being billed in US dollars [12]. This has resulted in several local universities, colleges and training institutions providing various forms of cybersecurity training and education. However, most of these would have been based on insight gained from international cybersecurity skills frameworks. For example, the National Initiative for Cybersecurity Education (NICE) framework developed by the National Institute of Standards and Technology (NIST), a United States based institute.

The NICE framework attempts to create a better understanding of what cybersecurity jobs entail and what knowledge, skills, and abilities (KSAs) are needed to complete certain tasks based on job roles. This is a useful tool for organisations seeking guidance on their cybersecurity workforce development. However, while the NICE framework is good at defining job descriptions, there are over 1600 KSA's and more than 50 job roles, making it rather unmanageable. In addition, some of their KSAs are vague and not well defined [13].

A further framework of particular interest to this study is the Skills Framework for Infocomm Technology (SFw for ICT). This framework aims to provide information on career paths, existing and emerging skills, as well as occupations and job roles and their respective knowledge, skills, abilities and tasks (KSATs). It is therefore useful for employers and educational facilities, as well as individuals who are job seeking or planning their careers. Although this framework does not focus specifically on cybersecurity, it does include cybersecurity as one of the seven career pathway tracks [14].

A study by Parker and Brown provides some insight into various cybersecurity jobs advertised in South Africa, together with the typical skills required by such cybersecurity professionals. However, Parker and Brown consider their work as an initial exploratory study providing a basis for future studies [6]. Further, it can be argued that cybersecurity skills are required by IT professionals at all levels of the profession since they are all personally responsible for the information they are entrusted with.

3 Thematic Content Analysis Using ATLAS.ti

Before starting the formal data collection process, it was decided to conduct a pilot study to gain a better understanding of the data to be collected for this study. In September 2020, the pilot study began. Data was collected weekly on three job posting websites, namely: LinkedIn, Careers24 and Career Junction. During the pilot study it was found that the adverts on LinkedIn provided greater depth of information compared to other job posting websites, and was therefore chosen for the rest of the study.

The official data collection for this study took place over a four-month period from 1st October 2020 to 31st January 2021. The search results were filtered by relevant IT and cybersecurity-related jobs each week and set to South African based job postings only. A total of 280 job postings were collected. These job postings were then analysed by conducting a thematic content analysis using ATLAS.ti, a popular software analysis tool for analysing qualitative data.

A three-phased approach was used for the thematic content analysis as proposed by [15]. Using ATLAS.ti in combination with this three-phased approach is considered a promising strategy for conducting a thematic content analysis [15]. Figure 1 presents the three phases of the thematic content analysis and the associated steps taken in ATLAS.ti.

Phases of thematic content analysis	Steps in ATLAS.ti
First phase: Pre-analysis.	Creating the project. Adding documents. Grouping documents into document groups. Writing first memos on the overall project aim including research questions.
Second phase: Material exploration.	Reading the data, selecting data segments and creating quotations. Creating and applying codes. Writing memos and comments. Grouping codes and memos
Third phase: Interpretation.	Exploring the coded data using various analysis tools. Linking quotations, codes, and memos on the conceptual level. Continuing memo writing. Generating network views. Extracting reports.

Figure 1: Three-Phased Thematic Content Analysis [15]

These phases are discussed in more detail in the following sub-sections.

3.1 First phase: Pre-analysis

Firstly, a new project was created in ATLAS.ti. All the data collected for the four months from 1st October 2020 to 31st January 2021 were added to this project by importing the MS Word documents containing the job postings for each month into the project. Once imported, these documents were grouped according to month, resulting in four groups named “OCT”, “NOV”,” DEC” and “JAN”. Each monthly group contained four MS Word documents, one for each week of the month.

3.2 Second Phase: Material Exploration

To start the second phase of the thematic content analysis, a document group was opened, and a document was chosen. This started with the document group called “OCT”, and the document for the first week of October was selected. This document was then read, and important data segments were selected, and quotations created for these segments. Each of the quotations were assigned a code. Thereafter the next document in the group was selected which in this case was called “Week 2 Oct” after it had been completed the same process was followed for the documents “Week 3 Oct” and “Week 4 Oct”. Once document group “OCT” was completed, the next group was selected, that being document group “NOV”, and the documents for each week in document group “NOV” completed. The same process was followed for document groups “DEC” and “JAN”, as well as their respective documents. There was a total of 640 codes and 3580 quotations after completing the coding for each of the document groups. Each quotation was linked to only one data segment. Each quotation was assigned a single code, and a code

belonged to only one code group. For example, the quotation “Ideal candidate must have a Security + certification” would be assigned the code “Security +”.

Once all job postings had been coded, these codes needed to be organised. To do this, a similar process to that used for the document groups was followed, called code groups. Each of the different types of codes were grouped according to their type. For example, all certifications were grouped into a group called Certifications. The same was done for all the other types of codes. A total of six code groups were identified, namely: Certifications, Industries, Job Levels, Job Roles, Job Types and Regions.

Once all codes had been grouped, each group was inspected individually to find possible duplications. For example, in the case of the Certifications group, it contained multiple occurrences of the same certifications due to them often being referred to in various ways by different employers. One such case was the certification Security+. It was referred to as S+ in some cases and as Security+ in others. In this case the two codes were merged into a single code, named Security+.

After the codes had been grouped and checked for duplicates, there was a total of 552 codes in the project, thus a reduction of 88 from the original 640 codes.

3.3 Third Phase: Interpretation

In the third phase, the primary focus was on the code group called “Job Roles” since these could be further analysed according to their related knowledge, skills and abilities (KSAs). A total of 223 job roles were identified in the “Job Roles” code group on starting this third phase of the thematic content analysis. However, on further analysis, some of these job roles were found to be similar, but were named differently due to employers using different naming conventions. For example, a job role named “Software Developer” and a job role named “Application Developer” were merged into a single job role named “Software Developer” since they were considered to be similar job roles.

Each job role was individually assessed according to their associated knowledge, skills and abilities (KSAs) and their required certifications were noted in a comment associated with the job role. To further determine whether job roles were the same, their KSAs were compared. If they had the same KSAs, the job roles were deemed similar and were merged into one. After the completion of this phase, the initial 223 job roles were substantially reduced to a total of 20 job roles, each having defined KSAs, as well as various certifications associated with them.

The completed thematic content analysis process resulted in 353 codes spread over five key job categories, down from the initial number of 640 codes at the beginning of the Material Exploration Phase.

4 General Results and Findings

Of the 280 postings analysed, approximately 90% were full-time positions. From the thematic content analysis conducted, the following key categories were deemed most relevant to this study, and were therefore defined and coded for further analysis. These key categories were derived from the code groups described in Section 3.2 and included:

- the industry (where five main industries were identified)
- the job location (this was indicated by province)
- the job level (ranging from entry-level to executive-level)
- the minimum qualifications and certifications

These key categories are further analysed in their respective sub-sections below, while job roles and their related KSAs are discussed in Section 5.

4.1 Identified Industries

From the thematic content analysis conducted, it was found that most of the job postings indicated the specific industry of the job advertised. In total, there were 43 industries identified from the 280 job postings analysed. Of the identified industries Information Technology and Services was mentioned 140 times (25%), Financial Services was mentioned 122 times (21.7%) and Computer Software mentioned 84 times (15%).

4.2 Job Locations

South Africa has a total of nine provinces, eight of which had job listings during the four-month data collection period from 1st October 2020 to 31st January 2021. Gauteng accounted for most of the job postings (178 postings, 63.6%), followed by the Western Cape (67 postings, 23.9%). These two provinces, accounted for 87.5% of the total job postings.

4.3 Job levels

Most job postings collected over the four-month period had a job level assigned to it. Each job posting was therefore classified according to whether it was entry-level, mid-level, senior level or executive-level. Those that did not specify the job level were classified under "Not Specified". Entry-level jobs made up the majority of the job postings (101 postings, 36.1%), followed by mid-level (87 postings, 31.1%) and senior level (65 postings, 23.2%). Executive-level only made up 3.5% of the total job postings, while 6.1% did not specify a job level.

4.4 Qualifications and Certifications

The minimum required qualifications and most common certifications listed in the job postings were analysed. Of the 280 job postings analysed, 231 job postings (82.5%) listed a specific requirement in terms of formal tertiary education. This implies a strong emphasis on meeting specific academic requirements to enter the IT industry. More than half of the job postings (65.8%, 152 job postings) specified that they require a degree in either Computer Science, Information Systems or Information Technology, as a minimum qualification. This indicates that there is a demand for academic qualifications needed for most of the job postings and that in most cases a diploma would not suffice. A diploma was specified as a requirement for 69 job postings (29.9%), with 10 job postings (4.3%) requiring either a master's degree or some form of relevant postgraduate qualification.

In terms of certifications, Certified Information Systems Security Professional (CISSP) was the most listed (55 times in the 280 job postings). This was followed by Information Technology Infrastructure Library (ITIL) with 46 listings, and two of the certifications provided by COMPTIA, namely, Network+ with 45 listings and A+ with 42 listings.

The following section discusses the identified job roles and their related KSAs.

5 Job Roles Results and Findings

The job roles and knowledge areas identified during the thematic content analysis were mapped against the following five job categories, namely:

- Cybersecurity [CS]
- Operations and Support [OS]
- Data and Artificial Intelligence [DA]
- Strategy and Governance [SG]
- Software and Application Development [SA]

Furthermore, the skills and abilities identified during the thematic content analysis were grouped according to whether they were technical or non-technical in nature.

5.1 Identified Job Roles, Knowledge, Skills and Abilities

Table 1 presents the 20 job roles categorised according to the five job categories listed above. Cybersecurity had seven related job roles (CSJ01 to CSJ07), followed by Strategy and Governance with six (SGJ01 to SGJ06) and Data and Artificial Intelligence with three (DAJ01 to DAJ03). Operations and Support (OSJ01 and OSJ02) and Software and Application Development (SAJ01 and SAJ02) each had two related job roles identified.

Table 1: *Job Roles Identified per Job Category*

Cybersecurity [CS]		**Strategy and Governance [SG]**	
Code	**Description**	**Code**	**Description**
CSJ01	Cybersecurity Specialist	SGJ01	Information Technology Manager
CSJ02	Digital Forensics Analyst	SGJ02	Information Technology Auditor

CSJ03	Security Engineer	SGJ03	Compliance Specialist
CSJ04	Data Privacy and Protection Specialist	SGJ04	Project Manager
CSJ05	Cybersecurity Manager	SGJ05	Quality Assurance Analyst
CSJ06	Application Security Specialist	SGJ06	Chief Information Officer
CSJ07	Penetration Tester	**Data and Artificial Intelligence [DA]**	
Operations and Support [OS]		**Code**	**Description**
Code	**Description**	DAJ01	Systems Administrator
OSJ01	Desktop Technician	DAJ02	Data Warehousing Engineer
OSJ02	Network Engineer	DAJ03	Cloud Architect
Software and Application Development [SA]			
Code	**Description**		
SAJ01	Software Developer		
SAJ02	DevOps Engineer		

Table 2 presents the 54 knowledge areas identified and categorised according to their relevant job category. The most knowledge areas fall within the Strategy and Governance job category (SGK01 to SGK15), followed by Operations and Support (OSK01 to OSK13).

***Table 2**: Knowledge Areas Identified per Job Category*

Cybersecurity [CS]		**Strategy and Governance [SG]**		**Software and Application Development [SA]**	
Code	**Description**	**Code**	**Description**	**Code**	**Description**
CSK01	Security Proxies	SGK01	Project Management	SAK01	SDLC
CSK02	Security Frameworks	SGK02	IT Risk	SAK02	Secure Coding
CSK03	Anti-Virus Software	SGK03	NIST	SAK03	Application Security
CSK04	Security Best Practices	SGK04	ISO	SAK04	SQL
CSK05	Penetrating Testing	SGK05	COBIT	SAK05	Coding Languages
CSK06	Security Vulnerabilities and Exploits	SGK06	Business Operations	SAK06	Functions
CSK07	Firewalls	SGK07	King IV	SAK07	Databases
CSK08	SSL	SGK08	Problem Management	SAK08	Stored Procedures
CSK09	IPS/IDS	SGK09	Incident Management	SAK09	Database Design
Operations and Support [OS]		SGK10	Access Management	SAK10	API Management Tools
Code	**Description**	SGK11	Compliance	SAK11	Version Control
OSK01	Operating Systems	SGK12	Change Management		
OSK02	PC Hardware and Software	SGK13	IT Governance		
OSK03	Backups	SGK14	ITIL		
OSK04	VMWare	SGK15	IT Security Policies		
OSK05	Active Directory	**Data and Artificial Intelligence [DA]**			
OSK06	VPN	**Code**	**Description**		
OSK07	IIS	DAK01	Data Warehousing		
OSK08	OWASP	DAK02	Data Analysis		
OSK09	Routers	DAK03	Data Modelling		
OSK10	Switches	DAK04	Machine Learning		
OSK11	IP/VOIP/TCP	DAK05	Cloud Services		
OSK12	Network Security	DAK06	Automation		
OSK13	Network Monitoring Tools				

Table 3 presents the 23 skills identified and categorised according to their technical or non-technical nature. 17 skills were identified as non-technical (NTS01 to NTS17) and six were considered to be technical (TS01 to TS06).

Table 3: *Non-Technical and Technical Skills Identified*

Non-Technical Skills		**Technical Skills**	
Code	**Description**	**Code**	**Description**
NTS01	Planning Skills	TS01	Troubleshooting Skills
NTS02	Leadership Skills	TS02	Technical writing Skills
NTS03	Presentation Skills	TS03	Diagnostic Skills
NTS04	Analytical thinking Skills	TS04	General programming Skills
NTS05	Communication Skills	TS05	Administration Skills
NTS06	Adaptability Skills	TS06	Problem solving Skills
NTS07	Fast learner Skills		
NTS08	Organisational Skills		
NTS09	Time management Skills		
NTS10	Attention to detail Skills		
NTS11	Conflict management Skills		
NTS12	Collaboration Skills		
NTS13	Customer service Skills		
NTS14	Strategic thinking Skills		
NTS15	Negotiation Skills		
NTS16	Decision making Skills		
NTS17	Logical thinking Skills		

Table 4 presents the 16 non-technical abilities (NTA01 to NTA16) and 11 technical abilities (TA01 to TA11) that were identified.

Table 4: *Non-Technical and Technical Abilities Identified*

Non-Technical Abilities		**Technical Abilities**	
Code	**Description**	**Code**	**Description**
NTA01	Ability to manage human resources	TA01	Ability to solve technical problems
NTA02	Ability to lead teams	TA02	Ability to write reports
NTA03	Ability to work with leadership	TA03	Ability to obtain forensic evidence
NTA04	Ability to work in teams	TA04	Ability to provide technical assistance
NTA05	Ability to maintain confidentiality	TA05	Ability to troubleshoot
NTA06	Ability to research	TA06	Ability to maintain hardware and software
NTA07	Ability to manage many priorities concurrently	TA07	Ability to analyse data
NTA08	Ability to engage and contribute	TA08	Ability to investigate malware, intrusion attempts and vulnerabilities
NTA09	Ability to execute instructions	TA09	Ability to learn new technology independently
NTA10	Ability to be proactive and efficient	TA10	Ability to create network diagrams and related documentation
NTA11	Ability to work under pressure	TA11	Ability to write secure code
NTA12	Ability to adapt to changing environments		
NTA13	Ability to stay organised		
NTA14	Ability to communicate effectively and efficiently		
NTA15	Ability to prioritise		
NTA16	Ability to work independently		

The skills depicted in Table 3 and the abilities shown in Table 4 were further analysed and mapped against the five main job categories, as discussed in the next sub-section.

5.2 Mapping of Identified Skills and Abilities to Job Categories

Table 5 highlights the four most relevant non-technical skills, namely: NTS04 (Analytical thinking skills), NTS05 (Communication skills), NTS10 (Attention to detail skills), as well as NTS17 (Logical thinking skills). NTS04,

NTS05, NTS10 and NTS17 are required by all job categories. Further, both Cybersecurity [CS] and Strategy and Governance [SG] require 15 of the 17 identified non-technical skills.

Table 5: Non-Technical Skills Mapped According to Job Categories

	Non- Technical Skills																	
Job Category	NTS 01	NTS 02	NTS 03	NTS 04	NTS 05	NTS 06	NTS 07	NTS 08	NTS 09	NTS 10	NTS 11	NTS 12	NTS 13	NTS 14	NTS 15	NTS 16	NTS 17	TOTAL
CS																		15
OS																		8
DA																		8
SG																		15
SA																		9
TOTAL	2	3	2	5	5	4	3	4	3	5	2	3	1	2	2	4	5	

Notable technical skills shown in Table 6 are TS01 (Troubleshooting skills) and TS06 (Problem solving skills). TS01 is present in all job categories identified and TS06 had been identified in all but one category, Software and Application development [SA]. Cybersecurity [CS] has been shown to require all but one of the technical skills identified.

Table 6: Technical Skills Mapped According to Job

	Technical Skills						
Job	TS01	TS02	TS03	TS04	TS05	TS06	TOTAL
CS							5
OS							4
DA							4
SG							3
SA							4
TOTAL	5	3	3	3	2	4	

It can be seen in Table 7 that TA01 (Ability to solve technical problems) and TA05 (Ability to troubleshoot) have been identified as required for all the identified job categories. Cybersecurity [CS], Operations and Support [OS] as well as Data and Artificial Intelligence [DA] mapped against 7 of the 11 technical abilities.

Table 7: Technical Abilities Mapped According to Job Categories

	Technical Abilities											
Job	TA01	TA02	TA03	TA04	TA05	TA06	TA07	TA08	TA09	TA10	TA11	TOTAL
CS												7
OS												7
DA												7
SG												5
SA												5
TOTAL	5	2	1	4	5	2	4	1	3	2	2	

As seen in Table 8, both NTA04 (Ability to work in teams) and NTA09 (Ability to execute instructions) are required by all identified job categories. Further, Cybersecurity [CS] and Strategy and Governance [SG] both required 13 of the 17 non-technical abilities identified.

Table 8: Non-Technical Abilities Mapped According to Job Categories

	Non-Technical Abilities																
Job Category	NTA 01	NTA 02	NTA 03	NTA 04	NTA 05	NTA 06	NTA 07	NTA 08	NTA 09	NTA 10	NTA 11	NTA 12	NTA 13	NTA 14	NTA 15	NTA 16	TOTAL
CS																	13
OS																	7
DA																	10
SG																	13
SA																	6
TOTAL	1	3	2	5	3	3	4	3	5	3	3	4	2	4	1	3	

The mappings of the various skills and abilities to the five job categories identified by this study provides valuable detail for companies offering positions relating to these job categories and related job roles.

6 Discussion and Implications

From this study it is evident that IT professionals with cybersecurity KSAs are required in various industries in South Africa. Many job postings specified the job as an entry-level position, despite there being a need for security knowledge, and in some cases, certifications related to cybersecurity for these entry-level positions. CISSP was the most mentioned certification, yet it requires a minimum of 5 years cybersecurity experience to qualify for the certification. In 65.8% of the job postings, the employers expect the ideal candidate to have a degree in either Computer Science, Information Systems or Information Technology. In addition, cybersecurity-related certifications were considered an advantage, if not a requirement, for many of the 280 job postings analysed. It was interesting to note that there were some cases where an entry-level job required a CISSP certification, as well as a relevant degree, further indicating the high level of experience and academic requirements for IT professionals with cybersecurity KSAs. Skills and abilities relating to the Cybersecurity [CS] job category is by far the most in demand based on the job postings analysed.

Several trends were identified from this study. Table 2 presents the knowledge areas found in the 280 job postings analysed. However, many of the knowledge areas could be considered as technical skills rather than knowledge areas. For example, Penetration Testing (CSK05) and Secure Coding (SAK02) are often considered to be technical skills. However, employers seem to focus more on knowledge requirements and non-technical skills, with the technical skills mentioned being less specific and more generalised, for example Problem-Solving skills (TS06). This is also evident in Table 3, when comparing the number of technical (6) and non-technical (17) skills. It is interesting to note the emphasis on non-technical skills and abilities especially in the Cybersecurity [CS] and Strategy and Governance [SG] job categories.

Based on this study one can more clearly determine what is required in terms of KSAs when employing IT professionals in the five identified job categories. This information could be used towards a cybersecurity skills framework for South Africa, which may contribute to improving the South African cybersecurity posture.
The KSAs identified in this study closely align with the Skills Framework for Infocomm Technology (SFw for ICT), sharing many knowledge areas, skills and abilities. Due to this study's alignment with (SFw for ICT), it could provide a good baseline for a cybersecurity skills framework for South Africa. This could be used to better inform employers and future employees, as well as to assist in the further development of cybersecurity curricula in the education sector.

7 Conclusion

Despite the limitation of only analysing job postings over a four-month period from 1st October 2020 to 31st January 2021, this study contributed further understanding of the cybersecurity skills demand in South Africa. In addition, it demonstrated that ATLAS.ti is a suitable tool to use for analysing such datasets using the three-phased approach as proposed by [15].

Most countries are developing their own workforce and skills frameworks for IT and cybersecurity professionals. Australia, Canada, the United Kingdom and Singapore are among those who have developed, or are in the process of developing, their own frameworks. South Africa has a need for a similar framework that identifies cybersecurity knowledge, skills and abilities for different IT and cybersecurity job roles in the South African context. Future work will therefore use the results of this study to propose a cybersecurity skills framework for the South African context.

References

1. CEI. (2020). *Country statistics – Cyber Exposure Index*. https://cyberexposureindex.com/country-statistics/
2. Smith, C. (2019). *Major spike in SA cyber attacks, over 10 000 attempts a day*. News24. https://www.fin24.com/Companies/ICT/major-spike-in-sa-cyber-attacks-over-10-000-attempts-a-day-security-company-20190429
3. Cisco (2017). *What Is Cybersecurity? - Cisco*. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html
4. Tunggal, A. T. (2020). *What is a Cyber Threat?* Upguard. https://www.upguard.com/blog/cyber-threat
5. Ahola, M. (2019). *The Role of Human Error in Successful Cyber Security Breaches*. Usecure. https://blog.getusecure.com/post/the-role-of-human-error-in-successful-cyber-security-breaches
6. Parker, A., & Brown, I. (2018). Skills Requirements for Cyber Security Professionals: A Content Analysis

of Job Descriptions in South Africa. *International Information Security Conference ISSA 2018: Information Security*, Pages 176-192. https://link.springer.com/chapter/10.1007/978-3-030-11407-7_13

7. Oltsik, J. (2017). *2017 ISSA ESG Survey Results - Information Systems Security Association*. https://www.members.issa.org/page/2017_issaesg_surv
8. Oltsik, J. (2020). *ESG Research Report: The Life and Times of Cybersecurity Professionals 2020*. *July*. https://www.esg-global.com/research/esg-research-report-the-life-and-times-of-cybersecurity-professionals-2020
9. ISACA. (2019). *ISACAs State of Cybersecurity 2019 Survey Retaining Qualified Cybersecurity Professionals*. https://www.isaca.org/why-isaca/about-us/newsroom/press-releases/2019/isacas-state-of-cybersecurity-2019-survey-retaining-qualified-cybersecurity-professionals
10. Burning Glass Technologies. (2019). *The State of Cybersecurity Hiring*. *June*, 1–26.
11. Bucchianeri, S. (2019). *The cybersecurity skills gap offers SA an opportunity to lead in the 4IR*. https://www.iol.co.za/business-report/opinion/the-cybersecurity-skills-gap-offers-sa-an-opportunity-to-lead-in-the-4ir-31762949
12. Doyle, K. (2016). Wanted: Cyber security expertise | ITWeb. *ITWeb's Corporate IT Training Guide*, *4th Issue*, Page 27. http://books.itweb.co.za/tg/
13. NIST. (2020). NICE Cybersecurity Workforce Framework Use Cases and Success Stories. English Journal, 1–21 . https://www.nist.gov/news-events/events/2020/03/nice-webinar-nice-cybersecurity-workforce-framework-use-cases-and-success
14. IMDA(2017) Skills Framework For ICT. https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html
15. Soratto, J., Pires, D. E. P. de, & Friese, S. (2020). Thematic content analysis using ATLAS.ti software: Potentialities for researchs in health. *Revista Brasileira de Enfermagem*, *73*(3), e20190250. https://doi.org/10.1590/0034-7167-2019-0250

Appendix D: Turnitin Report

ORIGINALITY REPORT

18%	15%	6%	8%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	technationcanada.ca Internet Source	2%
2	www.researchgate.net Internet Source	1%
3	nvlpubs.nist.gov Internet Source	1%
4	examples.complianceforge.com Internet Source	<1%
5	core.ac.uk Internet Source	<1%
6	Submitted to University of Sheffield Student Paper	<1%
7	Submitted to Kennesaw State University Student Paper	<1%
8	hdl.handle.net Internet Source	<1%
9	Submitted to University of Cape Town Student Paper	<1%

Appendix E: Proof Reader Certification

Ricky Woods Academic Editing Services

Editing Certificate

Ricky Woods Academic Editing Services **Proofreading certificate**
Cell: +27 (0)83 3126310
Email: rickywoods604@gmail.com

To Whom it May Concern

Nelson Mandela University

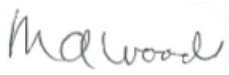
Editing of Dissertation

I, Marietjie Alfreda Woods, hereby certify that I have completed the editing and correction of the dissertation: **Towards a Cybersecurity Skills Framework for South Africa** by **Madri Kruger,** submitted in fulfilment of the requirements of the degree **Master of Information Technology** in the **Faculty of Engineering, the Built Environment and Technology** at the **Nelson Mandela University.** I believe that the dissertation meets with the grammatical and linguistic requirements for a document of this nature.

Name of Editor: Marietjie Alfreda (Ricky) Woods

Qualifications: BA (Hons) (Wits); Copy-editing and Proofreading (UCT); Editing Principles and Practice (UP); Accredited Text Editor (English) (PEG)

9 November 2022



Professional EDITORS Guild

Ricky Woods
Accredited Text Editor (English)

Membership number: WOO003
Membership year: March 2022 to February 2023

083 312 6310
rickywoods604@gmail.com
www.rickywoods604.wixsite.com/website

www.editors.org.za