AN INFORMATION SECURITY FRAMEWORK FOR REDUCING INFORMATION SECURITY COSTS AND SUSTAINING INFORMATION SECURITY CULTURE

by

Sunthoshan G. Govender

Supervisors:

Prof. M. Loock

Prof. E. Kritzinger

Prof. S Singh

Submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy (Information Systems)

College of Science, Engineering and Technology
University of South Africa
2023

Keywords

Information Security, Information Security Architecture, Information Security Assessment, Information Security Culture, Information Security Cost, Information Security Framework, Information Security Risk, Organisational Behaviour, Organisational Culture, Design Science Research

Abstract

As the velocity and volume of data breaches increases, information security is a cornerstone to the sustainability of business functionality in organisations. The focus of traditional information security has been to address concerns through the implementation of technology. Nonetheless, the profound catalyst behind data breaches often stems from the influence of individuals on information security, necessitating human involvement to bolster the intricate array of information security technologies. Elevating the information security culture among staff members should stand as a pivotal impetus in tandem with the enhancement of information security technology. This leads to a greater need to focus on sociological solutions with lesser emphasis on technological solutions. This research aims to concentrate on mitigating the risks associated with information security breaches through the enhancement of information security culture, while decreasing the overall expenses tied to managing information security within organisations. The study was conducted using Design Science Research Methodology (DSRM), wherein artefacts, including three models, a framework and a supporting evaluation tool were developed. Through the DSRM process, these artefacts were evaluated, tested and iteratively improved. The results obtained from the assessments of the framework and tool demonstrated their efficacy in enabling organisations to derive value by assessing their security posture, prioritising cost-reduction endeavours, and formulating strategies to enhance information security culture. The practical significance of this research lies in the fact that the developed framework and tool offer a streamlined and comprehensive approach to appraising an organisation's information security status, particularly emphasising non-technical aspects for improvement. What sets these artefacts apart is their unique integration of elements that emphasise the human impact on information security, aligning with both cost-reduction goals and the enhancement of security assessment within an organisation. Through testing, second iterations of the framework and tool were designed along with a web-based application for using the framework. Information was also gathered to be able to determine a roadmap to further improve the framework and tool over time.

Table of Contents

List of Figures

List of Tables

Achievements and General Statement

The following research was translated into five published peer reviewed articles. The publication dates and journals are noted in the publications table on pg. xxi. The researcher presented on these articles at four conferences. These publications were written systematically as the researcher progressed through the development of this thesis. As such, Turnitin has detected several similarities between the articles published and this thesis document. The similarities are predominantly in the keywords, theoretical concepts, models, framework and analysis outputs.

The thesis document was reviewed and edited by a certified editor. The certification of editing is attached as Appendix E.

List of Abbreviations

AD	Active Directory
ADM	Architecture Development Methodology
AHP	Analytical Hierarchical Process
ARCS	Assessment, Reduction of Cost and Sustainability of Culture
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
BCM	Business Continuity Management
BIOSS	Board Input on Security Spend
CCP	Common and Couple Processes
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISM	Certified Information Security Manager
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information Technology
CPO	Chief Privacy Officer
CSI	Cyber Security Insurance
CSVP	Common Security Values and Principles
DLP	Data Loss/Leakage Prevention
DSR	Design Science Research
EIST	Employee Information Security Training
ESA	Enterprise Security Architecture
FEAF	Federal Enterprise Architecture Framework
FMCG	Fast Moving Consumer Goods
GDPR	General Data Protection Regulation
GSOC	Global Security Operation Centre
HACISO	Having a CISO
HACPO	Having a CPO
HIPAA	Health Insurance Portability and Accountability Act
HOD	Head Of Department
IBM	International Business Machines
ICIS	Information Security Input Costs

ICT	Information Communications Technology
ID	Identity Document
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute for Electrical and Electronics Engineers
IFIP	International Federation for Information Processing
IPS	Intrusion Prevention System
IRT	Incident Response Team
IS	Information Security
ISA	Information Security Architecture
ISF	Information Security Forum
ISIC	Information Security Input Costs
ISMS	Information Security Management System
ISO	International Organization for Standardization
IST	Information Systems and Technology
IT	Information Technology
NPV	Net Present Value
OEM	Original Equipment Manufacturer
OWASP	Open Web Application Security Project
PCI DSS	Payment Card Industry Data Security Standard
POPIA	Protection of Personal information Act
PREC	Peer Recognition
PRR	Positive Reinforcement and Reward
ROA	Return on Attack
ROI	Return on Investment
RSKASSESS	Risk Assessment
SABSA	Sherwood Applied Business Security Architecture
SANS	Escal Institute of Advanced Technologies
SAS	Security Analytics Services
SECARCH	Security Architecture
SECASSESS	Security Assessment
SIEM	Security Incident and Event Management

SOC	Security Operations Centre
SOX	Sarbanes Oxley
TAS	Threat Analysis and Sharing
TOGAF	The Open Group Architecture Framework
TTSA	Technical Training and Awareness of Security Issues
UM	Utility Maximisation
UNISA	University of South Africa
UOE	Use of Encryption
URL	Uniform Resource Locator
US	United States
USA	United States of America
USB	Universal Serial Bus

Publications

1.	Govender, S., Kritzinger, E. & Loock, M. The Influence of National Culture on Information Security Culture. IST-Africa 2016 Conference Proceedings. 11-13 May 2016. Durban. ISBN:978-1-905824-54-0
2.	Govender S.G.; Loock, M. and Kritzinger, E. 2018. Enhancing Information Security Culture to Reduce Information Security Cost: A Proposed Framework. Lecture Notes in Computer Science. ISBN 978-3-030-01688-3 ISBN 978-3-030-01689-0 (eBook).
3.	Govender, S., Kritzinger, E. & Loock, M. 2020. Information Security Cost Reduction through Social Means. Communications in Computer and Information Science. ISBN: 978-3-030-43275-1
4.	Govender, S., Kritzinger, E. & Loock, M. A framework and tool for the assessment of information security risk, the reduction of information security cost and the sustainability of information security culture. Personal and Ubiquitous Computing. 25, 927–940 (2021). https://doi.org/10.1007/s00779-021-01549-w
5	Govender, S., Kritzinger, E., Loock, M & Singh, S. Using Design Science Research to Iteratively Enhance Information Security Research Artefacts. Springer Series: Lecture Notes in Networks and Systems - ISSN 2367-3370. Accepted and to be published in 2023

Statement of Original Authorship

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature:

Date: 13 June 2023

Acknowledgements

To my parents, Rookmoney and Govindasami, both of whom were teachers. I would like to thank them for instilling the value of education in me.

To my wife, Melissa, for supporting me through the years of study.

To Pippen, Lulu Belle, Kimiko, Koshka, Mischa, Stella, Phoebe and Blaze, the companions that sat with me whenever I worked.

Finally, to my supervisors, Prof. Kritzinger and Prof. Loock, for their academic guidance and support.

Chapter 1: Introduction

1.1 BACKGROUND

Information technology has transformed the business landscape, shifting the paradigms of traditional businesses and transcending the limitations of human resource-based work processes while still providing platforms, products and services that allow people to excel in a post-digital world. Information assets created through information technology bring immense value to consumers, enhance organisations' business models and allow for significant scientific and educational improvement (Mithas and Rust 2016; Saunders and Brynjolfsson 2016; Nazarian, Irani and Ali 2013). Nevertheless, as the utilisation of information technology continues to proliferate, the security of individuals, data, and technologies has become a significant area of concern (Safa, Maple, Watson and Von Solms, 2018; Soomro, Shah and Ahmed, 2016). The imperative of information security management applies to all organisations that consider their corporate information to be valuable assets (Haqaf and Koyuncu 2018). Implementing, evaluating and managing information security depends on having strong human subject matter expertise in order to achieve the expected level of information security governance (Schinagl and Shahim 2020; Tanimoto, Nagai, Hata, Hatashima, Sakamoto and Kanai 2017). Information security remains a top priority as both business technology solutions and employees present a significant cyber security risk (Mukherjee 2019; Van Slyke, Clary, Ellis and Maasberg 2019). However, security management objectives such as information security risk assessments, evaluation of information security culture and minimising cost overruns for information security technology and resources are limited when general strategic planning is conducted (Dhillon, Torkzadeh and Chang 2018).

The occurrence and public exposure of information security breaches are on the rise (Lord 2017). Limited compliance, governance and information security risk management are key drivers in these data breaches (Chatterjee and Sokol 2019; Jeong, Lee and Lim 2019). Reports on cyber breaches show that in just a three year period between 2017 and 2019, there have been in excess of seven thousand reported breaches, which have exposed several billion information records (Winder 2019; Targett 2018; Lord 2017). Large-scale data breach studies show that over a greater period of five years, the cost per breach has been reduced progressively as organisations adopt improved security technology, organisational structures and awareness; however, the number of attacks and subsequent breaches has increased (Ponemon Institute 2020; Verizon 2017; Kaspersky Lab 2016). Therefore, the cost to improve and enhance information security products and service will increase as the volume of attacks becomes greater.

Major data breach attack vectors are those that exploit actions that have been determined to contribute significantly to information security compromise. Several remediation actions have also been established to remediate the risk of these attack vectors. These remediation actions are a combination of operational and awareness activities, which are social functions of an organisation, while the acquisition of products and services are technical functions. Technical solutions are the prevalent method that organisations use to reduce the likelihood of data breaches (Chong 2018). However, there is a significant cost associated with information security products and solutions as well as the limited availability of qualified and capable information security professionals required to support, administer, monitor, maintain and manage these solutions (Debar 2019; Wilczek 2019).

In addition to the need for people to operate these technologies, the enhanced values and behaviour of non-technical employees in the understanding of information security risk are critical. Van Niekerk and Von Solms (2010) and Ruighaver, Maynard and Chang (2007) describe models and metrics to comprehend and quantify the impact of organisational culture on information security. This research proposes a multi-dimensional framework that aims to evaluate the methods used to assess information security, the models and approach to manage information security cost and the methods used to improve information security culture in order to reduce risk, sustain information security culture and reduce the cost of information security management in organisations.

1.2 CONTEXT

In Africa, there has been a proliferation in the usage of mobile devices and increased access to personal computers where growth in this usage is twice as fast as it is in the rest of the world (Chingapi and Steyn 2022). The ability of people to use these devices has great potential to launch economic and social development. However, as device usage increases, so too will the vulnerabilities associated with information available on the device and access to the device itself (Yildirim 2016). Computing devices allow users to broadcast a lot of information but this also exposes them to tangible and intangible risks (Almaiah, Al-Zahrani, Almomani and Alhwaitat 2021).

As new environments are developed, new applications and markets will become available, which lead to greater integration of services. While these new environments are being introduced there will also be a greater integration of business application into the mobile computing environment (Ghadi 2021). Therefore, it is apparent that as services and data requirements increase on computing devices, so too will the information security vulnerabilities (La Polla, Martinelli and Sgandurra 2013).

New platforms must provide comprehensive and usable security infrastructure. Expanded usage of mobile devices for commerce, finance, or business applications has led to mobile devices becoming a more desirable target for criminals (Enck, Ongtang and McDaniel 2009). The limitation of battery life and processing power makes mobile devices less defensively capable and the size and mobility make the devices susceptible to theft or loss (La Polla et al. 2013). While not currently common in rural areas, identity theft will become a bigger threat as users use more complicated services (Chingapi and Steyn 2022).

Considering this proliferation, there is also a shift to the usage of less secure devices in the business environment, with more and more companies adopting a “Bring-Your-Own-Device” policy. This leads to a greater need to secure company information (Almaiah et al. 2021). In addition, the current tools of the trade have started to include tablets and smartphones, where sensitive company information is now being stored, transmitted, or manipulated. Current development methods favour secure networks and operating systems, policy-driven software implementation and physical securing of devices. These methods are not congruent with the mobility, inter-connectedness and open access of current generation internet applications (Othman, Norman and Kiah 2021).

Information security in an organisation requires more than physical and technical controls (Berti and Rogers 2004). It, therefore, requires that the people within the organisation assimilate their behaviours in line with security expectations. This assimilation can be expressed as an information security culture (Schein 2009). Incorporating an information security culture into an organisation is limited to the line-of-business staff and the purveyors of information technology, namely the ICT operational staff. Software development methodologies must become security aware (Othman et al. 2021) and security management criteria must be explicit in all operations of ICT (Siponen 2002). The key to creating an environment in which information security is culturally ingrained lies in bridging the gap in the lack of knowledge, skills and commitment by employees to protect information (Gupta and Sharman 2008).

1.3 RATIONALE AND PURPOSE

This section outlines the rationale of the study research questions and objectives, which will address the research purpose.

According to the FBI Internet Crime Report (Internet Crime Complaint Centre 2020), there was a significant increase in reported losses, reaching USD $4.2 billion in 2020—an astonishing 200 percent rise from 2017. Among the paramount areas of risk, cyber vulnerability stands out prominently. Neglecting the necessity to assess, comprehend, and respond to cyber threats is a risk too substantial for any organisation to disregard (Arcuri, Brogi, and Gandolfi 2018). It is imperative for companies to have confidence in the effective management of information security to safeguard against cyber-attacks, unauthorized access, and data breaches. Data breaches impose significant burdens in terms of time, cost, and adverse business consequences (Akhtar, Sheorey, and Bhattacharya 2021). Inadequate data security can result in the loss or theft of critical information, thereby generating an unfavourable customer experience that may translate into business losses and damage to reputation. Costs related to information extracted during data breaches can lead to significant regulatory fines of up to 10 percent of annual revenue, but a study has found that market shifts, soon after a data breach, have a greater economic impact than fines (Ford, Al-Nemrat, Ghorashi and Davidson 2022). Therefore, it is important to delve into whether organisations in South Africa have the capability and know-how to assess the organisation's security needs, align budgets to optimal security spend and sustain an information security culture in order to reduce information security risk.

1.3.1 Research Questions

The primary research question is:

> **What constitutes a framework and an associated tool that evaluates an organisation regarding how the organisation assesses information security, aligns cost-reducing of information security products and services and sustains improved information security culture?**

In order to address this question, the following sub-research questions (SRQs) will be answered:

> SRQ1: What frameworks and evaluation tools exist to assess information security in organisations?
>
> SRQ2: What are the common factors that influence information security costs?
>
> SRQ3: What constitutes information security culture and how can this be improved?

1.3.2 Research Objectives

The main research objective is to:

> **Develop a framework and related tool that evaluates an organisation regarding how the organisation assesses information security, aligns cost-reducing of information security products and services and sustains improved information security culture.**

For this purpose, the following three models will be developed:

- Model 1 - Social and technical cost reduction factors, which describe factors that influence information security cost.
- Model 2 - Human intervention in information security capability, which describes information security assessment methodologies.
- Model 3 - An information security culture enhancement model, which describes factors that improve information security culture.

Components of these models will be combined to form the main framework, which is called the ARCS Security Framework. Furthermore, an evaluation tool will be developed to support the application and use of the framework.

The study research objectives (SRO) are to:

> SRO1: Determine and assess what frameworks and evaluation tools exist to assess information security in organisations.
>
> SRO2: Evaluate frameworks and models that exist to manage information security costs.
>
> SRO3: Assess models and evaluation tools that exist to improve information security culture.

1.4 RESEARCH METHODOLOGY

The chosen research methodology for this study is Design Science Research (DSR). DSR encompasses a spectrum of synthetic and analytical methodologies and perspectives used to conduct research within the domain of information systems (Vaishnavi, Kuechler, and Petter 2004). These methodologies complement positivist, interpretive, and critical research approaches. In essence, DSR entails the development of artefacts and/or design theories aimed at enhancing the present state of practice and augmenting existing research knowledge (Baskerville 2008).

Vaishnavi, Kuechler, and Petter (2004) delineate two pivotal undertakings within Design Science Research (DSR) that contribute to the enhancement and comprehension of behavioural facets in information systems:

- Forging fresh knowledge via the conception of novel or innovative artefacts.
- Scrutinising the utilisation and/or effectiveness of the artefact through introspection and abstraction.

The artefacts generated within the Design Science Research (DSR) process encompass a range of elements, including but not confined to, models, frameworks, or methods (Vaishnavi and Kuechler 2012). The theories formulated through DSR contribute to knowledge by establishing a collection of principles or concepts along with a range of potential specific outcomes guided by the theory.

Design Science Research (DSR) is highly compatible with the realms of information systems and information security due to the dynamic nature of technology, which often gives rise to fresh concepts and ideas. This, in turn, empowers researchers to propose and assess new notions or concepts (Orlikowski and Iacono 2001). DSR aligns well with this exploratory approach to research in the field of Information Technology (IT), a stance that is strongly endorsed by DSR (Orlikowski and Iacono 2001).

The artefacts that will be developed in this research are:

- A model describing the relationship between the social and technical aspects of cost-saving information security initiatives.
- A model describing the impact of human intervention in implementing and supporting information security technologies.
- A model describing five pillars to be able to sustain and improve information security culture.
- A framework that includes features related to the evaluation of information security assessments, information security costs and information security culture.
- An evaluation tool that applies the framework.

The framework will be synthesised from the models that have been derived through the evaluation of the literature. The DSR process that will be used to develop, demonstrate, evaluate and communicate these artefacts is based on Peffers, Tuunanen, Rothenberger and Chatterjee’s (2007) DSR process model. A detailed discussion on the methodology and research approach is described in Chapter 3.

1.5 ETHICAL CONSIDERATIONS

Ethical clearance was granted by the University of South Africa (UNISA) as per the clearance certificate in Appendix A. All ethical considerations and concerns to promote research integrity were undertaken in line with UNISA’s research ethics policy. The communications to participants of the study and their consent to participate are documented in Appendix B. All personal information provided was anonymised, while paper and electronic responses were stored on a secure portable hard drive that was encrypted and password protected. Where paper documents were used, these documents were scanned and the original documents were kept in the researchers personal safe.

1.6 RELEVANCE AND CONTRIBUTION

The research relevance and contributions are:

- Developing a framework that combines the key features of information security management, which include information security assessment, cost and behaviours and values (culture)
- To support the framework, this research contributes to theory by creating a model that describes the relationship between information security culture and information security assessment methods
- To support the framework, this research contributes to theory by creating a model that describes how information cost saving factors are related to human factors
- To support the framework, this research contributes to theory by creating a model that describes key activities or programmes that can be implemented to improve information security culture
- Making a practical contribution by creating an evaluation tool for applying the framework that can allow organisations to use the framework immediately.

1.7 SCOPE AND LIMITATIONS

The scope of the research was limited to IT departments in medium to large organisations where medium is defined as a company with more than two hundred and fifty employees, and large is defined as a company with more than one thousand employees (Tsatsenko 2020; Masutha and Rogerson 2014). As the focus of the study was limited to medium to large organisations, the resulting assessment artefacts may not be fully applicable to smaller organisations. The resulting artefacts may also have limited applicability for resource constrained organisations, where the information security capacity and capability may not allow the organisation to effect the changes expected from the application of the artefacts.

Five organisations were selected to participate in the demonstration and evaluation phases. In addition, five participants on a senior and executive level working in information technology departments in these organisations were selected to act as expert reviewers in the evaluation phase. The sample size was based on DSR theory that shows that Exploratory Focus Groups (EFGs) and Confirmatory Focus Groups (CFGs) do not need to be of a large sample size (Tremblay, Hevner and Berndt 2010) and that limited sample size affords a key practical advantage when designing, demonstrating and evaluating artefacts (Venable and Baskerville 2012; Offerman, Levina, Schönherr and Bub 2009). Three areas of concern related to information security programmes were considered for review, namely, information security assessment, information security cost and information security culture. Additional systemic perspectives such as a strategic perspective that considers how organisations would respond to continuously changing threat landscapes or organisational perspectives wherein an organisation’s ability to respond to assessment in of itself, where not considered and form part of further studies or expansions of the artefacts developed within this research.

The literature surveyed for the information security assessment feature of the artefacts included popular and commonly used information security risk assessment methodologies, information security architecture frameworks and information security best practices and standards. The literature surveyed for the information security cost reduction feature of the artefacts included strongly cited information security cost models and recently surveyed information security cost evaluation reports. The literature surveyed for the information security culture feature of the artefacts included key historical literature on organisational culture and more recently developed information security culture models.

The limitation of the participation in the research was the geographical constraints imposed with travelling to meet any prospective participants that were not in the Gauteng province, as well as the need for face-to-face participation to combat misunderstanding of artefacts and related content. As such, only participants that were physically located in Gauteng were selected. Considering that culture was a key component of the study, it was determined based on national culture studies, discussed in Chapter 2, that there would not be a significant deviation in security culture across the provinces in South Africa.

1.8 SUMMARY

Cyber security breaches are becoming greater and more common. Organisations and people are more aware than ever of these breaches, as these are frequently reported on by the mainstream media. Managing information security has traditionally focused efforts on security technology implementation at significant cost and complexity. However, organisations have neglected the consideration that the complexity, amount and sophistication of attacks and potential threats are larger and more frequent than ever before. Incorporating information security into the culture of the employees that support and are protected by these technologies, is a key capability that must be considered in parallel to improved security technology.

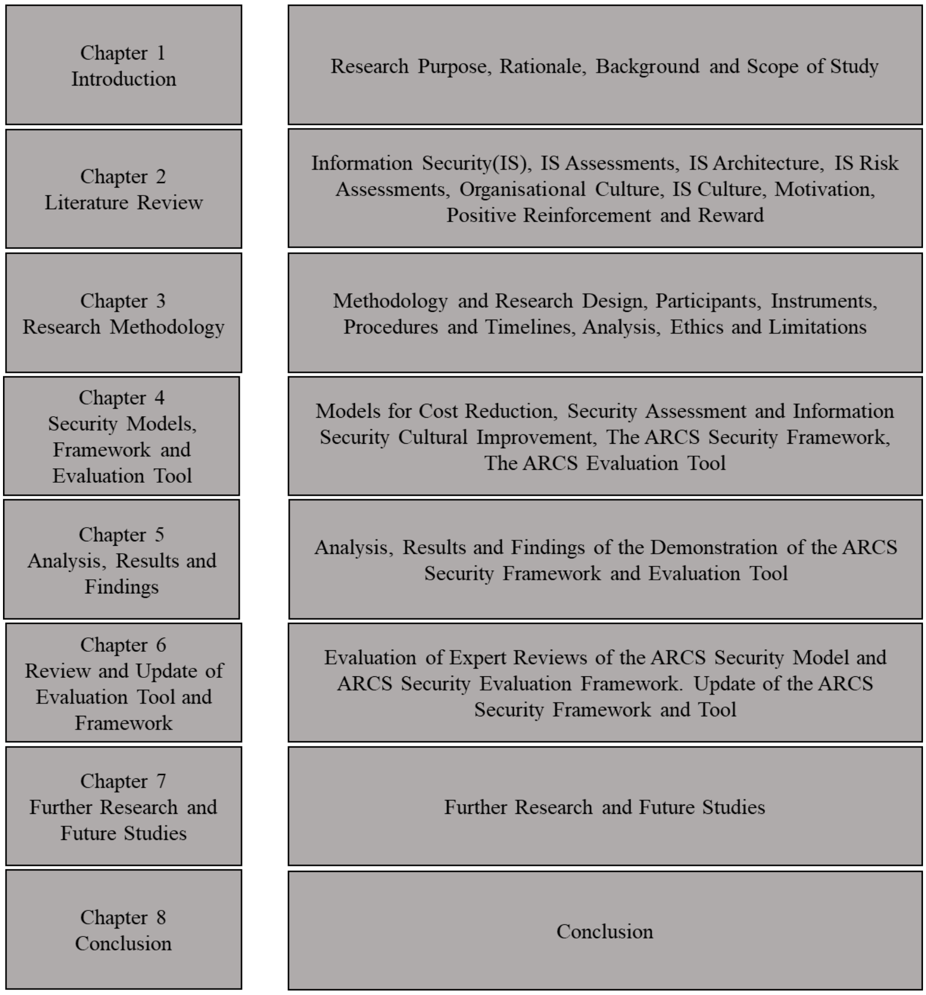
The structure of the thesis document is as follows:

- In Chapter 2, a literature review is conducted related to key topics pertinent to the research. Information assessment methods, cost models and culture models are reviewed. Implementation science is discussed with a view to developing the basis for the artefacts created in the study.
- In Chapter 3, the research philosophy and methodology are discussed and described. DSR process models are evaluated and a process model that determines the steps carried out in this research, is selected.
- In Chapter 4, three models, a framework and an evaluation tool are designed and developed to help organisations better support and enhance information security management. These artefacts consider the implementation of information security products, services and structures that reduce costs, while structuring the correct information security behaviour and values in employees and strengthening an organisation's ability to improve information security assessment capabilities.
- In Chapter 5, the demonstration and evaluation of the artefacts conducted with research participants are communicated.
- In Chapter 6, a second iteration of the security framework and evaluation tool is developed.
- In Chapter 7, improvements and potential enhancements of the framework and evaluation tools are discussed. Potential future research is also discussed.

- Finally, in Chapter 8, the study is summarised and aligned to the research questions and research objectives described in this chapter.

A structure of the thesis document is depicted in Figure 1-1.

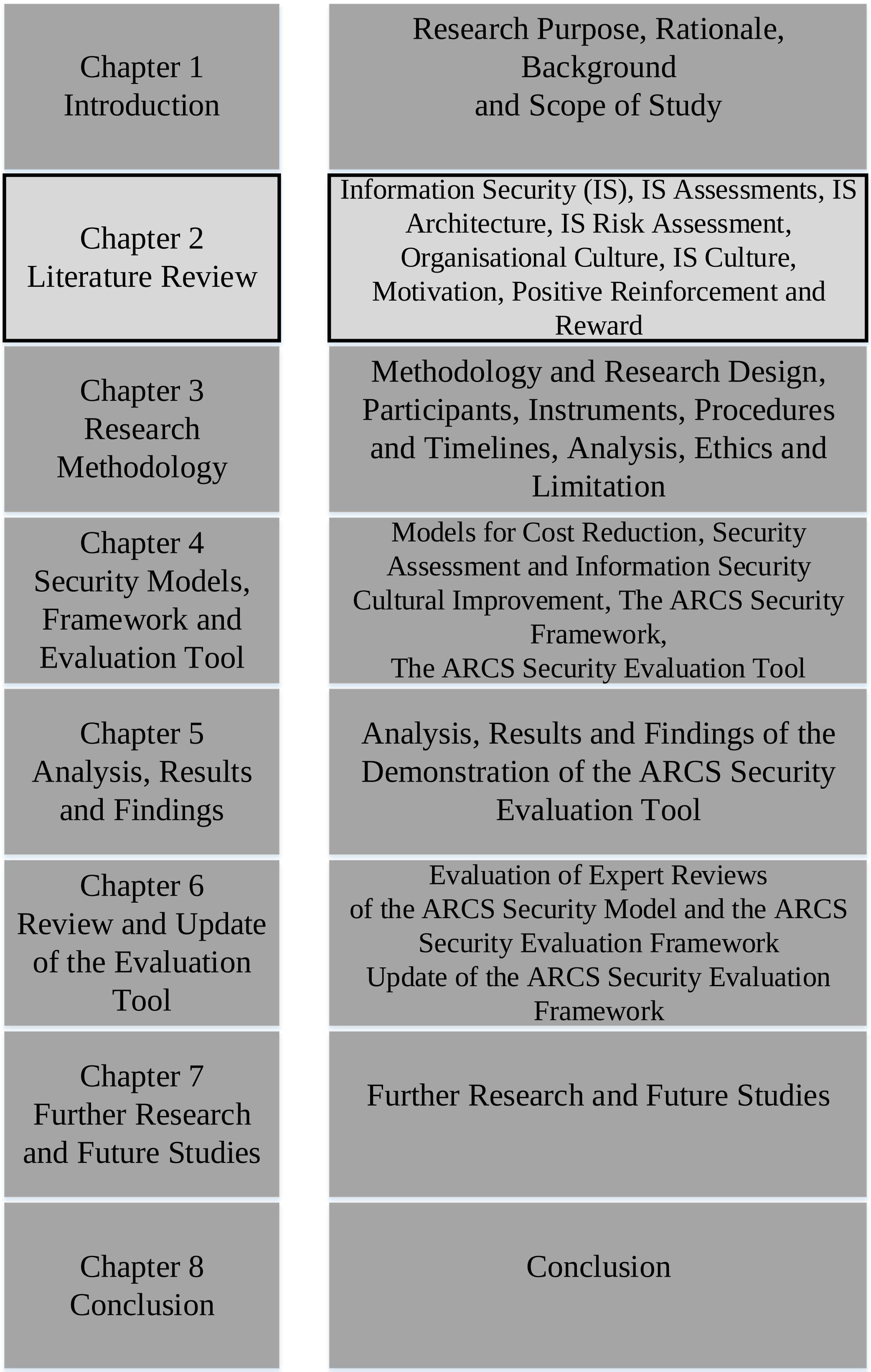
1.9 THESIS OUTLINE



Chapter 1 Introduction	Research Purpose, Rationale, Background and Scope of Study
Chapter 2 Literature Review	Information Security(IS), IS Assessments, IS Architecture, IS Risk Assessments, Organisational Culture, IS Culture, Motivation, Positive Reinforcement and Reward
Chapter 3 Research Methodology	Methodology and Research Design, Participants, Instruments, Procedures and Timelines, Analysis, Ethics and Limitations
Chapter 4 Security Models, Framework and Evaluation Tool	Models for Cost Reduction, Security Assessment and Information Security Cultural Improvement, The ARCS Security Framework, The ARCS Evaluation Tool
Chapter 5 Analysis, Results and Findings	Analysis, Results and Findings of the Demonstration of the ARCS Security Framework and Evaluation Tool
Chapter 6 Review and Update of Evaluation Tool and Framework	Evaluation of Expert Reviews of the ARCS Security Model and ARCS Security Evaluation Framework. Update of the ARCS Security Framework and Tool
Chapter 7 Further Research and Future Studies	Further Research and Future Studies
Chapter 8 Conclusion	Conclusion

Figure 1-1 Outline of the Thesis

Chapter 2: Literature Review



Chapter 1 Introduction	Research Purpose, Rationale, Background and Scope of Study
Chapter 2 Literature Review	Information Security (IS), IS Assessments, IS Architecture, IS Risk Assessment, Organisational Culture, IS Culture, Motivation, Positive Reinforcement and Reward
Chapter 3 Research Methodology	Methodology and Research Design, Participants, Instruments, Procedures and Timelines, Analysis, Ethics and Limitation
Chapter 4 Security Models, Framework and Evaluation Tool	Models for Cost Reduction, Security Assessment and Information Security Cultural Improvement, The ARCS Security Framework, The ARCS Security Evaluation Tool
Chapter 5 Analysis, Results and Findings	Analysis, Results and Findings of the Demonstration of the ARCS Security Evaluation Tool
Chapter 6 Review and Update of the Evaluation Tool	Evaluation of Expert Reviews of the ARCS Security Model and the ARCS Security Evaluation Framework Update of the ARCS Security Evaluation Framework
Chapter 7 Further Research and Future Studies	Further Research and Future Studies
Chapter 8 Conclusion	Conclusion

Chapter 2: Literature Review

In Chapter 1, the background, purpose and proposed structure of this research were discussed. Primary research questions, sub-questions and research objectives were outlined.

In this chapter, the researcher will critically evaluate the literature on topics relevant to the primary research question and sub-questions posed in Chapter 1. The research questions and research objectives discussed in Chapter 1 focus on information security cost, information security and organisational culture, assessments methodologies and security architecture. This, therefore, informed the need to understand information and artefacts (theories, models and frameworks) related to these topics. Furthermore, to supplement the understanding of information security culture topics on organisational behaviour, recognition and reward and national culture are also discussed. By delving into these key topics, the current knowledge on these topics informed the researcher on gaps in knowledge, and on where the current knowledge could be expanded to formulate more applicative artefacts such as enhanced models and frameworks. The literature review is organised thematically around the key focus areas noted and is based on investigations into each these areas, to draw on seminal, highly cited, recently surveyed and recently developed related knowledge. The literature reviewed will contribute to the understanding of key topics discussed in this research and will assist in the formulation of artefacts developed in later chapters.

The key topics of review in Section 2.1 will be the importance of information security considering the proliferation and ubiquity of computing devices and the increase in data breaches and malicious threat actors. In Section 2.2, implementation science and its definition of theories, frameworks and models and these constructs’ validity to information systems research are discussed.

The traditional models and methods of quantifying information security investment and the limitation of these in managing information security in a new age of information security technology and threats, will be evaluated in Section 2.3. In terms of information security assessment, three topics will be reviewed. These topics, which are discussed in Sections 2.4, 2.5 and 2.6, are the value, objectives and processes of assessing information security risk, implementing information security architecture and conducting traditional risk assessments in organisations.

National culture and organisational culture are discussed in Sections 2.7 and 2.8. The discussion in these sections forms the basis for components of the culture model designed later in this study. Information security culture is discussed in Section 2.8 and will be evaluated through an overview of organisational culture theory and the value, objectives and processes of information security culture in organisations. Finally, in Section 2.10, an overview of motivation, positive reinforcement and reward as supporting drivers for the improvement of information security culture will be reviewed. The topics noted were selected, as preliminary research prior to this study, led the researcher to determine that these key topics formed the basis of seminal research towards the understanding information security culture and improving organisational culture in general. As a key aspect of this study is rooted in understanding non-technical methods of information security risk reduction it is expected that reviewing these topics will give an input into artefacts that support the outputs of the primary and secondary research questions and objectives.

Using the literature as a guide, it will be demonstrated that there are several models, frameworks, or tools that focus on the specific areas of information security assessments, cost and culture, but there are none that encompass evaluating all three areas. The value in incorporating all three areas is that these areas are inherently linked. The need for human intervention in all these areas as described by the models developed in section 4.1.3 support a need for a combined framework.

2.1 INFORMATION SECURITY

In a world where organisations are dependent on technology, there is an increase in the number, type and complexity of technologies (Holicza and Kadëna 2018; Tiller 2010). This creates a challenge to be able to balance usability and information security. Information security, therefore, is an essential feature in an organisation being successful, as it strives to protect its information assets (Burkett 2012). Information security and the management system that supports it, can be defined as something that will ensure that data is safeguarded against unauthorised access, unauthorised alterations, and unavailability when necessary. (Dronov and Dronova 2022; Anderson 2003).

Intrusion by threat actors and malicious software causes a financial loss and loss of reliability and veracity. The objectives of information security can be classified into several categories: avoidance, traceability and reviewing, monitoring, privacy and confidentiality, multi-level security, secrecy, validation, and integrity (Yasar, Preuveneers, Berbers and Bhatti 2008). In addition, stringent legislation and standards are required to protect personal data and to implement strict IT controls, such as GDPR (Zerlang 2017), POPIA (Netshakhuma 2019), HIPAA (Herold and Beaver 2014), Sarbanes Oxley; (Kim, Robles, Cho, Lee and Kim 2008) and PCI DSS (Wu, Guo, Wu and Wu 2018) to create a complex security management environment that is relevant to all functions of the business. However, instating an information security program within an organisation is a complex endeavour. This necessitates robust backing from top-level management and the establishment of pragmatic security policies and procedures, underpinned by the necessary authorization to ensure compliance. Moreover, there should be a provision of substantial data on program efficacy, along with a consistent emphasis on periodic scrutiny of the program (Peltier and Peltier 2016).

The trend in information security is to use common defence mechanisms, such as intrusion detection systems, firewalls, antivirus, internal and external policies, encryption and forced operating system controls (Zissis and Lekkas 2012; Subashini and Kavitha 2011). Furthermore, information security is implemented as a program, where best practice methodology and frameworks, such as SABSA (Sherwood, Clark and Lynas 2004), ISO 27000 (Prislan and Bernik 2010), or CoBIT (Lepofsky 2014), are used to align policies and procedures to requirements for securing information assets (Peltier and Peltier 2016).

Information security is a crucial element in allowing a business to flourish, innovate and excel. Therefore, information security must essentially now be built into the operations and function of an organisation (Dronov and Dronova 2022; Chess and Arkin 2011).

The next generation of open operating systems is tailored not for desktop computers or mainframe systems, but for mobile devices (Enck et al. 2009). These devices function as extended desktops and in some cases have the same functionality as a traditional computing environment (Almaiah et al. 2021; Botha, Furnell and Clarke

2009). Organisations are actively seeking methods to seamlessly integrate their internal operations onto mobile platforms and as such, there will be a greater opportunity for susceptibility of these devices as these will contain more significant amounts of business-related information (Chingapi and Steyn 2022).

Mobile device intrusions are greater in scope than traditional information security breaches, as these devices also integrate microphones and cameras (Othman et al. 2021). Cyber-attacks may also include activating these components or alternatively engaging power-intensive services on the device to kill battery life (La Polla et al. 2013; Becher, Freiling, Hoffmann, Holz, Uellenbeck and Wolf 2011).

Limitations of these devices such as memory, processing power, storage, battery power and form factor, reduce an organisation's ability to use traditional means to secure the device (Goodman and Harris 2010). Due to these constraints, there is difficulty installing anti-virus products and providing physical locking mechanisms, lock down configuration, or control access as one would use firewalls or an intrusion detection system. Additionally, storage in these devices is generally removable and may be easily extracted from a stolen or lost device. Ultimately, the security experience for the organisation and the user must be a seamless effort between the traditional and mobile environments (Almaiah et al. 2021; Botha et al. 2009).

An information security programme is key in any organisation. All data managed and processed by an organisation is susceptible to potential threats stemming from attacks, errors, disasters, or inherent vulnerabilities (Yildirim 2016). In order to protect that information, the organisation should identify inherent risks, monitor and evaluate the effectiveness of controls and securing procedures and optimise controls. Adopting a framework for security management within an organisation is of paramount importance (Schinagl and Shahim 2020).

The fundamental problem with incorporating information security disciplines into IT processes and functions lies with the people's behaviour and actions (Haqaf and Koyuncu 2018). For the seamless assimilation of information security into an organisation's corporate culture, safeguarding data must be seamlessly woven into daily operations, becoming a natural and ingrained behaviour among employees (Thomson, von Solms and Louw 2006). Information security in an organisation is greater than practical and technical restrictions (Berti and Rogers 2004). It, therefore, requires that the people within the organisation assimilate their behaviours in line with security expectations. This assimilation can be expressed as an information security culture (Schein 2009).

Cultivating an organisational culture of information security extends beyond the scope of just the line-of-business personnel and information technology providers, namely the Information and Communications Technology (ICT) operational staff. Software development methodologies must become security aware (Othman et al. 2021) and security management criteria must be explicit in all operations of ICT (Siponen 2002).

The key to creating the environment in which information security is culturally in-grained is in bridging the gap in the absence of knowledge, skills, and dedication among employees concerning information protection (Dronov and Dronova 2022; Thomson et al. 2006).

2.2 THEORIES, MODELS AND FRAMEWORKS

The field of implementation science provides a researcher with an effective theoretical approach to determining why and how an implementation will succeed or fail (Nilsen 2015). The three high-level theoretical aims within implementation science encompass the ability to delineate or direct the progression of converting research into practical application, comprehending or elucidating the factors affecting implementation, and appraising the execution of implementation (Nilsen 2015). To achieve these aims, Nilsen (2015) proposes implementation constructs that are described in Table 2-1.

Table 2-1 Five Categories of Theories, Models and Frameworks (Nilsen 2015)

Category	Description
Process Models	Describes the steps or phases encompassed in translating research into real-world application, which involves implementing and utilising research outcomes. Process models strive to illustrate and offer guidance for this process. process of transforming research into practical implementation. An

	action model is a type of process model created to provide practical direction for both the planning and execution stages.
Determinant Frameworks	Outlines categories of factors and individual-level specific factors, acting as barriers and enablers (independent variables), influencing the outcomes of implementation (dependent variables). Some frameworks also illustrate linkages between different types of factors. The ultimate goal is to comprehend and/or elucidate the factors that affect implementation outcomes, such as forecasting outcomes or retrospectively interpreting them.
Classic Theories	Theories originating from fields beyond implementation science, such as psychology, sociology, and organisational theory, can be embraced to provide understanding and elucidation on diverse aspects of implementation.
Implementation Theories	Theories developed by researchers in the field of implementation, whether by generating novel theories or by adapting existing ones and concepts, aim to provide understanding and clarification of various aspects within the scope of implementation.
Evaluation Frameworks	Outline elements of implementation that can be assessed to ascertain the achievement of successful implementation.

The following alignment of these constructs to implementation science aims are depicted in Figure 2-1.

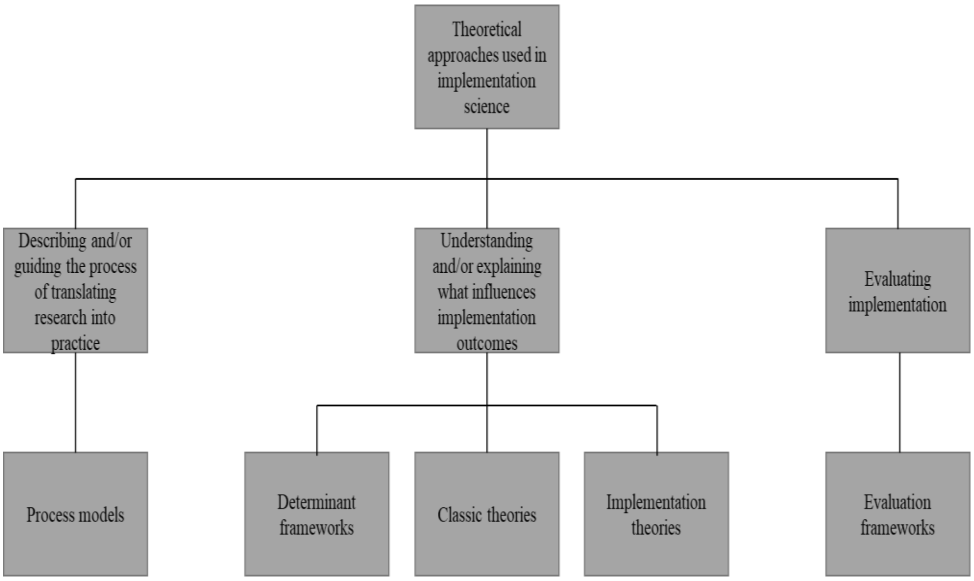

Theoretical approaches used in implementation science
Describing and/or guiding the process of translating research into practice
Understanding and/or explaining what influences implementation outcomes
Evaluating implementation
Process models
Determinant frameworks
Classic theories
Implementation theories
Evaluation frameworks

Figure 2-1 Three Aims of Theoretical Approaches in Implementation Science Linked to Five Categories of Theories, Models and Frameworks (Nilsen 2015)

In the realm of implementation science, theories are characterised as a collection of analytical statements or principles devised to observe, depict, and clarify an environment (Nachmias and Nachmias, 1976). Models offer a purposeful simplification of a phenomenon or a portion thereof, and they need not be a wholly precise portrayal of reality to hold significance (Bluedorn and Evered, 1980). While a model is descriptive, a theory serves an explanatory purpose. On the other hand, a framework signifies a structure, summary, outline, system, or blueprint capable of comprehensively representing a phenomenon. A framework may consist of categories such as concepts, constructs, or variable (Nachmias and Nachmias 1976). Frameworks are not explanatory but present phenomena in categories (Wacker 1998).

In the context of this study, the models developed provide a representation of reality taken from real-world studies such as the Ponemon and Kaspersky's studies as well as observations from published research. The framework developed extracts the components of the models to create a structure and system to account or, in this case, evaluate key topics (information security assessment, cost and culture).

2.3 INFORMATION SECURITY COST

In organisations, the financial management of information security costs is of material interest to senior leadership (Mercuri 2003). In order to justify information security investments, cost-benefit analyses are essential (Debar 2019). However, quantifying information security cost comprehensively and comparably has been difficult. For this reason, Chief Information Security Officers (CISO) need to articulate the value of their information security investments in economic terms (Scholtz 2011). The constantly changing and challenging landscape of information security, especially regarding the tools, techniques and practices (TTPs) of threat actors requires multiple approaches that encompass several focus areas to achieve a reasonable view of information security investment (Schatz and Bashroush 2017). Additionally, traditional business management and economic principles help quantify the cost of information security investment (Brecht and Nowey 2013).

While there is a noted decline in hiring cyber security staff, research found (Cavusoglu, Cavusoglu, Son and Benbasat 2015) that companies admit their information security programme experienced deficits in at least one of the domains: employees, technology, or knowledge. Subsequent research revealed that 53% of organisations are confronted with a shortage of cybersecurity skills (Oltsik, 2019). Given that labour expenses constitute a major portion of an organisation's operational costs, and the dearth of information security resources exacerbates this, ensuring a comprehensive and proficient staffing approach for the information security function becomes a pivotal consideration. Striking a balance between implementing information security technology solutions and the requisite personnel to oversee, manage, and sustain these technologies is crucial for establishing an economically viable solution to safeguarding organisational information.

Cavusoglu et al. (2015) present a conceptualisation of organisational influences that impact the extent of implementation of information security controls and, consequently, the associated information security costs. Mimetic pressure pertains to an organisation's actions taken in response to the actions of others, such as competitors (Latif, Mahmood, Tze San, Mohd Said, and Bakhsh, 2020). Coercive pressure is associated with internal organisational or cultural expectations (Latif et al., 2020). Normative pressure involves conforming behaviour based on input from the organisation's business or provider network, which includes business partners, trade associations, and professional groups (Latif et al., 2020). Traditionally, investments in information security are determined through assessments, risk analysis, or institutional necessities.

Making comparisons in terms of information security expenditure among industry peers or relying on standardised regulations is unfeasible due to the absence of a universal definition or accounting approach for normalising costs (Asen, Bohmayr, Deutsche, Gonzalez, 2019). The cost of information security is also multifaceted within an organisation, as budgets might be allocated across various departments such as IT, risk management, fraud prevention, physical security, compliance, and legal affairs (Wilczek, 2019). Elevated levels of security standards, such as those related to card payment or regulatory controls, can also contribute to an escalation in costs.

In 2017, Schatz and Bashroush conducted a systematic literature review on approaches to investment in IT Security. Their analysis summarised the key elements, focus areas, challenges and benefits of available methods to calculate information security costs.

Schatz and Bashroush’s (2017) study of two hundred and seventy relevant academic articles found that the key elements of information security cost models were benefits, cost, function, impact, resource, threat, volatility and vulnerability. This is further explained in Table 2-2.

Table 2-2 Focus Areas for Information Security Investment adapted from Schatz and Bashroush (2017)

Element Category	**Description**
Benefit	Components possessing immediate advantageous qualities, such as cost reduction and revenue enhancement, or those that are explicitly outlined as advantages.
Cost	Elements that encompass costs either incurred directly or indirectly, including operating expenses, opportunity costs, and costs associated with switching.

Element Category	**Description**
Function	Elements that are abstract constructs, such as decision trees, quality benchmarks for mitigation, and imprecise numerical values.
Impact	Facets that provide a comprehensive view of the influence within the given approach's context, such as potential harm or an aggregation of resulting consequences.
Resource	Elements that are considered as resources, including set budgets, asset valuations, or resources accessible to potential attackers.
Threat	Elements that illustrate or measure threats within the specific approach's context, such as the likelihood of threats, attacker effectiveness, or occurrence frequency.
Volatility	Elements that are explicitly identified as the volatility factor in the primary investigation.
Vulnerability	Elements that articulate vulnerability within the context of the approach, encompassing factors like exposure rate, estimates of vulnerability parameters, or rates of circumvention.

Many models and approaches are aligned to these elements, but it was also found that there are several challenges, no matter which model is used. Traditional models determine cost through Return on Investment (ROI) or Net Present Value (NPV). Newer models focus on vulnerabilities and threats through Return on Attack (ROA) and Analytical Hierarchical Process (AHP). ROA is the coupling of the ROI index with a corresponding index aimed at measuring the convenience of attacks (Cremonini and Martini 2005). AHP is a method used for making decisions in intricate settings where numerous variables or criteria are taken into account to prioritise and choose alternatives or projects. (Schmid and Pape 2019). Furthermore, the scarcity of information security human resources has also led to costing models based on Utility Maximisation (UM). UM refers to the concept that individuals and firms seek to get the highest satisfaction from their economic decisions (Huang, Hu and Behara 2008).

However, no matter which model or amalgamation of models is chosen, challenges are still evident. These challenges are summarised in Table 2-3.

The direct economic consequences of information security risk in both the immediate short-term and long-term significantly influence the process of quantifying the cost of managing information security (Tsiakis and Stephanides, 2005). Additionally, the challenge of assessing information security management costs is amplified by current technology trends, which introduce hybrid technology models involving both cloud and on-premises infrastructure along with business applications (Kaspersky Lab, 2015).

Table 2-3 Challenges related to Information Security Investment Approaches adapted from Schatz and Bashroush (2017)

Challenge Category	**Description**
Accurate estimates	Challenges related to gauging critical parameters or inputs within the mentioned approach, including factors like the frequency of malicious events, extent of losses, or the overall accuracy of estimations.
Difficult to implement	Challenges linked to the intricacy of the approach, including intricate calculations, subjectivity, and the modelling of attacker functions, among others.
Constraint not considered	Challenges associated with factors explicitly highlighted as being deliberately left out of consideration by the corresponding approach, such as catastrophic losses or temporal factors.
Limited scenarios	Challenges tied to the constraints regarding suitability, like being confined to targeted attacks or unsuitable for comparing more than two solutions.
Actial benefit	Challenges connected to the discernment of the actual advantages offered by the approach.

Brecht and Nowey (2013) presented a succinct, high-level framework that illustrates the primary drivers influencing information security costs, as depicted in Figure 2-2. Nonetheless, these drivers don't align distinctly with the accounting conventions of assigning costs to functional sectors within an organisation, nor do they address the expenses associated with structural alterations geared towards reducing information security costs (Cavusoglu et al., 2015; Bojanc, Jerman-Blažič, and Tekavčič, 2012). The challenge in attributing costs to information security also stems from actions taken to manage the risk associated with it (Gordon, Loeb, Lucyshyn, and Zhou, 2015; Cremonini and Martini, 2005). For instance, if risk mitigation involves implementing more stringent programming guidelines or utilising infrastructure such as firewalls, it becomes intricate to precisely allocate costs to bespoke software development, system infrastructure teams, or the broader budget of the information security programme.

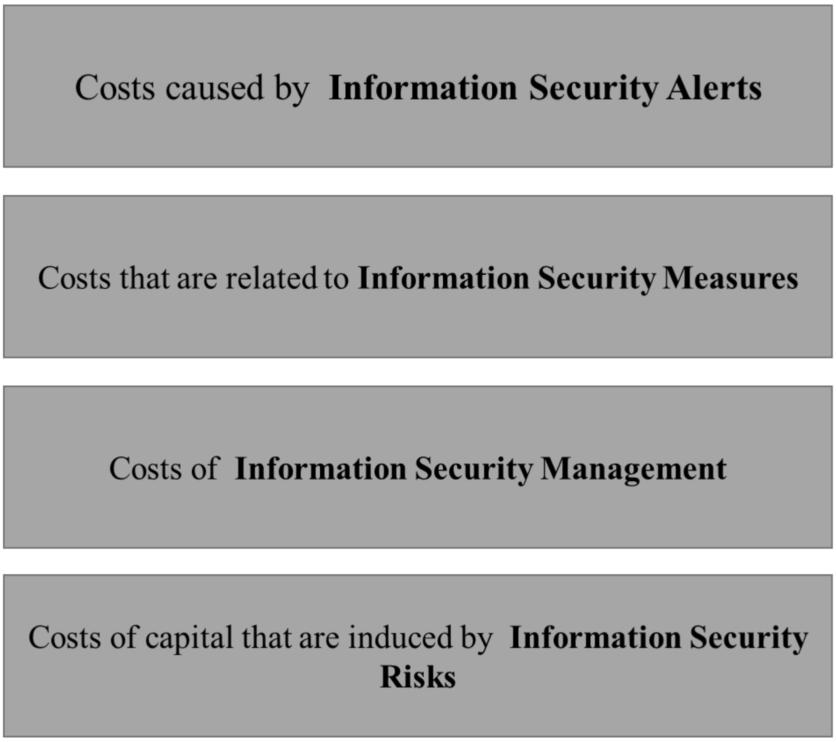

Costs caused by **Information Security Alerts**
Costs that are related to **Information Security Measures**
Costs of **Information Security Management**
Costs of capital that are induced by **Information Security Risks**

Figure 2-2 Key Drivers of Information Security Cost (Brecht and Nowey 2013)

Given that information security management operates across various functions, the rationale for the program's existence must be distinctly quantifiable. Moreover, this capacity to grasp the economic implications of information security on an organisation facilitates strategic investment-oriented long-term planning (Mitnick and Simon, 2003).

In line with the focus areas described in Table 2-2, this research will develop a framework that aligns to the benefit, cost, impact, resource, threat and vulnerability elements of information security cost determination. The precursor to developing the framework will be a model that determines the most and least costly information security initiatives that protect an organisation's information assets. These most and least costly factors are described as part of developing a new cost model in Chapter 4, Section 4.1. This model, in conjunction with the traditional models described in this section, form the basis for Feature 2 (F2) of the security framework developed in Chapter 4, Section 4.2.

2.4 INFORMATION SECURITY ASSESSMENTS (BEST PRACTICES AND STANDARDS)

In Chapter 4, a model describing the relationship between human interaction and security assessment is developed. The model describes the key information security risk assessments methodologies discussed in this section along with Section 2.5 and 2.6 and shows that there is a significant dependency on people to conduct and evaluate these assessments. The model is also the basis for a key feature of the overall framework also developed in Chapter 4.

Information security functions and capabilities in organisations are difficult to assess (Alshahrani, Alotaibi, Ansari, Asiri, Agrawal, Khan, Mohsen and Hilal 2022). Due to the scarcity of information security resources, organisations frequently engage third-party entities to furnish technology and business services (Davies, Mison, and Eden, 2022). Entrusting sensitive data to service providers potentially enlarges the organisation's vulnerable points for potential attacks (Edwards, Jacobs, and Forrest, 2019). The information security stance of an organisation characterizes its efficacy in addressing established risks and responding to emerging threats. However, assessing the security landscape usually involves audits and questionnaires, which are challenging to quantify, lack objectivity, and might not accurately reflect current threats (Edwards et al., 2019).

The main purpose of conducting an information security risk assessment is to recognise and measure risks associated with the organisation's information assets (Schmittling, 2010). This encompasses potential risks in areas such as strategy, operations, finance, and reputation.

The purpose of information security assessments is to adopt a proactive, pragmatic, and recurrent strategy for rectifying deficiencies in information security. Furthermore, legal, compliance, and regulatory mandates intended to safeguard sensitive or personal data, along with broader public security requisites, generate an anticipation for businesses of various scales to allocate paramount focus and priority to information security risks. The insights gathered through these assessments aid organisations in establishing optimal methods to address the identified risks.

Additional justifications for conducting information security assessments, have been adapted from Edwards et al. (2019), Mayer, Aubert, Grandry, Feltus, Goettelmann and Wieringa (2019) and Schmittling (2015) and are aligned with this study as noted in Table 2-4.

Table 2-4 Key Justifications for conducting Information Security Assessments

Justification Type	**Description**
Cost	Information security assessments do not generally provide a positive business in that spending on technology and people does not necessarily generate income. However, security assessments will advise leaders on the critical technology risks and therefore business risks that the organisation is exposed to, will enable them to concentrate their security investments on these critical areas that require corrective action. This study establishes a connection between vital factors driving cost reduction and the process of information security assessment. This is described in the development of the Security Evaluation Tools in Chapter 4, Section 4.3
Productivity	Through the identification and mitigation of technology and system risks, the potential for extended system uptime will be enhanced. As a result, the organisation will experience increased productivity, as business systems will operate for more extended durations.

Overcoming obstacles	Information security assessments unveil risks in systems, technology, and processes. IT employees play a pivotal role as primary drivers of these processes and technologies. The risks brought to light during an information security assessment dismantle the notion of attributing risks solely to technology and IT personnel. In this study, the correlation between information security assessments and human values and behaviour is expounded upon through a model elaborated and documented in Chapter 4, Section 4.1. This is further incorporated into the Security Evaluation Framework, described in Chapter 4 – Section 4.2.
Self-analysis	Conducting an information security assessment provides the IT team with a chance for introspection. The identified risks offer IT employees an occasion to contemplate their skills and know-how. This empowers them to take ownership of information security concerns within their respective areas. The notion of self-assessment and the adoption of a standardised thinking approach form essential elements of the model for enhancing information security culture, as detailed in Chapter 4, Section 4.1. Moreover, the discussion on information security culture and its interaction with individuals within the organisation is further elaborated in subsequent sections of this chapter.

The information security risk management lifecycle requires that information security assessments are conducted so that deficiencies can be identified and treated. This risk identification process allows for risks to be treated by resolution, remediation or acceptance (Mayer et al. 2019). The risk management approach to security evaluation is discussed in detail in Section 2.6.

A common approach to assessing information security is conducting vulnerability testing, penetration testing, or information security audits (Schmittling 2015). These evaluations can be harmonized with industry best practices, such as the Centre for Internet Security (CIS) benchmarks (Edwards et al., 2019), or compliance with standards like ISO 27002 audits (Kosutic, 2017). Nevertheless, regardless of the chosen assessment approach, a standardized procedure should be adhered to for conducting the assessment.

An information security assessment process adapted from Beaver (2016), is described in Table 2-5.

Table 2-5 Information Security Assessment Process

Process Step	**Description**
Support	Security assessment endeavours should possess the qualities of being both repeatable and proactive. Additionally, they necessitate robust backing from senior management to enable the information security management team to conduct investigations autonomously, free from interference by colleagues and other teams subject to evaluation. Moreover, these initiatives must garner endorsement from senior leadership to ensure efficient dissemination of inputs, processes, and outcomes throughout the organisation.
Scope	During the process of carrying out an information security assessment, it's imperative to subject all organisational environments to rigorous scrutiny and evaluation. While IT personnel might possess insights into areas with inherent risks and attempt to omit them from the assessment, the recommended approach is to appraise all internal and external systems. This evaluation should extend to encompass people and processes as well.
Testing	Testing should be consistently executed following a designated testing benchmark, guideline, or best practice. The outcomes of testing need to be replicable, ensuring that the process is repeatable and reliable. It's essential to establish Key Performance Indicators (KPIs) to define the criteria for addressing identified risks before initiating testing.
Reporting	Given that tools conducting automated security tests generate extensive technical reports, it becomes essential to generate more straightforward, lucid, and compact reports that categorise the

	identified risks as high, medium, or low. These reports should also outline potential means of addressing these risks. The reports need to be easily comprehensible, emphasising the crucial risk areas that require priority resolution, all while considering the context of both systems and business operations.
Process Step	**Description**
Resolution	A resolution necessitates well-defined action plans that encompass the specific resolution steps, the individual or team accountable for implementation, and the designated timeframe for completing the action. Resolution stands as the pivotal step within this process, as it ultimately aids in mitigating information security risks.
Oversight	The security team is responsible for maintaining continuous security management even in the intervals between regular security assessments. During these periods, it's crucial to uphold adherence to controls, policies, and procedures. Recognising the dynamic nature of the security landscape, it becomes essential to enhance security incident handling and alert management gradually rather than striving for flawless security. Furthermore, management should be consistently engaged to ensure compliance with contractual obligations and industry standards.

A comprehensive security risk assessment will help to determine the value and criticality of data generated and stored across the organisation. This determination will assist the business in prioritising and allocating information security resources where they are most impactful in reducing business risk (Alshahrani et al. 2022).

Hence, IT security risk assessments stand as a pivotal approach for an organisation to gauge its information security standing. These assessments enable organisations to pinpoint and enhance their comprehensive security stance, fostering collaboration among information security, IT teams, operational management, and other staff members to gain a comprehensive view of the business's information security risk landscape (Mayer et al., 2019). This procedure is essential to secure senior management's commitment to allocate resources and deploy suitable security solutions.

In Chapter 4 Information Security Assessment is a key feature, which is part of the main developed framework and aims to evaluate whether an organisation is aligning its security assessment methodology to security risk assessment processes and to what extent and whether it is effective. The evaluation area within the feature is called Security Assessment (SECASSESS), which is part of Feature 1 (F1), described in the Security Framework.

2.5 INFORMATION SECURITY ARCHITECTURE

Competent information security management entails establishing accountability and offering assurance (Innerhofer-Oberperfler and Breu, 2006). Information Security Architecture (ISA) is considered to be an effective way of managing information risk in an environment of business and infrastructure change. ISA needs to be rooted in business objectives and should outline a well-structured correlation between technical and procedural measures to effectively cater to the organisation's enduring security requirements. (Burkett 2012). Security architecture achieves this by precisely translating business security requirements into security controls and objectives, which can be applied to the IT infrastructure and systems (Pulkkinen, Naumenko and Luostarinen 2007).

Organisations running IS and information and communications technology find that while in almost all instances, a certain level of security architecture exists, it is often not documented. Documenting this in architectural artefacts allows the organisation to establish a baseline for the as-is security position (Alwadain, Fielt, Korthaus and Rosemann 2011). Understanding the as-is position makes it possible for the organisation to plan as changes occur within the business. This allows the organisation to move to a to-be position to address the risk factors inherent within its security position.

ISA entails the implementation of a thorough and meticulous approach to delineate the present and/or future assembly and functioning of an organisation's security controls, information security technology, human resources, and constituent structural components (Sherwood et al., 2004). This endeavour is in harmony with the fundamental objectives and strategic orientation of the organisation. While frequently linked exclusively with information security technology, it has broader applicability encompassing the security aspect of business enhancement, encompassing corporate security blueprints, performance monitoring, and architecture of security processes (Burkett, 2012).

The principal objective of establishing an ISA is to guarantee the synchronisation of business strategy and IT security, facilitating the linkage from business strategy down to the foundational technology layer. This not only underscores various potential advantages, including (Wahe and Petersen 2011):

- Improved communication of information security requirements.
- Well-documented security architecture can help improve communication between various individuals involved in managing information risk within an organisation.
- An overall architecture can help bridge the gap between IT personnel, information security practitioners and business representatives.
- Faster implementation of security projects within business requirements.
- Security architecture typically results in standard security controls that have been previously tested and approved for use within the enterprise.

Well-documented security architecture should be risk-focused by improving predictability and consistency in highlighting gaps in the provision of information security (e.g. exposed networks, inadequate protection of critical systems or single points of failure) and allowing corrective action to be taken. This may also help an organisation achieve any legal and regulatory compliance related to information security and information risk.

Effective security architecture will help individuals to make more comprehensive decisions about information security. ISA also supports scalable and granular budgeting, allowing for transparent processes while enabling full audit ability for effective expenditure.

The following guidelines and frameworks were selected for further exposition in this chapter due to the prevalence of usage in industry.

- Open Enterprise Security Architecture Framework [O_ESA] (Wahe and Peterson 2011) – O-ESA was selected as it focuses on functionality and technical security controls. This implies security architecture related tangible security functions such as access control, system hardening, security scans and security awareness.
- The Federal Enterprise Architecture Framework [FEAF] v2 (US Office of Management and Budget 2013) - FEAF serves as a conventional Enterprise Architecture (EA) framework, offering guidance for the amalgamation of strategic, business, and technology management architectural processes. Notably, FEAF is among the limited EA frameworks that explicitly incorporate an Information Assurance (Security) layer.
- Sherwood Applied Business Security Architecture Framework [SABSA] (SABSA Institute 2018; Sherwood et al. 2004) – SABSA was selected because it is overarching framework for an enterprise security architecture. It has a holistic approach, from business objectives to the source code level. This architecture layer model in SABSA is strong due to its simplicity and familiarity for people working in the information security industry. SABSA gives a good conceptual view of enterprise security architecture.
- Control Objectives for Information Technology [COBIT] v5 (Prislan and Bernik 2010) – COBIT is a more commonly used IT lifecycle control framework but the Security component offers an all-encompassing framework for seamlessly integrating security into business processes. Additionally, it furnishes a collection of facilitators that, upon implementation, contribute to securing stakeholder buy-in and effective business functioning.

2.5.1 The Open Group Enterprise Information Security Architecture (EISA)

The Open Group’s Enterprise Information Security Architecture Framework, described in Figure 2-3, defines a structured blueprint for the organisation’s information security programme. A fundamental facet of this framework is the clear demarcation between the components it encompasses and the processes it incorporates. Processes are characterised as a series of interconnected and interdependent procedures. At each stage of these processes, various resources like employee time, energy, machines, and funds are utilized to transform inputs, including data, materials, or parts, into specific outputs. These outputs subsequently function as inputs for the subsequent stage until a definite organisational objective is attained. Conversely, components signify tangible outputs and can, therefore, function as either inputs or outputs within this context.

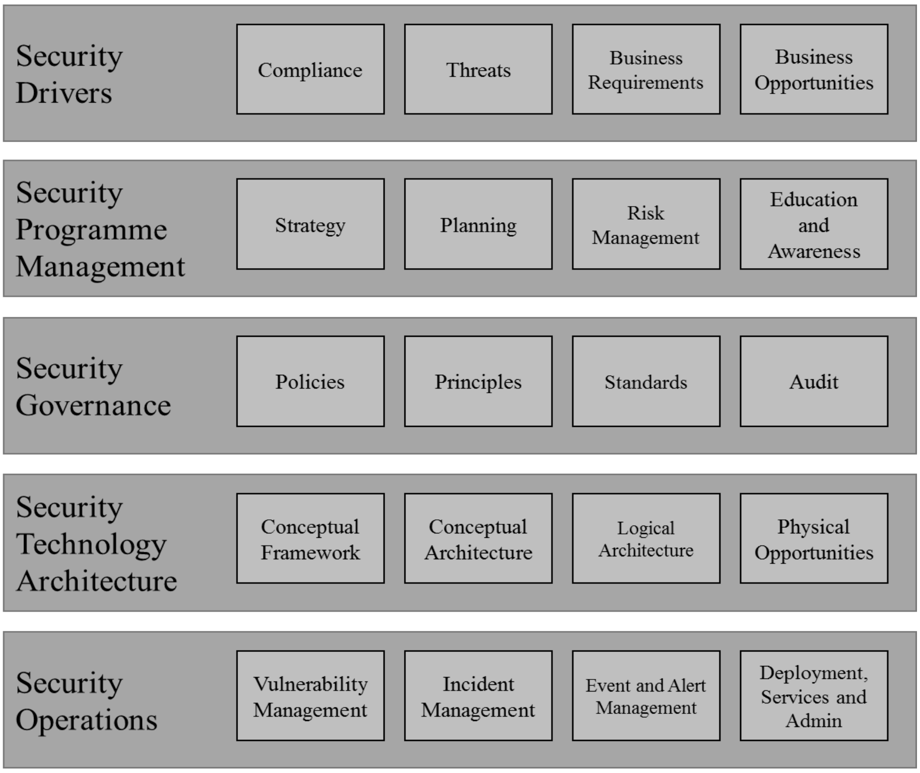


Figure 2-3 Adapted from The Open Group Enterprise Information Security Architecture Framework (Wahe and Petersen 2011)

The five areas of this framework are described as follows:

- **Security Drivers** – identifies the fundamental origin of security prerequisites that necessitate attention and resolution.
- **Security Programme Management** – offers comprehensive input to the security drivers and demonstrates the interrelation of these drivers within the entirety of the security program.
- **Security Governance** – furnishes overarching governance procedures and policies, succeeded by an elucidation of individual components and processes.
- **Security Technology Architecture** – describes the overall framework at the following four levels of abstraction:

    - Contextual Architecture: A universal technical framework encompassing policy-driven services.
    - Conceptual Architecture: A conceptual arrangement governing management judgement and strategy implementation across the range of security services.
    - Logical Architecture: The configuration and interconnections of pivotal components and services delineated within the conceptual architecture.
    - Physical Architecture: Identifies the arrangement of distinct products, illustrating the positioning and connectivity relationships necessary to ensure functionality, performance, and reliability while adhering to the logical architecture's limitations.
- **Security Operations** – describes the components and processes that make up security operations. This is also the environment where security is executed.

2.5.2 Federal Enterprise Architecture Framework (FEAF) v2

The purpose of the Federal Enterprise Architecture Framework (US Office of Management and Budget 2013) described in Figure 2-4, is to recognise and evaluate the necessary accomplishments for comprehending the principal catalysts for transformation. Subsequently, defining, confirming, and giving precedence to the mission and objectives occurs through collaboration with stakeholders and operational personnel. In this manner, the needs of stakeholders and operational imperatives are ratified, thereby aligning all stakeholder factions towards a shared, thoroughly comprehended, and endorsed outcome. (Ji and Xia 2007).

To initiate, preliminary performance metrics are established, aiming to ensure uniformity in gauging success across various stakeholder segments. Subsequently, a sponsor is designated for overseeing the planning endeavour, encompassing roles ranging from an executive leader to a functional head or an application owner. This step also serves the purpose of determining and involving suitable governance mechanisms.

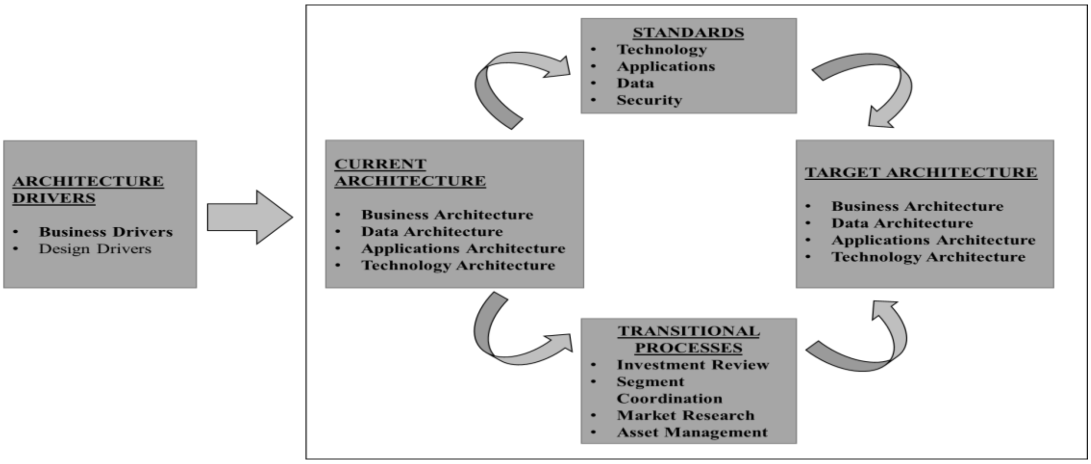


Figure 2-4 Adapted from the FEAF Architecture Framework (US Office of Management and Budget 2013)

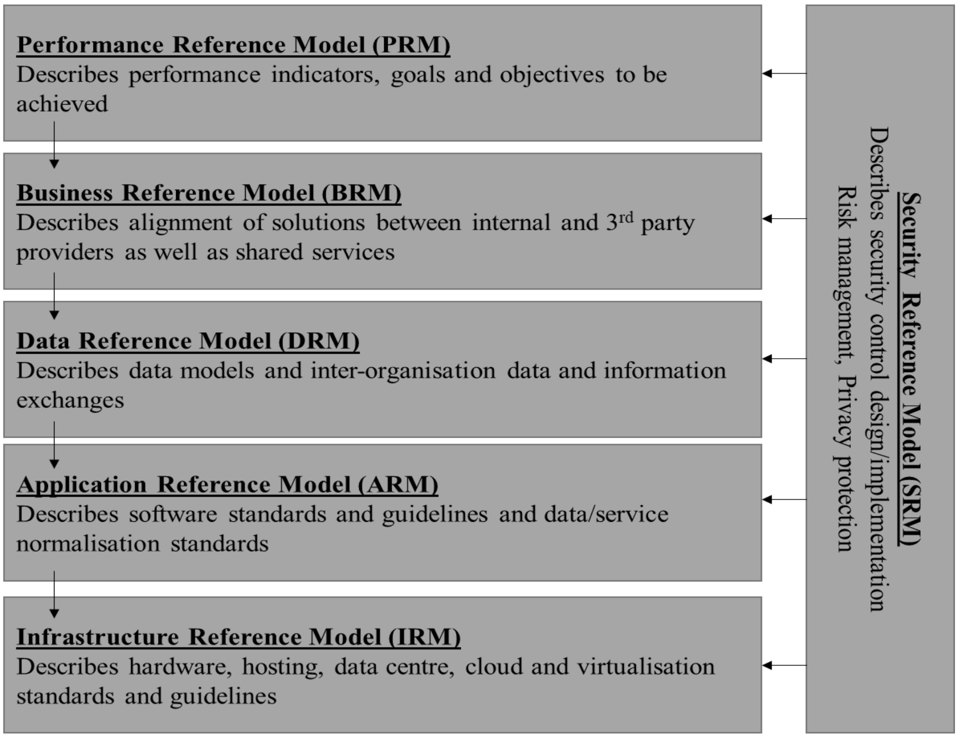

Performance Reference Model (PRM)
Describes performance indicators, goals and objectives to be achieved
Business Reference Model (BRM)
Describes alignment of solutions between internal and 3rd party providers as well as shared services
Data Reference Model (DRM)
Describes data models and inter-organisation data and information exchanges
Application Reference Model (ARM)
Describes software standards and guidelines and data/service normalisation standards
Infrastructure Reference Model (IRM)
Describes hardware, hosting, data centre, cloud and virtualisation standards and guidelines
Security Reference Model (SRM)
Describes security control design/implementation
Risk management, Privacy protection

Figure 2-5 Adapted from the FEAF Reference Model including Security (US Office of Management and Budget 2013)

This framework uses policy-driven security architecture in defining the security programme within a Security Reference Model, as depicted in Figure 2-5. This framework delves extensively into three primary constituents constituting the enterprise security architecture, namely:

- Governance

- Technology architecture
- Security operations.

The three major components are foundational structures described within the FEAF guidelines.

2.5.3 Sherwood Applied Business Security Architecture Framework (SABSA)

The Sherwood Applied Business Security Architecture Framework (SABSA), described in Figure 2-6, is an approach used for crafting risk-centric information security blueprints and providing security technology solutions that align to business onjectives. The central hallmark of the SABSA model is its foundation in deriving all aspects from an evaluation of security-related business necessities, particularly those that facilitate novel business prospects and their effective utilisation. (SABSA Institute 2018; Sherwood et al. 2004).

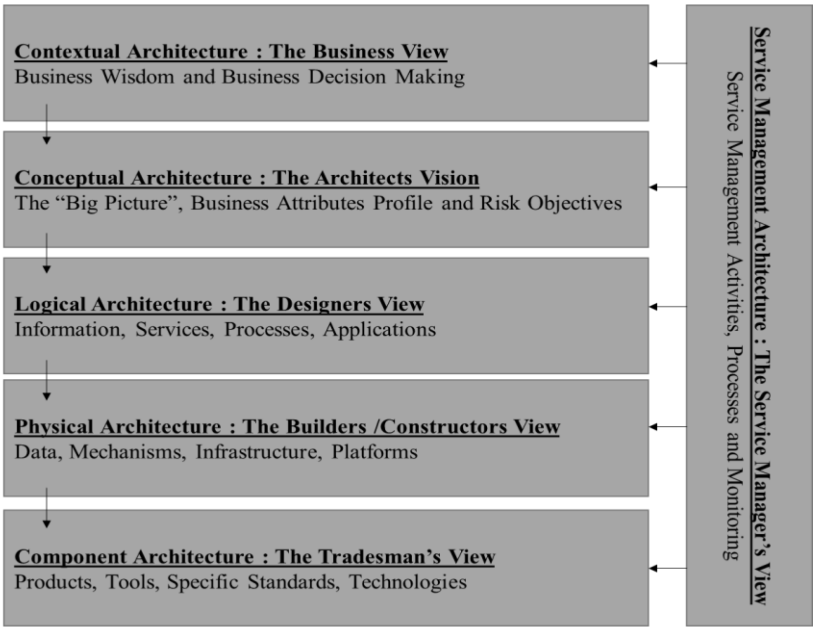

Contextual Architecture : The Business View
Business Wisdom and Business Decision Making
Conceptual Architecture : The Architects Vision
The "Big Picture", Business Attributes Profile and Risk Objectives
Logical Architecture : The Designers View
Information, Services, Processes, Applications
Physical Architecture : The Builders /Constructors View
Data, Mechanisms, Infrastructure, Platforms
Component Architecture : The Tradesman's View
Products, Tools, Specific Standards, Technologies
Service Management Architecture : The Service Manager's View
Service Management Activities, Processes and Monitoring

Figure 2-6 Adapted from the SABSA Security Architecture Framework (SABSA Institute 2018)

In the context of the Figure 2-6 the SABSA framework derives architectural artefacts from the each of components (e.g. Business Decision Making or Business Risk) of each of the views (e.g. The Business View). SABSA requires an artefact to be developed in the form of Assets (What), Motivation (Why), Process (How), People

(Who), Location (Where) and Time (When). SABSA therefore allows one to map their business and security landscape.

2.5.4 Control Objectives for Information Technology v5 (COBIT) for Information Security

COBIT 5 is a governance model for enterprise IT. COBIT 5 for Security introduces a better focus on information security rather than general IT Control Objectives related to the IT Lifecycle. This framework encompasses all facets involved in ensuring practical and fitting security measures for information assets. It is underpinned by a collection of principles on which an organisation should construct and assess security policies, standards, guidelines, processes, and controls. (Lepofsky 2014).

With COBIT 5 for Information Security, the benefit is that it fosters much tighter integration between disparate information security systems, processes, standards and conventions. This assists in cutting down complexity, reduces costs, boosts employee and customer satisfaction and leads to an elevated information security position and amplified levels of awareness across the organisation.

2.5.5 Summary of Information Security Architecture Frameworks

An Information Security Architecture Framework has been used as a common reference to describe ISA to achieve maximum value from information technology through achieving a balanced alignment between realising benefits, optimising risk levels, and efficiently utilising resources. In addition, various best practices have been used to facilitate ease of use and to improve the communication of information security requirements, enabling faster implementation of security projects considering business requirements; thus, facilitating more effective information security and information risk management.

In Sections 2.5.1 to 2.5.4, ISA was established as an essential technique for an organisation to appraise its information security effectiveness. In addition, it allows an organisation to plan for short-, medium- and long-term information security initiatives, which significantly assists in budgeting. O-ESA focused on functional and technical controls. This had a direct effect on the cost reduction and security assessment models developed in Chapter 4, wherein technical factors for cost reduction are key. O-ESA also had an impact on several evaluation areas within the developed framework that test the competency of an organisation against technical factors. SABSA focused on a holistic approach, from business objectives to the technical level, while COBIT provided a comprehensive framework for integrating security into business processes. This had a direct effect on the cost reduction and security culture models developed in Chapter 4 and contributed to the evaluation areas that relate to management intervention in information security and resources structures related to the security team.

In Chapter 4, a model describing the relationship between human interaction and information security architecture is developed. This model is also the basis for a key feature of the overall framework also developed in Chapter 4. This feature aims to evaluate whether an organisation is implementing a security architecture methodology and to what extent it is effective. The feature contains an evaluation area called Security Architecture (SECARCH) which is part of the Feature 1 (F1), described in the Security Framework, developed in Chapter 4.

2.6 INFORMATION SECURITY RISK MANAGEMENT

In most countries, organisations are required to adhere to some regulatory, compliance, or legislative requirements such as HIPAA (Herold and Beaver 2014) in the USA, GDPR in Europe (Zerlang 2017), POPIA in South Africa (Netshakhuma 2019), Sarbanes Oxley compliance (Kim et al. 2008) or PCI DSS (Wu 2018) in the financial services industry. Regulations do not define how organisations should protect their systems and data. However, it is expected that technical and process controls are implemented so that the organisation can provide relevant evidence when tested by auditors or regulators. In order to identify and treat findings related to the controls set out, using a risk assessment system is the general method used to detect and manage systemic risk (Tashi 2009).

IT staff are seen as responsible for addressing IT risk as these employees would hav ethe best understanding of the components of the computing environment (Schmittling 2015). IT security risk assessments are performed in order to evaluate the as-is security position of the organisation with a view to be able to determine security gaps that can be addressed. These gaps are then rated based on the effect on the organisation. The security risk analysis output is then used to obtain management commitment to address the related findings by allocating the relevant financial and human resources and identifying the relevant remediating technology (Tashi 2009).

Traditional risk analysis relies on skilled and practised judgment to identify risks, their causes and to determine the categorisation of risk in terms of likelihood and consequence. Consequently, the results of such risk analysis are contingent upon the participants' background, experience, and knowledge. When analysts do not have the requisite knowledge and experience this can lead to uncertainty regarding the validity of the findings (Erdogan, Nguyen, Seehusen, Stølen, Hofstad and Aagedal 2019).

To address this uncertainty, security risk analysis can be augmented with alternative methods of gathering relevant information (Bahit and Regragui 2013). An approach to tackle this challenge involves integrating security risk analysis with security testing, where the testing process is utilised to verify and refine the results of the risk analysis. This methodology is known as test-driven security risk analysis. (Everett 2011). Information security risk management is a process developed or adapted to determine the appropriate level of risk to ensure optimum management and technical controls. To achieve set information security risk management objectives, a defined set of processes and activities that needs to be executed is applied (Everett 2011). An example of a comprehensive risk management framework is the IS0 27005 Standard depicted in Figure 2-7 (Fenz, Heurix, Neubauer and Pechstein 2014). Risk Assessments are performed to determine the information security position of an organisation. Different information processes are assessed using different types of risk assessment techniques. An Information Risk Assessment process encompasses the steps described in Table 2-6.

Table 2-6 Risk Assessment Steps (Prislan and Bernik 2010)

1.Information Asset Classification	2.Threat Identification	3.Vulnerability Identification
4. Control Analysis	5.Likelihood Determination	6. Impact Analysis

7. Risk Determination	8.Control Recommendations	9. Results Documentation

Risk evaluation and treatment is a process, as described in Figure 2-7, of selecting and implementing measures and controls to manage risks to an adequate level. The following considerations are taken concerning risks; these will then inform the risk treatment strategy and the treatment plan:

- Evaluate current controls in place
- Evaluate cost benefits
- Evaluate risk level on the risk chart (tolerance = probability versus impact)
- Evaluate actions that can be taken if the risk occurs
- Evaluate other controls that can be taken as a precautionary measure

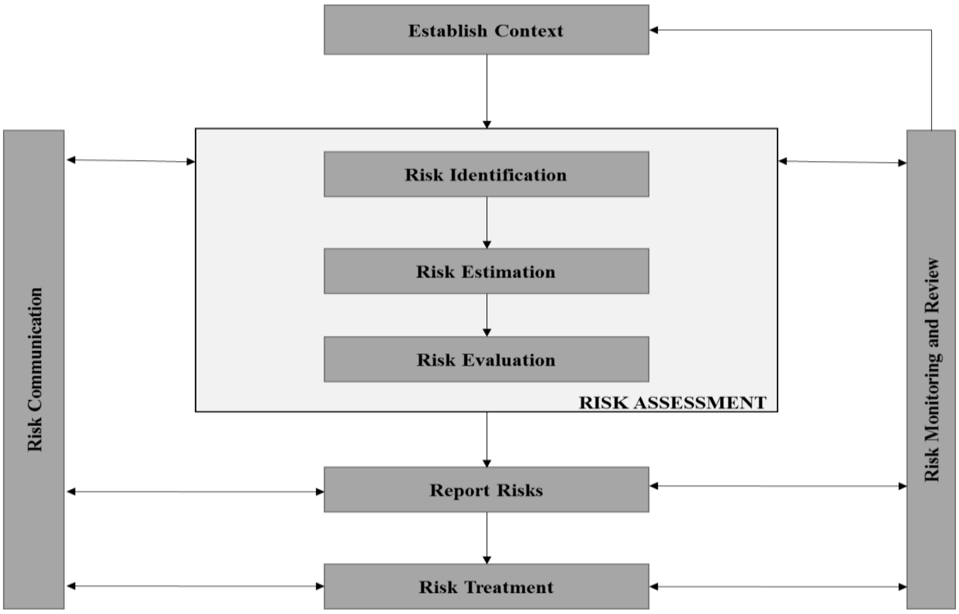


Figure 2-7 Adapted from the ISO 27005 Information Security Risk Management Methodology (Prislan and Bernik 2010)

The risk evaluation process will inform the decision on what action to take. The following actions are possible options (Alshahrani 2022):

- Manage: Managing risk implies implementing controls to reduce risk levels. Control implementation is dependant on the availability of resources (human, cost and time). Based on available resources an organisation may determine to what level risk may be reduced.

- Transfer: Where risk cannot be managed by an organisation risk may be transferred. An example may be the purchase of insurance to be able to transfer the risk to the underwriting organisation.
- Avoid: Avoiding risk is when measures or procedures are taken to completely circumvent risk. Implications such as cost and complexity of avoidance measures need to be considered in order to avoid risks.
- Accept: Accepting risk implies that no controls will be implemented to reduce risk. When accepting risks no plans or actions will be undertaken.

The treatment plan is a living document and needs to be continuously monitored (Alshahrani 2022). The plan and actions are monitored and reviewed as few risks remain static. Monitoring can be done in many ways, such as inspections, review of the strategies, internal audits, feedback and debriefing sessions.

Information security risk communication will happen continuously amongst the different stakeholders such as lines of business and the Information Security Services division in collaboration with the Chief Risk Officer.

Information security risk management is a traditional reactive method of understanding information security risks and planning to treat those risks. It is reactive in that the scoping and planning of the risk assessment is defined in advance of the action of the assessment. Due to the requirement of specialised skills and limited budgets, this type of assessment does not address zero-day threats and the fast-changing security threat landscape. However, it is still a valuable tool that can be used to improve information security management in an organisation.

One feature of this study is to evaluate whether an organisation is aligning its risk assessment methodology to information security risk management practices and to what extent and whether it is effective. The evaluation area is called Risk Assessment (RSKASSESS) which is part of Feature 1 (F1), described in the Security Framework, developed in Chapter 4.

2.7 NATIONAL CULTURE

Defining the culture of a nation is a complex task due to the presence of various ethnic, social, and political groups, resulting in substantial cultural diversity within the nation. (Oliver 2011). Moreover, in an era of increased globalisation and movement of people worldwide, individuals are more aware of cultural distinctions than ever before. Despite these differences, both governments and businesses are compelled to participate in the global economy. Consequently, there is an increasing interest with comprehending the influence of national culture on organizations. (Oliver, 2011).

Hampden-Turner (1990) has presented prevalent culture models, but the most prominent, rigorously tested, and widely replicated model regarding cultural values that potentially affect businesses is credited to the research of Geert Hofstede. Hofstede identified four cultural dimensions—individualism/collectivism, power distance, uncertainty avoidance, and masculinity/femininity (Hofstede 1994)—that can substantially shape the business landscape. His cultural dimensions emerged from comprehensive research involving employees in 50 countries (Hofstede 2001). Hofstede emphasizes that national cultural variations have a lesser impact on activities dictated by technical necessity (Hofstede 2001). This suggests that fields like information management might not be significantly influenced by national culture.

2.7.1 The Influence of National Culture on Organisations

Numerous studies, including Hofstede's seminal work (1994), a Serbian replication of Hofstede's study (Dusan 2004), and extensive undertakings like the GLOBE study (House, Hanges, Javidian, Dorfman, and Gupta 2004), have established a correlation between organisational culture and national culture. The extent of national culture's impact on organisational culture varies in different circumstances, but empirical evidence from these studies indicates percentages ranging from 7 to 23 percent. National culture also directly affects the workplace's learning capacity (Kim and Mclean 2014), subsequently influencing innovation and organisational growth. Marquardt, Berger, and Loan (2004) contend that the considerable influence of national culture on learning emerges due to nations fostering strong integrative forces across language, mass media, laws, education, politics, sports, and the economy. Research has also demonstrated that managerial personnel are less impacted by national culture compared to operational staff members (Kim and Mclean 2014; Dusan 2004). This phenomenon can be attributed to the fact that management personnel are predominantly moulded by senior members who actively shape and guide the organisational culture. Conversely, operational staff are more profoundly affected by the "clan culture," signifying the sub-culture of the nation or group to which they belong (Nazarian et al. 2013). Across various studies, the primary and consistent finding regarding the impact of national culture is that its influence level remains stable over the long term (Nazarian et al. 2013; Dusan 2004; Van Muijen and Koopman 1994).

2.8 ORGANISATIONAL CULTURE

Organisational culture has its theoretical roots in understanding a business from a human resource, organisational climate, national culture and business structure point of view (Brown 1998). Organisational culture can be considered to be a shared system of behaviour or values that distinguish one organisation from another (Martins and Martins 2002). This perspective emphasises that culture is primarily shaped by repetitive behaviours or habits while downplaying the significance of people's feelings, thoughts, or beliefs (Watkins 2013). However, national culture can and does have a significant impact on people’s behaviour within an organisation (Van Muijen and Koopman 1994). Organisational culture can be considered to be the unique norms, beliefs, principles, and behaviours that come together to form the distinct character of each organisation (Arnold, Randall, Patterson, Silvester, Robertson, Cooper, Burnes, Swailes, Harris, Axtell and Harthog 2010). Organisational culture coalesces over some time and is a manifestation of the historical tendencies of an organisation (Brown 1998).

In terms of defining organisational culture, the length and breadth of research have distinguishing points of view on what and how culture impacts an organisation. The majority of definitions follow the premise that an organisation may be a machine or organism that evolves through cultural practice, while others believe that an organisation is its culture and all systems and practices stem from that culture (Brown 1998). These beliefs are contrasted by research that suggests that culture is determined by an employee’s basic assumption or predisposed ideas (Schein 2009).

Ultimately, the common practices, individual psychology and internal learning of the organisation lead to organisational culture. The elements that Brown (1998) defines support this. These elements are as follows:

- Artefacts encompass the entire physical and socially constructed environment of a company. Some examples of artefacts include policies, procedures, operational guidelines, corporate buildings, furniture, and equipment.
- Language serves as the shared means through which an organisation assesses and comprehends the world it operates in. Examples of language in this context encompass anecdotes, descriptions, stories, and traditions.
- Behaviour patterns refer to the customary routines of behaviour that become ingrained in the organisational life. These patterns encompass rites, rituals, ceremonies, and celebrations.
- Norms of behaviour are guidelines and procedures that govern how employees are expected to behave, defining what is deemed appropriate and inappropriate in their responses. As time passes, employees collectively arrive at a consensus on how to address company issues, leading to the establishment of these norms.
- Heroes are employees who make success possible, motivate other employees, provide leadership and direction and provide positive insight to external parties.
- Symbols and symbolic actions are the language, outputs, environment and features of an organisation, which employees can identify with. Examples of symbols are corporate logos, marketing style and products.
- Beliefs, values and attitudes. Values are the morals, ethics, ideals and principles closely linked to an organisation to which employees should align their value system. Beliefs, however, refer to what employees perceive is and is not true. Finally, attitudes link values and beliefs with feelings.
- Basic assumptions are assumed explanations to an identifiable problem. Basic assumptions guide employee’s insight, intuition and emotions about functions and features of the workplace.
- History. Through the continued historical process of learning, unlearning and adding new information, culture is developed.

The relationship between these elements, as noted by Schein (2009), is depicted in Figure 2-8.

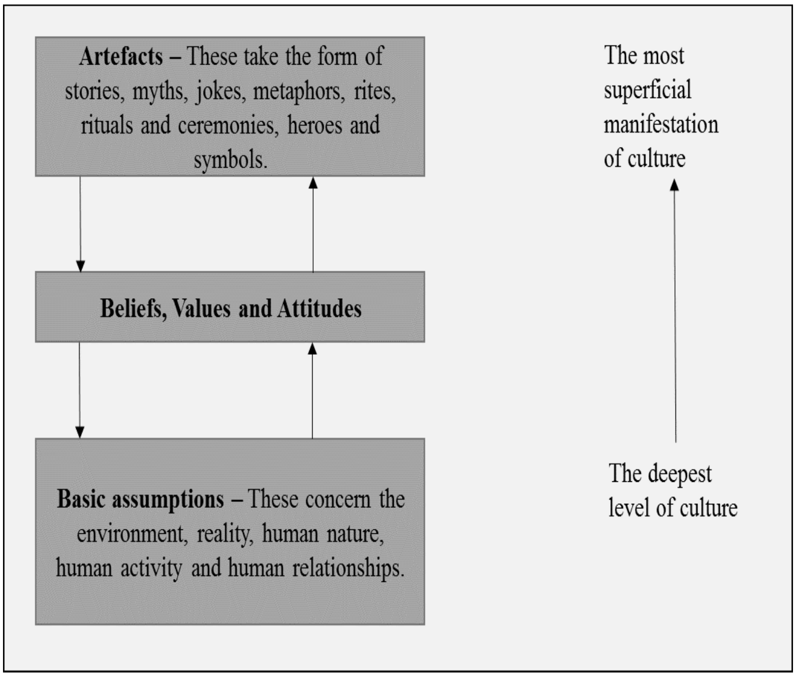

Artefacts – These take the form of stories, myths, jokes, metaphors, rites, rituals and ceremonies, heroes and symbols.
Beliefs, Values and Attitudes
Basic assumptions – These concern the environment, reality, human nature, human activity and human relationships.
The most superficial manifestation of culture
The deepest level of culture

Figure 2-8 Culture Relationship Model (Schein 2009)

It must be noted that there may also be a fundamental difference between the espoused culture and the culture actually practised within an organisation. In some cases, the outward public personae of the company is the ideal culture or the desired state of the organisation, while internally, employees may have different values (Brown 1998). As a result, companies and employees find contradictions or inconsistencies between what they hear or read about the company and what they experience on a day-to-day basis.

Furthermore, the culture within an organisation may be fragmented. Groups, individuals or job levels may coalesce to form sub-cultures. Sub-cultures may form around particular disciplines.

2.8.1 Drivers of Organisational Culture

According to Brown (1998), the three primary drivers of organisational culture are as follows:

- The societal or national culture in which the organisation is physically located.

- The vision, management style, and personality of the organisation's founder or dominant leader.
- The type of business the organisation engages in and the nature of its operations.

The foremost leader of the determinants and influence of national and societal culture has been Hofstede (1994, 2001). His studies summarise the four national or societal factors that have an impact on organisational culture.

- **Power distance** This pertains to the extent to which less influential members within an organisation either acknowledge or expect the allocation of power. In low power distance nations, power is shared and inequalities are minimised. In high power distance nations, inequalities are desirable and power is centralised.
- **Individualism/collectivism** – This factor relates to whether people within a nation are predisposed to function as independent individuals or cohesive societies. People in individualist societies tend to look after themselves; hence, organisation decisions are structured around skills and rules. On the other hand, people in collectivist societies tend to be individuals that typically become integrated into unified in-groups and receive protection in return for displaying unwavering loyalty.
- **Masculinity/femininity** – This relates to the degree that gender influences that society. For example, in high–masculine societies, the focus is on material success, competition and a live-to-work ethos. In high feminine societies, the focus is on overlapping gender roles, quality of life, compromise and negotiation.
- **Uncertainty avoidance** – This factor pertains to the level of comfort or discomfort individuals in a nation experience in the face of uncertain or unfamiliar circumstances. In cultures with weak uncertainty avoidance, people are generally unaffected by uncertainty or ambiguity in their work environment. People only work when it is necessary and precision and punctuality are not common. In high uncertainty avoidance cultures, people fear ambiguity and work towards being precise, punctual and highly motivated.

Through these dimensions, further studies prove that national or societal culture may have an effect on the implementation of IT programmes (Twati 2006), or have an impact on performance and organisation absenteeism (Peretz and Fried 2012) or, more importantly, in the context of this study, have an impact on the success of security programmes (Khalil 2011). This dimension of national culture and its influence on organisational culture are discussed in a related section.

When one considers organisational culture, one first thinks that the state of leadership and the values they espouse are directly related to such culture. In several studies, the source of culture has proven to be directly related to leadership (Schein 2009; Davis 1984). Organisational cultures demonstrated a favourable connection with leadership conduct and contentment in work. Additionally, leadership behaviour displayed a noteworthy and positive association with job satisfaction (Tsai 2011). This type of leadership, namely transformational leadership, also impacts organisational performance by nurturing the growth of organisational education and improvement (García-Morales, Jiménez-Barrionuevo and Gutiérrez-Gutiérrez 2012).

The influence and goals of leaders, especially in the infancy of an organisation, can set the path towards the ultimate culture. Stronger leaders tend to have a stronger impact on culture and relevant to this study, this has been tested in technology firms (Chatman, Caldwell, O'Reilly and Doerr 2014).

How an organisation conducts business and the type of business can impact corporate culture (Deal and Kennedy 1982). Public services versus private companies conduct business in different ways and culturally are significantly different. In comprehensive studies of emerging markets, it was found that organisational culture directly impacts market responsiveness and that each industry type influences organisational conduct and culture (Wei, Samiee and Lee 2014).

2.8.2 Development of Organisational Culture

The influential factors of organisation culture development are easily summarised in two areas, namely trauma and positive reinforcement (Schein 2009).

People in an organisation tend to act to reduce any work-related negativity or anxiety (Brown 1998). Uncertainty and ambiguity are prevalent in any organisation and people tend to find generally acceptable solutions to relieve the traumatic effect of this situation. These solutions formulate as a culture over time. Brown (1998) also advises that because trauma-based learning is psychologically rewarding, it is challenging to undo.

People learn from negative and positive feedback but tend to repeat the actions related to positive feedback (Brown 1998). Therefore, traits and values that are perceived to be beneficial to the desired organisational culture can be developed in staff members by rewarding staff for those behaviours.

2.9 INFORMATION SECURITY CULTURE

Information Security is indispensable for the survival and success of organisations, emphasizing the necessity of safeguarding their valuable information assets. A considerable portion of the procedures essential for the protection of these assets relies heavily on collaborative human behaviour (Garrett 2004). However, the prevailing approach tends to prioritize addressing information security issues through technological means, often sidelining the involvement of individuals who could champion the cause (Gupta and Sharman 2008). Whether through conscious intent or unintentional oversight, employees, often due to limited awareness, emerge as the foremost threat to information security (Mitnick and Simon 2003). . Studies highlight that a substantial majority of data breaches trace back to human actions. There are several potential reasons for this (Garrett 2004):

- Individuals receive inadequate training and possess limited security consciousness.
- People lack the drive to meet the necessary performance standards.
- There exist individuals with malicious intent who intentionally jeopardise the organisation's security.

• Awareness of security issues exists among individuals, yet both managers and employees consistently make suboptimal decisions.

Hence, individuals, along with their conduct, mindset, and cultural norms, need to be seamlessly integrated as a fundamental defence within the realm of information security. (Rotvold 2008).

The management of the human response to information security risks has been established to be a factor of an organisational sub-culture of information security. Therefore, understanding this sub-culture is key to managing employees' information security behaviour (Van Niekerk and Von Solms 2010). Access to their information resources is indispensable for the functioning of numerous organisations. Nonetheless, safeguarding these resources usually does not yield a direct return on investment. As a general rule, securing information resources does not generate income for an organisation, despite its criticality in conducting business operations (Wylder 2003). Therefore, business people are rarely interested in how their information resources are protected (Van Niekerk and Von Solms 2010).

Organisations are aware of the immense business value of information assets and maintain the validity and integrity of those assets. In order to place more rigour and value in the protection of those assets, organisations are creating or elevating CIO or CISO roles to executive committee roles to integrate information security planning into the strategic management process (Garrett 2004). However, the development of information security culture is not generally solved by senior leadership to subordinate management approach. Employees' usage of technology, the complexity of the organisation's technology landscape, the rapid changes and uptake of new technology and the associated controls, which must be implemented to improve information security, are complex issues. Human attributes like learned biases, unique social traits, and cognitive abilities exert a significant impact on the efficacy of information security management (Parsons, Mccormac, Butavicius and Ferguson 2010). Moreover, individual biases and personal encounters sway people's assessment of risk, subsequently influencing their security-related choices (Parsons et al. 2010). Comprehensive comprehension of information security risks and active employee engagement play pivotal roles in fortifying an organisation's security stance. In cases where an organisation lacks a robust security culture, even substantial technological security provisions may prove insufficient (Siponen 2001).

2.9.1 The Human Factor of Information Security Culture

To develop and maintain effective information security, an organisation’s progress of an information security culture is necessary (Thomson et al. 2006; Eloff and Von Solms 2000). However, corporate culture has a significant influence; therefore, information security culture cannot be assessed in isolation (Ruighaver, Maynard and Chang 2007). As noted in Section 2.8, sub-cultures may be formed, which are a split in organisation culture. Sub-cultures can differ across professional levels, job functions and individual roles, resulting in differing attitudes, beliefs and values (Hampden-Turner 1990). Various sub-cultures can either completely align, partially align, or be completely incongruent with the corporate culture (Martin and Siehl 1983). The presence of diverse sub-cultures within an organisation can pose challenges and have detrimental effects on performance, particularly when these sub-cultures hold contrasting priorities and agendas (Furnham and Gunter 1993).

Elements that affects information security sub-cultures is the way staff members perceive business risk. Parsons et al. (2010) summarise these elements as:

- **Availability Heuristic** – This represents a perceptive bias where employees tend to assess risk based on the rate of recurrence or probability of an issue. As time passes, recurrent risks may be perceived as less significant, leading to an underestimation of the severity of risk (Lichtenstein, Slovic, Fischhoff, Layman and Combs 1978), while under-reported risks or risks that are perceived to have no severe impact will also be underestimated. An example, in terms of information security, is if the recurrence of security incidents and alerts are not shared with employees, they may believe that there is little risk of a security breach within the organisation, which may lead to employee perceiving a lower security risk level (Parsons et al. 2010).
- **Optimism Bias** – Relates to the perception of employees risk affects others and not themselves (Gray and Ropeik 2002). This bias is particularly relevant in the context of information security as people tend to believe that the information they retain is not valuable to attackers while information their peers hold might make them more valuable targets (McIlwraith 2016). People tend to disregard that attackers may just use their information as a foothold to

compromise further systems or escalate their level of access to systems of value (McIlwraith 2016).

- **Level of Control** – This element relates to the perception that information within their control is less risky (Kreuter and Strecher 1995). An example of this in the context information security, is that users would believe that actions conducted on their personal laptops are less risky than if they performed the same actions on a corporate laptop. This leads to people conducting riskier actions on trusted electronic equipment.
- **Level of Knowledge** – Limited knowledge about information security can have an effect on a user's ability to evaluate risk. When information security knowledge is limited this can affect risk perception and actions taken when using computing devices (Fischhoff 2002). This implies that many users will not understand the technical implications of using particular technology and therefore they are not aware of what being "secure" means (Lacohee, Phippen and Furnell 2006).
- **Risk Homeostasis** – This element focuses on how people compensate for risk as the risk severity increase or decreases. An example of this is where users may conduct riskier actions, when more severe business process limitations are implemented, in order to bypass controls.
- **Cumulative Risk** - This element focuses on the fact that many risks are aggregated over time. Many small risks taken by employee may lead to a major risk in time. (Fischhoff 2002).
- **Omission Bias** – This element pertains to the perspective individuals hold, which favours inaction over making an erroneous response to risk. For instance, within the domain of information security, the illustration of choosing not to regularly alter a password compared to jotting down new passwords each time exemplifies the concept of omission bias.
- **The Influence of Familiarity** – This element is tied to the extent of people's familiarity with a specific risk. The greater the familiarity individuals have with the risk, the more likely they are to exhibit complacency when confronted by that risk.
- **The Influence of Framing** – This element concerns the way a risk is presented to an individual. When a risk is framed with a focus on potential losses,

individuals might become more inclined to take risks. Conversely, if the emphasis is on potential gains, individuals may perceive there's more at stake. Consider the scenario of conveying information security risks from a loss perspective – for instance, providing employees three passes as an alternative to losing their job if they fail to lock their computers. In such cases, individuals are less likely to consistently lock their computers.

- **Personality and Cognitive Style** – This element is linked to an individual's personality and cognitive approach, influencing their interpretation of the risks they encounter (Lion and Meertens 2005). People can be categorised based on their risk inclination, ranging from those who are extremely cautious about risks to those who actively seek out risk (O'Neill 2004). Their inclination toward embracing risk has a bearing on how they handle information and subsequently, impacts their approach to information security.
- **The Influence of Social Factors** – This element concerns the impact of groupthink on individuals. Taking this into account, if a person is a member of a group characterizsed by a robust information security culture, it will affect the individual's stance on information security culture.

2.9.2 Information Security Culture Frameworks

Studies in information security culture are inherently based on organisational culture models (Parsons et al. 2010; Van Niekerk and Von Solms 2010; Kuusisto and Kuusisto 2008). In reviewing the literature on culture frameworks, it was found that there are a limited number of models discussing the relationship between organisational culture and information security culture. In this section, two conceptual models, which evaluate that link, are considered to use as a basis to expand as part of this study.

Van Niekerk and Von Solms Security Information Security Culture Framework

In the Van Niekerk and Von Solms (2010) framework, Schein's (1999) model of organisational culture is adopted. This model summarises culture in three layers:

- **Artefacts** – Artefacts represent the visible components of an organisation's culture. They encompass tangible elements that are perceptible through sight, sound, or touch, and they hold the potential to exert both positive and negative influences on individuals (Schein 2009). Nevertheless, solely analysing these artefacts doesn't provide a comprehensive grasp of the underlying layers of culture (Schein 2009).

- **Espoused Values** – The espused values of an organization provide a more profound significance to its artefacts. These values elucidate the reasons behind the existence of these artefacts and imbue them with purpose and significance.
- **Shared Tacit Assumptions** - The shared tacit assumptions within an organisation are beliefs that originate in its early stages due to the success of specific strategies (Schein 2009). As these strategies stand the test of time, they evolve into the convictions and principles held by the organisation's members. Gradually, these implicit assumptions disseminate throughout the organisation, shaping the core of its culture.

Van Niekerk and Von Solms extend Scheins' layers to consider gauging the effectiveness of information security, with the "human factor" being a key aspect. Consequently, a robust information security culture hinges on the depth of knowledge about information security. This model is depicted in Figure 2-9.

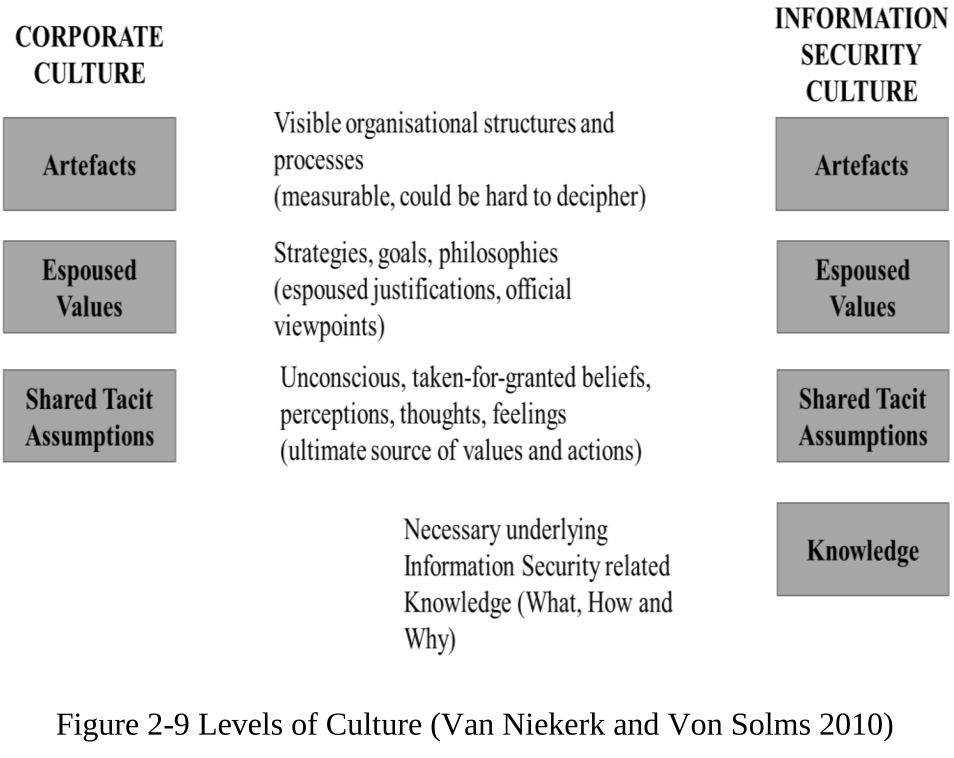

CORPORATE CULTURE
INFORMATION SECURITY CULTURE
Artefacts
Visible organisational structures and processes (measurable, could be hard to decipher)
Artefacts
Espoused Values
Strategies, goals, philosophies (espoused justifications, official viewpoints)
Espoused Values
Shared Tacit Assumptions
Unconscious, taken-for-granted beliefs, perceptions, thoughts, feelings (ultimate source of values and actions)
Shared Tacit Assumptions
Necessary underlying Information Security related Knowledge (What, How and Why)
Knowledge

Figure 2-9 Levels of Culture (Van Niekerk and Von Solms 2010)

Expanding on the concept of economic elasticity, this enriched model assesses how alterations in interconnected variables lead to changes in one variable. Drawing from this principle, Van Niekerk and Von Solms propose a conceptual framework for information security that builds upon this notion, which:

- measures the baseline level (BL) of the effect of security culture in an organisation, which is the minimum accepted level.
- measures the nett security level (SL), which is the effect of security culture at the current level.
- develops artefacts (AF), which measure the strength of the level of security culture artefacts.
- develops espoused values (EV), which measure the strength of the level of espoused security culture values.
- shares tacit assumptions (SA), which measure the strength of the level of shared tacit security culture assumptions.
- knowledge representation (KN), which defines the level of information security knowledge of employees.

The framework is depicted in Figure 2-10

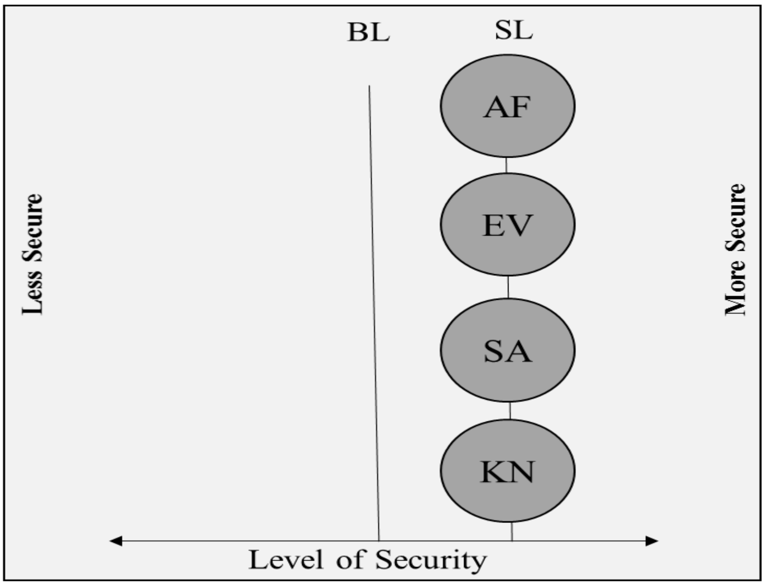


Figure 2-10 Basic elements of the conceptual framework (Van Niekerk and Von Solms 2010)

Ruighaver's Security Culture Framework

The framework by Ruighaver et al. (2007) expands and adapts Detert, Schroeder and Mauriel's (2000) organisation culture framework, which divides culture into eight dimensions. The eight dimensions are as follows:

- **The Basis of Truth and Rationality** – This dimension pertains to how employees perceive the authenticity of security beliefs and practices. The cultural dimension within this context suggests that when employees witness their peers embracing a positive security culture, they develop a belief that protective measures for the organisation are being executed effectively.
- **The Nature of Time and Horizon** – This dimension centers on the organisation's security orientation across short, medium, and long-term horizons. The more forward-thinking and visionary the security strategy is, the more pronounced its impact on shaping the security culture becomes.
- **Motivation** – This dimension this aspect is linked to the motivation of employees to embrace secure behaviours and practices. Employing positive reinforcement can effectively incentivise staff and elevate the overall security culture.
- **Stability vs Change** – This dimension advocates for the importance of change management in embracing the organisation's security culture. Incorporating innovation and consistently evolving the security program contribute to cultivating an elevated security culture.
- **Orientation to Work, Tasks and Co-Workers** – This dimension pertains to the sense of ownership and accountability employees have towards their roles and positions within the organisation. It also encompasses their connection and interaction with their employer.
- **Isolation vs Collaboration/Cooperation** – This dimension addresses whether an organisation promotes or undermines collaborative work behaviour.
- **Control, Coordination and Responsibility** – This dimension concerns the extent to which management control is enforced and whether employees operate autonomously or are constrained by formal procedures.
- **Orientation and Focus** – This dimension centers around whether an organisation is impacted by external factors, such as customers or consumers, or whether its decisions are shaped by its internal dynamics and operations.

2.10 MOTIVATION, POSITIVE REINFORCEMENT AND REWARD

Motivation can be defined as a complex process driven by individual, socially driven, mental and emotional factors further contextualised by a person’s lived experience (Kanfer, Chen and Pritchard 2008). People are influenced by psychological and environmental factors, which implies external and internal stimulus to motivation (Malik, Butt and Choi 2015). Employees are not naturally motivated to adopt secure practices and therefore, adopting and practising secure culture is of great importance.

Motivation can be described in the following general groupings (Hendijani, Bischak, Arvai and Dugar 2016):

- Intrinsic motivation is developed based on a person’s interests in an activity and, consequently, drives their pursuit in the successful completion of that activity.
- Autonomous motivation arises from an individual's recognition of the significance or meaning of engaging in an activity.
- Introjected motivation arises from a personal desire or need to complete an activity in order to demonstrate achievement, even if the person doesn't inherently value that activity.

Rewards in the variability of arrangements are used to stimulate people and enhance their work performance (Eisenberger and Aselage 2009; Bartol and Durham 2000). Thus, rewards are one of the key external drivers of motivation.

Positive reinforcement is an approach that introduces incentives and rewards to inspire and reinforce new behaviour (Catania 2001). Examples of rewarding employees for pursuing positive reinforcement are work promotions, company benefits, verbal and written commendations or improved salaries. Intrinsic and extrinsic are the two categories of rewards. An intrinsic reward is that which is intangible such as commendation or recognition of work well done. Extrinsic rewards are tangible such as improved pay, bonuses and additional leave days. Intrinsic and extrinsic rewards are intimately linked with the achievements of employees within an organisation (Wei and Yazdanifard 2014).

2.10.1 Extrinsic Reward

Extrinsic motivation involves the inclination to complete a task in order to attain an outcome beyond the task itself (Deci, Koestner and Ryan 2001). Rewards that stimulate extrinsic motivation among employees are referred to as extrinsic rewards. These rewards align with extrinsic motivation, encompassing tangible offerings for employees, such as salary increments or additional perks. A fundamental drive for individuals in their work is the receipt of a salary, which has a direct correlation with job satisfaction. (Malik et al. 2015; Linz and Semykina 2012). Studies in the US and Taiwan (Hübner and SchÏsser 2010; Liu 2010; Schuster, Weatherhead and Zingheim 2006) demonstrate that robust extrinsic rewards are associated with heightened productivity, attentiveness, and effectiveness in work performance. Eisenberger and Aselage (2009) found that creative work performance can also be positively affected by extrinsic rewards. Additionally, Cerasoli, Nicklin and Ford (2014) and Garbers and Konradt (2014) discovered that extrinsic rewards exhibit a positive correlation with tangible enhancements in performance..

2.10.2 Intrinsic Reward

Intrinsic rewards pertain to non-monetary sources of motivation and encompass verbal or written commendation, task delegation, empowerment, and recognition (Howard 2008; Sonawane 2008). These rewards are straightforward to implement yet wield a positive influence on employee performance (Wei and Yazdanifard 2014). Research conducted by Gohari, Ahmadloo, Boroujeni, and Hosseinipour (2013), as well as Shiraz, Rashid, and Riaz (2011), underscores that intrinsic rewards contribute to employees feeling valued and aligned with a shared purpose within the organisation. This, in turn, translates to enhanced job performance, increased customer satisfaction, and heightened employee commitment to the organisation (Elloy 2012; Sarwar and Khalid 2011).

2.11 SUMMARY

In Section 2.1, it was established that the implementation and management of information security technology and processes are of great importance in reducing the risk of an organisation to function. Unfortunately, data breaches are more frequent and more public than ever before due to the proliferation of devices and computing mobility.

Section 2.2 discussed information security cost models. These models are generally aligned to business costing principles, but it is challenging to align costs to business functions due to information security risks spread across the business. Information security cost is also determined through risk analysis, security assessments (including security architecture), information security technology and services implementation. Cyber security resources are also scarce, which drives the cost of such resources up and increases the overall cost of information security management.

Section 2.3 focused on implementation science. In order to evaluate implementations, constructs must be created. These can be in the forms of theories, models or frameworks. This discussion assists in understanding the models and frameworks evaluated later in Chapter 2 and forms the theoretical basis for the models and frameworks developed in Chapter 4.

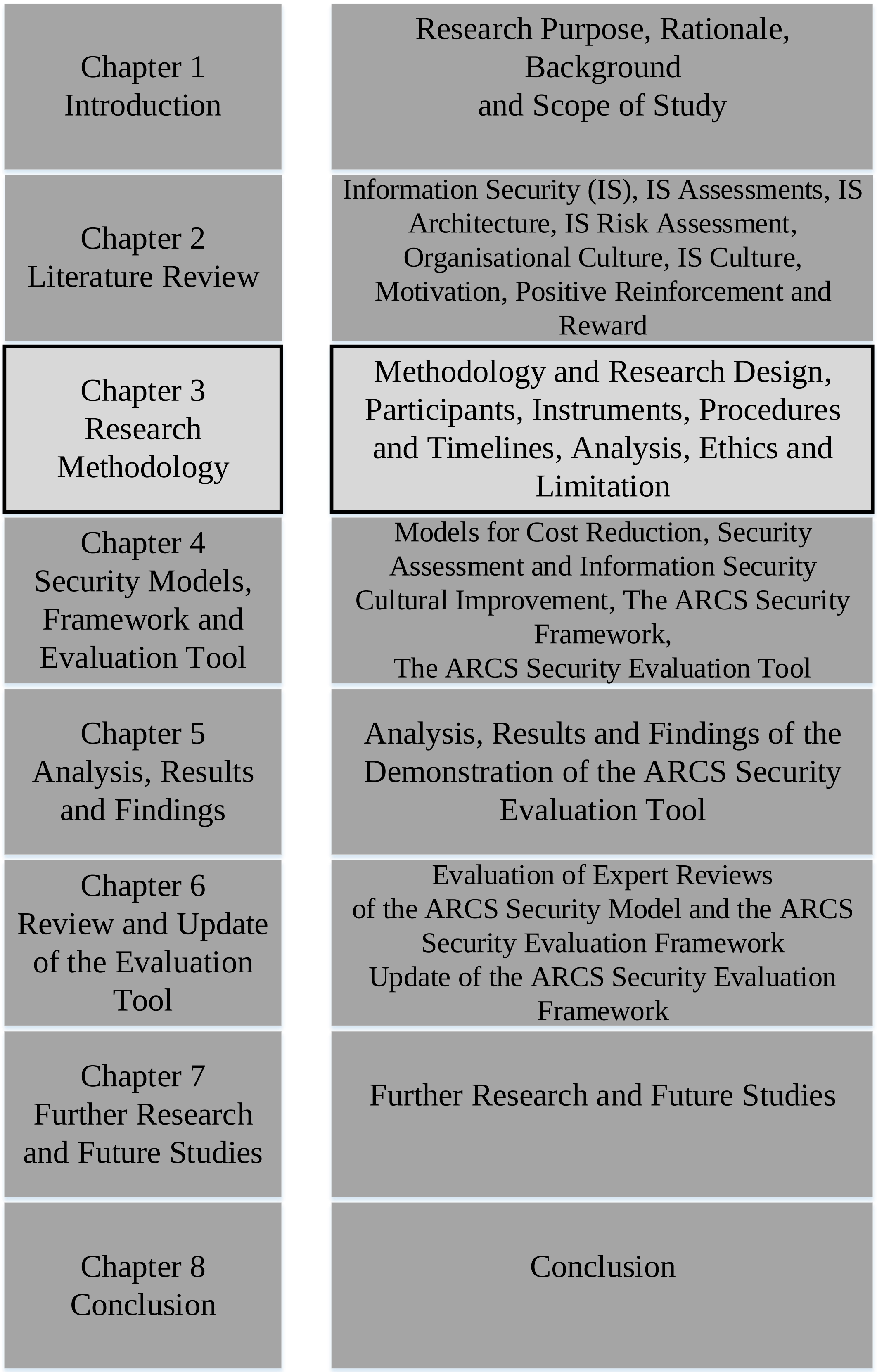
In Sections 2.4, 2.5 and 2.6, it was established that security assessments are essential but require leadership support, are human resource-intensive and require significant planning. Security architecture is vital for long-term planning and budgeting but is complex to implement, while high-level architecture resources are scarce. Risk assessments are the most traditional way to address information security concerns. However, this is a reactive approach to risk mitigation and does not suit the constant changes in threats that an organisation faces daily. Risk assessment also requires specialised skills and planning.

These gaps identified through assessments require human resources to implement, support, administer, maintain and manage, in order to resolve. As human resources are key to improving information security assessments and reducing information security costs, improving information security culture will ultimately support and sustain these activities. In Section 2.7, it was established that improving information security culture can create a long-term foundation for improving information security management and provide a non-technical approach to risk reduction.

In Chapter 3, the research methodology of this study is discussed and expands on the artefacts created as part of this study. These align in definition to the models and evaluation frameworks discussed in Section 2.2.

In creating these models, frameworks and evaluation tools, the researcher aligns to the Design Science Research methodology and process described in Chapter 3. This is done by creating new artefacts aligned with the existing literature or expanding from existing frameworks described in the literature.

Chapter 3: Research Methodology



Chapter 1 Introduction	Research Purpose, Rationale, Background and Scope of Study
Chapter 2 Literature Review	Information Security (IS), IS Assessments, IS Architecture, IS Risk Assessment, Organisational Culture, IS Culture, Motivation, Positive Reinforcement and Reward
Chapter 3 Research Methodology	Methodology and Research Design, Participants, Instruments, Procedures and Timelines, Analysis, Ethics and Limitation
Chapter 4 Security Models, Framework and Evaluation Tool	Models for Cost Reduction, Security Assessment and Information Security Cultural Improvement, The ARCS Security Framework, The ARCS Security Evaluation Tool
Chapter 5 Analysis, Results and Findings	Analysis, Results and Findings of the Demonstration of the ARCS Security Evaluation Tool
Chapter 6 Review and Update of the Evaluation Tool	Evaluation of Expert Reviews of the ARCS Security Model and the ARCS Security Evaluation Framework Update of the ARCS Security Evaluation Framework
Chapter 7 Further Research and Future Studies	Further Research and Future Studies
Chapter 8 Conclusion	Conclusion

Chapter 3: Research Methodology

In Chapter 2, the literature was reviewed to develop a view of the current artefacts related to theories, models and frameworks that support the three key features of this research, namely information security assessment methods, cost and culture. Information security assessment methods include risk assessments and security architecture. Culture was viewed from a traditional organisational culture perspective and models related to information security culture were discussed.

In this chapter, the researcher outlines the theory, design and methodology of the research. In Section 3.1.1 the philosophy of using Design Science Research (DSR) in this research is discussed. In Section 3.1.2 the researcher reviews three important process models and discusses theoretical artefacts that can be created through DSR with a view to choosing the research process. Section 3.1.3. links information systems design theory to DSR in order to show the application of DSR in developing solutions or applied artefacts in the IS field. Section 3.2 focuses on the alignment of this research to a selected DSR process model. The sub-sections 3.2.1. to 3.2.4 describe the process steps followed and links the process steps to outcomes as discussed or described in various chapters of the research document. Section 3.3 focuses on the participants of the study while Section 3.4. discusses the research instruments used. Sections 3.5 and 3.6 discuss the procedures and timeline and the analysis method of the study respectively. Section 3.7 briefly discusses how this study contributes within the expected DSR contribution framework, with a further exposition on this topic in Chapter 8. Lastly, Section 3.8 deals with the ethics and limitations of the study.

This chapter will discuss why DSR (Drechsler and Hevner 2016) was selected to develop the three models, Security Framework and the Security Evaluation Tool, discussed in Chapter 4 and the basis for the selection of the DSR process model of Peffers et al. (2007) in developing the framework and tools. The value of DSR in information systems research is linked to the Information Systems Design Theory.

3.1 METHODOLOGY AND RESEARCH DESIGN

3.1.1 Research Paradigm

Research involves a methodical process of inquiry that encompasses gathering data, documenting crucial information, and then analysing and interpreting the collected data or information using appropriate methodologies (Johnson and Onwuegbuzie 2004). Research is undertaken to assess the credibility of a hypothesis or an interpretive framework by amassing foundational knowledge and discoveries. A researcher disseminates this information to foster learning and to spark inquiries for future exploration.. Research is generally conducted for a group or community with some common interest in the concept being researched. When there is universal agreement on the phenomenon of interest, these are referred to as paradigmatic communities or groups. Where there is overlap in terms of the concepts being researched, these are multi-paradigmatic groups (Vaishnavi and Kuechler 2012). IT-based disciplines are good examples of multi-paradigmatic communities.

In information systems research, different philosophies are applied that develop knowledge in the multi-paradigmatic community (Johnson and Onwuegbuzie 2004). These are positivist, interpretive, critical and pragmatist philosophies, as explained below:

- **Positivist research**

  Positivist research operates on the assumption that the gathered data is presented objectively and free from bias, unaffected by either the researcher or the researcher's tools (Myers 1997). Positivist researchers generally aim to test hypotheses in order to enhance predictive comprehension of quantifiable events..

- **Interpretive research**

  Interpretive researchers anticipate that the gathered data could be influenced by external factors and previous experiences of both the researchers and the participants (Myers 1997). Within the ICT environment, interpretive research methodologies strive to generate an understanding of the information system's context and the reciprocal relationship where the information system impacts and is impacted by the context (Walsham 1993).

- **Critical research**

  The critical research method operates on the premise that individuals' behaviours are influenced by past interactions and are consistently replicated (Myers 1997). This method expects that although individuals can consciously strive to alter their social and economic situations, they might be hindered by diverse forms of social, cultural, and political control. Critical research is intended to serve as a societal critique that unveils these constraining elements.

- **Pragmatism**

  Rather than emphasizing the quantitative or qualitative nature of the issue, pragmatism centers on recognising and dealing with 'what works' to resolve the problem. It embraces the design and methodology that are most effective for resolving the problem and gaining knowledge. (Van Aken 2004). If desired changes are to be achieved, such as the successful coexistence of actions and knowledge, pragmatism believes that purpose and knowledge should guide actions (Myers 1997). There should, therefore, be an improvement to IS practices and a contribution to society.

This study employs the Design Science Research Methodology (DSRM). DSRM comprises a collection of synthetic and analytical techniques and viewpoints for conducting research in the field of Information Technology (Vaishnavi and Kuechler 2012). These techniques align with positivist, interpretive, critical, and pragmatic research methods. DSRM typically entails creating an artifact and/or design theory as a way to enhance the current state of practice and augment existing research knowledge (Baskerville 2008). Natural sciences focus on how and why things are, whereas DSR focuses on devising artefacts to test and move research forward (Vaishnavi and Kuechler 2012).

The ontological, epistemological, methodological and axiological beliefs of positivist, interpretive and design science researchers are described in Table 3-1.

Table 3-1 Research Perspectives (Vaishnavi, Kuechler and Petter 2004)

Basic Belief	Research Perspective			
	Positivist	**Interpretive**	**Critical**	**Pragmatist**
Ontology	A single reality; knowledge, probabilistic	Multiple realities, socially constructed	Power relations and history shape reality	A multi-layered, fragmented and fluid reality has multiple facets
Epistemology	Objective; dispassionate. Detached from the observer of truth	Subjective, i.e. values and knowledge emerge from the researcher-participant interaction	The research is mediated, hidden, distorted and created through power relations	Knowledge has practical meaning in a specific context that draws on experience, focuses on problems, practices and relevance
Methodology	Observation; quantitative, statistical	Participation; qualitative. Hermeneutical and dialectical	Deconstruction with textual and discourse analysis	In addition to using multiple qualitative, quantitative and action research methods, the emphasis is on practical solutions and results
Axiology	Truth; universal and beautiful; prediction	Understanding is situated and descriptive	Researchers may not be neutral in their research, as their values affect the study and therefore, they need to understand the context of the inquiry	Value-driven research. Research is initiated and sustained by the researcher's doubts and beliefs

Within the realm of DSR, the research paradigm being introduced could be entirely or partially constructed rather than arising naturally (Lakatos 1976; Kuhn 1970). The research carried out using the DSR methodology should hold significance and interest for the research community in which it is conducted to ensure acceptance and recognition. Design science creates and evaluates IT artefacts intended to solve identified organisational problems (Hevner and Chatterjee 2010). DSR adheres to a disciplined and cyclical procedure to generate artifacts, allowing them to be assessed for the purpose of enriching the pertinent research community's knowledge. Any crafted item containing a potential solution can serve as the outcome of DSR. Contributions to research involve appraising the output, comprehending it, and sharing it through various means such as publications, articles, and books (Peffers et al. 2007). The best-suited philosophy for this study is to apply pragmatism as it can be used to solve practical problems and contribute to society through the development of this framework and tool emanating from this study. During the demonstration and evaluation-phases (see Section 3.2.4) in the study, interpretivism will be applied for the qualitative feedback from the organisations.

Two key activities in DSR assist in improving and understanding the behaviour of aspects of information systems:

- the creation of new knowledge through the design of new or inventive artefacts; and
- analysing the artefact's use and/or performance with reflection and abstraction.

The artefacts produced within the DSR process encompass a wide range, encompassing processes, frameworks, or methods, among other things. Theories emerging from DSR contribute to knowledge by establishing a framework of principles or concepts, accompanied by a range of potential specific outcomes rooted in theory.

DSR is particularly well-suited for the realm of information systems, including the information security field. The emergence of novel concepts and ideas in the technology sphere allows researchers to propose and assess new notions for testing. This approach aligns with the exploratory nature of research in information systems and technology (Orlikowski and Iacono 2001), which is notably supported by DSR.

Design, by definition, involves the act of generating or actualizing something (an artefact) that didn't exist before. In accordance with DSR, there exist diverse types of artifacts, typically introducing fresh ideas and concepts for testing, capable of inducing a transformative shift in a researcher's comprehension. (Gregor and Hevner 2013).

This study will develop a framework, called the ARCS Security Framework, that will be used as a support or guide for information security research. In addition, another artefact from this study is the ARCS Security evaluation tool, which is described in Section 4.3.

3.1.2 The approach and processes in DSR

In considering an approach to the research design for this study, three DSR process models were evaluated. These models are summarised in Tables 3-2, 3-3 and 3-4 in order to show the steps a researcher would take to conduct a DSR study and to show the commonality in the relevant processes. The evaluation of these models allowed the researcher to consider the type of problem that was defined, the artefacts that could be created and the methods expected to be used, to assess, explain and convey the value of the artefacts. For the purpose of this study, the Peffers, Tuunanen, Rothenberg and Chatterjee (2007) model was chosen. The reason for the choice of model is further explained in Section 3.2.

Table 3-2 DSR Process Model (Vaishnavi, Keuchler and Petter 2004)

Vaishnavi and Keuchler, DSR Process Model, 2004
Awareness of problem: Research problems may be identified through multiple sources, such as the literature, developments in industry or considered issues in a particular discipline. DSR related problems are those that are generally focused on resolution through problem-solving as opposed to explanation. A researcher will consider criteria that can be part of a final product or artefact as part of the research effort. The output of this phase is a formal or informal proposal for a new research effort.
Suggestion: Once a proposal is developed in the Awareness phase, the following step is to create new functionality or process based on existing research or a wholly new concept. A preliminary design or a proof of concept can be created at this stage.

Development: The design can be progressed and executed during this phase. A plethora of artefact forms can be cultivated, spanning from design theories (Gregor and Jones 2007) to concepts, models, processes, instantiations, and frameworks. (March and Smith 1995; Hevner and Chatterjee 2010; Vaishnavi and Keuchler, 2012). The process and approach to implementing the design will vary based on the type of artefact created. The new concept is primarily in the design and not in the implementation method.
Evaluation: At this stage, the artefact is evaluated according to detailed criteria in the Awareness phase. Any qualitative or quantitative deviations identified in the implementation of the artefact must be documented and explained. In this phase, educated assumptions are made about the expected functionality and impact of the artefact. The researcher can conduct evaluations based on expected behaviours and impacts of the artefact (Venable, Pries-Heje and Baskerville 2016). This is fundamentally different from positivist research in that at this stage in positivist research the analysis would prove or disprove the researcher's hypothesis. In DSR research, this evaluation and analysis will lead to additional information being gained about the artefact.
Conclusion: In this stage, the research effort could end, or additional research could be posited. In both cases, the final output or write-up is concluded and the expected knowledge contribution is addressed. Suppose the significant deviation is noted from theoretical expectations after multiple revised re-designs and tests of the artefact. In that case, the knowledge contribution must contain information on the revised designs and best efforts must be communicated comprehensively (Hevner and Chatterjee, 2010).

Table 3-3 DSR Process Model (Peffers et. al. 2007)

Peffers, Tuunanen, Rothenberger and Chatterjee's DSR Process Model, 2007
Activity 1: Problem identification and motivation – During this phase, the researcher will delineate the research problem. It is crucial for the researcher to dissect the problem into its most basic components to comprehend its complexity. Additionally, in this stage, the significance of the solution is also rationalised.

The importance of this lies in inspiring the researcher's endeavours and galvanising the research community to pursue the suggested solution.
Activity 2: Define the objectives for a solution – During this phase, the goals for crafting an artefact are outlined to tackle each of the smaller conceptual challenges established in phase 1. These objectives can take on quantitative forms, aiming to propose a solution surpassing current alternatives, or qualitative forms, delineating how a novel artefact is anticipated to facilitate solutions for previously unaddressed problems.
Activity 3: Design and development – During this stage, the artefact is brought into existence. These artefacts can encompass constructs, models, methods, or even redesigns of attributes of existing constructs. In essence, a design research artefact could be any crafted entity wherein a research contribution is incorporated within the design (Peffers et al. 2007). This process involves defining the intended functionality and architecture of the artefact, followed by the actual creation of the artefact.
Activity 4: Demonstration – During this phase, the artefact needs to be showcased. It should be capable of addressing, either partially or entirely, the hypothesised problem. This might entail its application in experimentation, simulation, case studies, proofs, or other relevant activities.
Activity 5: Evaluation – During this phase, the researcher observes and assesses the extent to which the artefact aids in resolving the problem. The envisaged results of the solution should have been formulated, and these need to be compared with the real outcomes achieved by employing the artefact. The assessment of the artefact can take a quantitative route, involving output outcomes or satisfaction surveys, or a qualitative approach, considering factors like response times or availability metrics. Based on the assessed findings, researchers might opt to revisit phase 3 to enhance the artefact's effectiveness or proceed to the subsequent phase, sharing the outputs while leaving potential improvements for further research.

Activity 6. Communication – During this phase, the researcher is tasked with conveying the problem's significance, the artefact's essence, its practicality and innovation, the meticulousness of its design, and its efficacy to the pertinent researchers and other relevant audiences, as suitable. This could also include sharing the findings with practicing professionals when applicable.

Table 3-4 DSR Process Model (Drechsler and Hevner 2016)

Drechsler and Hevner's Four Cycle DSR Model, 2016
The change and impact cycle This phase allows for researchers to contextualise the effect that artefacts may directly or indirectly have on the environment that the research is being conducted on. The Change and Impact Cycle affords the researcher to be able to determine the organisational or societal change of the utilisation acceptance, or even the evaluation of the artefact. The viability or utility of the artefact may create a create a change within an environment in terms of introducing problems or perceptions that did not previously exist or may trigger the solution to questions that could not be previously solved. In effecting those changes this cycle allows for the researcher to conduct iterative improvements in line changes identified or redefine artefacts in order to align to the changes.
The relevance cycle In this phase, (Hevner and Chatterjee 2010) notes that the requirement or problem statement must be identified and the acceptance criteria for the evaluation of the solution must be defined. Finally, it must be clear that the design artefact will improve the environment and measure this improvement. The result of the evaluation of the design and test must be communicated back to the research community. The test results will inform whether the design must be iteratively improved to address deficiencies or whether the design in itself has inherent flaws that may limit its use in practice.
The rigor cycle The rigor cycle incorporates prior knowledge into the research project to ensure its novelty. It is incumbent upon the researchers to extensively explore and reference the knowledge repository to ensure that the designs generated are research contributions and not commonplace designs derived solely from the

implementation of widely recognized procedures (Hevner, March, Park and Ram 2004).
The design cycle Within the design cycle, research activities undergo iteration among crafting an artefact, its evaluation, and subsequent feedback to enhance its precision. This constitutes a process of formulating alternatives to the proposed design and consistently re-assessing until a satisfactory design is attained (Hevner and Chatterjee 2010). The problem statement is delineated in the relevance cycle, and the theories and methods for design and evaluation are drawn from the rigor cycle. Throughout the execution of the design cycle, it is pivotal to maintain a delicate equilibrium between the endeavours invested in constructing and evaluating the evolving design artifact. Both endeavours must remain firmly anchored in their relevance and rigor. A robust, well-founded rationale for constructing the artifact is inadequate if the subsequent evaluation lacks strength.

As noted in all the DSR process models discussed, artefacts must be created to address the problem defined. The artefact must have some method to be quantitatively or qualitatively evaluated.

Artefacts can take the shape of constructs, models, frameworks, architectures, design principles, methods, and/or instantiations, as outlined in Table 3-5 (Vaishnavi and Kuechler 2012) and Section 2.2 in Chapter 2. Material artefacts are often termed instantiations, whereas the remaining types of artefacts are denoted as abstract artefacts. A design theory typically amalgamates abstract artefacts and material artefacts.

Table 3-5 Outputs of DSR Artefact Development (Vaishnavi and Kuechler 2012)

Output	Description
Constructs	The conceptual vocabulary of a domain
Models	Sets of propositions or statements expressing relationships between constructs
Frameworks	Real or conceptual guides to serve as support or guide
Architectures	High level structures of systems
Design principles	Core principles and concepts to guide design
Methods	Sets of steps used to perform tasks- how-to knowledge
Instantiations	Situated implementations in certain environments that do or do not operationalise constructs, models, methods and other abstract artefacts
Design theories	A perspective set of statements on how to do something to achieve a certain objective. A theory usually includes abstract artefacts.

This study will develop three models and a framework. A model entails a collection of propositions or statements that articulate connections among constructs, along with a proposition about how things are or ought to be. A model is presented in terms of its functionality and may be encompassed within a construct that elucidates the model's interaction with a theory. On the other hand, a framework is a foundational structure around which something can be constructed, or a system of regulations, notions, or convictions utilized for planning or decision-making. A framework can be an abstract representation of a set of concepts or ideas that assist in problem-solving.

The artefacts will be developed to serve as support or guidance for information security research, as outlined below.

- Model 1- Social and Technical Cost Reduction Factors, which describe factors that influence information security cost.
- Model 2 - Human Intervention in Information Security Capability, which describes information security assessment methodologies.
- Model 3 - Five Pillars of Information Security Culture Enhancement Model, which describe factors that improve information security culture.

- ARCS Security Framework – Combines components of Models 1 to 3 to form key features which are then expanded into evaluations areas.

Another artefact from this study will be the ARCS evaluation tool, which is formulated from the ARCS Security Framework.

3.1.3 Information Systems Design Theory

Information systems design theory is a research theory linked to DSR where specific information systems research is conducted (Gregor and Jones 2007). Information systems design theory seeks to assist in developing solutions or applied artefacts for management problems while also understanding the problems (Van Aken 2004). Information systems design theory can be considered as the fifth of five types of research theories related to information systems which can be categorised as (1) theory for analysing, (2) theory for explaining, (3) theory for predicting, (4) theory for explaining and predicting and (5) theory for design and action (Gregor 2006). It is often stated that information systems design theory does not fit within the historical definition of a theory as described within the behavioural and natural sciences realms (March and Smith 1995) because that definition states that theories can only be defined of unchanging phenomena. However, Venable (2013) argues that this concept can be applied to information systems, as design theories of information systems do fit into the description of a theory because the theory put forward is unchanging within the world of natural space in which it was developed and because the design theory is not prescriptive in nature and may evolve as the world evolves. As described in Section 3.1.1, the theoretical components of information systems design theory lie in the definition and design of the constructs, models, frameworks and methods defined in order to create the artefact(s) for evaluation and testing (Gregor and Jones 2007). These can be considered the formalised statement of knowledge created through a DSR process for information systems artefacts (Venable 2013). Information systems design theory can be considered the abstract of those created components that can also instantiate in the real world (Gregor and Jones 2007).

In order to show that the artefacts developed as a part of the DSR and information systems design theory are principally based on some understanding of IT and human behaviour, Gregor and Jones (2007) define a framework that describes the eight components of information systems design theory as described in Table 3-6.

Table 3-6 Eight components of Information Systems Design Theory (Gregor and Jones 2007)

	Component	**Description**
	Core Components	
1	Purpose and scope (*the causa finalis)*	"The purpose of the system," the collection of meta-requirements or objectives that indicate the category of artifact to which the theory is relevant, concurrently outlining the scope or limits of the theory.
2	Constructs *(the causa materialis)*	Depictions of the pertinent entities within the theory.
3	Principle of form and function (*the causa formalis)*	The conceptual "blueprint" or architecture that delineates an information systems artefact, which could be a product or a method/intervention.
4	Artefact mutability	The alterations in the anticipated state of the artefact as envisaged by the theory, essentially encapsulating the extent of changes to the artefact.
5	Testable propositions	Statements of truth pertaining to the design theory.
6	Justificatory knowledge	The foundational knowledge or theory originating from natural, social, or design sciences that provides a basis and rationale for the design.
	Additional components	
7	Principles of Implementation *(the causa efficiens)*	An account of procedures for applying the theory (whether it pertains to a product or a method) within particular contexts.
8	Expository instantiation	A tangible embodiment of the artefact that aids in illustrating the theory, serving as an explanatory tool as well as for the purpose of testing.

Table 3-6 focuses on the structural components of information systems design theory but as in DSR also assists with developing how these ideas may be used in practice. It is possible that a developed theory may contain some or all the components described in Table 3-6, where the instantiation of the artefact may not even be present (Kwok, Hall, Paradice and Courtney 2003). In this research, all components are developed and described, including artefacts, consisting of three models, a framework and a physical implementation of the artefacts through an evaluation tool. This alignment to information systems design theory is described in Chapter 4, Section 4.4.

3.2 DSR METHODOLOGY OF THIS STUDY

In reviewing the DSR process models described in Tables 3-2, 3-3 and 3-4, the researcher aligned the study development to the Peffers, Tuunanen, Rothenberg and Chatterjee (2007) process. Overlaps in process steps were identified between the three models but it was found that the model selected was best aligned to the researcher’s study in terms of the types of artefacts to be created and the method expected to be used to evaluate and demonstrate the artefacts. However, to align with the expectation of a DSR study, there are four essential questions that DSR should address (Hevner and Chatterjee 2010). Table 3-7 maps these questions to the research questions and thesis chapters.

Table 3-7 Mapping Questions for DSR Research (Adapted from Hevner and Chatterjee 2010)

Mapping Questions for DSR Research to the Thesis Research		
Questions for DSR Research	**Thesis Research Mapping**	**Chapters**
1. What is the research question or design requirements?	What constitutes a framework that addresses information security assessment methods, the reduction of information security cost and the sustainability of information security culture?	Chapter 1: Introduction. Research purpose, background and rationale.
2. What is the artefact? How is the artefact represented?	Develop a framework and related tool that evaluates an organisation regarding how the organisation assesses information security, aligns to cost reducing information security products and services and	Chapter 4: ARCS Security Framework and ARCS Security Evaluation Tool

Mapping Questions for DSR Research to the Thesis Research		
Questions for DSR Research	**Thesis Research Mapping**	**Chapters**
	sustains improved information security culture.	
3. What design processes (search heuristics) will be used to apply (or develop) the artefact?	SRQ1: What frameworks and evaluation tools exist to assess information security in organisations.? SRQ2: What are the factors that influence information security costs? SRQ3: What constitutes information security culture and how can this be improved?	Chapter 2: Literature review
4. How are the artefact and the design processes grounded by the knowledge base? What, if any, theories support the artefact design and the design process?	SRO1: Determine what frameworks and evaluation tools exist to assess information security risk. SRO2: Determine what frameworks and evaluation tools exist to evaluate information security costs. SRO3: Determine what frameworks and evaluation tools exist to improve information security culture.	Chapter 2: Literature review Chapter 4: Development of models related to Assessment, Cost, Culture and Human Intervention

Mapping Questions for DSR Research to the Thesis Research		
Questions for DSR Research	**Thesis Research Mapping**	**Chapters**
5. What evaluations are performed during the internal design cycles? What design improvements are identified during each design cycle?	Alignment of the artefact to models and the literature review Demonstration and Evaluation of Artefacts	Chapter 2: Literature Review Chapter 5: Analysis, Findings and Results
6. How is the artefact introduced into the application environments and how is it field-tested? What metrics are used to demonstrate artefact utility and improvement over previous artefacts?	Expert Review of Artefact	Chapter 6: Review and Update of ARCS Security Evaluation Tool
7. What new knowledge is added to the knowledge base and in what form (e.g. peer-reviewed literature, meta-	Development of the ARCS Security Framework and ARCS Security Evaluation Tool Peer-reviewed literature	Chapter 4: ARCS Security Framework and ARCS Security Evaluation Tool Publications – pg. iv

Mapping Questions for DSR Research to the Thesis Research		
Questions for DSR Research	**Thesis Research Mapping**	**Chapters**
artefacts, new theory, new method)?		
8. Has the research question been satisfactorily addressed?	Demonstration and Evaluation of Artefacts	Chapter 5: Analysis, Findings and Results

The following sections describe the alignment of this study to the DSR process model of Peffers et al. (2007).

3.2.1 Problem Identification

Through the research problem outlined in Chapter 1 and the literature discussed in Chapter 2, it was established that information security management is a complicated discipline that is reliant on assessing and evaluating the existing as-is state of information security in an organisation while establishing the knowledge around the gaps in addressing deficiencies in the environment.

Investment in information security is not easily quantifiable and, in most cases, cannot be directly aligned to company growth or revenue. To assist financial managers with understanding the value of information security, it is usually addressed through the concept of risk. The way human beings consider their attitudes, beliefs and behaviour regarding information security makes risk an inherent factor. Information security culture, therefore, has an impact on business risk. Identified technical risks need to be addressed through the acquisition of products and services and to protect information and users generally. However, it was also established that technical solutions come at a human resource cost. The problem identified is that there is no comprehensive method to evaluate the quality of an organisation’s information security assessment methods versus the products, solutions and structures implemented to reduce cost versus the long-term viability (or sustainability) of the organisation's information security culture.

3.2.2 Definition of an Objective

The objective of this study was to develop a comprehensive security evaluation framework that encompasses the three facets of information security management:

- the quality, frequency and communication of security assessment methods in an organisation
- the extent and value of the implementation of cost savings security products, services and structures; and
- the depth and completeness of the sustainable human and social initiatives in place, to help improve information security culture

The objective was outlined as part of the research problem described in Chapter 1. The framework has been positioned based on the gaps identified through the literature review in Chapter 2, while the models and constructs that support the framework will be described in Chapter 4. In addition, the framework is linked to an evaluation tool to assist with reporting, which is also described in Chapter 4.

3.2.3 Development of the Artefacts

The artefacts developed are described in detail in Chapter 4. Three models are developed:

- **Model 1**- Social and Technical Cost Reduction Factors, which describes factors that influence information security cost.
- **Model 2** - Human Intervention in Information Security Capability, which describes information security assessment methodologies.
- **Model 3** - Five Pillars of Information Security Culture Enhancement Model, which describes factors that improve information security culture

Components of these three models are then synthesised into the ARCS Security framework. The framework, therefore, consists of three features. Each of these features will contain several evaluation areas. Furthermore, each evaluation area is divided into several questions related to that evaluation area.

A tool was developed as a product that can be used to evaluate the features, either as stand-alone concepts or holistically. The tool was developed in the Microsoft Excel spreadsheet application, with reporting in the form of output charts.

The tool contained a scoring system that links interdependent evaluation areas and questions together. The scoring system applies a higher score for these interdependent components. The output score from the tool could give an organisation a simple metric to evaluate the organisations' current information security level. The outputs charts and metrics from the tool could assist organisations in understanding where the deficiencies are in the organisation's security programme. This will further allow organisations to focus on their assessment methodologies, cost reduction activities, long-term security culture, or all of these features.

The development of the models, framework and evaluation tool is described in detail in Chapter 4.

3.2.4 Demonstration, Evaluation and Communication

When selecting participants for a study, the selection should be led by the ability to repeat the research or replication logic, rather than led by statistical logic (Yin 2003). Organisations that are selected should yield comparable outcomes, known as literal replication, or generate entirely divergent outcomes, termed theoretical replication (Yin 2003). Considering this rationale and the outcome of the preliminary screening process, five organisations were chosen for the purpose of collecting data pertaining to the presentation and assessment of the developed artifacts. The selection of these five organisations was predicated on the scale and intricacy of their information security capabilities. The sample size was based on DSR theory which shows that Exploratory Focus Groups (EFGs) and Confirmatory Focus Groups (CFGs) do not need to be of a large sample size (Tremblay et al. 2010) and that limited sample size affords a key practical advantage when designing, demonstrating and evaluating artefacts (Venable and Baskerville 2012; Offerman et al. 2009). Morgan (1988) suggests a lower bound of four participants with an upper bound of twelve participants. Tremblay et al. (2010) suggest that, when conducting DSR studies, larger sized focus groups cause complexity in analysis as the topic under review is more complex.

In the DSR research method, the researcher is not the regulator of the setting in which data is collected (Yin 2003). The participants' availability determines the research action (Johnson and Stake 1996). The study was conducted through personal interaction between the researcher and the participants. Participants were advised in advance that all data collected about them and their organisation would be anonymised. Any data collected would be stored in a secure location and not publicly available.

The selection of research instruments adhered to the perspective that comprehensive and intricate data can be used to construct social explanations and arguments (Demeyer 2011). Surveys and questionnaires might offer a broad grasp of surface-level patterns (Delmont and Mason 1997). Nevertheless, they lack the capacity to furnish a profound comprehension of the information security culture, assessment, and cost-related details that this research aims to uncover. Qualitative research emerged within the social realm as a means for researchers to thoroughly explore social and cultural phenomena that might not be sufficiently examined through quantitative methodologies (Myers 1997). Consequently, employing interviews in this study would enable the researcher to cultivate a more intricate perspective of the factors and concerns influencing the assessment of the framework and the developed tool.

3.2.4.1 Five Steps Completed to Demonstrate DSR Artefacts

In order to conduct the study, five steps were completed to demonstrate the artefacts developed and elicit results for improvement in iterations and communication of the study.

The five steps are described as follows:

Step 1 - Presentation of the framework and evaluation tool – The details and function of the Security Framework and Evaluation Tool will be presented and explained to the participants. The underlying concepts and models used to generate the Security Framework will be explained to the participants. The Security Framework is described in Chapter 4 – Section 4.2.

Step 2 – Conduct the evaluation and present results of evaluation – The evaluation tool developed is directly aligned to the framework developed and used to evaluate the implementation of the framework. This tool contains scoring logic that will analyse responses and output a quantitative score for the organisation evaluated. The scoring methodology was developed based on the value of the relationship of questions developed for the security framework. Where areas of importance are linked, scores were deemed to be weighted higher than non-related questions. A detailed description of the scoring methodology and the relationship between evaluation areas is captured in Chapter 4 – Section 4.3.

After the scoring is concluded, the results of the evaluation generated by the evaluation tool will be presented to participants in the form of the output scoring charts generated by the tool. The scoring charts and the outputs depicted therein will be explained to the participants.

Step 3 - Review of evaluation results - Participants will be given an opportunity to review the results. The researcher will then collect information on the participants' views of the outcomes and whether the outcomes were an accurate reflection of the information security position of the organisation in its current state. This is considered to be an expert review as the participants chosen, display significant years of experience and capability in the information security field.

Step 4 - Review of the Security Framework – The researcher will conduct interviews with participants on their views of the components of the Security Framework, the value and applicability of the components to their organisation, the structure of the framework, the components that they feel are not covered, their views of improvements or changes and their general views on the framework. A semi-structured interview questionnaire will be used for this part of the interview, along with researcher observations in regard to the participant's responses.

Step 5 - Review of the Security Evaluation Tool – The researcher will conduct interviews with participants on their views of the Security Evaluation Tool, the value and applicability of the tool, the scoring mechanism and weighting of questions, the quality and value of the output charts generated, their views on improvements and changes and their general views on the evaluation tool. The Security Evaluation Tool is described in Chapter 4 – Section 4.3 A semi-structured interview questionnaire will be used for this part of the interview along with researcher observations in regard to the participant's responses.

Further to the first pass evaluation, input regarding the framework from the expert review will be considered to improve and redevelop parts of the evaluation questions and tool. The updated framework and evaluation tool are described in Chapter 6.

Outputs of the evaluation scoring were time and date stamped and stored in secure storage. The analysis and results of the demonstration of the artefact and summary of resultant expert reviews conducted are described in Chapter 5.

3.2.4.2 Summary of Process Steps to Research Conducted

In summary, Table 3-8 describes the DSR process steps aligned to the chapters of this research. In Chapter 7, Section 7.3, the design of artefacts is evaluated in line with the researcher's observation after developing, analysing, experimenting with, testing and describing the artefacts as described by Hevner's (2004) Design Evaluation Methods.

Table 3-8 Summary Alignment of DSR Process Steps to Research Document

DSR Process Step	**Alignment to Chapter**	**Description**
Problem identification	Chapter 1	Problem identified based on introduction and problem statement defined in Chapter 1
Definition of an objective	Chapter 1 and Chapter 2	Objective defined based on research problem statement and the literature reviewed
Development of the artefacts	Chapter 2 and Chapter 4	Artefact developed based on the literature reviewed and models and framework developed
Demonstration of the artefacts	Chapter 5	Artefact demonstrated based on evaluation tool developed

DSR Process Step	Alignment to Chapter	Description
Evaluation and refinement of the artefacts	Chapter 5	Evaluated based on evaluation tool demonstration and subsequent interviews with participants
Communication of the results	Chapter 5 and Chapter 6	Communicated based on the evaluation of results and iterative review of participants comments and redevelopment of the framework and evaluation tool

3.3 PARTICIPANTS

A summary of the organisation size and function is described in Table 3-9. The information described in Table 3-9 was received from participants during the interview phase and through the access to these companies' public websites. The researcher engaged with senior management and leadership working in the IT/IS function within these organisations. As expected by DSR theory, participants were selected based on their characteristics in relation to the topic being discussed and form part of a population that is familiar with the environment for which the artefacts were developed, so that they could adequately inform the refinement and evaluation of the artefacts (Tremblay et al. 2010). A summary of the expert reviewers' details that are pertinent to this study is described in Table 3-10. All participants selected were selected as they met the criteria of being expert reviewers.

Table 3-9 Description of Organisations Evaluated

Organisation Function	Organisation Size
Large Multinational FMCG Company	Large (+200k employees)
National Government Department	Large (+200k employees)
State Owned Company	Large (+4k Employees)
International IT Consulting Company	Medium (+250 employees)
National Government Department	Large (+4k employees)

Table 3-10 Description of Expert Reviewers

Participant number	Yrs of experience	Current field of work	Job level
1	25 years in IT	General Management Architecture and Information Security	Director
2	35 years in IT	Information Security	Senior Manager
3	30 years in IT	General Management in Information Security and Architecture	Director
4	22 years in IT	Information Security	Information Security Manager
5	30 years in IT	Information Security	Director

3.4 DATA COLLECTION INSTRUMENTS

The data collection instruments used in the study are a deep literature review, artefacts developed, semi-structured questionnaire used for interviews, expert reviews and researcher observation.

The artefacts developed are:

- **Model 1** - Social and Technical Cost Reduction Factors, which describes factors that influence information security cost.
- **Model 2** - Human Intervention in Information Security Capability, which describes information security assessment methodologies.
- **Model 3** - Five Pillars of Information Security Culture Enhancement Model, which describes factors that improve information security culture
- **The ARCS Security Framework**, a three-dimensional model that features components from the models, related to the evaluation of information security assessment methods, cost reduction of information security investment and information security culture improvement.

- **The ARCS Security Evaluation Tool**, which is a Microsoft Excel based implementation of the ARCS Security Framework. This tool was also used to conduct the reporting that was part of the demonstration and evaluation of the framework.

The academic literature and publicly available documentation on information security were evaluated to conduct a deep study on the specific topics of information security assessment methods, information security cost, organisational culture, organisational behaviour and information security culture.

The semi-structured interview questionnaire contained fifteen open-ended questions related to the Framework and Evaluation Tool. The questionnaire is described in detail in Chapter 4.

The expert review was conducted by participants who were selected due to their significant experience, seniority and capability in the information security field. A summary of the participants' experience is described in Table 3-10, while a more detailed description is noted for each participant's evaluation in Chapter 5.

The researcher also observed and interpreted the expert reviewers' comments during the interviews based on his experience and capability in the information security field.

3.5 PROCEDURE AND TIMELINE

The procedures of this study were divided into four phases, which generally align to the DSR process model steps selected.

In phase one, the literature was surveyed on the topics relevant to information security assessment, information security cost and information security culture. In understanding the literature and from the researcher's own experience, it was determined that a comprehensive framework encompassing an evaluation of all of these topics did not exist. This led to the formulation of the primary research question.

In phase two, based on the problem identified and the literature reviewed, models were developed to define a relationship between the key topics. The models were then synthesised to develop the overall ARCS Security Framework. The ARCS Security Evaluation tool was then developed based on the defined Framework.

In phase three, prospective participants were contacted to determine if their organisation would consider allowing the researcher to demonstrate the ARCS

Security Framework and ARCS Security Evaluation Tool. Furthermore, these participants were asked to evaluate the Framework and Evaluation Tool. Organisations whose participants responded positively were evaluated to determine if the organisation meets the criteria of being a medium to large size organisation, contained a standalone IT function and possibly a standalone information security function. Meeting dates and times were set up with these participants, where the researcher visited each participant at their corporate offices. The researcher conducted the demonstration of the Framework and Tool as described in Section 3.2.4 and collected data to be analysed.

In phase four, the researcher collated and informally documented the responses from the participants. The researcher then analysed and formally documented the outcomes of the evaluation phase. Responses were also analysed for possible improvements and changes to the Framework and Evaluation Tool. The improvements and changes were then be documented to contribute to the second iteration of the Framework and Tool.

3.6 ANALYSIS

In this study, the collected data was analysed as the data became available and the emerging results were used to shape the next set of observations and communication. The process of analysing qualitative data involves scrutinising, categorising, tabulating, and reconfiguring the empirical evidence in order to explore the initial relationships identified in the research problem and to discover new concepts and connections. (Yin 2003). By developing analysis strategies and techniques in advance of conducting the research, a researcher is compelled to carefully assess the data that will be gathered and its significance in relation to the research. (Huberman and Miles 1994). A qualitative data analytical procedure suggested by Yin (2003) consists of the following three steps:

- Step 1 - Selecting a broad strategy to aid in determining what to analyse and the rationale for analysis.
- Step 2 - Applying coding to the evidence.
- Step 3 - Employing an analytical approach to formulate or verify theories.

3.6.1 General Analytic Strategy

The process of classifying, coding and sorting the data is the outcome of analysing the content of interviews and observations (Patton 2002). In this study, the questions asked in the interviews as part of the evaluation phase define a descriptive structure to arrange the collected data (Yin 2003).

3.6.2 Analytic and Coding Techniques

Qualitative research can be conducted through either inductive or deductive approaches. Inductive studies typically commence with a broad research question rather than a stringent hypothesis. The collected data is then analysed using inductive principles, rather than deductive ones. On the other hand, quantitative research primarily employs the deductive method. In this case, the researcher gathers data to test a pre-established hypothesis. Deductive reasoning guides researchers to gauge the relative achievement of predetermined, well-defined, and specific objectives. Inductive reasoning, in contrast, steers researchers towards centering on program or product impacts and effects. In this study, through the DSR methodology, the research question posits the development of artefacts related to the quality and validity of a framework and evaluation tool.

3.6.3 Validity

The value of qualitative research relies on the fulfilment of conditions that must be considered (Yin 2003). These conditions are construct validity, internal validity, external validity and reliability.

3.6.3.1 Construct Validity

Construct validity focuses on establishing suitable operational measures for the constructs under investigation. To ensure the construct validity within a study, three principles have been put forth for data collection: employing triangulation, establishing an exhaustive repository of gathered data, and upholding a consistent chain of evidence (Yin 2003; Patton 2002). These methodologies were adhered to during both the data collection and analysis stages, as outlined below:

- Utilisation of multiple sources of evidence: Employing multiple data sources is a method referred to as triangulation. (Yin 2003; Huberman and Miles 1994). Triangulation is employed as a method to enhance both the reliability and validity of qualitative research .In this study, five organisations were selected to evaluate the framework and tool.

- Establish a chain of evidence: Creating a chain of evidence enables the reader to trace the progression of evidence from the original research questions to the eventual communication of conclusions regarding the developed artifacts. Moreover, if the chain of evidence is coherent and transparent, the DSR process will tackle the procedural challenges associated with construct validity and reliability (Yin 2003).

3.6.3.2 Internal Validity

Internal validity relates to the degree of researcher extrapolations concerning cause-effect or causal relationships. It is specifically relevant in cases that involve causality (explanatory cases). In this study, each participant’s comments will be individually evaluated against the artefacts developed and not interpreted as a single collective critique.

3.5.3.3 External Validity

External validity relates to whether findings of a study can be generalised (Yin, 2003). It encompasses considerations regarding the study's sample and if conclusions drawn may apply beyond the specific sample under investigation (Boudreau, Ariyachandra, Gefen and Straub 2011). Yin (2003) suggests employing replication logic to enhance the external validity of findings in a study involving multiple participants. The replication process involves an iterative pattern-matching approach across subjects. In this study, the evaluation of the framework and tool will allow for iterative improvement of those artefacts. Furthermore, as the framework and tool are general in nature, these can then be implemented outside of the study and should provide consistent results.

3.6.4 Reliability

The reliability of a study ensures the mitigation of errors and biases within the study. Moreover, reliability demands that the research process, as implemented in the study, remains consistent, enabling any subsequent researcher to replicate the exact procedures and obtain the same results. (Yin 2003).

Leveraging more than one data source is strongly advised as a strategy to enhance the reliability of qualitative research (Huberman and Miles 1994; Yin 2003). According to Huberman and Miles (1994), utilising multiple participants is crucial to prevent research findings from being solely attributed to specific characteristics of the research setting.

In this study, the researcher acknowledges that his experience and knowledge in the field of information security may lead to inferences on the results of the data collected in response to the evaluation of the framework and tools. However, without the context of normalising and improving the framework and tool, this experience and knowledge will help interpret the responses from participants.

3.7 CONTRIBUTION OF THIS STUDY

Gregor and Hevner (2013) provided the DSR contribution framework where DSR research can be classified in two dimensions based on the existing knowledge of the problem and the maturity of the solution domain, as shown in the Figure 3-1.

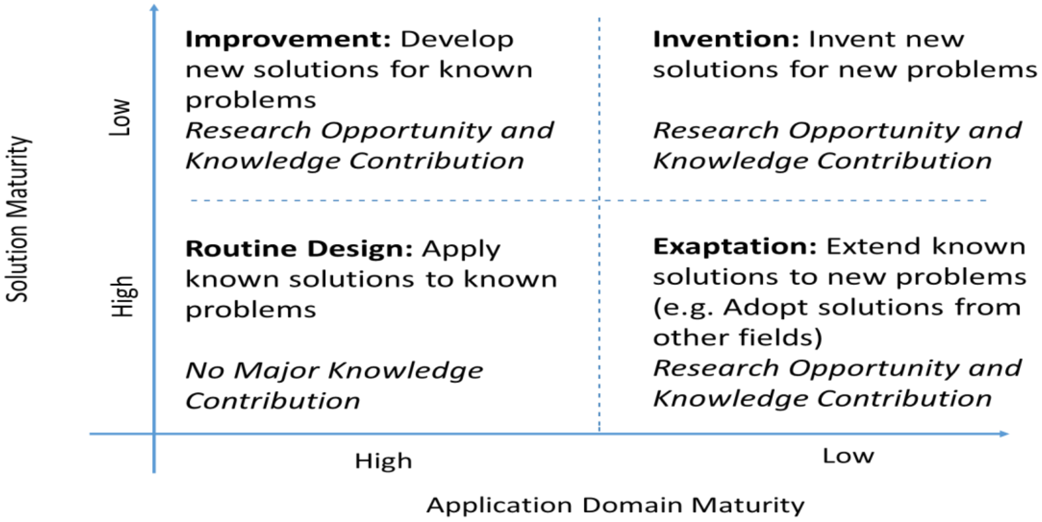

Improvement: Develop new solutions for known problems
Research Opportunity and Knowledge Contribution
Invention: Invent new solutions for new problems
Research Opportunity and Knowledge Contribution
Routine Design: Apply known solutions to known problems
No Major Knowledge Contribution
Exaptation: Extend known solutions to new problems (e.g. Adopt solutions from other fields)
Research Opportunity and Knowledge Contribution
Solution Maturity
Low
High
High
Low
Application Domain Maturity

Figure 3-1: DSR knowledge contribution framework (Gregor and Hevner 2013)

In this study, the area where the contribution to knowledge was made is under the low solution but high domain maturity axel referred to as ‘improvement’ as the framework and the tool are both new solutions to known problems in information security. More information regarding the contributions of this study can be found in Chapter 8, Section 8.3.

3.8 ETHICS

There were no ethical concerns related to this study. No personal information was captured and where information was available, this was anonymised before being communicated. There were no psychological, social or physical constraints attached to participation in this study. All information collected on the organisations that participated has no material impact on those organisations’ reputations or business functions. All information collected and synthesised was stored on secure storage where only the researcher had access to the data. The researcher believes that he acted ethically when collecting, collating and analysing the information and does not perceive a threat to the validity of the outcome of the study. The researcher acknowledges that there may be potential risks in the collection and analysis of sensitive information about the participating organisations’ security environment but believes that these risks have been mitigated by the methods of protecting the information collected as discussed in Section 1.5.

3.9 SUMMARY AND IMPLICATIONS

In this chapter, the core philosophy of this research was described in form of the theoretical methodology of Design Science Research and the related DSR process models. The applicability of DSR to information systems research was discussed in terms of the alignment of DSR to Information Systems Design Theory. A methodology aligned to the DSR processes was chosen and the researcher described how the processes steps would be achieved in the study. The artefacts developed through this research approach were also defined.

The research instruments were described along with how these instruments would be used in practice. The theory of the analysis method for this study and the actions taken to analyse data were described. Lastly, the ethical considerations and limitations of the study were discussed.

In Chapter 4, the first iteration of artefacts is developed. These are the basic models on information security assessment methods, cost and culture respectively. Components of each of these models are then selected to be included in an overall Security Framework. Based on the constructs of the framework, an evaluation tool is then described.

Chapter 4: Security Models, Framework and Evaluation Tool

Chapter 1 Introduction	Research Purpose, Rationale, Background and Scope of Study
Chapter 2 Literature Review	Information Security (IS), IS Assessments, IS Architecture, IS Risk Assessment, Organisational Culture, IS Culture, Motivation, Positive Reinforcement and Reward
Chapter 3 Research Methodology	Methodology and Research Design, Participants, Instruments, Procedures and Timelines, Analysis, Ethics and Limitation
Chapter 4 Security Models, Framework and Evaluation Tool	Models for Cost Reduction, Security Assessment and Information Security Cultural Improvement, The ARCS Security Framework, The ARCS Security Evaluation Tool
Chapter 5 Analysis, Results and Findings	Analysis, Results and Findings of the Demonstration of the ARCS Security Evaluation Tool
Chapter 6 Review and Update of the Evaluation Tool	Evaluation of Expert Reviews of the ARCS Security Model and the ARCS Security Evaluation Framework Update of the ARCS Security Evaluation Framework
Chapter 7 Further Research and Future Studies	Further Research and Future Studies
Chapter 8 Conclusion	Conclusion

Chapter 4: Security Models, Framework and Evaluation Tool

In Chapter 3, the DSR methodology and its alignment to Information Systems Design Theory were discussed. A DSR Process model was selected. A key element of the process model selected is the development of artefacts to be tested and iteratively improved.

Information security breaches have received significant publicity and have become more frequent. Studies conducted by IBM and Kaspersky indicate that even though the cost per breach has been reduced incrementally with the adoption of better technology, organisational structures and awareness, the number of breaches has risen (Ponemon Institute 2020; Verizon 2017; Kaspersky Lab 2016). This implies that the overall cost to protect an organisation has and will continue to increase. The factors that are considered as remediation to the major data breach vectors are a combination of social (structural and awareness) and technical (product and service acquisition). With the increased likelihood of breaches, technical solutions are increasingly employed to reduce risk. However, these solutions incur a high cost for the solutions themselves and the scarce information technology (IT) human resources required to manage, maintain, monitor and administer these solutions. Improved behaviour and understanding of information security risk and technology in IT employees is key. Models such as those defined in Van Niekerk and Von Solms (2010) describe metrics to understand the effect of culture on information security, but in this chapter, a social alternative with practical application activities is presented to reduce risk and thereby reduce the cost of information security management in organisations.

In this chapter, the researcher will focus on the Design and Development process steps of the selected DSR process model described in Chapter 3. Section 4.1 focuses on the design and development of models for Cost Reduction, Security Assessment and Information Security Cultural Improvement. In this section, three models are developed. These comprise a model for cost saving security remediation factors and its relationship to human behaviour, a model for security assessment in line with reliance on human intervention and non-technical actions and a model of five key activities or programmes an organisation can employ to improve behaviour and culture in respect of information security to address the sustainability of information security management, risk reduction and hence, cost reduction within an organisation.

Section 4.2. focuses on the design and development of the ARCS Security Framework. In this section, the ARCS Security Framework is developed by combining and relating components of the security assessment, reduction of cost and information security culture models. The constructs of the components and sub-components of the framework are described, along with the relationship of the components to the sub-components. Lastly, the relationship of the framework to the models is defined.

Section 4.3. focuses on the design and development of the ARCS Security Evaluation Tool. In this section, the ARCS Security Evaluation Tool is developed. The Weighting and Scoring Methodology used in the ARCS Security Evaluation Tool is described. Lastly, the Reporting Outputs of the ARCS Security Evaluation Tool are defined.

Section 4.4. maps the literature reviewed, the conceptual framework and tool created to Information Systems Design Science Theory.

4.1 MODELS FOR COST REDUCTION, SECURITY ASSESSMENT AND INFORMATION SECURITY CULTURAL IMPROVEMENT

In the following sections, the three foundational models that contribute to the overall security framework are first developed and discussed. The models developed are synthesised from the theory described in Chapter 2. Components of each of the models are extracted and expanded to develop an information security evaluation framework. A reference model is defined for the framework to allow for the further expansion of the framework in future. A relationship model for the framework's components is also defined to give input to the scoring model used and give the output metrics when applying the framework. Lastly, a basic evaluation tool is developed and described to apply the framework.

4.1.1 Information Security Breach Vectors

Information security breach vectors are defined as the methods or means by which attackers may gain access, deliver malicious software or exploit system vulnerabilities. In a 2020 study conducted by Ponemon (Ponemon Institute 2020) of four hundred and nineteen large companies in thirteen countries, the average cost of a data breach was found to be US$3.62 million, where the cost was determined by:

- the unexpected or unplanned loss of customers due to the data breach
- the size of the breach in terms of the number of records lost
- the time taken to identify a data breach
- the detection and escalation costs of the breach; and
- post data breach costs.

A Kaspersky study of five thousand five hundred organisations of varied sizes in twenty-six countries showed that the average cost was greater than US$600 000 (Kaspersky Lab 2016). Furthermore, the Kaspersky study shows that the larger the organisation, the greater the potential cost of poor information security management controls.

The aforementioned studies broadly categorised the types of breaches as malicious or criminal attacks, cyber espionage, system glitches, third party failures, human error or employee fraud. In most organisations, the attacks or breaches are focused on applications, while the most significant security spend is on networks (Gunter 2017).

Irrespective of the type of breaches, 20 percent were attributed to malware, 60 percent were related to phishing attacks and 20 percent were attributed to data leakage by employees (Utzerath and Dennis 2021; Bey and Agyeman 2022). The per breach type cost was also equivalent to similar ratios. Based on these statistics, it can be inferred that by reducing malware, phishing and data leakage, an organisation may significantly increase its information security position and significantly reduce its cost of security events.

In organisations, the approach to remediating these types of breaches is a combination of technical and social solutions. The technical solutions include operational products such as Intrusion Detection or Prevention (IDS/IPS) devices, anti-virus and malware products, web and email traffic analysis products and Data Loss Prevention (DLP) tools (Chatterjee and Sokol 2019; Cremonini and Martini 2005). The social solutions are generally awareness and training programmes (Yildirim 2016).

The literature reviewed regarding how organisations budget for information security investment indicates that conducting a cost-benefit analysis is difficult and that applying traditional IT budgeting techniques may not work as business case outputs tend to not be positive, in that security investment does not generally generate income (Mercuri, 2003; Bodin, Gordon and Loeb, 2005; Schatz and Bashroush, 2017). Information security investment is generally focused on reducing cyber breaches through the implementation of technology (Cavusoglu et al. 2015). However, technical solutions are relatively expensive when compared to non-security technology and the expertise to manage and administer these products is scarce and expensive (Cavusoglu et al. 2015). Most importantly, information security tools tend to generate enormous amounts of information. The continuous analysis of that information and the remediating activities identified are dependent on human involvement, capability and motivation.

As described in Chapter 2, Section 2.8, using positive motivation theory for employees directly impacts information security systems and controls and an improvement on an organisation’s overall information security position (Lowry and Moody 2015). Therefore, it follows that having an approach to enhancing information security core values and behaviours and focusing on specific cost saving remediation factors will improve information security positions and significantly reduce information security costs.

4.1.2 Information Security Cost Saving Remediation Factors

Ponemon (2020) conducted a study where twenty factors were described as resolution or improvement actions to address information security breaches. Twelve factors were considered to decrease the cost of an information security breach and eight were considered to increase the cost. The factors that reduce and increase cost are described in Table 4-1.

Table 4-1 Information Security Cost Reducing and Cost Increasing Factors

Cost Reducing Factors	Cost Increasing Factors
Having an incident response team	Provision of ID protection
Extensive use of encryption	Consultant engaged after the breach
Employee training	Rush to notify business after the breach
Business continuity management processes	Lost or stolen devices
Participation in threat analysis and sharing	Extensive use of mobile platforms
Use of security analytics services	Compliance failures
Extensive use of data loss prevention products, policies and processes	Extensive cloud migration
Data classification	Third-party/outsourced management
Cyber security insurance	
Appointing a chief information security officer	
Board-level involvement in information security spend	
Having a chief privacy officer appointed.	

Fig. 4-1 separates the cost-reducing factors described in Table 4-1 into social and technical factors. When isolated six of these factors are socially (people, managerial or structurally) influenced and depicted in orange to the left. The other six factors are technically influenced and depicted in the blue colour to the right. Therefore, concentrating the information security management effort on these twelve factors will provide the best information protection at the lowest cost as determined by the Ponemon (2020) study. The study does not create a relationship between these cost reducing factors, previous investment and the current state of information security in surveyed organisations. However the study does relate the breach vectors, complexity of threat landscape in specific industries and related remedial activities and as such gives a competent, trustworthy result that is generally applicable in those industries.

For each of the six technical factors, some human intervention and response for these factors are required to be successful. For example, the technical factors may include management, participation, configuration, administration, continuous monitoring and evaluation and periodic ad hoc processes (Takemura and Komatsu 2013; Bojanc et al. 2012).

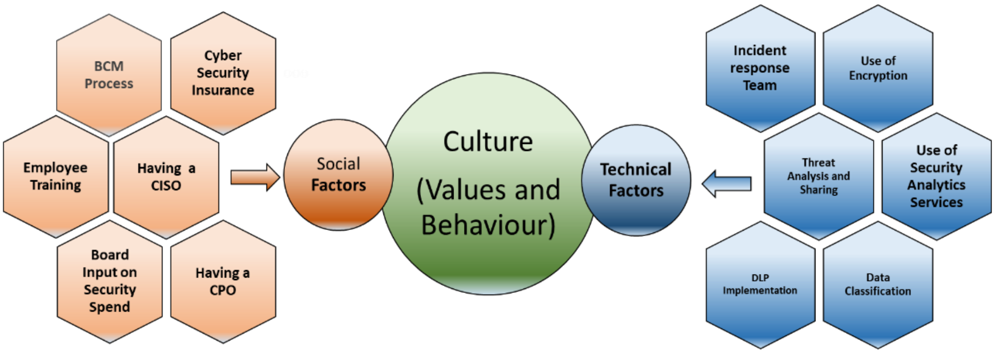


Figure 4-1 Social and Technical Cost Reduction Factors

Since this human interaction is social in nature, people’s behaviour and values within an organisation directly influence whether these actions, supporting information security management, are successful.

Improving the values and behaviour of technical resources (e.g. server and network administrators, application developers, desktop support specialists and email and file-server administrators) that support information security remediation requirements will also assist in reducing the risk of information security breach incidents. In effect, developing and enhancing the socially relevant factors creates a stronger foundation for the success of the technical factors. This is depicted in Figure 4-1 by the green circle, representing the dependence on human culture and behaviour to succeed in the social and technical cost-saving factors.

4.1.3 Information Security Assessment and Cultural Change

In Chapter 2, research reviewed established that organisations evaluate their information security position using several methods such as best practice assessments and standards (Prislan and Bernik 2010), risk assessments or longer-term information security strategic initiatives encompassed in an information security architecture programme. The outcomes of these assessments or programmes are supported by the selection of products and/or solutions that fit the information security and business needs. Information security technologies are complex in nature and require technical capability to function appropriately or effectively within the organisation. Security technologies purport to be autonomous and self-running but require significant human management and administration to function in a valuable way for the business. Figure 4-2, which has been developed for this study, describes the relationship between generalised common information security evaluation methods and the reliance on human resources to run, manage, monitor and maintain information security systems that are identified through these methods.

Security tools are not always managed by the security function within the organisation and staff that do manage these solutions are from alternative functional areas within the IT department, i.e. application development, infrastructure, end-user computing or networks. The motivation and behaviour for these IT staff members to consider security first is generally incongruent with their motivation for their primary job responsibilities. The effect of what staff consider additional work to their primary job responsibility is lower motivation to consider their information security responsibilities as important.

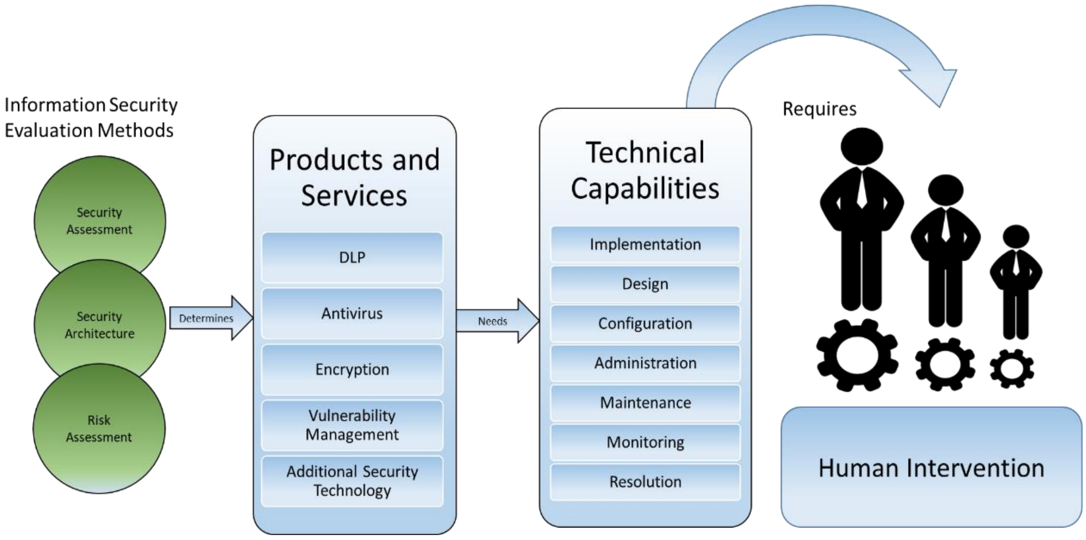


Figure 4-2 Human Intervention in Information Security Capability

The model in Figure 4-3, developed for this study, builds on the human intervention required and proposes five pillars of cultural change that are applicable in redefining staff members' values and behaviours, which will develop and enhance information security culture and behaviour. Five pillars were chosen to consolidate the concepts discussed in Chapter 2 related to societal, organisational and information security culture as well as proven recognition and reward psychology. While the literature reviewed in Chapter 2 considered several aspects of improving and supporting organisational culture, the key distinguishing component of the information culture frameworks discussed was related to knowledge or level of knowledge. The theory describing motivation, organisational behaviour, rewards systems and information security culture covered in Chapter 2 supports each pillar described. Pillars 1, 3, 4 and 5 are related to intrinsic rewards, which relate to intangible rewards but enhance organisational culture and introjected motivation, which is developed based on human want or requirement to finish an activity to prove an accomplishment to themselves. Pillar 2 is based on extrinsic reward which is a tangible reward system that enhances organisational behaviour. Each of the five pillars supports organisational behaviour theory and provides and external and internal stimulus to motivation. As such, this motivation supports sustained improvement in organisational culture and in the context of information security supports sustained improvement in information security culture as noted in the information security culture frameworks discussed in Chapter 2

In this study cultural sustainability relates to maintaining cultural beliefs and cultural practices that support the information security management programme. Sustainability in this context is the driver that supports non-technical risk reduction and ensures that as technology and management ideals change, information security culture continues to improve. The effect of improving IT employees' information security culture is two-fold: first, staff will be motivated within their job functions to consider information security a priority and secondly the enhancement of information security cultural aspects will allow for long-term value for the organisation and create the foundation for information security practices to become a prioritised norm. The model proposes five practical streams of activity that can be applied to enhance the information security culture of IT staff. The model is not interdependent and an organisation may execute each pillar independently or select to execute the necessary pillar that may be relevant to that organisation.

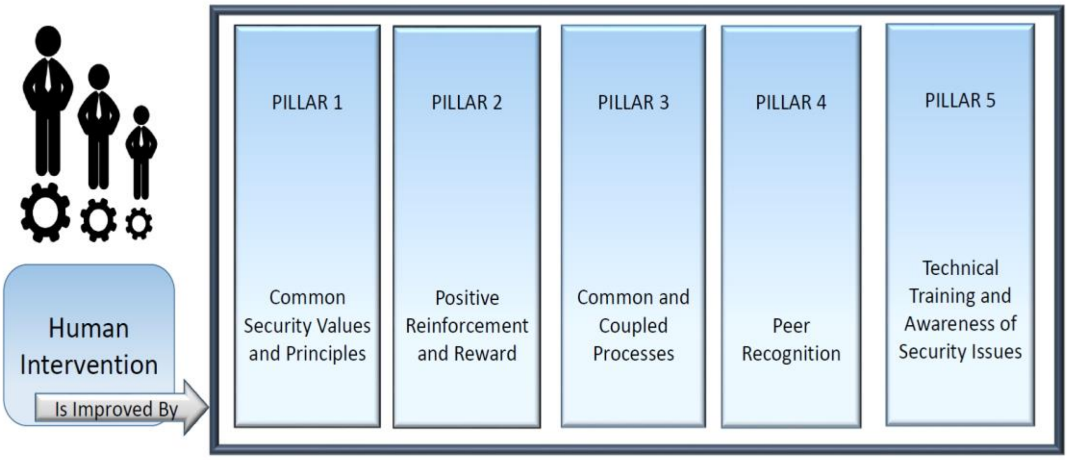

PILLAR 1
Common Security Values and Principles
PILLAR 2
Positive Reinforcement and Reward
PILLAR 3
Common and Coupled Processes
PILLAR 4
Peer Recognition
PILLAR 5
Technical Training and Awareness of Security Issues
Human Intervention
Is Improved By

Figure 4-3 Five Pillars of Information Security Culture Enhancement Model

The five pillars for the enhancement of information security culture in staff are as follows:

Pillar 1 - Common security values and principles

Information security management is the responsibility of different functional areas within an IT department. The areas are generally managed, focusing on the functional discipline and considering cross-functional responsibility a secondary matter. An example might be that a server support team focuses on the management of servers and rarely considers how server configuration may affect an application development team. This pillar informs the creation of common security values and principles that need to be shared amongst each IT discipline. The value of security must be embodied and communicated with the common view to distribute the responsibility of information security amongst all role players. The principles of information security must become part of the IT principles of the organisation and should not be considered a stand-alone discipline (Mithas and Rust 2016). IT security, as a concept, must be supported and championed by the executive and senior management and structures and roles must be developed to support these common values and principles (Schinagl and Shahim 2020; Soomro et al. 2016).

Pillar 2 - Positive reinforcement and reward

Organisational accomplishment is dependent on values and behaviours. Positive reinforcement often leads to improved behaviour and forming this into consistent and repeatable behaviour embeds it into the organisation's culture. Rewards may also support positive reinforcement to enhance values and behaviour through fewer social mechanisms. Three constructs generally support positive reinforcement and reward to make them effective in an organisation:

- They must be earned. IT staff should be supported to make good security decisions, live the values and principles and emphasise the security processes. Rewards may be awarded for consistent and continual adherence to positive security behaviour.
- They must be quick. IT staff should get immediate feedback and recognition for their adherence to the organisation's positive values of information security.
- They must be frequent. The organisation should consider smaller, more frequent rewards. When values and behaviour are supportive of the information security programme, short-term communication to those staff members involved should be commonplace.

Pillar 3 - Common and coupled security processes

When considering technical implementation, IT staff are generally internally focused on their area of expertise. The impact of layering security onto 'their' technology is rarely considered in the context of the IT disciplines that they support or are supported by (Fenz et al. 2014). IT staff should understand the effects of security monitoring, blocking, patching and processes as they affect each IT discipline in the IT value chain. Information security managers should develop and socialise information security processes, which are conceptually a common thread and where the impact of each IT discipline is transparent (Mukherjee 2019).

Pillar 4 - Peer recognition

As noted in Chapter 2 – Section 2.8, several studies show that peer recognition is one of the greatest motivators in the workplace. In the context of information security management, organisations should consider implementing a peer recognition programme managed and controlled by the staff themselves. Peer programmes managed by the staff and supported by senior management foster an environment of recognition and reward that is perceived to be less biased than those driven by management. Through this process, staff will be informed of the positive value that their peers in all disciplines are inputting into information security management and may be motivated to follow suit. Staff will also be able to see the impact of their contribution to information security, which will create a more consistent information security behaviour profile, thereby supporting the overall information security culture.

Pillar 5 - Technical training and awareness of security issues

Security awareness and training programmes in organisations focus predominantly on the general user (McIlwraith 2016). While this is useful, it was established in Section 3 that the key factors to the success of information security management and the reduction of information security costs are the technical factors of security products and solutions. IT staff should receive significant technical training in the security solutions that are implemented and be made aware of prevalent technical security issues (Yildirim 2016). IT staff should understand the scope of products selected and how these can be leveraged to support the information security values and principles. IT staff should also understand their value in threat remediation through patching and vulnerability management. Threat analysis and aggregated information from security analysis resources and information security staff should be shared with general IT staff. Lastly, information security awareness and training are rarely targeted at senior and executive management (Safa et al. 2018). As most governance best practices place data breach responsibility with the accounting officer of an organisation, a greater focus on information security awareness and training for senior and executive management should be part of the cultural enhancement programme (Soomro et al. 2016).

4.2 THE ARCS SECURITY FRAMEWORK

In sections 4.1.2 and 4.1.3, it was established that the key drivers to understanding the current state of an organisation’s information security position require an assessment or evaluation of the information security landscape. The outputs of those assessments expose information security gaps or deficiencies. Information security risk extends to the greater employee population as they use technology, provided by the organisation, to conduct their work. This was also established through the development of the models in Figures 4-1, 4-2 and 4-3, which was based on the theory described in Chapter 2. In Section 4.1.2, cost-reducing security initiatives were described and it was established that human culture and behaviour are a key part of implementing these initiatives. It is noted that these cost reducing initiatives do not give context to investment already conducted by an organisation nor the available capacity or capability to implement such initiatives. In Section 4.1.3, it was established that information security assessment methods are only successful with human intervention and whether the gaps identified are addressed through technology, structural or process changes. People are also required to manage, administer and support the information security environment. This human intervention is sustained and improved through improved information security culture. The framework discussed below combines the three concepts of Information Security Risk Assessment, Information Security Cost and Information Security Culture to establish a structured evaluation method, which will assist an organisation in addressing and improving its level of information security maturity.

The framework extracted from the models described in Figures 4-1, 4-2 and 4-3 is structured into three features (F1, F2 and F3) called **A**ssessment of Security Risk (F1), **R**eduction of Information Security **C**ost (F2) and **S**ustainability of Culture (F3) and is referred to as the ARCS Security Framework, as described in Figure 4-4. Each feature (F1, F2 and F3) is broken down into an evaluation area. Each evaluation area (E1, E2, $E_{n)}$ is given a shortened tagged description and is broken down further into questions (Q_{n}.1 to $Q_{n.n}$) related to that evaluation area, as depicted in Figure 4-5. The questions were then developed in line with the evaluation aim of the overall evaluation goal of the information security programme. This is further described in sections 4.2.1, 4.2.2 and 4.2.3.

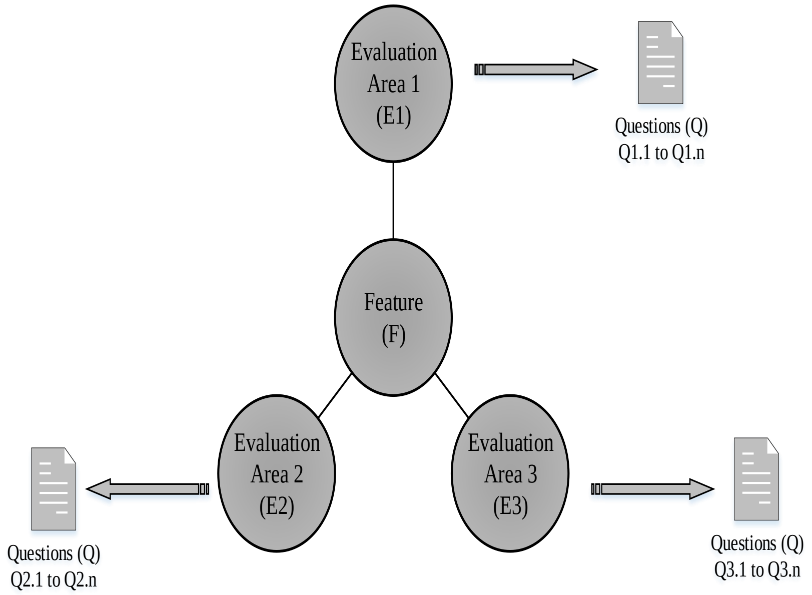

Evaluation Area 1 (E1)
Questions (Q) Q1.1 to Q1.n
Feature (F)
Evaluation Area 2 (E2)
Evaluation Area 3 (E3)
Questions (Q) Q2.1 to Q2.n
Questions (Q) Q3.1 to Q3.n

Figure 4-4 ARCS Security Framework Relationship Model

The framework compromises of three features established from the models developed in section 4.1.2 and 4.1.3, twenty-one evaluation areas created for the framework and eighty-three questions that have been developed for the framework aligned to the evaluation areas, all of which are described in Table 4-2.

The features F1 to F3 and the respective evaluation areas are described in sections 4.2.1 to 4.2.3 below. The eighty-three questions for each of these evaluation areas are collated in Tables 4-3, 4-4 and 4-5.

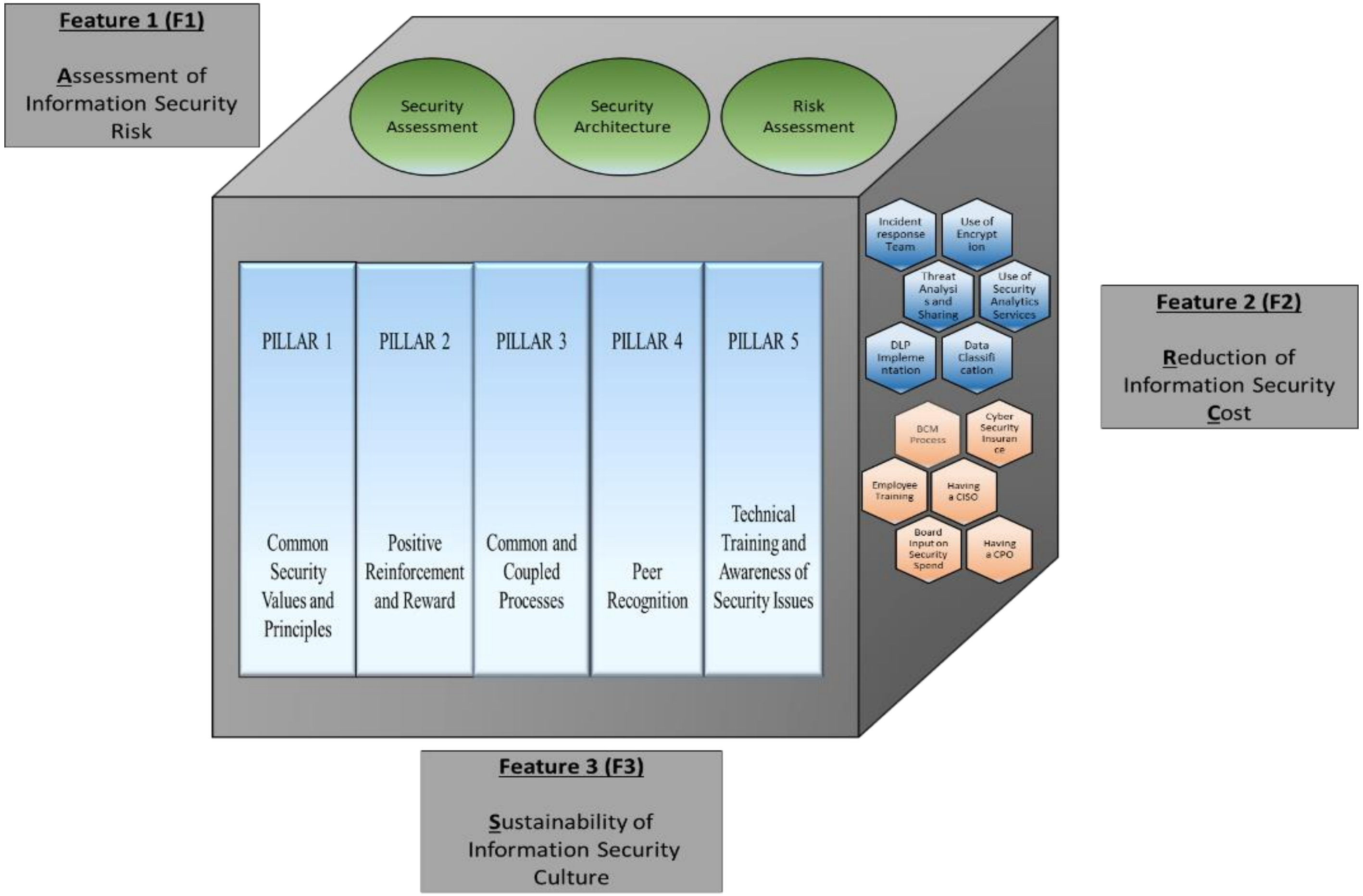

Feature 1 (F1)
Assessment of Information Security Risk
Security Assessment
Security Architecture
Risk Assessment
PILLAR 1
Common Security Values and Principles
PILLAR 2
Positive Reinforcement and Reward
PILLAR 3
Common and Coupled Processes
PILLAR 4
Peer Recognition
PILLAR 5
Technical Training and Awareness of Security Issues
Incident response Team
Use of Encryption
Threat Analysis and Sharing
Use of Security Analytics Services
DLP Implementation
Data Classification
BCM Process
Cyber Security Insurance
Employee Training
Having a CISO
Board Input on Security Spend
Having a CPO
Feature 2 (F2)
Reduction of Information Security Cost
Feature 3 (F3)
Sustainability of Information Security Culture

Figure 4-5 ARCS Information Security Evaluation Framework

Table 4-2 Details of the ARCS Security Framework

FEATURE NAME (F)	EVALUATION AREA TAG(E)	QUESTIONS (Q)
F1 ASSESSMENT OF INFORMATION SECURITY RISK	E1.1 Security Assessment (SECASSESS)	**Q**1.1.1 to **Q**1.1.6
	E1.2 Security Architecture (SECARCH)	**Q**1.2.1 to **Q**1.2.6
	E1.3 Risk Assessment (RSKASSESS)	**Q**1.3.1 to **Q**1.3.5
F2 REDUCTION OF INFORMATION SECURITY COST	E2.1 Business Continuity Management (BCM)	**Q**2.1.1 to **Q**2.1.6
	E2.2 Cyber Security Insurance (CSI)	**Q**2.2.1 to **Q**2.2.4
	E2.3 Employee Information Security Training (EIST)	**Q**2.3.1
	E2.4 Having a CISO (HACISO)	**Q**2.4.1 to **Q**2.4.2
	E2.5 Board Input on Security Spend (BIOSS)	**Q**2.5.1 to **Q**2.5.3
	E2.6 Having a CPO (HACPO)	**Q**2.6.1 to **Q**2.6.2
	E2.7 Incident Response Team (IRT)	**Q**2.7.1 to **Q**2.7.4
	E2.8 Use of Encryption (UOE)	**Q**2.8.1 to **Q**2.8.3
	E2.9 Threat Analysis and Sharing (TAS)	**Q**2.9.1 to **Q**2.9.4
	E2.10 Security Analytics Services (SAS)	**Q**2.10.1 to **Q**2.10.4
	E2.11 Data Loss Prevention (DLP)	**Q**2.11.1 to **Q**2.11.7
	E2.12 Data Classification (DC)	**Q**2.12.1 to **Q**2.12.2
	E2.13 Information Security Input Costs (ISIC)	**Q**2.13.1 to **Q**2.13.6
F3 SUSTAINABILITY OF INFORMATION SECURITY CULTURE	E3.1 Pillar 1- Common Security Values and Principles (CSVP)	**Q**3.1.1 to **Q**3.1.4
	E3.2 Pillar 2- Positive Reinforcement and Reward (PRR)	**Q**3.2.1 to **Q**3.2.4
	E3.3 Pillar 3- Common and Couple Processes (CCP)	**Q**3.3.1 to **Q**3.3.2
	E3.4 Pillar 4- Peer Recognition (PREC)	**Q**3.4.1 to **Q**3.4.3
	E3.5 Pillar 5- Technical Training and Awareness of Security Issues (TTSA)	**Q**3.5.1 to **Q**3.5.5
3 FEATURES	**21 EVALUATION AREAS**	**83 QUESTIONS**

4.2.1 Feature 1 – Assessment of Information Security Risk

The Assessment of Information Security Risk feature supports evaluating and understanding the current information security landscape, the risks faced by the organisation and the key success factors to help an organisation address information security management. The objectives of Feature 1 assist with creating short-, medium- and long-term goals in driving information security management and reducing risk in the organisation, as established in Chapter 2 – sections 2.4, 2.5 and 2.6.

The function of Feature 1 of the ARCS framework aims to evaluate:

- An organisation's ability to assess its current information security environment.
- The depth and breadth of the assessment methodology used.
- The alignment of the assessment(s) to best practice or standards.
- The frequency of assessment(s).
- The structural level to which the assessment is communicated.

Feature 1 is structured into three evaluation areas as depicted in Figure 4-6 and contains a total of seventeen questions.

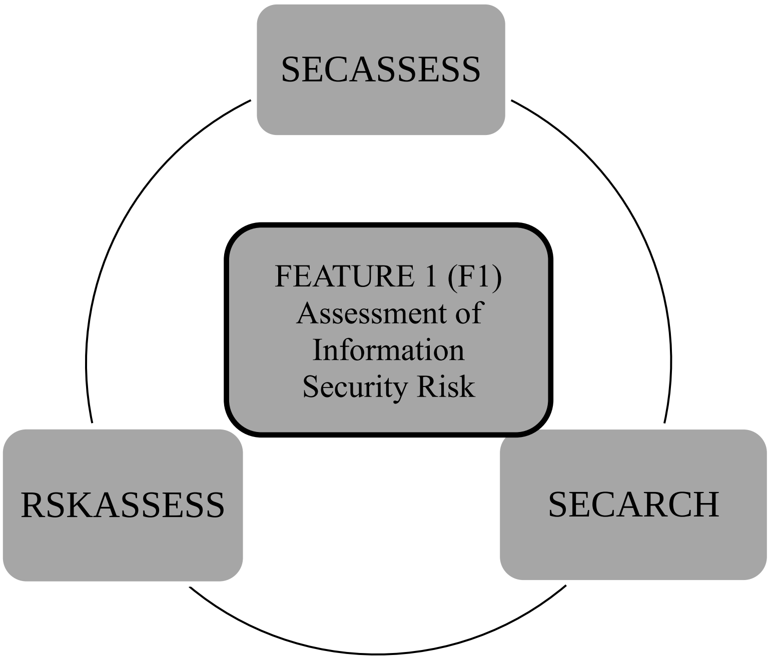


Figure 4-6 Structure of Feature 1 (F1)

In Feature 1 the evaluation areas are:

- E1.1 Security Assessment (SECASSESS) – this evaluation area focuses on general security assessments that may or may not be aligned to best practices or standards. Questions that relate to vulnerability management and penetration testing are weighted higher as these are linked to cost reduction factors.
- E1.2 Security Architecture (SECARCH) – this evaluation area focuses on the structured implementation of a security architecture programme. Questions in this area are rated higher as these are linked to sustainability factors.
- E1.3 Risk Assessment (RSKASSESS) – this evaluation area focuses on general information security risk assessments that may or may not be aligned to best practices or standards. No questions within this area are weighted higher.

4.2.2 Feature 2 - Reduction of Information Security Cost

The Reduction of Information Security Cost feature evaluates the factors noted in Figure 4-1. These factors have been established to help information cost reduction in an organisation, while inputs costs of information security have been established in Chapter 2, Section 2.2. Feature 2 focuses on whether and to what extent the cost reduction factors are implemented within an organisation. Furthermore, the inputs cost factors are evaluated.

The function of Feature 2 of the ARCS framework aims to evaluate:

- How many of the cost reduction remediation factors are implemented.
- The extent to which these factors are implemented.
- The alignment of the implementation(s) to best practices or standards.
- The structural level that is involved in the decision making of these implementations.
- The extent to which input cost factors are evaluated and measured.

The Reduction of Cost feature is structured into thirteen evaluation areas as depicted below in Figure 4-7 and contains forty-eight questions in total.

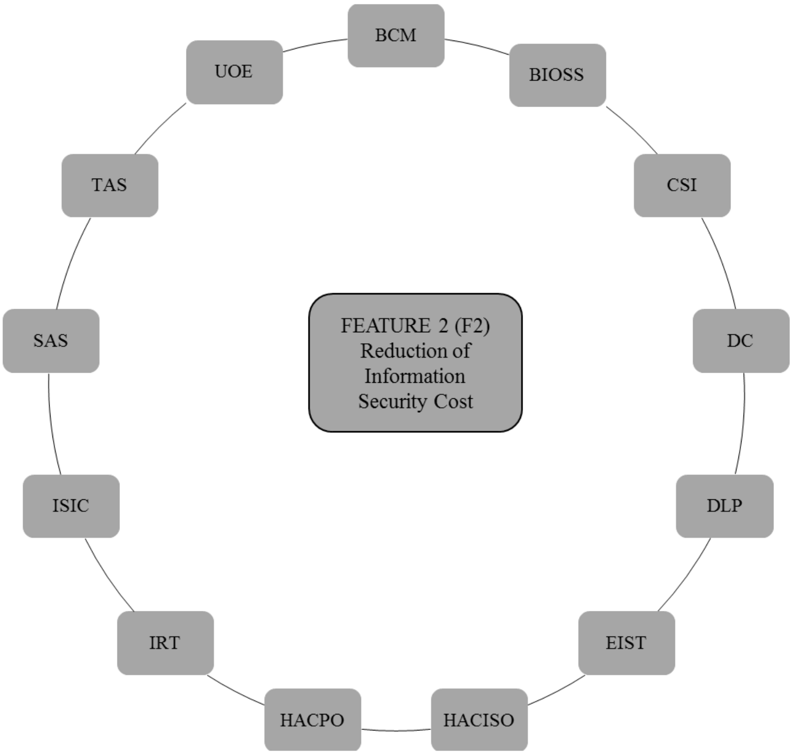


Figure 4-7 Structure of Feature 2 (F2)

In Feature 2 the evaluation areas are:

- E2.1 Business Continuity Management (BCM) – this evaluation area focuses on whether the organisation conducts a business continuity management programme, follows a business continuity process and is aligned to best practice or standards. It also evaluates how effective this process is and to what structural level the results of this process are communicated.
- E2.2 Cyber Security Insurance (CSI) - this evaluation area focuses on whether the organisation invests in cyber security insurance.
- E2.3 Employee Information Security Training (EIST) - this evaluation area focuses on whether the organisation implements regular and focused information security awareness and training, to what structural level and the evaluation thereof.
- E2.4 Having a CISO (HACISO) - this evaluation area focuses on whether the organisation has a Chief Information Security Officer (or equivalent) and the relevant supporting structure.
- E2.5 Board Input on Security Spend (BIOSS) - this evaluation area focuses on the input the board or highest managerial structure has on information security spending.

- E2.6 Having a CPO (HACPO) - this evaluation area focuses on whether the organisation has a Chief Privacy Officer (or equivalent) and the relevant supporting structure.
- E2.7 Incident Response Team (IRT) - this evaluation area focuses on whether the organisation has a security incident response team, the scope of their work and how they are measured.
- E2.8 Use of Encryption (UOE) - this evaluation area focuses on whether the organisation uses encryption as a standard.
- E2.9 Threat Analysis and Sharing (TAS) - this evaluation area focuses on whether the organisation conducts threat analysis activities, to what extent and whether this information is shared with peer organisations.
- E2.10 Security Analytics Services (SAS) - this evaluation area focuses on whether the organisation runs a Security Operations Centre (SOC) if security analytics are conducted and what is done with that analysis.
- E2.11 Data Loss Prevention (DLP) - this evaluation area focuses on whether the organisation runs a comprehensive DLP programme.
- E2.12 Data Classification (DC) - this evaluation area focuses on whether the organisation manages and classifies data.
- E2.13 Information Security Input Costs (ISIC) - this evaluation area focuses on whether the organisation evaluates and budgets for information security input costs.

In this feature, all the evaluation areas are weighted equally and, therefore, do not add additional points in the evaluation scoring.

4.2.3 Feature 3 – Sustainability of Information Security Culture

The Sustainability feature evaluates the readiness, behaviour and culture of the organisation in respect of information security. Feature 3 focuses on long-term human behaviour in relation to information security and is supported by the literature in traditional social sciences described in Chapter 2 – sections 2.6, 2.7 and 2.8. The assessment objective helps an organisation determine its current cultural and behavioural fit from an information security management perspective and assists in developing a longer-term sustainable road map to imbibe information security culture into the organisation rather than a traditional cycle of information security analysis and addressing gaps through technology products and services.

The function of Feature 3 of the ARCS framework aims to evaluate:

- An organisation's ability to assess whether common security values and principles exist within the organisation and to what extent these are entrenched.
- An organisation's ability to assess whether positive reinforcement and reward is applied for good information security behaviour.
- An organisation's ability to assess whether the organisation implements common and couple security processes across the IT/IS disciplines.
- An organisation's ability to assess whether peer recognition is conducted by employees for employees when good information security behaviour is identified.
- An organisation's ability to assess whether technical training and awareness of security issues is conducted within the organisation.

The Sustainability feature is structured into five evaluation areas as depicted below in Figure 4-8 and contains eighteen questions in total.

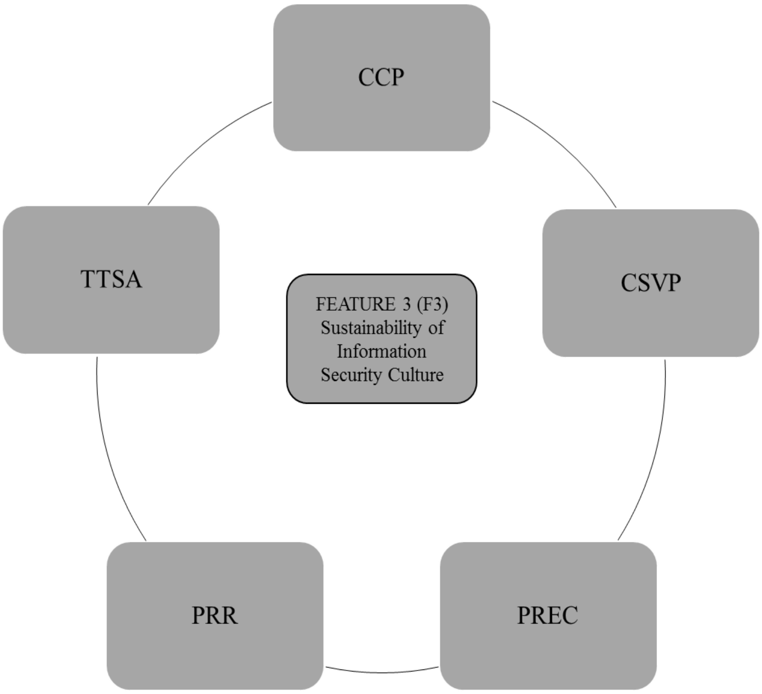


Figure 4-8 Structure of Feature 3 (F3)

In this feature, the evaluation areas are:

- E3.1 Pillar 1- Common Security Values and Principles (CSVP) – this evaluation area focuses on identifying, communicating and evaluating common security values and principles.
- E3.2 Pillar 2- Positive Reinforcement and Reward (PRR) – this evaluation area focuses on the communication, method and process of positive reinforcement and reward for good information security behaviour.
- E3.3 Pillar 3- Common and Couple Processes (CCP) – this evaluation area focuses on the communication and evaluation of common and couple security processes in the IT/IS environment.
- E3.4 Pillar 4- Peer Recognition (PREC) – this evaluation area focuses on evaluating, structural approach and visibility of peer recognition initiatives for good information security behaviour.
- E3.5 Pillar 5- Technical Training and Awareness of Security Issues (TTSA) - this evaluation area focuses on the approach, scope, evaluation of technical training and awareness of information security.

4.3 THE ARCS SECURITY EVALUATION TOOL

A multifaceted evaluation tool was developed in Microsoft Excel to supplement and support the ARCS Security Framework. The tool is multifaceted in that the evaluation can be isolated to either one of the three features or combined for an overall evaluation score of all three features. The value in creating a modular evaluation framework is that organisations may already understand where their deficiencies are and may just want to focus on specific targeted areas of evaluation or may find it easier to re-conduct an evaluation in a specific feature area that was initially found deficient. The evaluation tool documented in this research can be defined as a Layer 1: high level output, which with further development of the framework, can add layers of more detailed questioning below each of the evaluation areas.

To implement the ARCS Security Framework, an evaluation tool has been developed in Microsoft Excel. The tool contains tabs related to the Features described in the Framework, which each contain the Evaluation Areas split into questions. The assessment questionnaires for Feature 1 - Assessment of Information Security Risk, Feature 2 - Reduction of Information Security Cost and Feature 3 - Sustainability of Information Security Culture are described in Appendix G.

The response tables are embedded in the tool and the scoring logic is calculated based on the given responses. Weighting and output charts are also embedded in the tool. The evolution of this tool will be to develop it as a stand-alone web application with output charts developed in Microsoft PowerBI and is discussed further in Chapter 7.

The questions are weighted and scored to give each evaluation area an output score. The standard questions in the evaluation area follow a simple scoring mechanism of using one point for a "Yes" or zero points for a "No" or "N/A". The exception to this scoring is when a specific special question is weighted higher than a standard question due to its relationship with questions in evaluation areas in other features. This relationship was defined as the literature indicated that there would be some overlap between the implementation of certain action within the linked areas. Figure 4-9 describes the relationship between special evaluation areas. The specific links in terms of question linked in each feature is further described by the scoring model in Table 4-3 and in Appendix H.

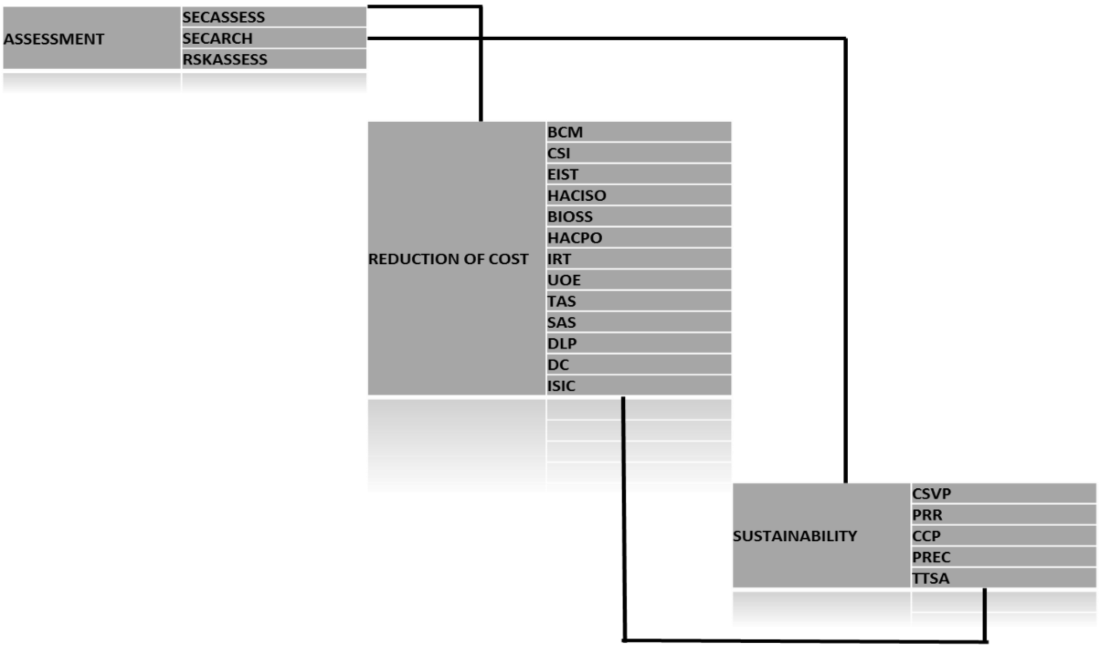


Figure 4-9 Relationship Between Special Evaluation Areas

In the case where a special question is asked, the scoring logic in the tool then reverts to using two points for a "Yes" or zero points for a "No" or "N/A". An example of this is evaluation area 1.1 which has two special questions of a total six. As such in this area the maximum score can be eight points made up of four normal questions at one point each plus two special questions at two points each. Table 4-3 describes which evaluation areas contain special question and the detail of the scoring is described in Appendix H.

The score per question in each evaluation area is summed and divided by the maximum points available to give an overall percentage score for each evaluation area. Evaluation of scoring is based on a scale where 0-50 percent implies Poor performance, 51 percent to 70 percent implies Satisfactory performance and 71 percent to 100 percent implies Good performance. In the discussion on sample evaluated outputs below and the analysis of the evaluation of artefacts in Chapter 5, the explanation of performance aligns to these levels but is described in the context of the evaluation areas value from an information security perspective.

Table 4-3 Summary of Higher Weighted Questions in Each Evaluation Area

EVALUATION AREA	NUMBER OF SPECIAL QUESTIONS
E1.1 - Security Assessment (SECASSESS)	2 of 6
E1.2 - Security Architecture (SECARCH)	6 of 6
E3.5 - Pillar 5- Technical Training and Awareness of Security Issues (TTSA)	2 of 5

Overall scores are depicted on a spider graph for that specific feature as described in Figure 4-13. The depiction in Figure 4-10 is merely an example of a possible output. In order to interpret the spider graph, one would look at the overall coverage of the graph. In the depiction in Figure 4-10, for example, for Feature 1, this organisation has done well in the Security Assessment Evaluation Area, but not so well in Security Architecture or Risk Assessment Evaluation Areas. Each score for each feature is then combined into an overall summary spider chart to show the organisation's final evaluation outcomes.

In the examples noted in Figures 4-10, 4-11 and 4-12, one can interpret the results based on the coverage in the spider graph.

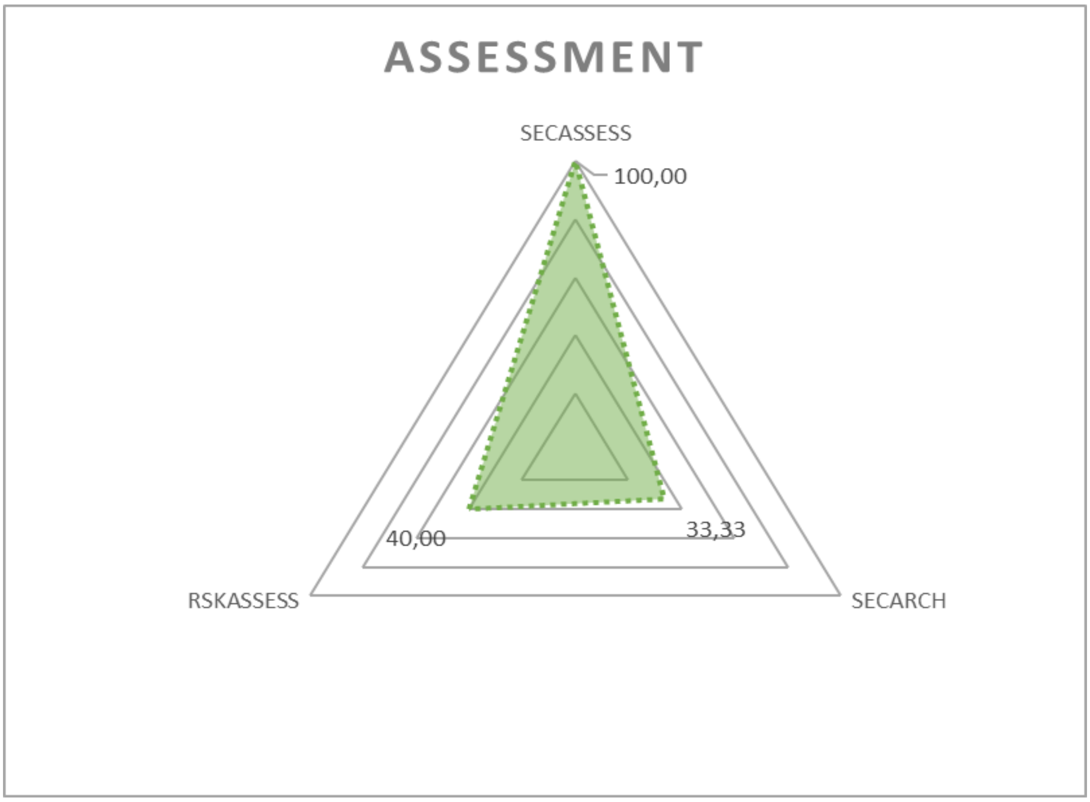


Figure 4-10 Feature 1 - Example of the Output Graph for Information Security Assessment Feature

In the graph for Feature 1 – Information Security Assessment in Figure 4-10, one can establish that the organisation has a good programme for information security assessment aligned to best practices and standards in this example. The organisation has some form of risk assessment methodology, but this is not effective. Lastly, one can establish that the security architecture function is not performed, which implies that long terms security strategy is not being developed, nor are security-related artefacts being developed.

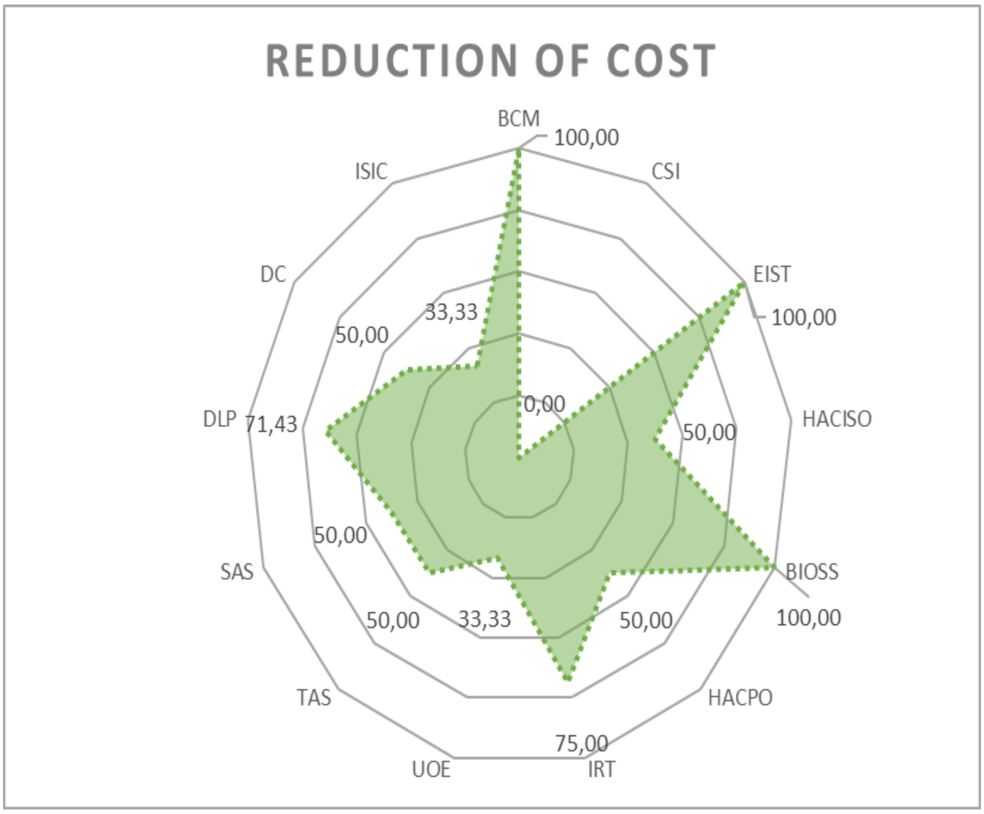


Figure 4-11 Feature 2 – Example of the Output Graph for the Reduction of Information Security Cost Feature

The graph for Feature 2 – Reduction of Information Security Cost in Figure 4-11 can establish that this organisation has a good business continuity management programme aligned to best practices and standards. Employee information security training is performed to a high level. The company board or senior leadership has a direct input on information security spend and has a view of the spend, however, budgeting and cost planning for information security are not done well. Data loss prevention is performed well but can improve.

The organisation does not invest in cyber security insurance and has a CISO and a CPO, but these people do not report to the highest level. Security analytical services are used but are not prevalent or consistently used. Training and awareness are not performed across all levels of the organisation. Encryption is not standardised and data classification is not performed to a standard.

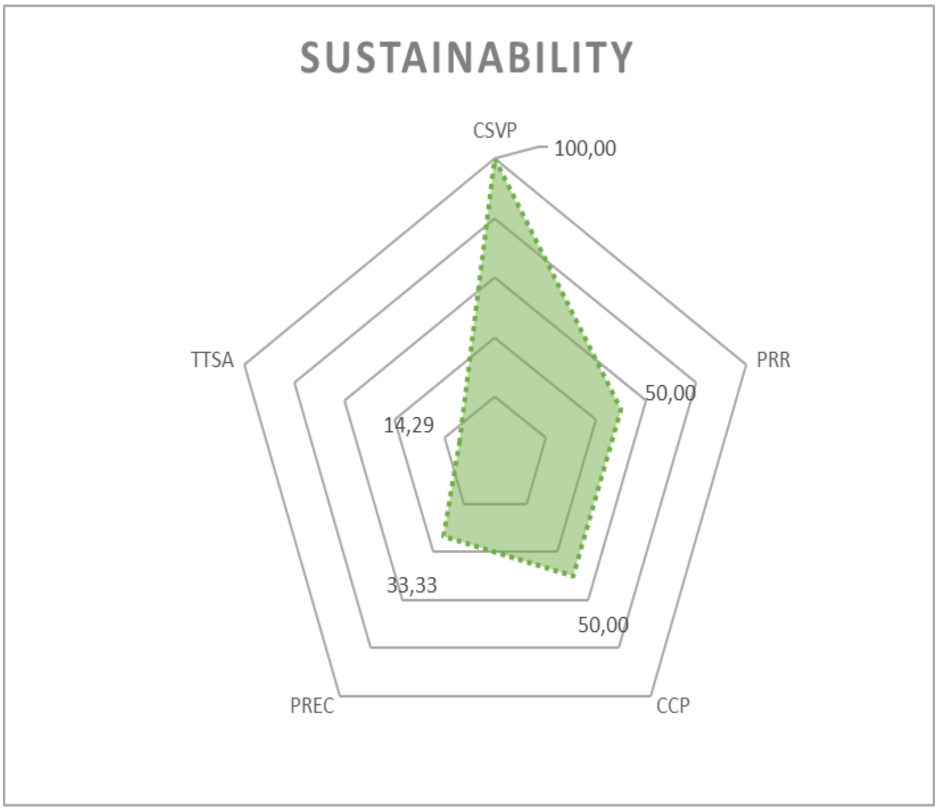


Figure 4-12 Feature 3 - Example of the Output Graph for the Sustainability of Information Security Culture Feature

The graph for Feature 3 – Sustainability of Information Security Culture in Figure 4-12 can establish that this organisation shares strong common security values and principles. Positive reinforcement and reward are practised but not effectively, while common security practices are not prevalent. Peer recognition for good security behaviour and strong training and awareness programmes are non-existent.

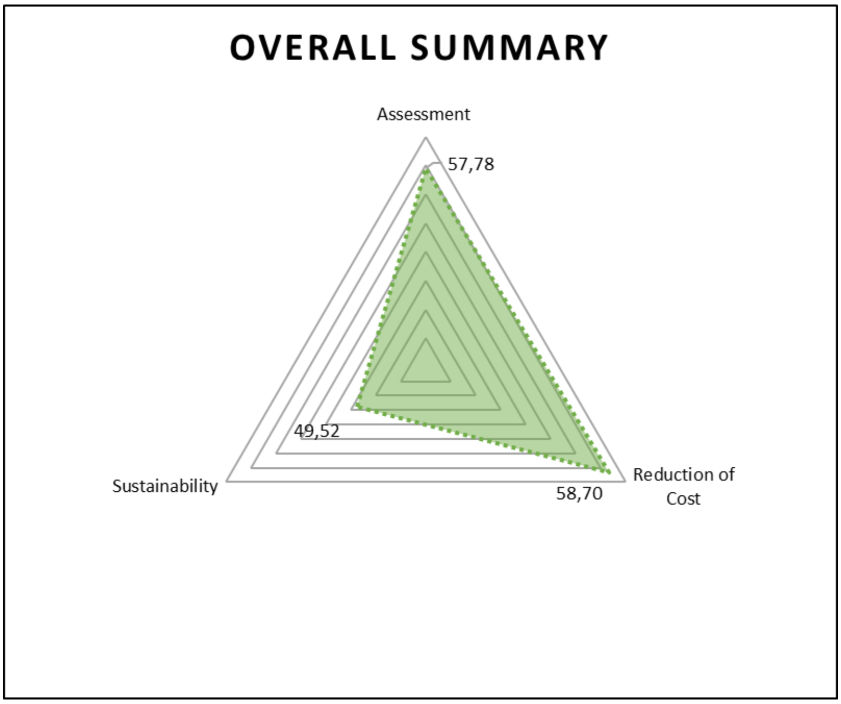


Figure 4-13 Example of the Output Scores of the ARCS Security Evaluation Tool

Lastly, the overall summary figure depicted in Figure 4-13 shows the average scores from each of the feature areas on one graph. In the figure, one can establish that this organisation performs well in the Security Assessment and Reduction of Cost functions. However, the long-term Sustainability of Culture feature is not performed well and has room for improvement. The interpretation is based on the calculation of the sum of overall scores for each evaluation area divided by the total number of evaluations areas per Feature.

4.4 ALIGNMENT OF RESEARCH TO INFORMATION SYSTEMS DESIGN THEORY

In Chapter 3, Section 3.2, the mapping of the overall research to the Design Science Research Methodology is described. In Chapter 3, Section 3.1.2, the concept of Information Systems Design Theory is described. Table 4-4 maps the artefacts created in this Chapter along with the literature reviewed in Chapter 2, as well as the basis for this research described in Chapter 1, to the Information Systems Design Theory components discussed in Chapter 3, Section 3.1.2.

Table 4-4 Mapping of Theory and Artefacts to Information Systems Design Theory Components

	Component	**Description**	**Mapping to Research**
	Core Components		
1	Purpose and scope *(the causa finalis)*	"What the system is for," the set of meta-requirements or goals that specifies the type of artefact to which the theory applies and in conjunction also defines the scope, or boundaries, of the theory.	Chapter 1 describes the problem statement in regard to the need for a comprehensive security evaluation framework that encompasses Information Security Assessment, Information Security Cost and Information Security Culture.
2	Constructs *(the causa materialis)*	Representations of the entities of interest in the theory.	Chapter 2 describes the theory in regard to the key features of this research and evaluates the efficacy of the independent components while showing that a comprehensive framework does not exist linked to the specific components.
3	Principle of form and function *(the causa formalis)*	The abstract "blueprint" or architecture describes an IS artefact, either product or method/ intervention.	Chapter 4 links the literature and gaps exposed from the literature to develop the core conceptual/abstract models for the information security evaluation framework.
4	Artefact mutability	The changes in the state of the artefact anticipated in theory, that is, what the theory encompasses the degree of artefact change.	Chapter 6 describes the changes in the state of the artefacts after evaluation and testing.

5	Testable propositions	Truth statements about the design theory.	Chapter 5 describes the testing of the artefacts in order to evaluate the theory proposed by the development of the models, constructs and framework in Chapter 4.
6	Justificatory knowledge	The underlying knowledge or theory from the natural or social or design sciences that gives a basis and explanation for the design.	Chapter 2 and Chapter 4 describes the underlying knowledge for the formation of the theory.
	Additional components		
7	Principles of Implementation *(the causa efficiens)*	A description of processes for implementing the theory (either product or method) in specific contexts.	Chapter 4 describes the transformation of the conceptual/abstract models into a usable information security framework.
8	Expository instantiation	A physical implementation of the artefact that can assist in representing the theory both as an expository device and for purposes of testing.	Chapter 4 describes a physical implementation of the framework through the development of an information security evaluation tool.

4.5 SUMMARY

In this Chapter, three models were developed from the literature reviewed in Chapter 2. The first model relates to the relationship between technical and non-technical cost reduction factors and information security culture. The second model relates to the relationship between information security assessment practices and human interaction. The third model defines the five-pillar approach to improve information security culture. Specific components of these models were then synthesised into a framework called the ARCS security framework. The framework consisted of features, evaluation areas and questions and a reference model for expanding the framework and a relationship model to show the relationship of components of the framework. Lastly, an evaluation tool was developed in Excel to apply the framework and to output relevant results through pictorial graphs.

In Chapter 5, the next steps of the DSR process model selected in Chapter 3 are conducted through the demonstration, evaluation and communication of the artefacts developed in this chapter.

Chapter 5: DSR Demonstration: Analysis, Results and Findings

Chapter 1 Introduction	Research Purpose, Rationale, Background and Scope of Study
Chapter 2 Literature Review	Information Security (IS), IS Assessments, IS Architecture, IS Risk Assessment, Organisational Culture, IS Culture, Motivation, Positive Reinforcement and Reward
Chapter 3 Research Methodology	Methodology and Research Design, Participants, Instruments, Procedures and Timelines, Analysis, Ethics and Limitation
Chapter 4 Security Models, Framework and Evaluation Tool	Models for Cost Reduction, Security Assessment and Information Security Cultural Improvement, The ARCS Security Framework, The ARCS Security Evaluation Tool
Chapter 5 Analysis, Results and Findings	Analysis, Results and Findings of the Demonstration of the ARCS Security Evaluation Tool
Chapter 6 Review and Update of the Evaluation Tool	Evaluation of Expert Reviews of the ARCS Security Model and the ARCS Security Evaluation Framework Update of the ARCS Security Evaluation Framework
Chapter 7 Further Research and Future Studies	Further Research and Future Studies
Chapter 8 Conclusion	Conclusion

Chapter 5: DSR Demonstration: Analysis, Results and Findings

In Chapter 4, five artefacts were developed. Three models were designed relating to the key focus areas of this study which are information security assessment methods, cost and culture. Components of the three models were synthesised to develop the ARCS Security Framework. Based on the features and evaluation areas of the ARCS Security Framework the Security Evaluation Tool was developed.

In this chapter, the researcher will focus on the Demonstration, Evaluation and Communication process steps of the selected DSR process model described in Chapter 3. The researcher will outline the findings of the analysis of the first iteration of artefacts developed, which was conducted with expert reviewers. The expert reviews were conducted on the security framework and evaluation tool.

Five expert reviewers participated in the study. Sections 5.1 to 5.15 will focus on the suitability of reviewers as expert evaluators, a description of the organisation that was evaluated, the output and analysis of evaluation results from the tool and the review of the framework and tool by the expert reviewers. Section 5.16 will summarise the inputs given by the participants and the observation of the researcher through the demonstration and evaluation processes.

5.1 PROCESS OF CONDUCTING RESEARCH

The researcher made initial contact with twelve prospective organisations via email outlining the study, the expectation of participating in the study and the expectations of the potential participant's time in completing the study. Based on positive responses from prospective participants, the researcher then set up a time to meet at the participant's place of work based on their availability. The researcher conducted the interviews in the following order:

i. The researcher introduced himself and the outline of the study.

ii. The participant was requested to read and accept the "Consent to Participate" document.

iii. The participant was asked to agree to the interview being recorded and was advised that this was only for the researcher's reference purposes and that all information would be anonymised in the study and any further publications.

iv. The researcher then explained the process that would be followed during the interview, which included; describing the models that led to the development of the ARCS Security Framework, describing the Security Framework, describing the Security Evaluation Tool

v. The researcher conducted an assessment using the Security Evaluation Tool, presenting the results of the tool to the participants.

The researcher then conducted an expert review of the framework and the evaluation tool and a review of the results from the assessment using a semi-structured interview questionnaire along with observations based on their experience and capability in the information security field. The results of this process are described in the following sections.

5.2 DETAILS OF PARTICIPANT ONE

Participant One (P1) has more than twenty-five years of experience in the security and IT industry. P1's role at the time of the interview was as Director: Security and Architecture for a large multi-national Fast-Moving Consumer Goods company. The company is a global organisation that employs almost two hundred thousand employees and has a revenue of more than forty billion US dollars annually. The company has an international security team that shares security products and services.

The participant has managed a cyber security environment for more than seven years and has strong operational experience to support his understanding of cyber security. Therefore, he was an excellent candidate to be able to give his expert opinion on the artefacts presented. The assessment and corresponding review took approximately two hours with this participant.

5.3 OUTPUT OF THE ASSESSMENT USING THE SECURITY EVALUATION TOOL FOR PARTICIPANT ONE

5.3.1 Participant One - Evaluation of the Assessment of Information Security Risk Feature

The evaluation output of Feature 1 – Information Security Risk for Participant One is depicted below in Figure 5-1. The output score for each evaluation area is described in Table 5-1 with an overall weighted score of 65.83 percent for the Feature.

Table 5-1 Participant One – Information Security Risk Assessment Feature (F1) Score

EVALUATION AREA	EVALUATION SCORE
E1.1 - Security Assessment (SECASSESS)	87.5%
E1.2 - Security Architecture (SECARCH)	50%
E1.3 - Risk Assessment (RSKASSESS)	60%
Overall weighted score	**65.83%**

In the SECASSESS evaluation area, the participant noted that security best practices were followed in line with the ISO 27000 (Prislan and Bernik 2010) series of security standards as well as aligning to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework (Strom, Applebaum, Miller, Nickels, Pennington and Thomas 2018). The organisation conducted ISO 27001 audits every three years and aligned its security strategy to the gaps identified, while the ATT&CK framework was used for short-term cyber security risk reduction. These security assessments were aligned to individual security employees and departmental KPIs.

The outputs of the assessments were shared with senior leadership within the organisation for high-level visibility.

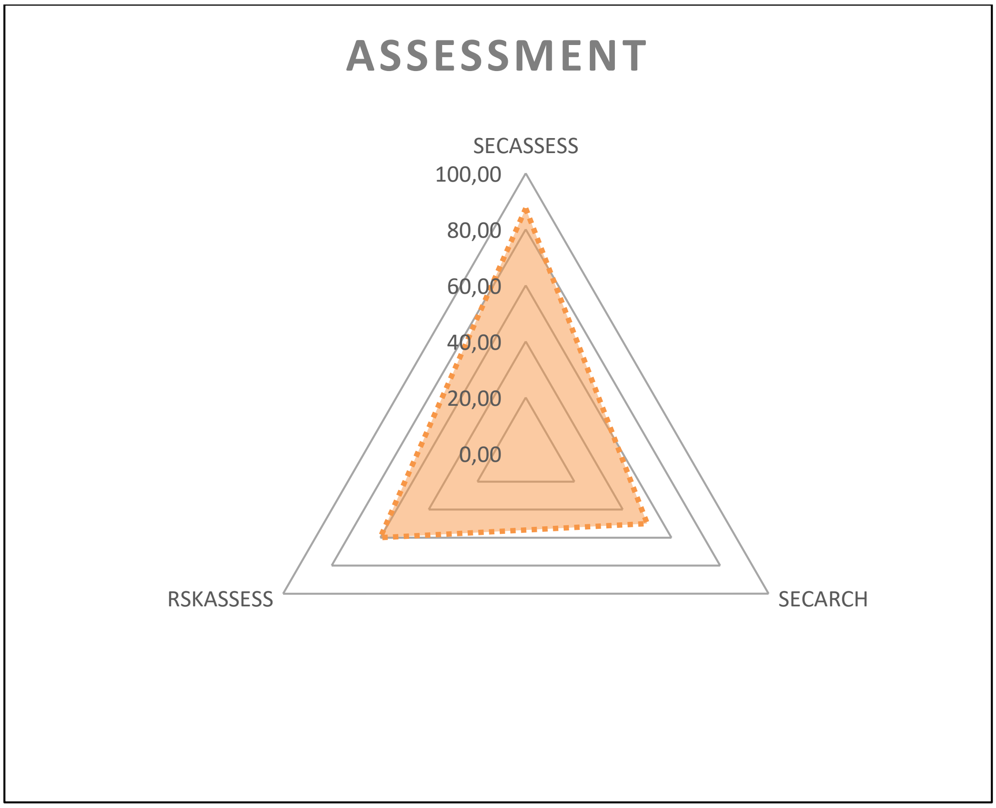


Figure 5-1 Participant One Assessment of Information Security Risk Feature Graph

In the SECARCH evaluation area, it was established that the organisation does not follow a defined security architecture method or approach, but it does follow specific best practices for IT/IS Policy, Governance and Operations.

In the RSKASSESS evaluation area, although risk is catalogued, reporting to senior leadership and following a best practice or standard are not followed throughout the organisation.

5.3.2 Participant One - Assessment of the Reduction of Information Security Cost Feature

The evaluation output of Feature 2 – Reduction of Information Security Cost for Participant One is depicted below in Figure 5-2. The output score for each evaluation area is described in Table 5-2 with an overall weighted score of 71.15 percent for the Feature.

Table 5-2 Participant One – Reduction of Information Security Cost Feature (F2) Score

EVALUATION AREA	**EVALUATION SCORE (%)**
E2.1 - Business Continuity Management (BCM)	100%
E2.2 - Cyber Security Insurance (CSI)	0%
E2.3 - Employee Information Security Training (EIST)	75%
E2.4 - Having a CISO (HACISO)	50%
E2.5 - Board Input on Security Spend (BIOSS)	100%
E2.6 - Having a CPO (HACPO)	50%
E2.7 - Incident Response Team (IRT)	100%
E2.8 - Use of Encryption (UOE)	33.33%
E2.9 - Threat Analysis and Sharing (TAS)	100%
E2.10 - Security Analytics Services (SAS)	100%
E2.11 - Data Loss Prevention (DLP)	100%
E2.12 - Data Classification (DC)	50%
E2.13 - Information Security Input Costs (ISIC)	66.67%
Overall weighted score	**71.15%**

In the BCM evaluation area, the participant noted that planning processes and standards were in place for business continuity. In addition, the organisation was certified against an international standard, while periodic tests were conducted to confirm the validity of plans and processes.

In the CSI evaluation area, it was confirmed that the organisation does not purchase cyber security insurance and does not plan to do so.

In the EIST evaluation area, it was established that the organisation has a good information security programme that includes specific training for specific levels and types of employees. The training was, however, noted as reactive and not dynamic.

In the HACISO evaluation area, the organisation has a CISO, but the person does not report to the board. The person does, however, report to the CFO, who reports to the board.

In the BIOSS evaluation area, it was confirmed that the board has security advice spending and that information security risk is regularly presented to the board for evaluation and guidance.

In the HACPO evaluation area, it was established that the organisation does not have a Chief Privacy Officer but that there is a robust data privacy programme in place. The organisation is in the process of establishing a Chief Privacy Officer role.

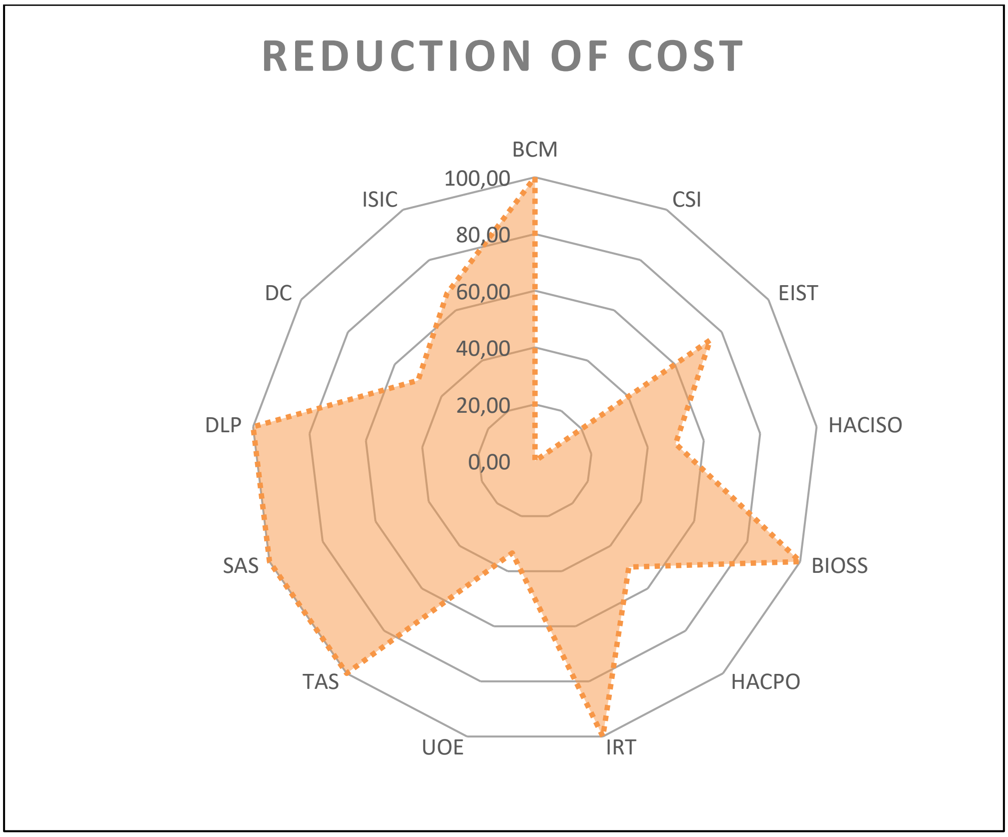


Figure 5-2 Participant One – Reduction of Information Security Cost Feature Graph

In the IRT evaluation area, the participant noted a highly competent Global Security Operations Centre (GSOC) that supports the organisation. This team also contains an Incident Response Team as well as a Red Team that conducts penetration testing. One of the KPIs of the in-country security team is directly aligned to the remediation of issues found by the Red Team.

In the UOE evaluation area, it was established that only data that is transmitted is encrypted. The participant noted that this is required as part of the control framework defined by the IT compliance team. However, other devices and data at rest are not encrypted.

In the TAS evaluation area, the GSOC team also contains a threat hunting team that conducts consistent analysis to evaluate information security threats proactively. The organisation further employs an outsourced partner to conduct deep and dark web threat analysis.

In the SAS evaluation area, it was established, as noted above, that an extensive GSOC supports the organisation. Threats, incident and alert analysis is conducted in this functional area. It was noted that this is a robust, mature function within the organisation.

In the DLP evaluation area, the organisation also performed very well. Data leakage or loss was actively evaluated and several preventative measures were in place. The technology is well supported by policy and governance.

In the DC evaluation area, it was established that a data classification policy exists but it is not strictly enforced.

In the ISIC evaluation area, the participant advised that strict budgeting is enforced for the purchase of information security products, services, technology and human resources. However, the organisation has not established a method to budget for incidents that may occur.

5.3.3 Participant One - Assessment of the Sustainability of Information Security Culture Feature

The evaluation output of Feature 3 – Sustainability of Information Security Culture for Participant One is depicted below in Figure 5-3. The output score for each evaluation area is described in Table 5-3 with an overall weighted score of 30.24 percent for the Feature.

Table 5-3 Participant One – Sustainability of Information Security Culture Feature (F3) Score

EVALUATION AREA	**EVALUATION SCORE**
E3.1 - Pillar 1- Common Security Values and Principles (CSVP)	25%
E3.2 - Pillar 2- Positive Reinforcement and Reward (PRR)	0%
E3.3 - Pillar 3- Common and Couple Processes (CCP)	50%
E3.4 - Pillar 4- Peer Recognition (PREC)	33.33%
E3.5 - Pillar 5- Technical Training and Awareness of Security Issues (TTSA)	42.86%
Overall weighted score	**30.24%**

In the CSVP evaluation area, the participant advised that while the values and company principles of information security were communicated, this was usually to the employees outside of the IT department. The organisation was not evaluated against these principles and the IT department did not focus on how each function in the department addressed and was responsible for information security.

In the PRR evaluation area, the participant advised that there was no programme in place to evaluate employees’ behaviour regarding information security. As such the organisation did not reward or recognise potential positive actions.

In the CCP evaluation area, it was established that the IT team was very aware of the impact of security remediation in their environments, but it was not communicated explicitly via the security department.

In the PREC evaluation area, it was established that the organisation does recognise good security behaviour as part of its information security awareness campaign, but it is a purely management-led programme and this good behaviour is not communicated to other employees as a means of peer recognition.

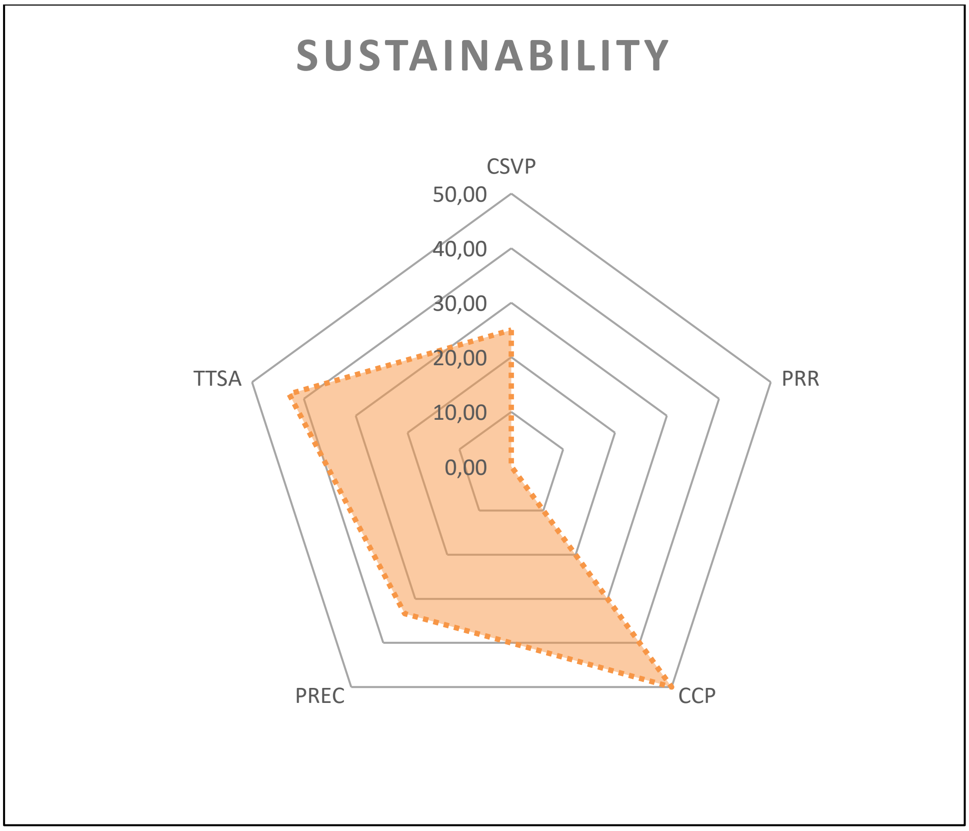


Figure 5-3 Participant One – Sustainability of Information Security Culture Feature Graph

In the TTSA evaluation area, it was established that the organisation has a robust security and awareness programme that includes awareness for IT staff but is not targeted at senior and executive employees. There is no measurement of the programme and the improvements derived thereof.

5.3.4 Overall Summary – Participant One

The overall summary showed that participant one’s organisation performed well in the Reduction of Information Cost feature, above average in the Assessment of Information Security feature and poorly in the Sustainability of Information Security Culture feature, as described in Figure 5-4.

The participant agreed on the overall summary output, which is further discussed in Section 5.3 below. The evaluation shows many technical products and solutions in place in the organisation, while it is generally aligned to information security best practices and standards.

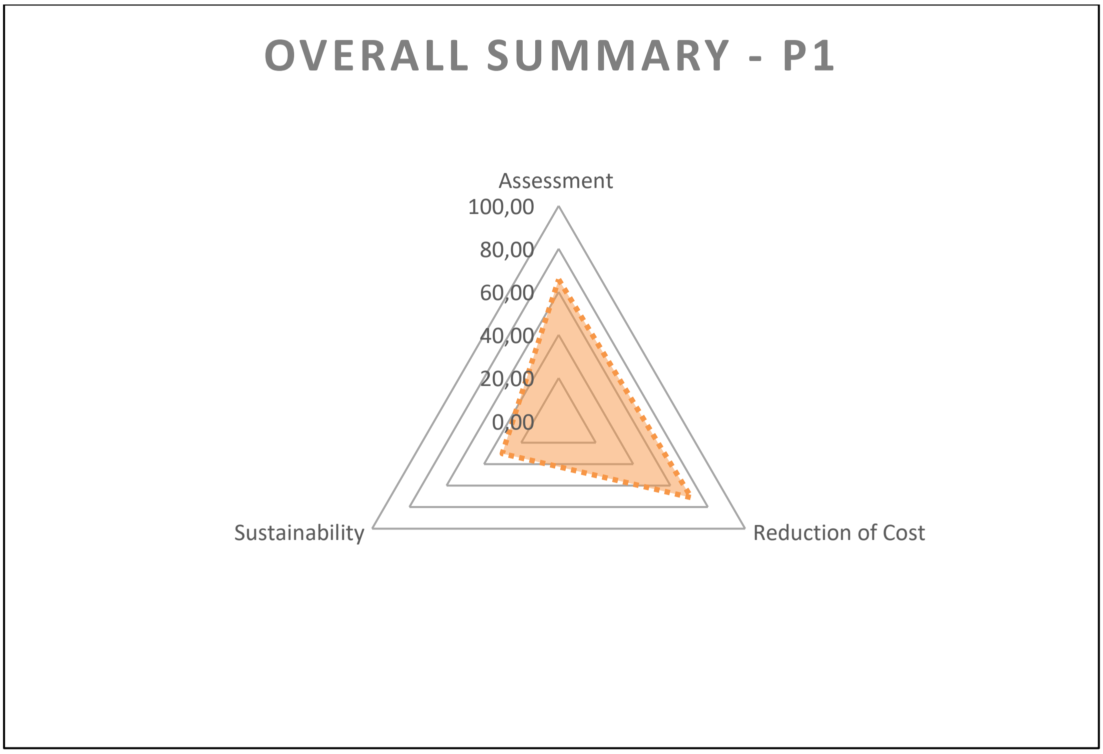


Figure 5-4 Overall Summary of Evaluation for Participant One

Furthermore, the company measures the work performance related to information security. However, the organisation does not communicate good practices to its employees nor forewarns employees about potential threats. As a result, the overall culture of information security is poor and may lead to potential information risk through people not understanding and being aligned to the information security concerns.

Overall, the organisation’s current position is very good but can be improved to allow for longer-term information security stability and reduced risk.

5.4 EXPERT REVIEWER’S EVALUATION OF FRAMEWORK AND TOOL

5.4.1 Evaluation of the Framework

Evaluation of the Framework - Participant One	
Question	**Response**
What are your views on the components of the ARCS Security Framework?	The participant noted that he did see value in the framework and that the features of the framework were easily identifiable areas that were aligned to his organisation.
Do you see value in the components of the framework?	The participant saw the value of improving culture and commented that long-term sustainability in improving information security was a key driver for his organisation.
Are the components of the framework applicable to your organisation?	The participant felt that the researcher needed to give more detail on the expected outcome of the evaluation tool and the framework’s application. In addition, he commented on the need to manage user expectations regarding the limits of the framework and output results. Finally, the participant required a better view of the relevant employee level that the framework and output of the evaluation tool were aimed at.
What are your views on the structure of the framework?	The participant noted the framework needs to translate the effect of the evaluation areas into the actual applicable actions, alluding to the practicality of dealing with the gaps identified by the evaluation. The researcher did advise that the framework as presented was a high-level evaluation and that detailed remedial actions could be delivered with a more detailed analysis or an expansion of the framework to a more detailed level.

Question	Response
What are the components that you feel were not covered?	The participant also wanted to understand the relationships between the evaluation areas and their respective feature (e.g. encryption linked to cost). The participant wanted better reporting regarding how the output of the evaluation assisted in creating a business case for investment /disinvestment in information security. He felt that the researcher needed to better articulate the framework's scope and limitations up front when communicating with a person using the framework.
What improvements and/or changes can you advise on for the framework?	The participant also felt that the framework did not cover the quality and efficacy of the technical components evaluated. He suggested a need to develop a deeper evaluation on the specifics of each evaluation area.
Are there any general views or comments on the framework?	The participant felt that the next iteration of the framework needs to be scaled. Since the answers are currently binary, some areas can be variable and he recommended a variable response scale. The participant also recommended benchmarking against other organisations or similar organisations. The researcher did advise that the framework is geared towards general analysis and could be enhanced for specific industries or company types. The participant also noted that he would like to have seen more comprehensive recommendations to give the users better insight into the results.

5.4.2 Evaluation of the tool

Evaluation of the Tool- Participant One	
Question	**Response**
Are outcomes of the evaluation tool an accurate reflection of the information security position of the organisation in its current state?	The participant advised that the outcomes of the tool was relevant to the organisation and aligned to the current landscape
What are your views on the structure and application of ARCS Security Evaluation Tool?	The participant noted that he does see a clear relationship between the tool and the framework but that there needs to be more information given upfront to the user to understand how the framework and tools work together.
Do you see the value in the Evaluation Tool concerning the Framework developed?	The participant felt that the parallel development of a tool with the framework was a good concept and would help an organisation apply the framework rather than just have a complex instrument that could not be used.
Do you see the applicability of the implementation of the tool in your organisation?	The participant did see the applicability of the implementation of the tool in his environment.
What are the views on the scoring mechanism and weighting of questions?	The participant felt that an explicit score should be displayed in the summary section of the tool and an overall risk or maturity level rating to be given based on the overall evaluation. The participant also wanted to understand better how the evaluation areas were linked and the logic of the scoring. Overall, he felt that the output score was a true reflection of his environment.

Question	Response
What are your views on the quality and value of the output charts generated?	The participant felt that the output charts must be synthesised for senior and executive engagement and communication to communicate business alignment and value of the output. He felt that output in its current form is only understandable for technical or IT employees.
What improvements and/or changes can you advise on for the evaluation tool?	The participant felt that there needs better reporting and recommendations. He also noted that the output reports need to look better and give more information. He noted that tags need to be made explicit as he did not necessarily know the abbreviations of tags in each evaluation area. The participant felt that the tool needed to be modernised in that it should move into an application rather than an Excel file. He suggested a web application with a dashboard and pro forma detailed management report.
What are your general views or comments on the evaluation tool?	The participant felt that the tool is applicable in the organisation and needs to take the output and create a recommendation in a business case or recommendation report. In addition, he felt the output needs to give guidelines so that if the evaluation is redone, the organisation would understand what needs to be done to improve.

5.5 DETAILS OF PARTICIPANT TWO

Participant Two (P2) has more than thirty years of experience in the security and IT industry. P2’s role at the time of the interview was as Senior Manager: Security Development for a large national information technology service provider. The company is a local organisation that employs approximately four thousand five hundred employees and has a revenue of more than five billion rands annually. The company is the main service provider for IT services to national, provincial and local governments and supports a very large user base. The company has an internal security team as well as multiple other teams that support specific customers. The assessment conducted with this participant was based on the internal organisation.

The assessment and corresponding review took approximately two hours with this participant.

The participant has managed a cyber security environment for more than 20 years and has strong operational experience in the information security space to support his understanding of cyber security. He was, therefore, a good candidate to be able to give his expert opinion on the artefacts presented.

5.6 OUTPUT OF THE ASSESSMENT USING THE SECURITY EVALUATION TOOL FOR PARTICIPANT TWO

5.6.1 Participant Two - Evaluation of the Assessment of Information Security Risk Feature

The evaluation output of Feature 1 – Information Security Risk for Participant Two is depicted below in Figure 5-5. The output score for each evaluation area is described in Table 5-4 with an overall weighted score of 71.67 percent for the Feature.

Table 5-4 Participant Two – Information Security Risk Assessment Feature (F1) Score

EVALUATION AREA	**EVALUATION SCORE**
E1.1 - Security Assessment (SECASSESS)	75%
E1.2 - Security Architecture (SECARCH)	100%
E1.3 - Risk Assessment (RSKASSESS)	40%
Overall weighted score	**71.67%**

In the SECASSESS evaluation area, the participant noted that security best practices were followed in line with the ISO 27000 (Prislan and Bernik 2010) series of security standards only. The organisation conducted ISO 27001 audits every year and aligned its security strategy to the gaps identified. The outputs of the assessments were shared with senior leadership within the organisation for high-level visibility. As this organisation is a State-Owned Company, the audit results are also shared with the main Government stakeholder.

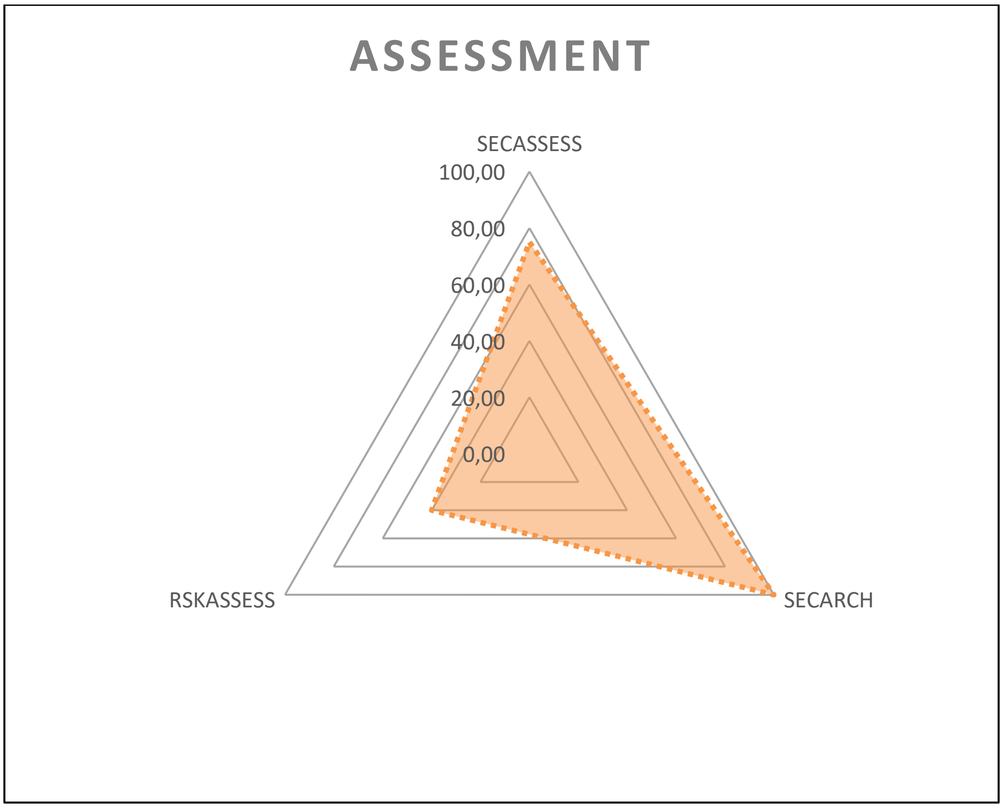


Figure 5-5 Participant Two Assessment of Information Security Risk Feature Graph

In the SECARCH evaluation area, it was established that the organisation does follow a defined security architecture method or approach. The organisation has developed a bespoke Security Architecture Framework based on inputs from The Open Group Enterprise Information Security Architecture, the Sherwood Applied Business Security Architecture (Sherwood et al. 2004), COBIT for Security Control Framework (Lepofsky 2014) and the ISO 27000 (Prislan and Bernik 2010)standard. The team plans a long-term security strategy based on this framework and uses it as input for security budgeting.

In the RSKASSESS evaluation area, it was established that a management framework is in place and assessed and evaluated independently via the organisation’s Internal Audit department. However, the risk management process is ad-hoc and not aligned to any specific remediation KPIs. As a result, security risk is not identified in new IT projects. The results of the assessments are shared with reporting to senior leadership.

5.6.2 Participant Two - Assessment of the Reduction of Information Security Cost Feature

The evaluation output of Feature 2 – Reduction of Information Security Cost for Participant Two is depicted below in Figure 5-6. The output score for each evaluation area is described in Table 5-5 with an overall weighted score of 26.10 percent for the Feature.

Table 5-5 Participant Two – Reduction of Information Security Cost Feature (F2) Score

EVALUATION AREA	EVALUATION SCORE
E2.1 - Business Continuity Management (BCM)	66.67%
E2.2 - Cyber Security Insurance (CSI)	0%
E2.3 - Employee Information Security Training (EIST)	100%
E2.4 - Having a CISO (HACISO)	0%
E2.5 - Board Input on Security Spend (BIOSS)	33.33%
E2.6 - Having a CPO (HACPO)	0%
E2.7 - Incident Response Team (IRT)	25%
E2.8 - Use of Encryption (UOE)	0%
E2.9 - Threat Analysis and Sharing (TAS)	50%
E2.10 - Security Analytics Services (SAS)	0%
E2.11 - Data Loss Prevention (DLP)	14.29%
E2.12 - Data Classification (DC)	50%
E2.13 - Information Security Input Costs (ISIC)	0%
Overall weighted score	**26.10%**

In the BCM evaluation area, the participant noted that planning processes and standards were in place for Business Continuity. The organisation followed an international standard, but periodic tests were not conducted to confirm the validity of plans and processes. When tests were conducted, the results were shared with senior leadership.

In the CSI evaluation area, it was confirmed that the organisation does not purchase cyber security insurance and does not plan to do so.

In the EIST evaluation area, it was established that the organisation has a good information security awareness and training programme that includes specific training for specific levels and types of employees. The training was, however, noted as reactive and not dynamic.

In the HACISO evaluation area, it was established that the organisation does not have a CISO. Instead, the security management team reports to the Head of IT Operations.

In the BIOSS evaluation area, it was confirmed that the board has a view of security budgets and spend. However, information security risk is not regularly presented to the board for evaluation and guidance.

In the HACPO evaluation area, it was established that the organisation does not have a Chief Privacy Officer, nor is there a data privacy programme in place. The participant noted that this is a significant deficiency considering that South Africa has specific legalisation focusing on data privacy, which is coming into effect.

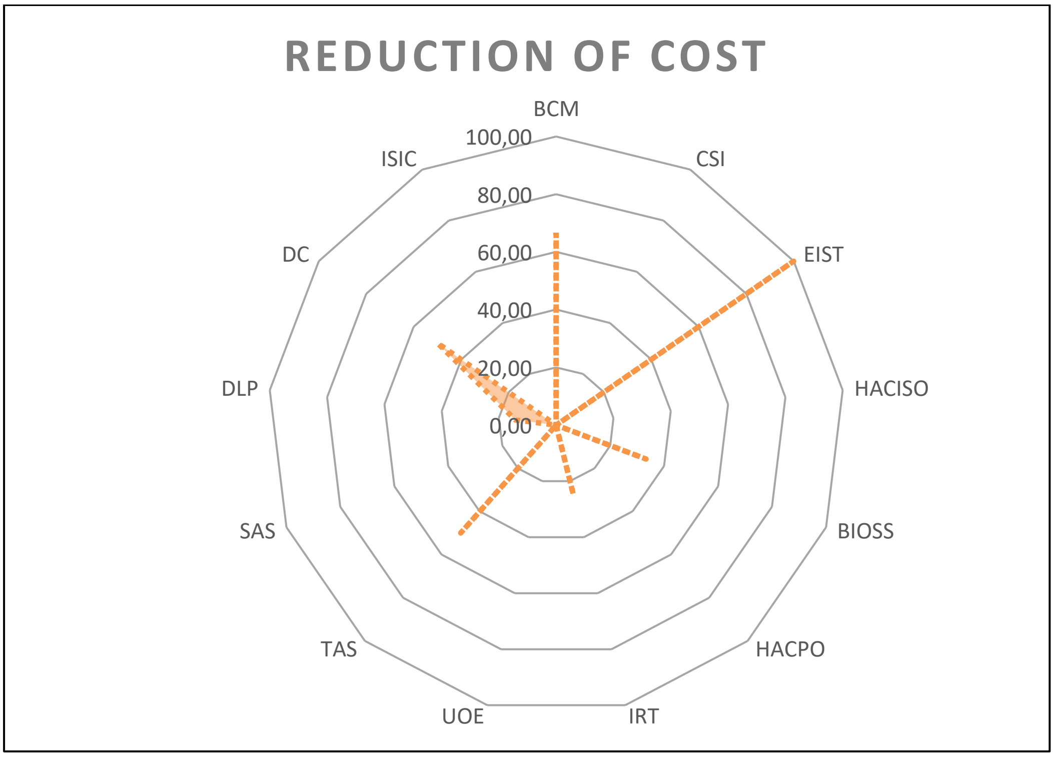


Figure 5-6 Participant Two – Reduction of Information Security Cost Feature Graph

In the IRT evaluation area, the participant noted that there is no Incident Response or Security Operation Centre in the organisation. Ad-hoc external penetration testing is done, but no active threat analysis is conducted. The results of the penetration tests are not shared with relevant stakeholders and there are no KPIs assigned to the remediation of the findings.

In the UOE evaluation area, it was established that encryption is not a standard for any type of data.

In the TAS evaluation area it was found that some level of threat analysis is conducted, but it not actively done. These activities are ad-hoc and are not done on a periodic basis.

In the SAS evaluation area, it was established the organisation has no Security Operations Centre, does not log or analyse security events in the environment and does not have a plan or process to address active security threats.

In the DLP evaluation area, the organisation does not have policies, procedures or technical controls for Data Loss prevention. For example, there is a data retention policy defined, but it is not enforced.

In the DC evaluation area, a Data Classification policy exists, but it is not strictly enforced.

In the ISIC evaluation area, the participant advised that basic budgeting is enforced to purchase information security products, services, technology and human resources. However, the organisation has not established a method to budget for incidents that may occur and does not use historical information to plan future budgets.

5.6.3 Participant Two - Assessment of the Sustainability of Information Security Culture Feature

The evaluation output of Feature 3 – Sustainability of Information Security Culture for Participant Two is depicted in Figure 5-7. The output score for each evaluation area is described in Table 5-6 with an overall weighted score of 54.29 percent for the Feature.

Table 5-6 Participant Two – Sustainability of Information Security Culture Feature (F3) Score

EVALUATION AREA	EVALUATION SCORE
E3.1 - Pillar 1- Common Security Values and Principles (CSVP)	75%
E3.2 - Pillar 2- Positive Reinforcement and Reward (PRR)	25%
E3.3 - Pillar 3- Common and Couple Processes (CCP)	100%
E3.4 - Pillar 4- Peer Recognition (PREC)	0%
E3.5 - Pillar 5- Technical Training and Awareness of Security Issues (TTSA)	71.43%
Overall weighted score	**54.29%**

In the CSVP evaluation area, the participant advised that security values and company principles of information security were communicated to all employees. The organisation was not evaluated against these principles. The IT department focuses on how each department's function addressed and was responsible for information security. This is prevalent because the organisation consists mainly of IT employees.

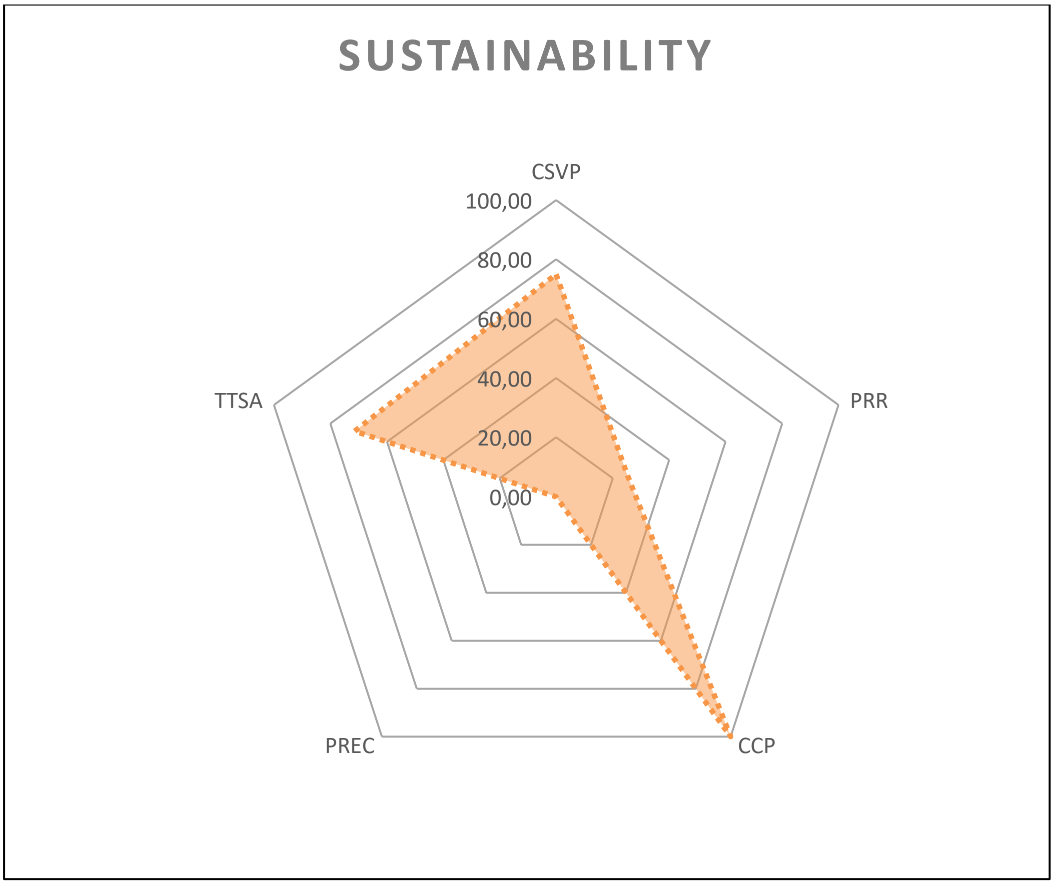


Figure 5-7 Participant Two – Sustainability of Information Security Culture Feature Graph

In the PRR evaluation area, the participant advised that the organisation does not reward staff for good security behaviour and as such, this is not periodic or immediate. The company does, however, generally communicate via email to all staff when good behaviour is observed.

In the CCP evaluation area, it was established that the IT team is very aware of the impact of security remediation in their environments. Furthermore, the importance of information security is a common theme that is supported and communicated by managers in all departments and units.

In the PR evaluation area, it was established that no peer group recognises good security behaviour. In addition, there is no employee-led security programme and therefore, no information provided about such programme to employees.

In the TTSA evaluation area, it was established that the organisation has a robust security and awareness programme that includes awareness for IT staff but is not targeted at senior and executive employees. As a result, there is no measurement of the programme and the improvements derived thereof.

5.6.4 Overall Summary – Participant Two

The overall summary showed that participant two's organisation performed well in the Assessment of Information Security feature but did not perform well in the Reduction of Information Cost feature or the Sustainability of Information Security Culture feature, as depicted in Figure 5-8.

The participant agreed on the overall summary output, which is further discussed in Section 5.6 below. The evaluation shows that the organisation is excellent at assessing and understand its security needs and current security position but does not perform well at addressing the gaps identified.

There are few technical products and solutions in place in the organisation and limited technical controls in place to reduce information security risk. The organisation does not measure the work performance related to information security and does not communicate good practices to its employees nor forewarns employees about potential threats. The overall culture of information security is poor and may lead to a potential information risk through people not understanding or being aligned with information security concerns.

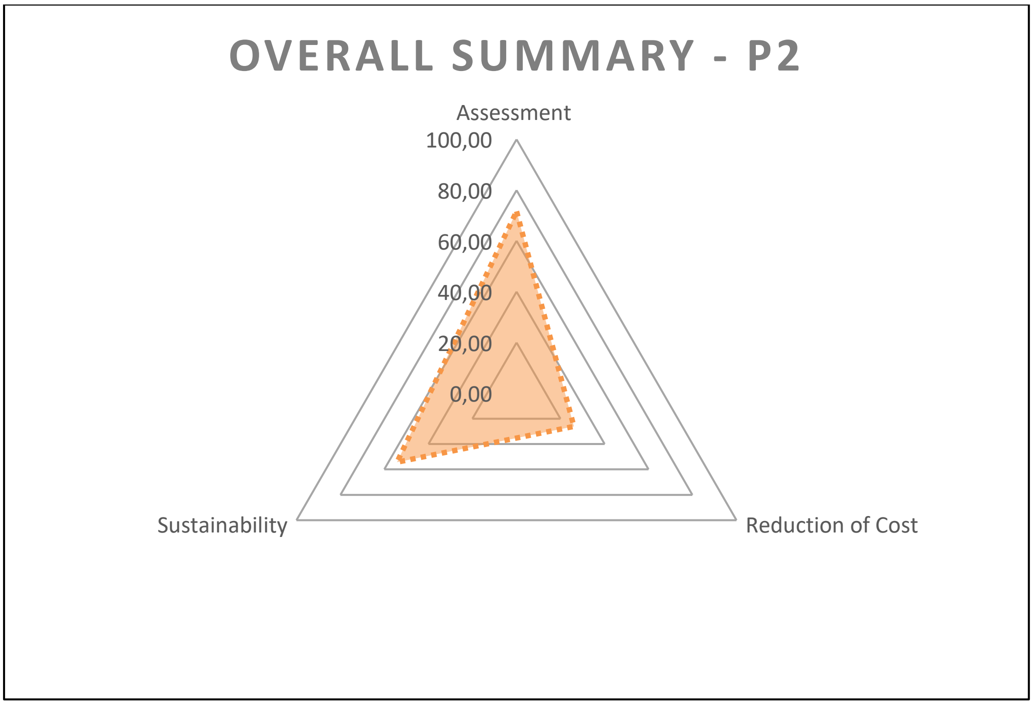


Figure 5-8 Overall Summary of Evaluation for Participant Two

Overall, the organisation’s current security position is average and can be improved significantly by identifying better security tools and products and improving the capability of the information security human resources. In addition, due to the poor approach to sustaining information security culture, the organisation has significant room for improvement in that area.

5.7 EXPERT REVIEWER’S EVALUATION OF FRAMEWORK AND TOOL

5.7.1 Evaluation of the Framework

Evaluation of the Framework - Participant Two	
Question	**Response**
What are your views on the components of the ARCS Security Framework?	The participant liked the relational part of the framework and felt that the linking of evaluation areas helped users understand more about their environment. P2 felt that that the framework was tangible and reusable. He felt that as we were dealing with a complex topic, the framework simplified an evaluation for less experienced people.
Do you see value in the components of the Framework?	The participant found that the modularity of the framework was beneficial. He noted that as the security industry changes, security management requires continuous improvement and that this framework would help with that. Overall, the participant found value in the framework.
Are the components of the framework applicable to your organisation?	The participant found the components of the framework very applicable to his organisation. He felt that the variance in themes was beneficial. He also felt that the framework is applicable to various organisations but probably more relevant to larger organisations.
What are your views on the structure of the framework?	The participant found the structure of the framework very easy to understand. He also felt that the structure was logical.

What are the components that you feel were not covered?	The participant felt that an evaluation of maturity levels was not covered in each feature area. He felt that for longer-term features such as information security culture, more information needs to be given to the user to develop a roadmap for improvement.
What improvements and/or changes can you advise on for the Framework?	The participant suggests including innovation components in the security field into the framework. He suggested the researcher consider introducing innovation in improving security as an evaluation area and would have liked to have seen a maturity rating as part of the framework.
Are there any general views or comments on the framework?	The participant generally felt that the framework was valuable and adaptable for future use. He could not comment on any improvements to the framework.

5.7.2 Evaluation of the Tool

Evaluation of the Tool- Participant Two	
Question	**Response**
Are outcomes of the Evaluation Tool an accurate reflection of the information security position of the organisation in its current state?	The participant advised that since empirical responses were used in the evaluation, the evaluation outcome was accurate and aligned to his organisation.
What are your views on the structure and application of ARCS Security Evaluation Tool?	The participant noted that he feels that the tool is accurate and aligned to the framework. P2 felt that the tool could be improved by implementing it as a technology application.
Do you see the value in the Evaluation Tool with respect to the Framework developed?	The participant felt that he does see the value of the application of the evaluation tool by bringing together people, processes and technology. In addition, he felt that the tool

	brings important areas of evaluation together in a cohesive application.
Do you see the applicability of the implementation of the tool in your organisation?	The participant did see the applicability of the implementation of the tool in his organisation. He felt that by using the tool, he would justify his security strategy in his organisation as the tool would be a scientific evaluation that gives input to decision making.
What are the views on the scoring mechanism and weighting of questions?	The participant felt that scoring was balanced and that outputs were relatively accurate. He felt that the tool was aligned with his tacit understanding of the environment that he worked in and that the evaluation confirmed his organisation’s views.
What are your views on the quality and value of the output charts generated?	The participant felt that the quality was good enough to explain the evaluation outputs. He felt that the tool could be improved with a narrative management report.
What improvements and/or changes can you advise on for the Evaluation Tool?	The participant felt that the user interface could be improved and that the spider graphs could be redefined in other forms to give more clarity on the data represented.
What are your general views or comments on the Evaluation Tool?	The participant felt that the tool is a valuable innovation. He reiterated that he sees good value and applicability of this tool to his organisation.

5.8 DETAILS OF PARTICIPANT THREE

Participant Three (P3) has more than twenty years of experience in the security and IT industry. P3’s role at the time of the interview was as Director: Information Security and Enterprise Architecture for a large national government department. The department is an organisation that employs almost two hundred thousand employees and commands a government budget in excess of sixty billion rands. The department has a small security team comprising mostly mid-management level employees supported by external vendors and services providers. The assessment and corresponding review took approximately two hours with this participant.

The participant has managed a cyber security environment for more than ten years and has strong IT operational experience to support her understanding of cyber security. She was therefore a good candidate to be able give her expert opinion on the artefacts presented.

5.9 OUTPUT OF THE ASSESSMENT USING THE SECURITY EVALUATION TOOL FOR PARTICIPANT THREE

5.9.1 Participant Three - Evaluation of the Assessment of Information Security Risk Feature

The evaluation output of Feature 1 – Information Security Risk for Participant Three is depicted below in Figure 5-9. The output score for each evaluation area is described in Table 5-7, with an overall weighted score of 90.28 percent for the Feature.

Table 5-7 Participant Three– Information Security Risk Assessment Feature (F1) Score

EVALUATION AREA	EVALUATION SCORE
E1.1 - Security Assessment (SECASSESS)	87.5%
E1.2 - Security Architecture (SECARCH)	83.33%
E1.3 - Risk Assessment (RSKASSESS)	100%
Overall weighted score	**90.28%**

In the SECASSESS evaluation area, the participant noted that security best practices were followed in line with the ISO 27000 (Prislan and Bernik 2010) series of security standards. The organisation conducted ISO 27001 audits annually and aligned its security strategy to the gaps identified. An independent third-party service provider conducted these assessments. These security assessments were aligned to individual and departmental KPIs. The outputs of the assessments were shared with senior leadership within the organisation for high-level visibility.

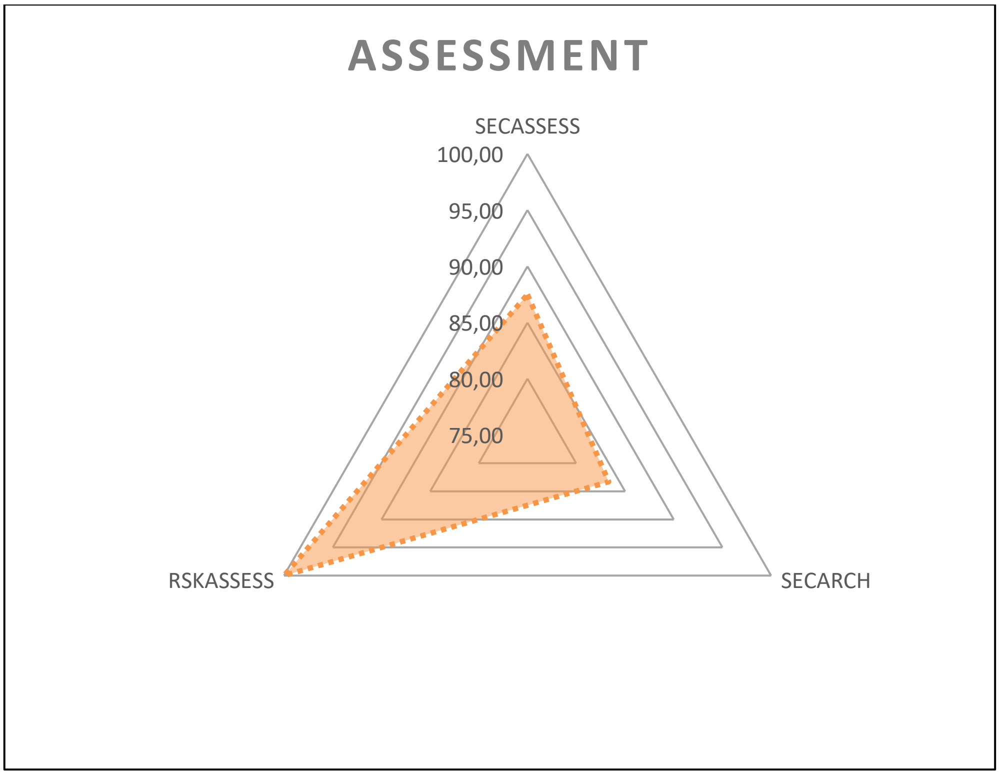


Figure 5-9 Participant Three Assessment of Information Security Risk Feature Graph

In the SECARCH evaluation area, the organisation follows a defined security architecture method or approach. The organisation used an external service provider to develop a bespoke Security Architecture Framework which is applied within the organisation. The team plans long-term security strategy based on this framework.

In the RSKASSESS evaluation area, it was established that an organisation-wide risk framework was implemented, with a specific focus on Information security risk. KPIs are defined for remediation of risks identified. Information security risk identification and risk management is also integrated into the IT project management process. Risks identified and planned to mitigate risks are communicated at the highest level of leadership.

5.9.2 Participant Three - Assessment of the Reduction of Information Security Cost Feature

The evaluation output of Feature 2 – Reduction of Information Security Cost for Participant Three is depicted below in Figure 5-10. The output score for each evaluation area is described in Table 5-8 with an overall weighted score of 43.96 percent for the Feature.

Table 5-8 Participant Three– Reduction of Information Security Cost Feature (F2) Score

EVALUATION AREA	**EVALUATION SCORE**
E2.1 - Business Continuity Management (BCM)	66.67%
E2.2 - Cyber Security Insurance (CSI)	0%
E2.3 - Employee Information Security Training (EIST)	50.00%
E2.4 - Having a CISO (HACISO)	0%
E2.5 - Board Input on Security Spend (BIOSS)	66.67%
E2.6 - Having a CPO (HACPO)	0%
E2.7 - Incident Response Team (IRT)	50.00%
E2.8 - Use of Encryption (UOE)	33.33%
E2.9 - Threat Analysis and Sharing (TAS)	0%
E2.10 - Security Analytics Services (SAS)	50.00%
E2.11 - Data Loss Prevention (DLP)	71.43%
E2.12 - Data Classification (DC)	100.00%
E2.13 - Information Security Input Costs (ISIC)	83.33%
Overall weighted score	**43.96%**

In the BCM evaluation area, the participant noted that business continuity planning was in place but not necessarily a process to test and verify the plans. The plans are aligned to an ISO standard and the business areas have input into the plan. The plans are tested on an ad-hoc basis. The test results are not communicated to senior leadership.

In the CSI evaluation area, it was confirmed that the organisation does not purchase cyber security insurance and does not have a plan to do so.

In the EIST evaluation area, it was established that the organisation has a good information security awareness programme. The programme is not tailored to nor targets senior leadership. The programme is not dynamic in that awareness and training are submitted to employees on a periodic static basis. There is some testing of employees understanding of the training and awareness initiatives, but it is not standardised across the entire organisation.

In the HACISO evaluation area, it was established that the organisation does not have a CISO. However, the participant does report to the most senior person in the IT department, who in turn reports to the head of the organisation.

In the BIOSS evaluation area, it was confirmed that this organisation, being a government entity, does not report to a board but to a ministerial committee and, in extension, to parliament. However, the budgets and security spend are visible to this committee and the committee directly impacts the budget and spend. Risks identified are communicated at this level as well.

In the HACPO evaluation area, it was established that the organisation does not have a Chief Privacy Officer, nor is there a data privacy programme in place.

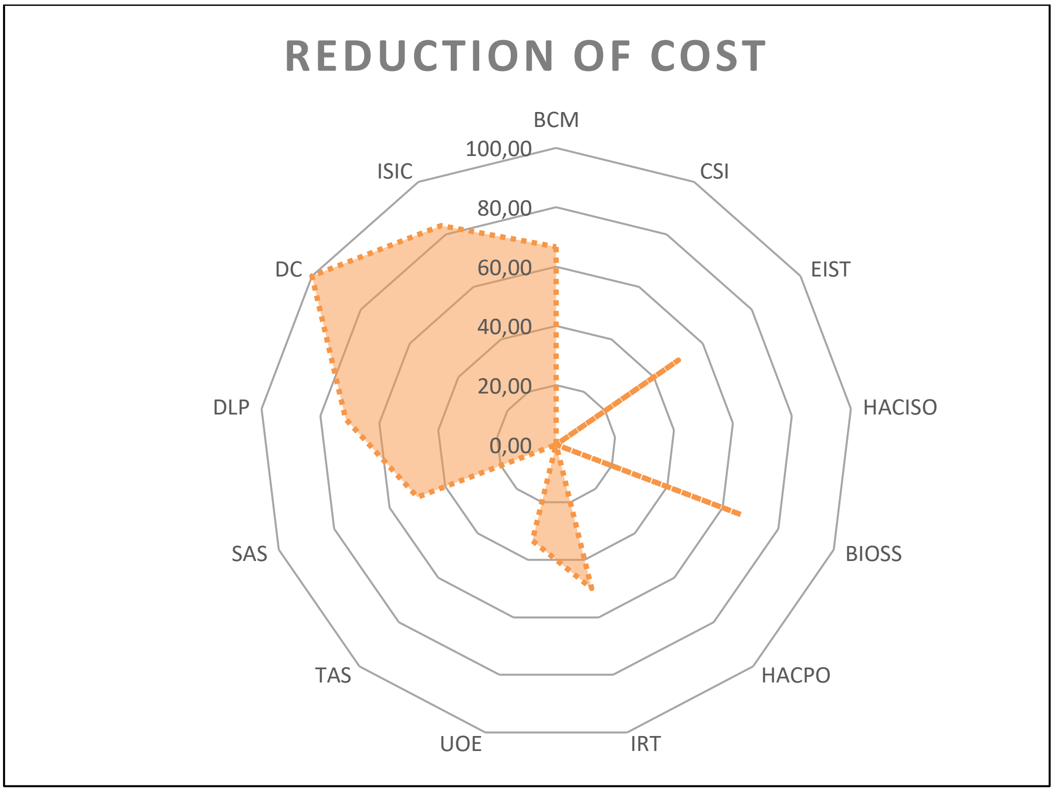


Figure 5-10 Participant Three– Reduction of Information Security Cost Feature Graph

In the IRT evaluation area, the participant noted no Security Operations Centre (SOC) that supports the organisation. Internal and external penetration tests are done, but these are done on an ad-hoc basis. There are no KPIs aligned to the remediation of the risk identified from these tests.

The UOE evaluation area established that only data at rest are encrypted as a standard. However, it was noted that the standard is not always adhered to and no other type of encryption is expected as part of the policy.

The TAS evaluation area found that the threat analysis or external security analysis is conducted actively or passively. Therefore, no team is associated with these activities and no information is shared with other parties.

The SAS evaluation area established that the organisation does not have a Security Operations Centre. Threat, incident and alert analysis are not conducted actively through a Security Incident and Event Management (SIEM) system. Logs and alerts are collected and analysed from the infrastructure and operating system level, but this is also done on an ad-hoc basis.

In the DLP evaluation area, the organisation also performed very well. Most non-sanctioned websites and information sharing sites were blocked while policies were in place from a governance perspective.

In the DC evaluation area, it was established that a Data Classification policy exists and that it is strictly enforced.

In the ISIC evaluation area, the participant advised that the organisation does not evaluate the costs of security incidents. This can be corroborated by the fact that very little evaluation of alerts and incidents is conducted. However, there are strict budgeting guidelines enforced for the purchase of information security products, services, technology and human resources and this is shared and evaluated by senior leadership.

5.9.3 Participant Three - Assessment of the Sustainability of Information Security Culture Feature

The evaluation output of Feature 3 – Sustainability of Information Security Culture for Participant Three is depicted below in Figure 5-11. The output score for each evaluation area is described in Table 5-9 with an overall weighted score of 74.29 percent for the Feature.

Table 5-9 Participant Three – Sustainability of Information Security Culture Feature (F3) Score

EVALUATION AREA	EVALUATION SCORE
E3.1 - Pillar 1- Common Security Values and Principles (CSVP)	75.00%
E3.2 - Pillar 2- Positive Reinforcement and Reward (PRR)	25.00%
E3.3 - Pillar 3- Common and Couple Processes (CCP)	100.00%
E3.4 - Pillar 4- Peer Recognition (PREC)	100.00%
E3.5 - Pillar 5- Technical Training and Awareness of Security Issues (TTSA)	71.43%
Overall weighted score	**74.29%**

In the CSVP evaluation area, the participant advised that information security values and company principles were communicated widely throughout the organisation. The organisation was not evaluated against these principles, but the IT department focused on how each department's function addressed and was responsible for information security.

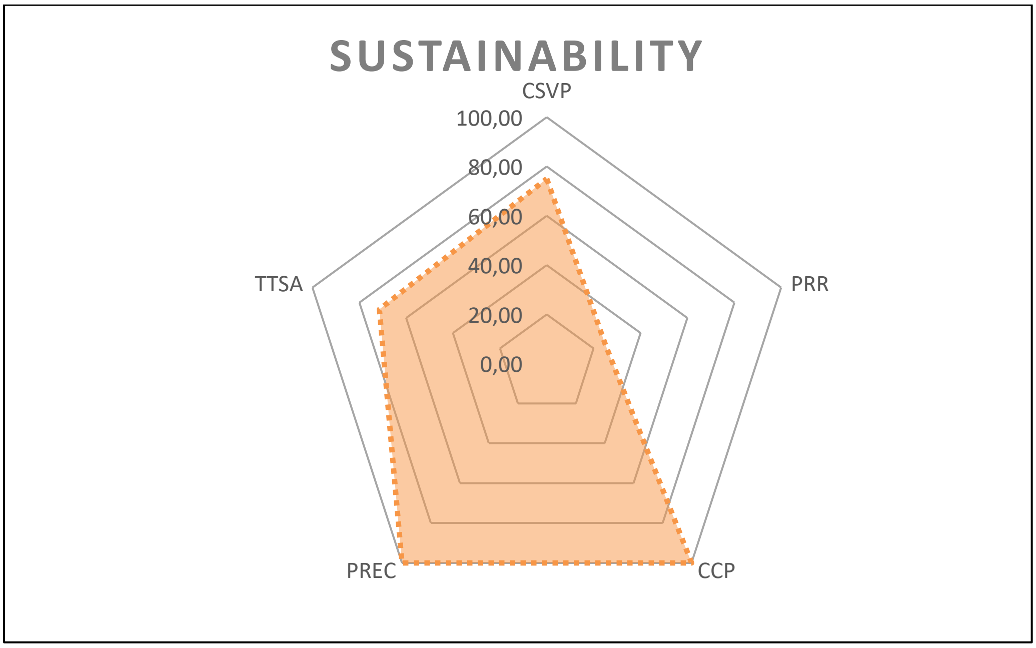


Figure 5-11 Participant Three – Sustainability of Information Security Culture Feature Graph

In the PRR evaluation area, the participant advised that there was no programme in place to evaluate employee’s behaviour regarding information security. As such, the organisation did not reward or recognise potential positive actions.

In the CCP evaluation area, it was established that the IT team is very aware of the impact of security remediation in their environments and it also communicated explicitly via the security department.

In the PREC evaluation area, it was established that the organisation does recognise good security behaviour as part of its information security awareness campaign and it is a peer-led programme specifically in the IT department. The results of this programme are communicated to other employees as a means of peer recognition.

In the TTSA evaluation area, it was established that the organisation has a robust security and awareness programme that includes awareness for IT staff but is not targeted at senior and executive employees. Their programme is measured and remedial actions are put in place based on the assessments.

5.9.4 Overall Summary – Participant Three

The overall summary showed that participant three’s organisation performed well in the Assessment of Information Security feature and the Sustainability of Information Security Culture feature, as described in Figure 5-12. The organisation will need to improve in the Reduction of Information Cost feature as not many security technologies are implemented or structurally aligned to good information security practices.

The participant agreed on the overall summary output. The evaluation shows that there are few technical products and solutions in place in the organisation, while it is generally aligned to information security best practices and standards. Furthermore, the company does not measure the work performance related to the remediation of information security risk. The organisation does well from a process and assessment perspective but does not follow through with the actual remediation of risks.

The organisation does communicate the good practices to its employees but does not forewarn employees about potential threats. The overall culture of information security is good and will lead to a potential reduction of information risk through people understanding and being aligned with information security concerns.

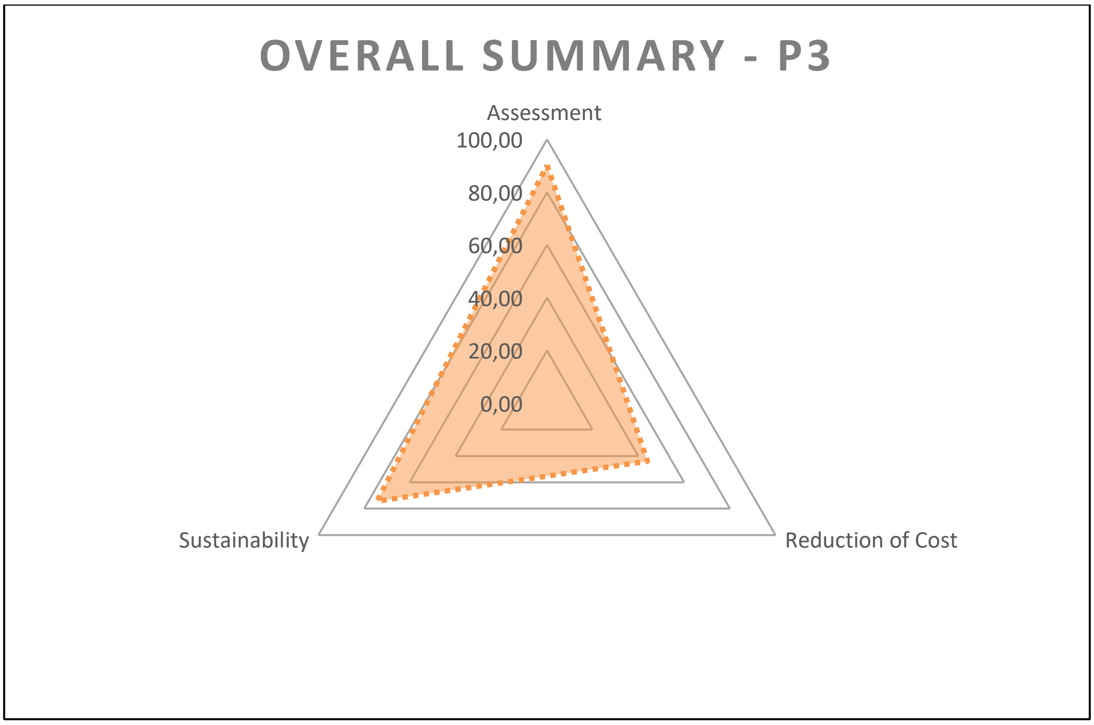


Figure 5-12 Overall Summary of Evaluation for Participant Three

Overall, the organisation's current position is very good but can be improved to allow for longer-term information security stability and reduced risk.

5.10 EXPERT REVIEWER'S EVALUATION OF FRAMEWORK AND TOOL

5.10.1 Evaluation of the Framework

Evaluation of the Framework - Participant Three	
Question	**Response**
What are your views on the components of the ARCS Security Framework?	The participant felt that the framework encompasses a wide coverage of information security topics. She felt that if an organisation adopted the framework, there would definitely be an improvement in the organisation's information security culture. The participant found specific value in the components

	related to data privacy and the importance of senior level leadership for information security and data privacy.
Do you see value in the components of the framework?	The participant found good value in the components of the framework. The question around budgeting and senior leadership's involvement in that evaluation area was of specific importance to her.
Are the components of the framework applicable to your organisation?	The participant found that all components were applicable to her organisation.
What are your views on the structure of the framework?	The participant found that the structure, logic and inter-relationship was good and understandable.
What are the components that you feel were not covered?	The participant felt that the alignment to corporate governance is not adequately covered. She felt there was limited linking between business compliance requirements to security compliance requirements from a governance perspective. The participant felt that in the training evaluation area, no questions were surrounding KPIs for training and awareness.
What improvements and/or changes can you advise on for the framework?	The participant suggested that there needs to be better communication of theory regarding the application. The participant felt that the framework and evaluation tool might be too high level. P3 felt that the framework focused mostly on the people and technology perspective while was limited on the process perspective. She also felt that the reduction of cost title could be better defined as cost-efficiency.

Are there any general views or comments on the framework?	The participant generally felt that the framework was comprehensive, valuable and applicable to her environment. P3 felt that the outputs of the framework could give a good baseline to information security experts and improve security culture. She also noted that she would advise that the weighting of Data Privacy could be scored higher.

5.10.2 Evaluation of the Tool

Evaluation of the Tool- Participant Three	
Question	**Response**
Are outcomes of the evaluation tool an accurate reflection of the information security position of the organisation in its current state?	The participant noted that the output was very well aligned to the real situation of her organisation. Therefore, it was accurate. She also felt that the tool was easy to use.
What are your views on the structure and application of ARCS Security Evaluation Tool?	The participant noted that she likes the logic and structure of the evaluation areas. P3 felt that the questions were thought-provoking and were basic enough to explain the focus.
Do you see the value in the evaluation tool with respect to the Framework developed?	The participant felt that the tool is important. P3 felt that the tool helped with interpretation and understanding of the context of the question. She noted that it might be good to have a reference page or executive description page to interpret the models in the related part of the tool.
Do you see the applicability of the implementation of the tool in your organisation?	The participant did see the applicability of the implementation of the tool in his organisation. P3 felt that the output was valid and fair.
What are the views on the scoring mechanism and weighting of questions?	The participant felt that scoring was balanced and outputs were relatively accurate. P3 felt she could not discern the difference between the

	weighting of the different evaluation areas and features. She felt that this allowed for an unbiased response from the participant.
What are your views on the quality and value of the output charts generated?	The participant felt that the quality of the graphs was below par and needed to be improved if the tool was aimed at senior or executive managers. P3 felt that the tool needs to be technically enhanced and moved away from an Excel file.
What improvements and/or changes can you advise on for the evaluation tool?	The participant felt that a comments field could be added to allow for the user to justify the response.
What are your general views or comments on the evaluation tool?	The participant felt that the tool is good and is easily linked back to the framework. P3 felt that the structure of the questions helps to understand the framework. She reiterated that she sees good value and applicability of this tool to her organisation.

5.11 DETAILS OF PARTICIPANT FOUR

Participant Four (P4) has more than fifteen years of experience in the security and IT industry. He comes from a former background of more than ten years in project management and business analysis. P4’s role at the time of the interview was as Information Security and IT Compliance Manager for a medium-sized IT consultation and services organisation based in South Africa that has clients in South Africa and some European countries. The company is a local organisation that employs almost five hundred employees and has a revenue of approximately one billion rands annually. The company has a local security team that focuses solely on the internal information security function. The company does not provide information security services to its clients. The assessment and corresponding review took approximately one hour with this participant.

The participant has managed a cyber security environment for more than four years and has strong IT operational and business experience to support his understanding of cyber security. Therefore, he was a good candidate to be able to give his expert opinion on the artefacts presented.

5.12 OUTPUT OF THE ASSESSMENT USING THE SECURITY EVALUATION TOOL FOR PARTICIPANT FOUR

5.12.1 Participant Four - Evaluation of the Assessment of Information Security Risk Feature

The evaluation output of Feature 1 – Information Security Risk for Participant Four is depicted below in Figure 5-13. The output score for each evaluation area is described in Table 5-10 with an overall weighted score of 93.33 percent for the Feature.

Table 5-10 Participant Four – Information Security Risk Assessment Feature (F1) Score

EVALUATION AREA	EVALUATION SCORE
E1.1 - Security Assessment (SECASSESS)	100%
E1.2 - Security Architecture (SECARCH)	100%
E1.3 - Risk Assessment (RSKASSESS)	80%
Overall Weighted Score	**93.33%**

In the SECASSESS evaluation area, the participant noted that multiple security best practices were followed, including the ISO standard and the OWASP and SANS best practices. The organisation conducted audits against the relevant standards and best practices annually. These security assessments were aligned to individual and departmental KPIs. The outputs of the assessments were shared with senior leadership within the organisation for high-level visibility.

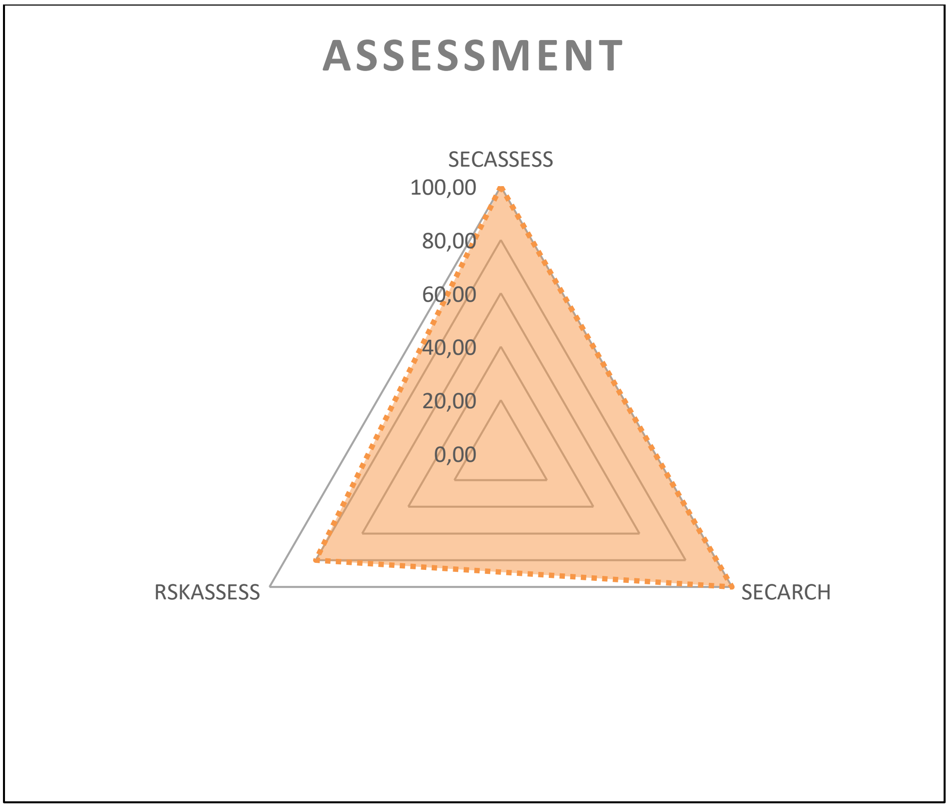


Figure 5-13 Participant Four Assessment of Information Security Risk Feature Graph

In the SECARCH evaluation area, it was established that the organisation does follow a defined security architecture method or approach. It defined its own security architecture aligned to the TOGAF architecture framework. The organisation also does follow specific best practices for IT/IS Policy, Governance and Operations.

In the RSKASSESS evaluation area, the participant noted that his team followed a strict company aligned risk framework and risk assessment process. Risks were catalogued and specific KPIs were defined within the risk framework to make sure that the team addresses the risks identified. All the reports outputs and actions are reported to senior leadership. Security risk management is not embedded into the project management process.

5.12.2 Participant Four - Assessment of the Reduction of Information Security Cost Feature

The evaluation output of Feature 2 – Reduction of Information Security Cost for Participant Four is depicted below in Figure 5-14. The output score for each evaluation area is described in Table 5-11, with an overall weighted score of 83.88 percent for the Feature.

Table 5-11 Participant Four – Reduction of Information Security Cost Feature (F2) Score

EVALUATION AREA	EVALUATION SCORE
E2.1 - Business Continuity Management (BCM)	83.33%
E2.2 - Cyber Security Insurance (CSI)	100%
E2.3 - Employee Information Security Training (EIST)	75%
E2.4 - Having a CISO (HACISO)	100%
E2.5 - Board Input on Security Spend (BIOSS)	100%
E2.6 - Having a CPO (HACPO)	100%
E2.7 - Incident Response Team (IRT)	100%
E2.8 - Use of Encryption (UOE)	66.67%
E2.9 - Threat Analysis and Sharing (TAS)	50%
E2.10 - Security Analytics Services (SAS)	75%
E2.11 - Data Loss Prevention (DLP)	57.14%
E2.12 - Data Classification (DC)	100%
E2.13 - Information Security Input Costs (ISIC)	83.33%
Overall Weighted Score	**83.88%**

In the BCM evaluation area, the participant noted that planning processes and standards were in place for business continuity. The organisation was not certified against an international standard but followed a standard. Periodic tests were conducted to confirm the validity of plans and processes and results are submitted to senior leadership as part of the defined process.

The CSI evaluation area confirmed that the organisation does purchase cyber security insurance with an international provider.

In the EIST evaluation area, it was established that the organisation has a good information security programme that includes specific training for specific levels and types of employees, including tailored training for senior leadership. The training was, however, noted as reactive and not dynamic.

In the HACISO evaluation area, the organisation has a CISO and that person does report to the board.

In the BIOSS evaluation area, it was confirmed that the board advises on security spend and that information security risk is regularly presented to the board for evaluation and guidance.

In the HACPO evaluation area, it was established that the organisation does have a Chief Privacy Officer and there is a robust data privacy programme in place.

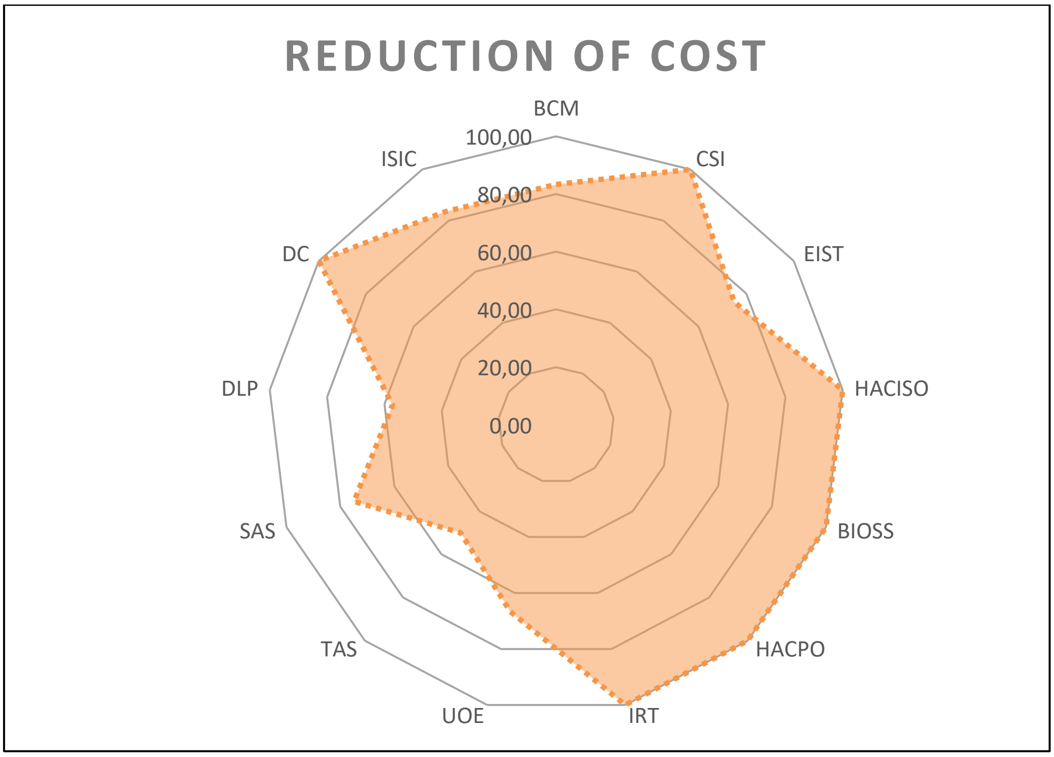


Figure 5-14 Participant Four – Reduction of Information Security Cost Feature Graph

In the IRT evaluation area, the participant noted that there is a small security team that supports the organisation. This team also contains an Incident Response Team. Penetration testing is done, but only on an ad-hoc basis. All alerts, risks and incidents are measured by KPIs to make sure remediation is conducted.

In the UOE evaluation area, it was established that only data that are transmitted are encrypted. However, other devices and data at rest are not encrypted. The use of encryption is also not standard in the environment but rather a best practice.

In the TAS evaluation area, it was found that the security team conducts threat analysis activities. Threat hunting is, however, not a formal function of the team. The organisation further does not employ outsourced partners to conduct deep and dark web threat analysis.

In the SAS evaluation area, it was established that this organisation does not have a SOC. System logging for security events is conducted and threats, incident and alert analysis is conducted but is reactive. However, the security team does have an incident and response plan to address identified threats.

In the DLP evaluation area, data, leakage, or loss were actively evaluated and several preventative measures were taken. The technology is well supported by policy and governance. Basic high-risk data leakage vectors are not blocked as the company uses those communication mechanisms as part of their daily work functions and allows users less restrictive access for personal use.

In the DC evaluation area, it was established that a data classification policy exists and that it is strictly enforced.

In the ISIC evaluation area, the participant advised that strict budgeting is enforced to purchase information security products, services, technology and human resources. However, the organisation has not established a method to budget for incidents that may occur.

5.12.3 Participant Four - Assessment of the Sustainability of Information Security Culture Feature

The evaluation output of Feature 3 – Sustainability of Information Security Culture for Participant Four is depicted below in Figure 5-15. The output score for each evaluation area is described in Table 5-12, with an overall weighted score of 83.81 percent for the Feature.

Table 5-12 Participant Four – Sustainability of Information Security Culture Feature (F3) Score

EVALUATION AREA	EVALUATION SCORE
E3.1 - Pillar 1- Common Security Values and Principles (CSVP)	100%
E3.2 - Pillar 2- Positive Reinforcement and Reward (PRR)	100%
E3.3 - Pillar 3- Common and Couple Processes (CCP)	100%
E3.4 - Pillar 4- Peer Recognition (PREC)	33.33%
E3.5 - Pillar 5- Technical Training and Awareness of Security Issues (TTSA)	85.71%
Overall Weighted Score	**83.81%**

In the CSVP evaluation area, the participant advised that as this was an organisation with predominantly technical IT employees, security values and principles were constantly communicated. The organisation was always evaluated against these principles and the IT department focused on how each department's function addressed and was responsible for information security.

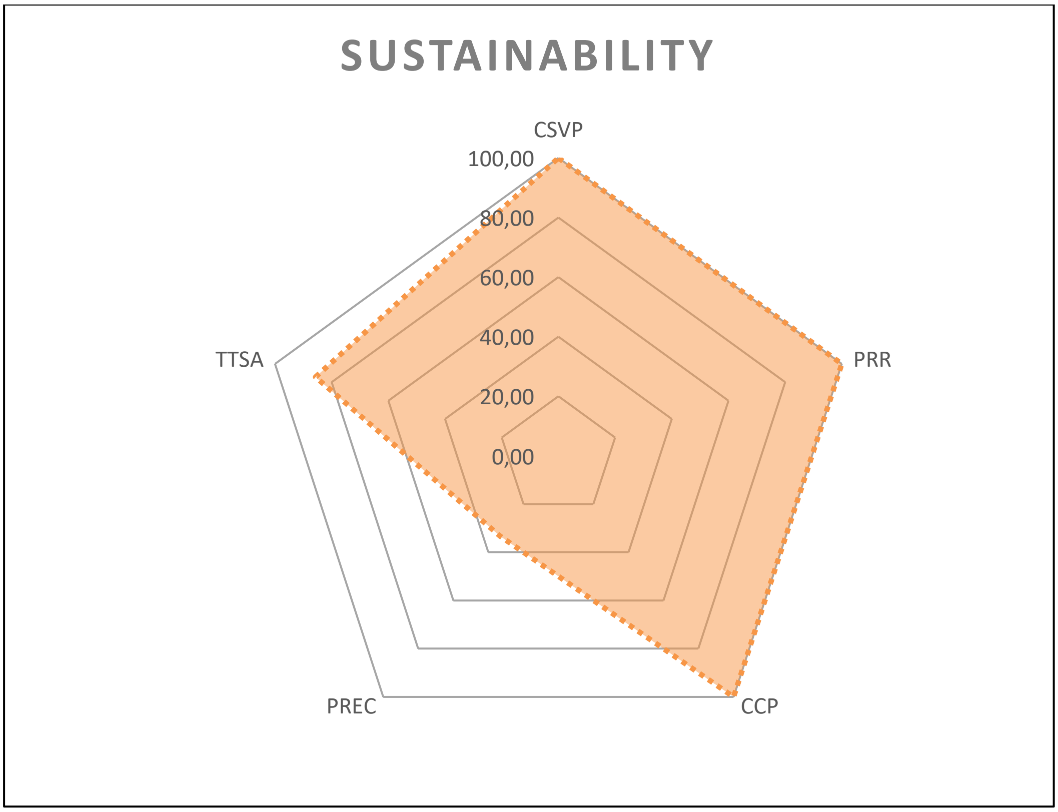


Figure 5-15 Participant Four – Sustainability of Information Security Culture Feature Graph

In the PRR evaluation area, the participant advised that there was no formal programme in place to evaluate employee's behaviour regarding information security. Still, as many of the employees were software developers, the company does reward people who pick up bugs or flaws in code developed for customers. This is communicated regularly and extensively through the organisation.

In the CCP evaluation area, it was established that, as noted above, the employees in this organisation are predominantly technical IT employees. Therefore, the IT team is very aware of the impact of security remediation in their environments and are supported strongly by the security team.

In the PREC evaluation area, it was established that the organisation does recognise good security behaviour as part of its information security awareness campaign, but it is a purely management-led programme and peers do not necessarily focus on supporting each other in their security initiatives.

In the TTSA evaluation area, it was established that the organisation has a robust security and awareness programme that includes awareness for IT staff. It is also targeted at senior and executive employees. There is no measurement of the programme and the improvements derived thereof.

5.12.4 Overall Summary – Participant Four

The overall summary showed that participant four's organisation performed well in the Assessment of Information Security and Reduction of Information Cost features. The organisation performed above average in the Sustainability of Information Security Culture feature, as described in Figure 5-16.

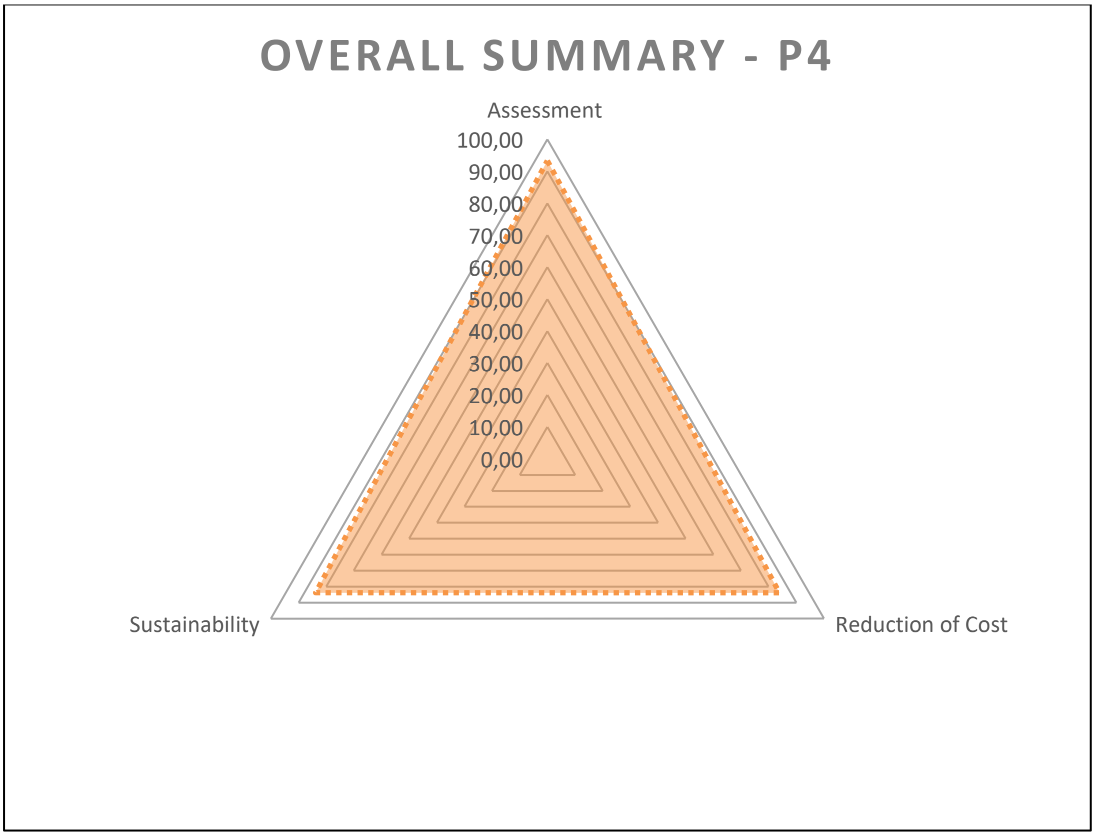


Figure 5-16 Overall Summary of Evaluation for Participant Four

The participant felt that the output of the overall summary was not completely accurate, which is further discussed in Section 5.13 below. The evaluation shows that there are few technical products and solutions in place in the organisation, while it is generally aligned to information security best practices and standards. Furthermore, the company measures the work performance related to information security. The organisation does communicate the good practices to its employees but does not forewarn employees about potential threats. The overall culture of information security is good and is quite sustainable to the changing needs of information security concerns.

Overall, the organisation's current position is very good, but as the participant noted, he felt that due to the binary nature of the responses in the evaluation tool, the organisation might have only partial implementation of necessary technology, best practices and standards. He felt that the organisation does have room for information security improvement.

5.13 EXPERT REVIEWER'S EVALUATION OF FRAMEWORK AND TOOL

5.13.1 Evaluation of the Framework

Evaluation of the Framework - Participant Four	
Question	**Response**
What are your views on the components of the ARCS Security Framework?	The participant felt that the framework was well constructed in that it covers the scope of important security features and functions. A key feature for him was data privacy due to pending South African legislation.
Do you see value in the components of the framework?	The participant found that many areas were of value to his organisation. However, he saw gaps and focus areas immediately through the evaluation areas of the framework.
Are the components of the framework applicable to your organisation?	The participant found the components of the framework very applicable to his organisation.
What are your views on the structure of the framework?	The participant found the structure of the framework good. He felt that the human-related factors in evaluation areas could be grouped. The researcher did explain that there are relationships in the scoring and that the grouping was applicable but not be visible.

What are the components that you feel were not covered?	The participant felt that an evaluation of maturity levels was not covered in each feature area. In addition, he felt that for longer-term features such as information security culture, more information needs to be given to the user to develop a roadmap for improvement.
What improvements and/or changes can you advise on for the framework?	The participant felt that the framework should delve into more technical details to get more detailed results.
Are there any general views or comments on the framework?	The participant felt the responses needed to allow for partial responses rather than binary answers. He noted that responses might have changed if he could have responded with an in-between rating. His overall view was that the framework was well thought out and would be beneficial to any organisation.

5.13.2 Evaluation of the Tool

Evaluation of the Tool- Participant Four	
Question	**Response**
Are outcomes of the evaluation tool an accurate reflection of the information security position of the organisation in its current state?	The participant advised the output was not a perfect representation of his organisation. He felt that the results were accurate within the context of the scoring method available but felt that the scoring should allow for partial responses instead of binary response.
What are your views on the structure and application of ARCS Security Evaluation Tool?	The participant noted that he feels that the tool is accurate and aligned to the framework.

Do you see the value in the evaluation tool with respect to the Framework developed?	The participant felt that he does see the value of the application of the evaluation tool but would like to see an output report and recommendations for organisational improvement as part of the tool.
Do you see the applicability of the implementation of the tool in your organisation?	The participant did see the applicability of the implementation of the tool in his organisation.
What are the views on the scoring mechanism and weighting of questions?	The participant felt that the information output was of good value but could be more accurate with more detailed scoring. As noted above the participant felt a partial scoring option should be added.
What are your views on the quality and value of the output charts generated?	The participant felt that the quality was good enough to explain the evaluation outputs. He felt that the tool could be improved with a narrative management report.
What improvements and/or changes can you advise on for the evaluation tool?	The participant reiterated that variable responses would improve the tool. He felt that the linking of the evaluation should be explained better. He felt that the tool evaluation was quick and easy to respond to and gave a good high-level view as a first pass tool.
What are your general views or comments on the evaluation tool?	The participant felt it could be modernised through developing it as an application. He felt that this would make the tool more accessible to users.

5.14 DETAILS OF PARTICIPANT FIVE

Participant Five (P5) has more than twenty-five years of experience in the security and IT industry. P5's role at the time of the interview was as Director: Information Technology for a medium-sized government department. The organisation is a national government department that employs approximately four thousand people.

The organisation does not have an information security team but a single information security manager who manages a small, outsourced security resource team.

The assessment and corresponding review took approximately two hours with this participant.

The participant has managed the information security team for more than thirteen years and has strong operational experience to support his understanding of cyber security. He was, therefore, a good candidate to be able to give his expert opinion on the artefacts presented.

5.15 OUTPUT OF THE ASSESSMENT USING THE SECURITY EVALUATION TOOL FOR PARTICIPANT FIVE

5.15.1 Participant Five - Evaluation of the Assessment of Information Security Risk Feature

The evaluation output of Feature 1 – Information Security Risk for Participant Five is depicted below in Figure 5-17. The output score for each evaluation area is described in Table 5-13, with an overall weighted score of 50.28 percent for the Feature.

Table 5-13 Participant Five – Information Security Risk Assessment Feature (F1) Score

EVALUATION AREA	**EVALUATION SCORE**
E1.1 - Security Assessment (SECASSESS)	37.50%
E1.2 - Security Architecture (SECARCH)	33.33%
E1.3 - Risk Assessment (RSKASSESS)	80%
Overall Weighted Score	**50.28%**

In the SECASSESS evaluation area, the participant noted that information security assessments are conducted against the ISO 27000 (Prislan and Bernik 2010) standard. He, however, noted that this is not done periodically and the last assessment at the time of this research was conducted two years before the discussion. These security assessments were not aligned to individual and departmental remediation KPIs. However, the outputs of the assessments were shared with senior leadership within the organisation for high-level visibility.

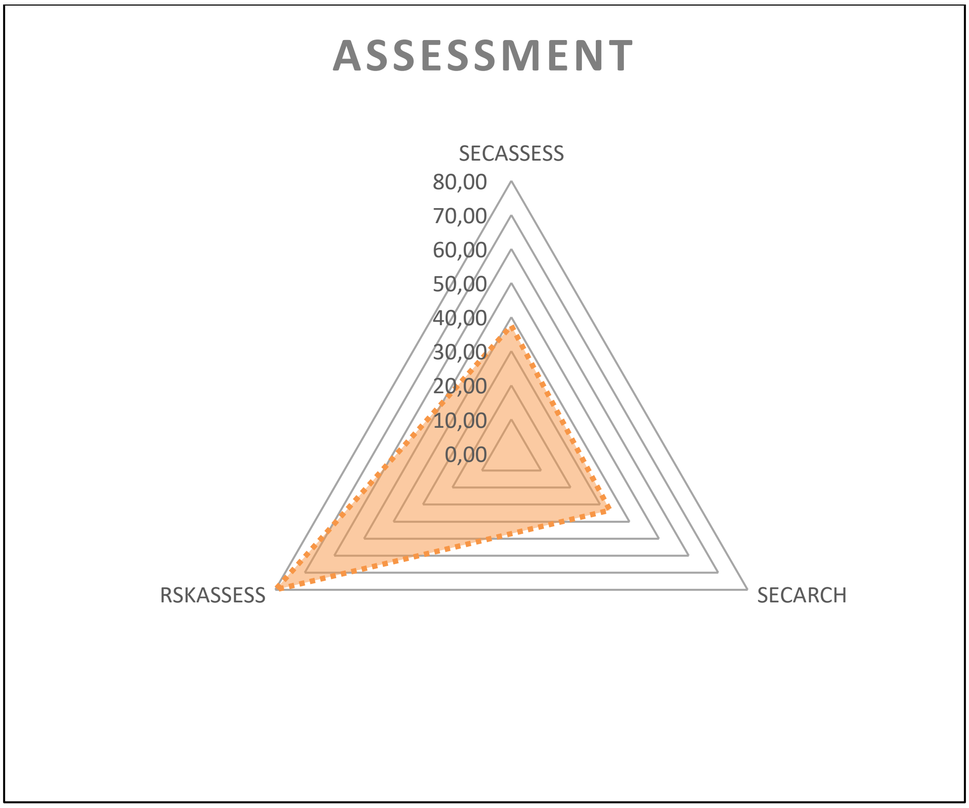


Figure 5-17 Participant Five Assessment of Information Security Risk Feature Graph

In the SECARCH evaluation area, it was established that the organisation does not follow a defined security architecture method or approach, but it does follow specific best practices for IT/IS Policy, Governance and Operations.

In the RSKASSESS evaluation area, it was established that a comprehensive risk management programme is followed. A risk framework is defined and adhered to. Risk assessments and reports are created on an annual basis, wherein KPIs for remediation are defined and addressed. This report is communicated to senior leadership.

5.15.2 Participant Five - Assessment of the Reduction of Information Security Cost Feature

The evaluation output of Feature 2 – Reduction of Information Security Cost for Participant Five is depicted below in Figure 5-18. The output score for each evaluation area is described in Table 5-14, with an overall weighted score of 45.7 percent for the Feature.

Table 5-14 Participant Five – Reduction of Information Security Cost Feature (F2) Score

EVALUATION AREA	**EVALUATION SCORE**
E2.1 - Business Continuity Management (BCM)	66.67%
E2.2 - Cyber Security Insurance (CSI)	0%
E2.3 - Employee Information Security Training (EIST)	50%
E2.4 - Having a CISO (HACISO)	0%
E2.5 - Board Input on Security Spend (BIOSS)	100%
E2.6 - Having a CPO (HACPO)	0%
E2.7 - Incident Response Team (IRT)	25%
E2.8 - Use of Encryption (UOE)	0%
E2.9 - Threat Analysis and Sharing (TAS)	25%
E2.10 - Security Analytics Services (SAS)	75%
E2.11 - Data Loss Prevention (DLP)	85.71%
E2.12 - Data Classification (DC)	100%
E2.13 - Information Security Input Costs (ISIC)	66.67%
Overall Weighted Score	**45.70%**

In the BCM evaluation area, the participant noted that planning processes and standards were in place for business continuity. However, a best practice or standard is not used and the BCM planning is not conducted with business stakeholders. The IT team does conduct tests against the BCM plan and submits these results to senior leadership.

In the CSI evaluation area, it was confirmed that the organisation does not purchase cyber security insurance and does not have a plan to do so.

In the EIST evaluation area, it was established that the organisation has an information security awareness programme. No training programme is in place. The awareness programme does not target senior or executive management. The awareness programme was reactive and not dynamic.

In the HACISO evaluation area, it was established that the organisation does not have a CISO. The participant, who is the Director of IT, leads the information security function. The participant does not report to the ministerial committee.

In the BIOSS evaluation area, it was confirmed that the board advises on security spend and that information security risk via the annual risk assessment report is regularly presented to the board for evaluation and guidance.

In the HACPO evaluation area, it was established that the organisation does not have a Chief Privacy Officer and there is no Data Privacy programme in place.

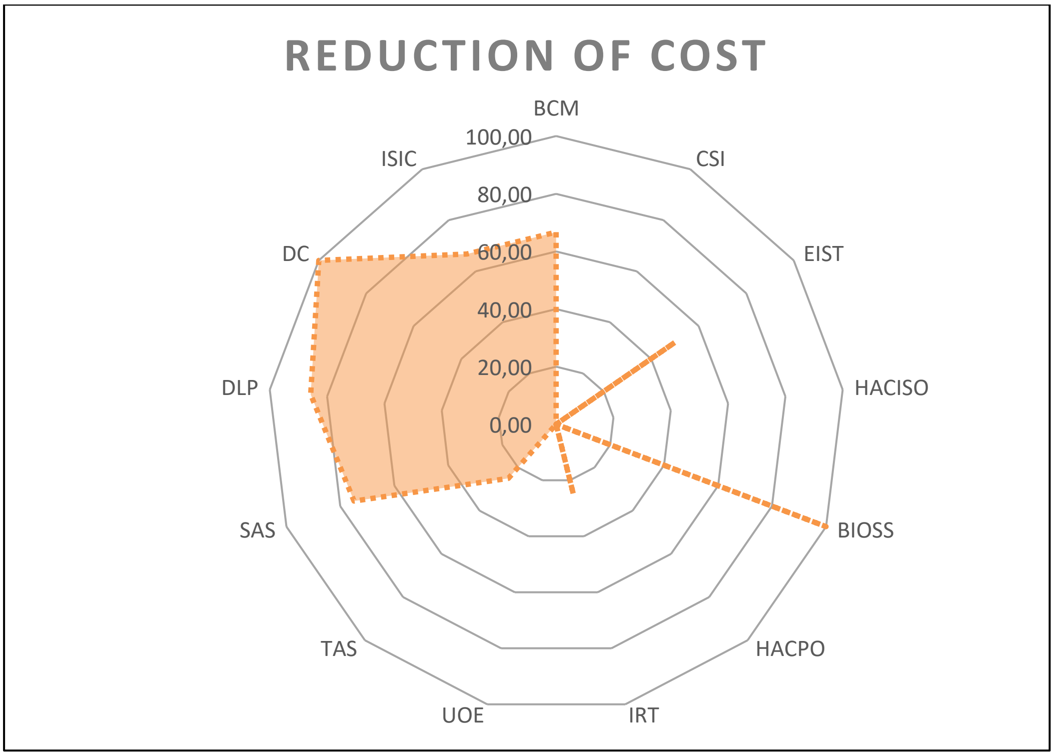


Figure 5-18 Participant Five – Reduction of Information Security Cost Feature Graph

In the IRT evaluation area, the participant noted that there is no SOC. Instead, an outsourced security team attend to security incidents and alerts on a reactive basis. The external team is tasked with managing the basic security technology such as anti-virus and firewalls. This is not a comprehensive security service.

In the UOE evaluation area, it was established that encryption of any form is not a standard, nor is it recommended.

In the TAS evaluation area, it was found that since there is no proactive security team function, threat analysis is non-existent.

In the SAS evaluation area, it was established, as noted above, that no SOC function exists. The infrastructure team, which manages servers and operating systems, conducts some system security logging and auditing of the environment. However, the outputs are not evaluated consistently or actively.

In the DLP evaluation area, the organisation also performed very well. Data leakage or loss was actively evaluated and several preventative measures were in place. In addition, the technology is well supported by policy and governance. In the DC evaluation area, it was established that a data classification policy has been developed and is strictly enforced.

In the ISIC evaluation area, the participant advised that as there is no comprehensive programme to evaluate security incidents and alerts, the organisation does not have a method to budget and plan for security incidents. Generally, the security budget is, however, planned for products, services and human resources. This is communicated and approved by senior leadership.

5.15.3 Participant Five - Assessment of the Sustainability of Information Security Culture Feature

The evaluation output of Feature 3 – Sustainability of Information Security Culture for Participant Five is depicted below in Figure 5-19. The output score for each evaluation area is described in Table 5-15, with an overall weighted score of 41.43 percent for the Feature.

Table 5-15 Participant Five – Sustainability of Information Security Culture Feature (F3) Score

EVALUATION AREA	**SCORE**
E3.1 - Pillar 1- Common Security Values and Principles (CSVP)	25%
E3.2 - Pillar 2- Positive Reinforcement and Reward (PRR)	25%
E3.3 - Pillar 3- Common and Couple Processes (CCP)	100%
E3.4 - Pillar 4- Peer Recognition (PREC)	0%
E3.5 - Pillar 5- Technical Training and Awareness of Security Issues (TTSA)	57.14%
Overall Weighted Score	**41.43%**

In the CSVP evaluation area, the participant advised that while the value and principles of information security were communicated, this was usually to the employees outside of the IT department. The organisation was not evaluated against these principles. The IT department did not focus on how each function in the department addressed, and was responsible for, information security.

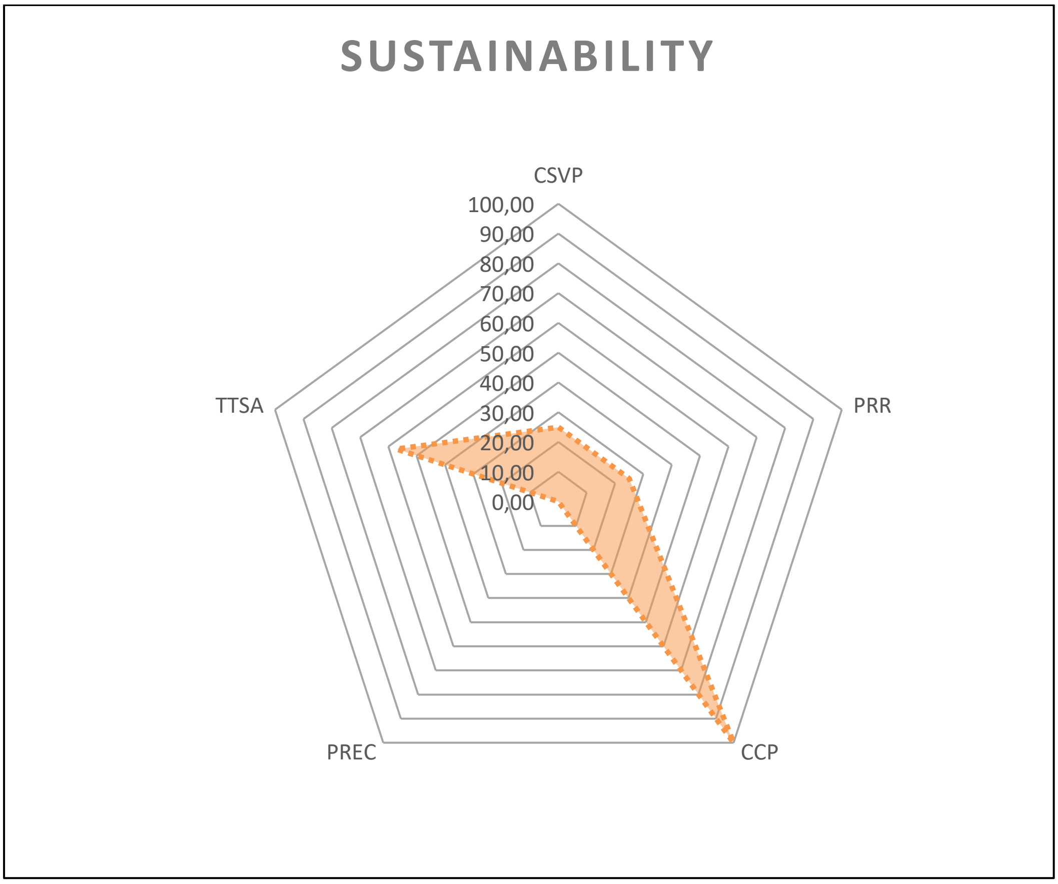


Figure 5-19 Participant Five – Sustainability of Information Security Culture Feature Graph

In the PRR evaluation area, the participant advised that there was no programme in place to evaluate employee’s behaviour regarding information security. As such, the organisation did not reward or recognise potential positive actions. Good behaviour as part of general awareness was communicated to employees.

In the CCP evaluation area, it was established that the IT team is very aware of the impact of security remediation in their environments and IT managers socialise the need for good security practices with their teams.

In the PR evaluation area, it was established that the organisation does not recognise good security behaviour as part of its information security awareness campaign. As a result, there is no peer-led recognition programme and as such, no information can be shared with employees.

In the TTSA evaluation area, it was established that the organisation has a robust security and awareness programme that includes awareness for IT staff but is not targeted at senior and executive employees. As a result, there is no measurement of the programme and the improvements derived thereof.

5.15.4 Overall Summary – Participant Five

The overall summary showed that participant five's organisation performed well in the Reduction of Information Cost feature, above average in the Assessment of Information Security feature and poorly in the Sustainability of Information Security Culture feature, as described in Figure 5-20.

The participant agreed on the overall summary output, which is further discussed in Section 5.16 below. The evaluation shows that there are not many technical products and solutions in place in the organisation. Processes and procedures are ad-hoc. The organisation does not measure the work performance related to information security. The organisation does not communicate any good practices that are enforced to its employees, nor forewarns employees about potential threats. The overall culture of information security is poor and may lead to a potential information risk through people not understanding and aligned to the information security concerns.

Overall, the current position of the organisation is not good and has significant room for improvement.

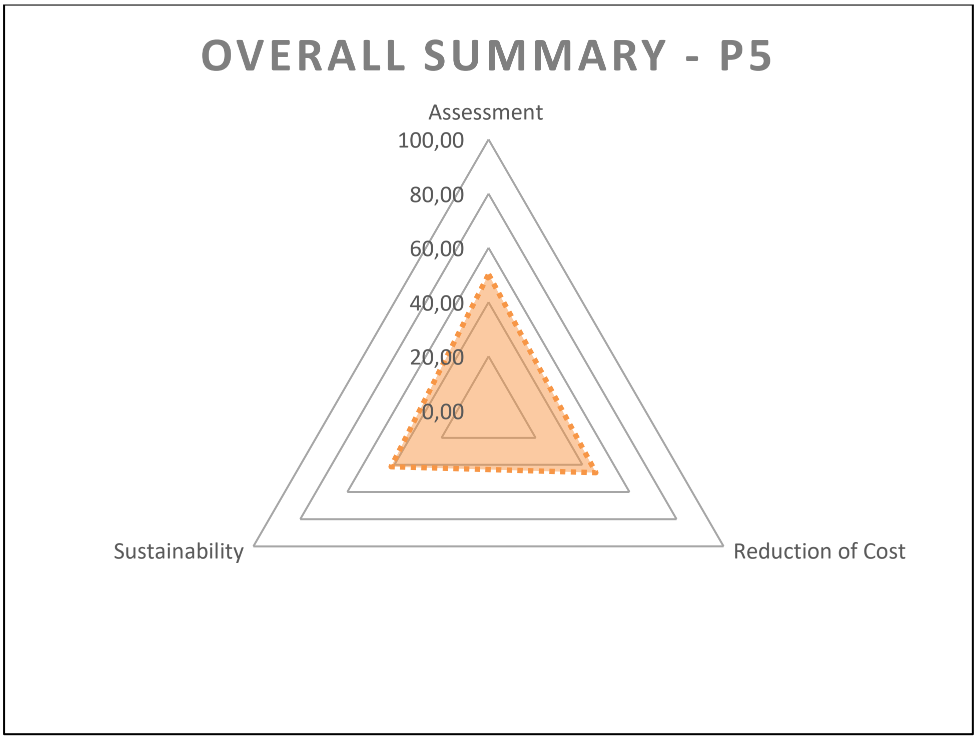


Figure 5-20 Overall Summary of Evaluation for Participant Five

5.16 EXPERT REVIEWER'S EVALUATION OF FRAMEWORK AND TOOL

5.16.1 Evaluation of the Framework

Evaluation of the Framework - Participant Five	
Question	**Response**
What are your views on the components of the ARCS Security Framework?	The participant felt that the framework had good features and that the evaluation areas were understandable and relevant. P5 felt that there were security concepts in the evaluation that were new to their organisation and therefore found the framework informative.
Do you see value in the components of the framework?	The participant found that there were many areas of value to his organisation. However, he noted that the areas that were new to the organisation could be immediate focus areas for improvement.
Are the components of the framework applicable to your organisation?	The participant found the components of the framework were applicable to his organisation.

What are your views on the structure of the framework?	The participant found that the structure of the framework was understandable. He would have preferred if the models discussed that make up the framework were more easily described in the framework.
What are the components that you feel were not covered?	The participant could not comment on any components that he felt were not covered. P5 felt that the framework was comprehensive in its current form.
What improvements and/or changes can you advise on for the framework?	The participant felt that more detail and explanation could be given as to the framework's components and why those components were chosen.
Are there any general views or comments on the framework?	Overall, the participant thought that the framework was comprehensive, valuable and applicable in his environment

5.16.2 Evaluation of the Tool

Evaluation of the Tool- Participant Five	
Question	**Response**
Are outcomes of the evaluation tool an accurate reflection of the information security position of the organisation in its current state?	The participant noted that the output of the tool somewhat reflected his environment. He felt that he could not answer effectively as many processes or structures were partially in place but that the scoring asked for a binary response.
What are your views on the structure and application of ARCS Security Evaluation Tool?	The participant noted that he feels that the tool is accurate and aligned to the framework.
Do you see the value in the evaluation tool concerning the framework developed?	The participant felt that he does see the value of having a tool aligned to the framework. He noted that frameworks were complex and a

Evaluation of the Tool- Participant Five	
Question	**Response**
	tool that conducts the assessment helps with applying the framework.
Do you see the applicability of the implementation of the tool in your organisation?	The participant did see the applicability of the implementation of the tool in his organisation.
What are the views on the scoring mechanism and weighting of questions?	The participant felt that the information output was of good value but could be more accurate with more detailed scoring.
What are your views on the quality and value of the output charts generated?	The participant felt that the quality was of the output charts could be improved. However, he noted that the graphs were valuable to give an immediate interpretation of the assessment.
What improvements and/or changes can you advise on for the evaluation tool?	The participant reiterated that variable responses would have improved the tool.
What are your general views or comments on the evaluation tool?	The participant would have liked to have seen more detailed reporting and more information about the evaluation areas described in the tool.

5.17 SUMMARY OF ANALYSIS AND FINDINGS

5.17.1 Evaluation Framework

Table 5-16 summarises the strengths, weaknesses and opportunities for improvement of the evaluation framework that were identified through the expert reviews.

Table 5-16 Analysis of Expert Reviews for the Security Framework

Strengths	The expert reviewers all noted that the framework was well structured and understandable. A common theme was that the framework was valuable for their organisation and would be applicable in any type of organisation that wanted to evaluate information security in their environment. The expert reviewers generally felt that the framework was comprehensive and covered most evaluable aspects of information security. Some reviewers felt that some evaluation areas of the framework were more relevant to them than other, for example, data privacy, senior or executive involvement in information security
Weaknesses	The common weaknesses in the framework identified by the expert reviewers were that the context and positioning of the framework regarding management or employee level needed to be better explained. Reviewers noted that the expectation of using the framework and the outputs thereof could be better defined so that the adoption of the framework would be more prevalent. Some reviewers would have liked more information on linking the evaluation areas and understanding the logic of the scoring.
Opportunities	• Creation of an improved executive description to the framework. • Creation of a more complex relationship model for the different evaluation areas. • Address the positioning of the framework and consider how expansion may include more technical evaluation areas or questions.

5.17.2 Evaluation Tool

Table 5-17 summarises the strengths, weaknesses and opportunities for improvement of the evaluation tool that were identified through the expert reviews.

Table 5-17 Analysis of Expert Reviews for the Security Evaluation Tool

Strengths	The tool was received well by the expert reviewers. Most participants advised that the output reports were well aligned to their view of the information security environment in their organisation. Participants felt that the tool was easy to use and that it complemented the framework well. Expert reviewers felt that the tool was logical and would be applicable for usage in their organisation.
Weaknesses	The expert reviewers felt that the tool could use more information in describing the evaluation areas and that output reports included a narrative management report rather than just output graphs. In addition, participants commented that the tool would be more effective with a variable scoring system rather than a binary scoring system. The participants also advised that the tool should be modernised to give a better look and feel, especially if the first iteration was developed for senior and executive management. In line with this input the reviewers also felt that the graphs could also be modernised.
Opportunities	• Creation of a better executive description to the tool. • Explanation of tags in the tool about evaluation areas. • Create a variable scoring system for the tool. • Modernisation of the tool by implementing it in a technology application. • Modernisation of outputs graphs. • Creation of an automated management reports to offer a narrative description of results.

5.18 SUMMARY AND IMPLICATIONS

In this chapter, the five steps required to conduct the demonstration, evaluation and communication components of the DSR process model were conducted and communicated. These five steps are summarily:

- Step 1 - Presentation of the framework and evaluation tool
- Step 2 - Conduct the evaluation and present results of evaluation
- Step 3 - Review of evaluation results
- Step 4 - Review of the Security Framework
- Step 5 - Review of the Security Evaluation Tool

In this chapter, the practical action taken to achieve these steps was discussed and described. The interviews conducted with participants who were expert reviewers were discussed in detail. As expected by DSR theory, participants were selected based on their characteristics in relation to the topic being discussed and form part of a population that is familiar with the environment for which the artefacts were developed. The results of the demonstration and evaluation are described for each of the five expert reviewers along with their critique of the framework and evaluation tool.

The summary evaluation data will be used for the enhancement of the framework and tool, which is described in Chapter 6, along with a roadmap for longer term iterative improvements and future research, discussed in Chapter 7.

Chapter 6: Review and Update of the ARCS Security Evaluation Tool Framework and Tool

Chapter 1 Introduction	Research Purpose, Rationale, Background and Scope of Study
Chapter 2 Literature Review	Information Security (IS), IS Assessments, IS Architecture, IS Risk Assessment, Organisational Culture, IS Culture, Motivation, Positive Reinforcement and Reward
Chapter 3 Research Methodology	Methodology and Research Design, Participants, Instruments, Procedures and Timelines, Analysis, Ethics and Limitation
Chapter 4 Security Models, Framework and Evaluation Tool	Models for Cost Reduction, Security Assessment and Information Security Cultural Improvement, The ARCS Security Framework, The ARCS Security Evaluation Tool
Chapter 5 Analysis, Results and Findings	Analysis, Results and Findings of the Demonstration of the ARCS Security Evaluation Tool
Chapter 6 Review and Update of the Evaluation Tool	Evaluation of Expert Reviews of the ARCS Security Model and the ARCS Security Evaluation Framework Update of the ARCS Security Evaluation Framework
Chapter 7 Further Research and Future Studies	Further Research and Future Studies
Chapter 8 Conclusion	Conclusion

Chapter 6: Review and Update of the ARCS Security Evaluation Framework and Tool

In Chapter 5, the demonstration and evaluation of the artefacts developed in Chapter 4 were communicated along with critiques and observations by expert reviewers.

In this chapter, as expected by the iterative approach of the DSR process methodology selected in Chapter 3, the researcher will develop a second iteration of the ARCS Security Framework and Evaluation Tool based on the analysis of input from expert reviewers and the researcher's own experience in testing the framework and tool with the expert reviewers.

In Section 6.1.1, the framework will be enhanced by creating a more complex relationship model for the different evaluation areas. The framework will also be enhanced by explicitly positioning it at a relevant management level.

Section 6.1.2 will focus on the evaluation tool, which will be enhanced by creating an improved executive description and the creation of an improved variable scoring system. In addition, the modernised tool in the form of a web application with improved graphs, reporting and more information on evaluation areas, will be described.

The second iteration enhancement to the security framework and tool focuses predominantly on the information provided by expert reviewers during their evaluation of the tool and the framework that was discussed in Chapter 5. Observations by the researcher during the demonstration and evaluation phases with expert reviewers, also led to further improvements.

The improvements noted have not been tested further with expert reviewers but may be considered for future research.

6.1 ENHANCEMENT OF THE SECURITY EVALUATION FRAMEWORK AND TOOL

In interviews with expert reviewers and based on observations by the researcher while demonstrating the artefacts, it was established that enhancements were required. These enhancements related to the expansion of the framework and evaluation tool in order to improve ease of use, provide more detailed information and address areas of information security that the expert reviewers considered to be of importance. The enhancements discussed in the following sections forms the second iteration of the framework and evaluation tool. This is completed as expected as part of the iterative improvement process described by the DSR process selected in Chapter 3.

6.1.1 Enhancement of Scoring and Redevelopment of the Relationship Model

In this section, the enhanced scoring and the new relationship model is discussed. The response tables that were originally created in Microsoft Excel are now embedded in the enhanced evaluation tool discussed in Section 6.1.2. The scoring logic is calculated based on the given responses and has been embedded in the online forms also discussed in Section 6.1.2.

The framework's structure remains the same with three feature areas, twenty-one evaluation areas and eighty-three questions. The questions remain weighted and scored to give each evaluation area an output score. The standard questions in the new iteration of the framework, for each evaluation area, follow an enhanced scoring mechanism that allows for a "Yes", "Partially", or "No" response. Where a question cannot be answered with a "Partially" response, for example, in Question 2.4.1 "Does the organisation have a Chief Information Security Officer (or equivalent)?", responses will be limited to a "Yes" or "No" response, while scoring will remain the same. For the standard questions, the scoring is described in Table 6-1. The exception to this scoring is when a specific special question is weighted higher than a standard question due to its relationship with questions in evaluation areas in other features.

Table 6-1 Enhanced Scoring for the Security Evaluation Tool

Response	Score Awarded
Yes	4
Partially	2
No	0
Response	**Special Score Awarded**
Yes	6
Partially	3
No	0

When a special question is asked, the scoring logic in the tool then reverts to using six points for a “Yes” response, three for a “Partial”. A “No” response remains at zero. Thus, each feature has a total weighting of 100 percent. The evaluation area that contains the special questions gets a higher weighting in respect to other evaluation areas within that feature.

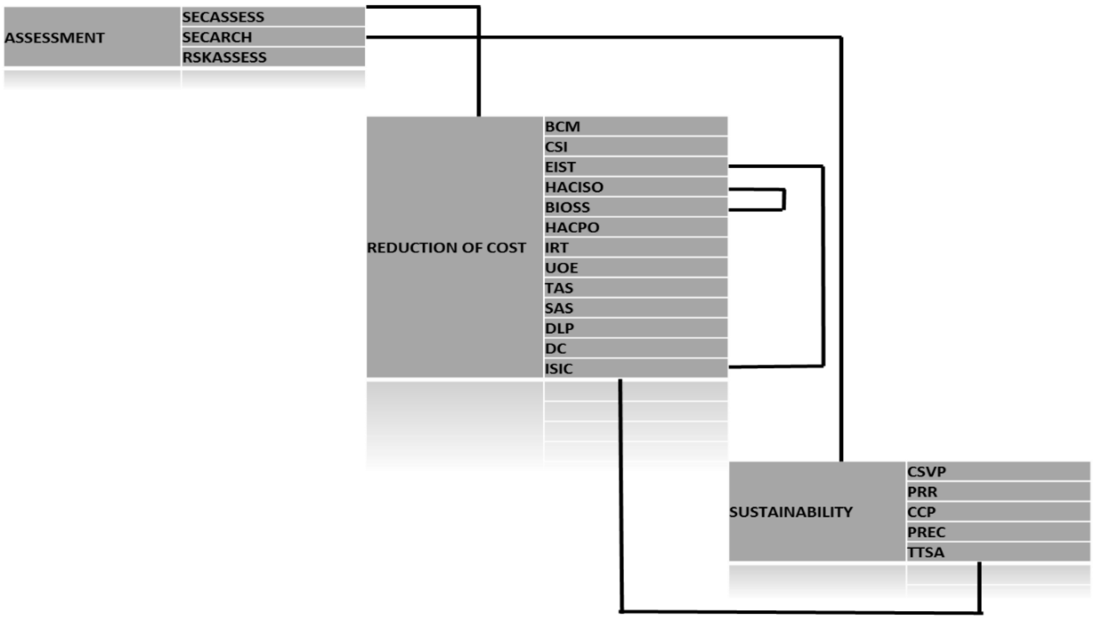


Figure 6-1 Enhanced relationship model between special evaluation areas

Figure 6-1 describes the relationships between special evaluation areas. The relationships have been enhanced from the model described in Chapter 4, based on inputs given by expert reviewers. Expert reviewers considered that these evaluation areas linked, as described in Figure 6-1, held more value than the original model. Expert reviewers noted that having a dedicated senior leader focusing on information security and having that senior leader be able to present information about information security to an organisation's board would benefit the IS programme. Board input on IS spending also expected that IS programme information would be discussed. As such the HACISO and BIOSS evaluation areas were linked. Reviewers also noted that information security training could have an impact on the reduction of information incidents within an organisation, leading to lower IS risk and fewer significant incidents. As such the EIST and ISIC evaluation areas were linked. Furthermore, reviewers noted that core questions from each of the evaluation area in Feature 3 were of significant importance and as such each of those areas were linked. Table 6-2 describes the updated weighting of each evaluation area within each feature.

Table 6-2 Summary of updated higher weighted questions in each evaluation area

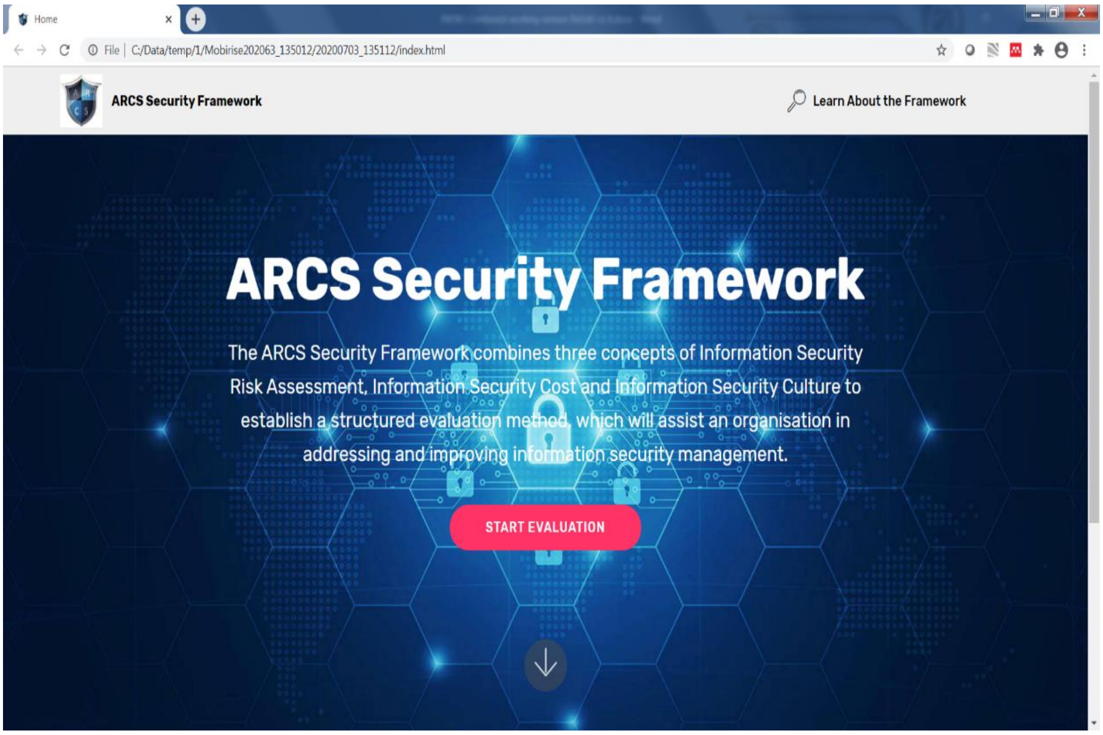
EVALUATION AREA	NUMBER OF SPECIAL QUESTIONS
E1.1 - Security Assessment (SECASSESS)	2 of 6
E1.2 - Security Architecture (SECARCH)	6 of 6
E2.3 - Employee Information Security Training (EIST)	1 of 6
E2.4 - Having a CISO (HACISO)	1 of 2
E2.5 - Board Input on Security Spend (BIOSS)	1 of 2
E2.13 - Information Security Input Costs (ISIC)	1 of 2
E3.1 - Pillar 1- Common Security Values and Principles (CSVP)	1 of 2
E3.2 - Pillar 2- Positive Reinforcement and Reward (PRR)	1 of 2
E3.3 - Pillar 3- Common and Couple Processes (CCP)	1 of 2
E3.5 - Pillar 5- Technical Training and Awareness of Security Issues (TTSA)	2 of 5

6.1.2 Enhanced Security Evaluation Tool

The following section describes the enhancement to the security evaluation tool based on the inputs from participants during the expert review.

The new tool was developed as a web application that contains information about the framework, an evaluation jump page, as well as links to an online forms system that collects the data. The following figures depict the components of the new tool.

Figure 6-2 depicts the landing page of the ARCS security framework. The landing page links to the evaluation page and a page dedicated to information about the framework.



Home

File | C:/Data/temp/1/Mobirise202063_135012/20200703_135112/index.html

ARCS Security Framework

Learn About the Framework

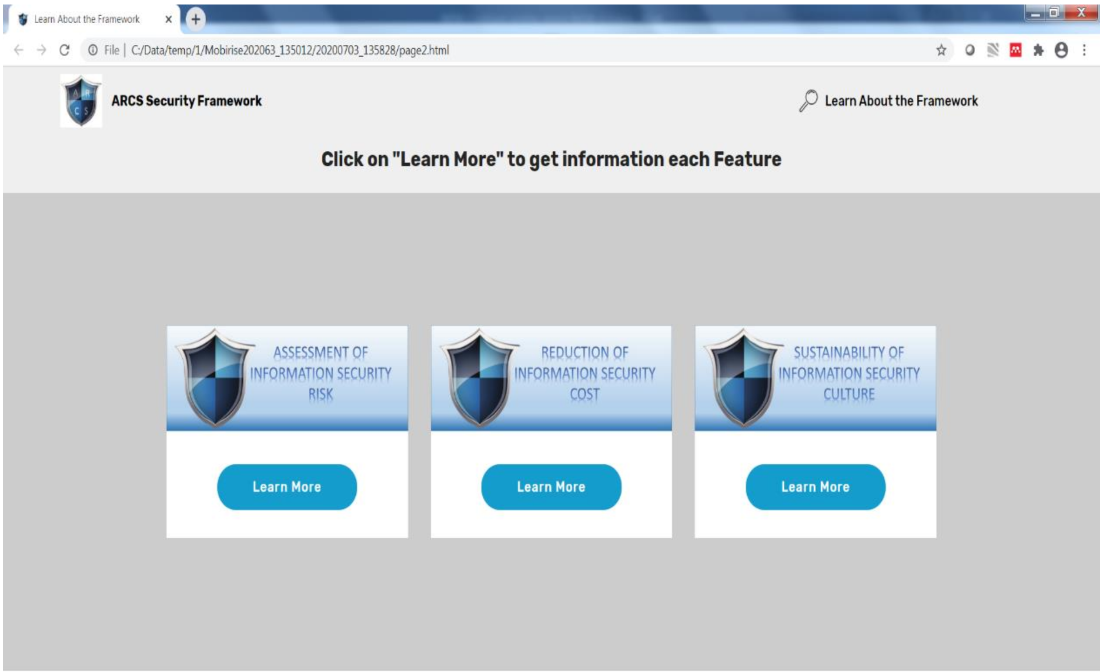
ARCS Security Framework

The ARCS Security Framework combines three concepts of Information Security Risk Assessment, Information Security Cost and Information Security Culture to establish a structured evaluation method, which will assist an organisation in addressing and improving information security management.

START EVALUATION

Figure 6-2 Landing page for the ARCS Framework Website

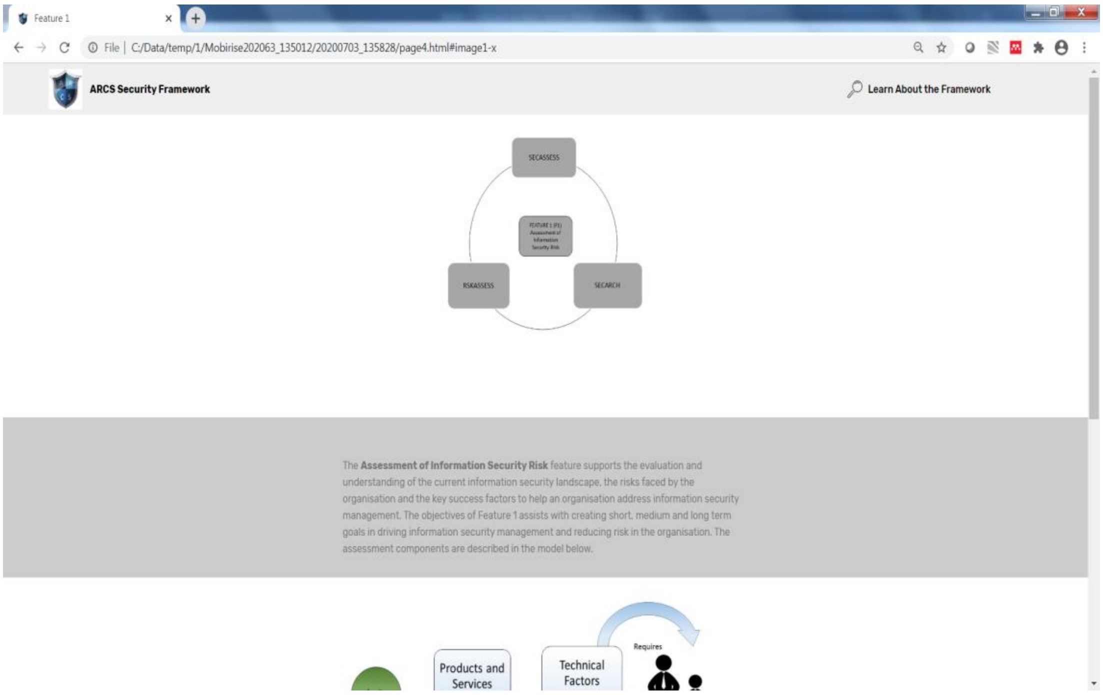
The jump page for information on each of the Feature areas of the framework is depicted in Figure 6-3.


Learn About the Framework
File | C:/Data/temp/1/Mobirise202063_135012/20200703_135828/page2.html
ARCS Security Framework
Learn About the Framework
ASSESSMENT OF INFORMATION SECURITY RISK
Learn More
REDUCTION OF INFORMATION SECURITY COST
Learn More
SUSTAINABILITY OF INFORMATION SECURITY CULTURE
Learn More

Click on "Learn More" to get information each Feature

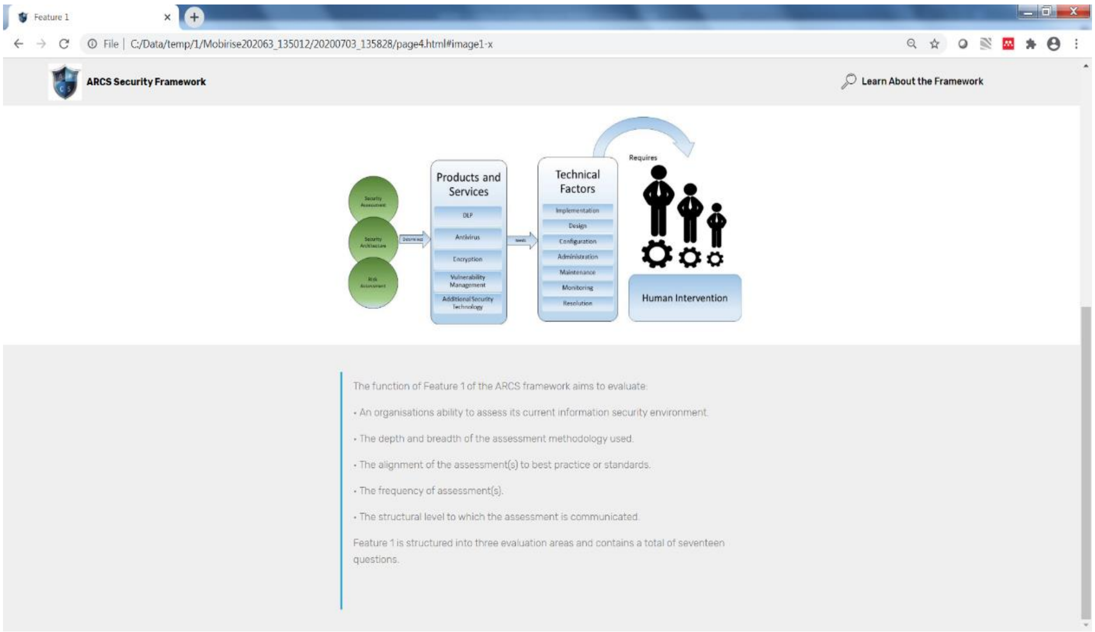
Figure 6-3 “Learn About the Framework” Jump Page

Figures 6-4 and 6-5 depict Feature 1 and the model from which the components evaluated are defined. Figures 6-6 and 6-7 depict Feature 2 and the model from which the components evaluated are defined. Figures 6-8 and 6-9 depict Feature 3 and the model from which the components evaluated are defined.


Feature 1
File | C:/Data/temp/1/Mobirise202063_135012/20200703_135828/page4.html#image1-x
ARCS Security Framework
Learn About the Framework
SECASSESS
FEATURE 1 (F1) Assessment of Information Security Risk
RSKASSESS
SECARCH
Products and Services
Technical Factors
Requires

The **Assessment of Information Security Risk** feature supports the evaluation and understanding of the current information security landscape, the risks faced by the organisation and the key success factors to help an organisation address information security management. The objectives of Feature 1 assists with creating short, medium and long term goals in driving information security management and reducing risk in the organisation. The assessment components are described in the model below.

Figure 6-4 Feature 1 – Information Page – Screenshot 1

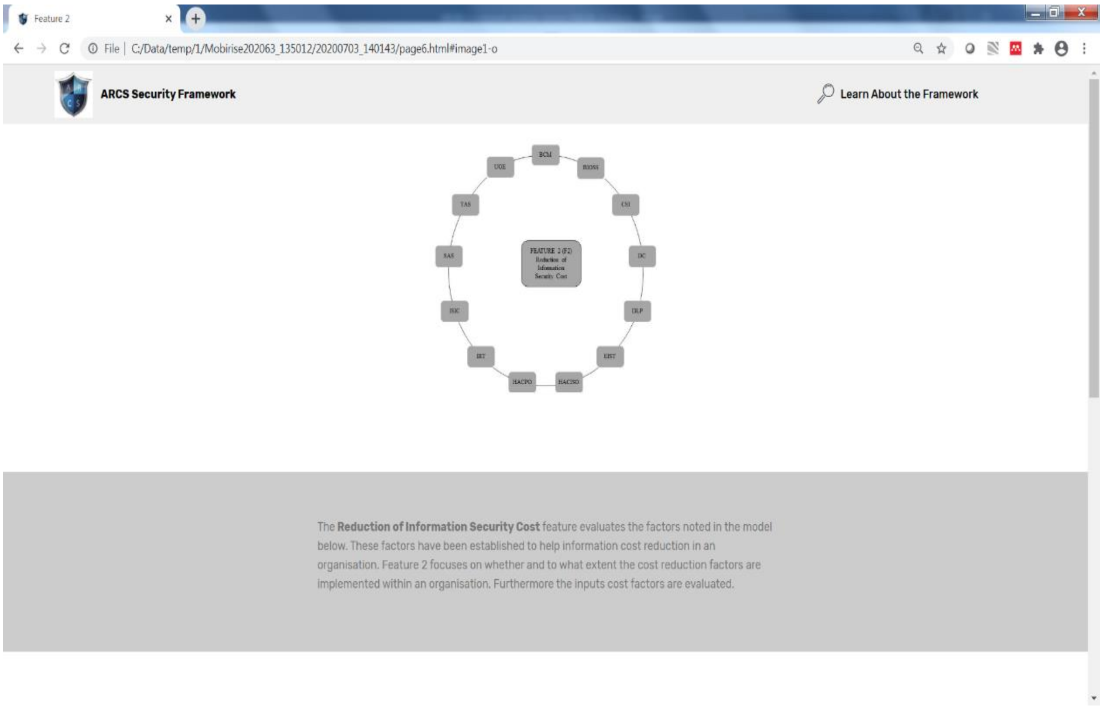


The function of Feature 1 of the ARCS framework aims to evaluate:

- An organisations ability to assess its current information security environment.
- The depth and breadth of the assessment methodology used.
- The alignment of the assessment(s) to best practice or standards.
- The frequency of assessment(s).
- The structural level to which the assessment is communicated.

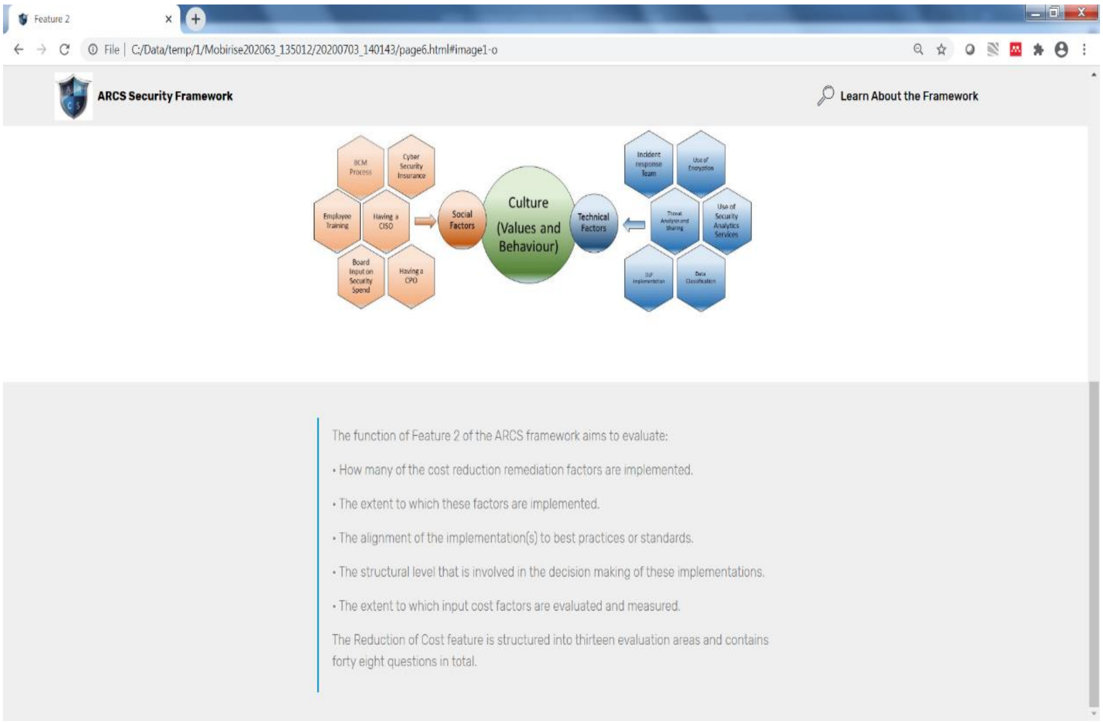
Feature 1 is structured into three evaluation areas and contains a total of seventeen questions.

Figure 6-5 Feature 1 – Information Page – Screenshot 2


Feature 2
File | C:/Data/temp/1/Mobirise202063_135012/20200703_140143/page6.html#image1-o
ARCS Security Framework
Learn About the Framework
FEATURE 2 (F2) Reduction of Information Security Cost
BCM
BIOSS
CSI
DC
DLP
EIST
HACISO
HACPO
IRT
ISIC
SAS
TAS
UOE

The **Reduction of Information Security Cost** feature evaluates the factors noted in the model below. These factors have been established to help information cost reduction in an organisation. Feature 2 focuses on whether and to what extent the cost reduction factors are implemented within an organisation. Furthermore the inputs cost factors are evaluated.

Figure 6-6 Feature 2 – Information Page – Screenshot 1

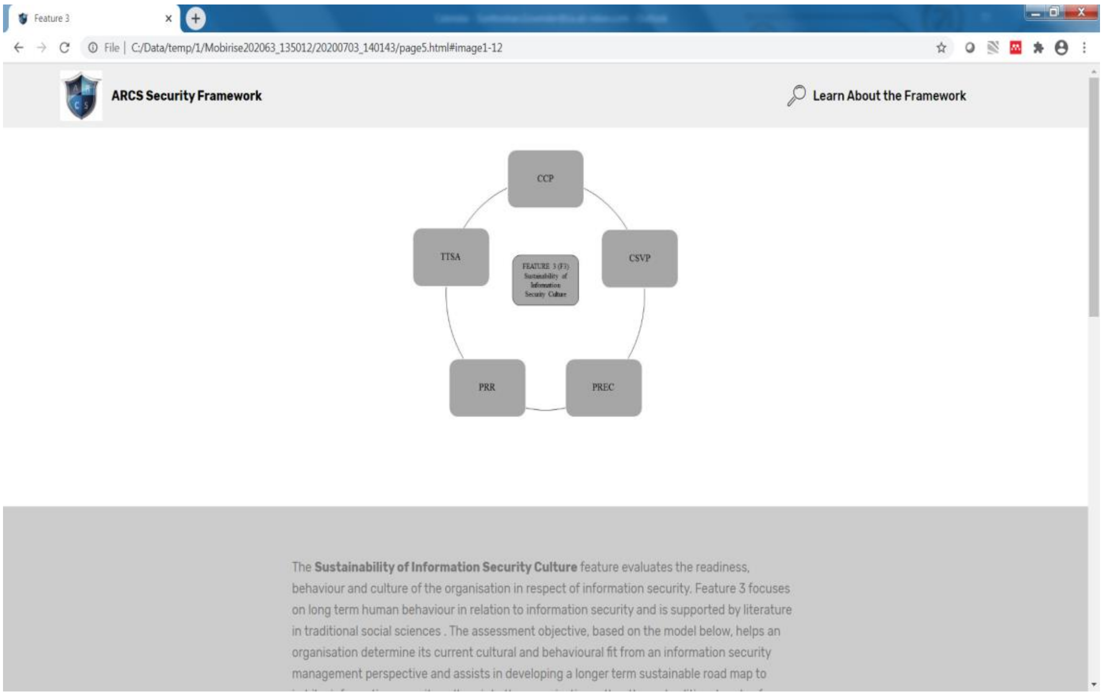

Feature 2
File | C:/Data/temp/1/Mobirise202063_135012/20200703_140143/page6.html#image1-o
ARCS Security Framework
Learn About the Framework
BCM Process
Cyber Security Insurance
Employee Training
Having a CISO
Board Input on Security Spend
Having a CPO
Social Factors
Culture (Values and Behaviour)
Technical Factors
Incident response Team
Use of Encryption
Threat Analysis and Sharing
Use of Security Analytics Services
DLP Implementation
Data Classification

The function of Feature 2 of the ARCS framework aims to evaluate:

- How many of the cost reduction remediation factors are implemented.
- The extent to which these factors are implemented.
- The alignment of the implementation(s) to best practices or standards.
- The structural level that is involved in the decision making of these implementations.
- The extent to which input cost factors are evaluated and measured.

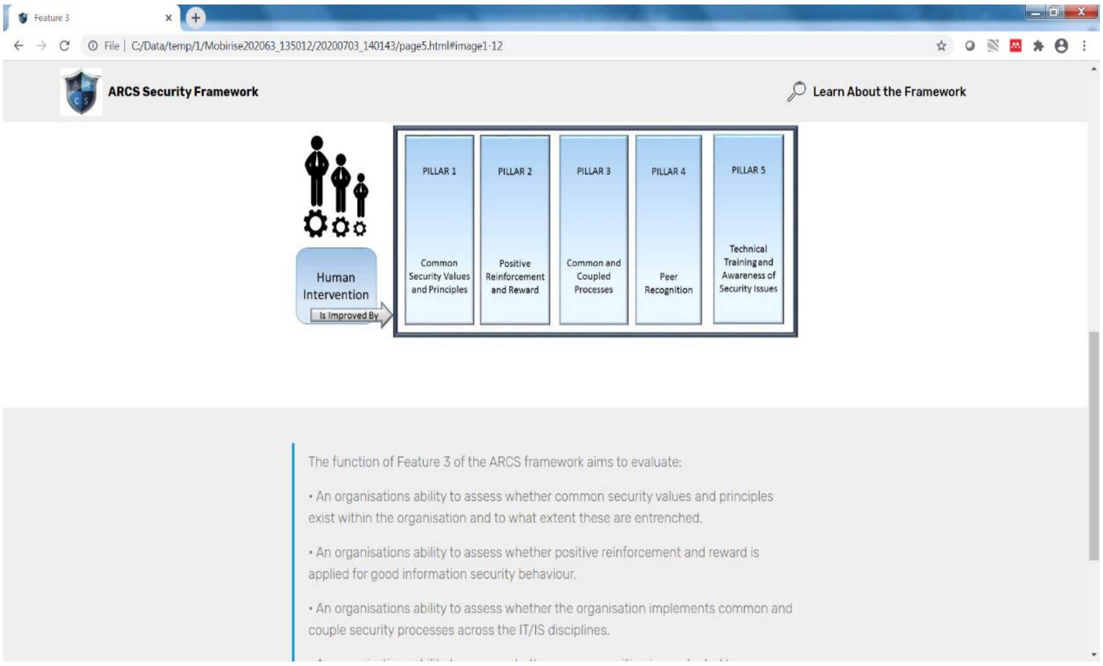
The Reduction of Cost feature is structured into thirteen evaluation areas and contains forty eight questions in total.

Figure 6-7 Feature 2 – Information Page – Screenshot 2


Feature 3
File | C:/Data/temp/1/Mobirise202063_135012/20200703_140143/page5.html#image1-12
ARCS Security Framework
Learn About the Framework
CCP
CSVP
PREC
PRR
TTSA
FEATURE 3 (F3): Sustainability of Information Security Culture

The **Sustainability of Information Security Culture** feature evaluates the readiness, behaviour and culture of the organisation in respect of information security. Feature 3 focuses on long term human behaviour in relation to information security and is supported by literature in traditional social sciences . The assessment objective, based on the model below, helps an organisation determine its current cultural and behavioural fit from an information security management perspective and assists in developing a longer term sustainable road map to

Figure 6-8 Feature 3 – Information Page – Screenshot 1


Feature 3
File | C:/Data/temp/1/Mobirise202063_135012/20200703_140143/page5.html#image1-12
ARCS Security Framework
Learn About the Framework
Human Intervention
Is Improved By
PILLAR 1
Common Security Values and Principles
PILLAR 2
Positive Reinforcement and Reward
PILLAR 3
Common and Coupled Processes
PILLAR 4
Peer Recognition
PILLAR 5
Technical Training and Awareness of Security Issues

The function of Feature 3 of the ARCS framework aims to evaluate:

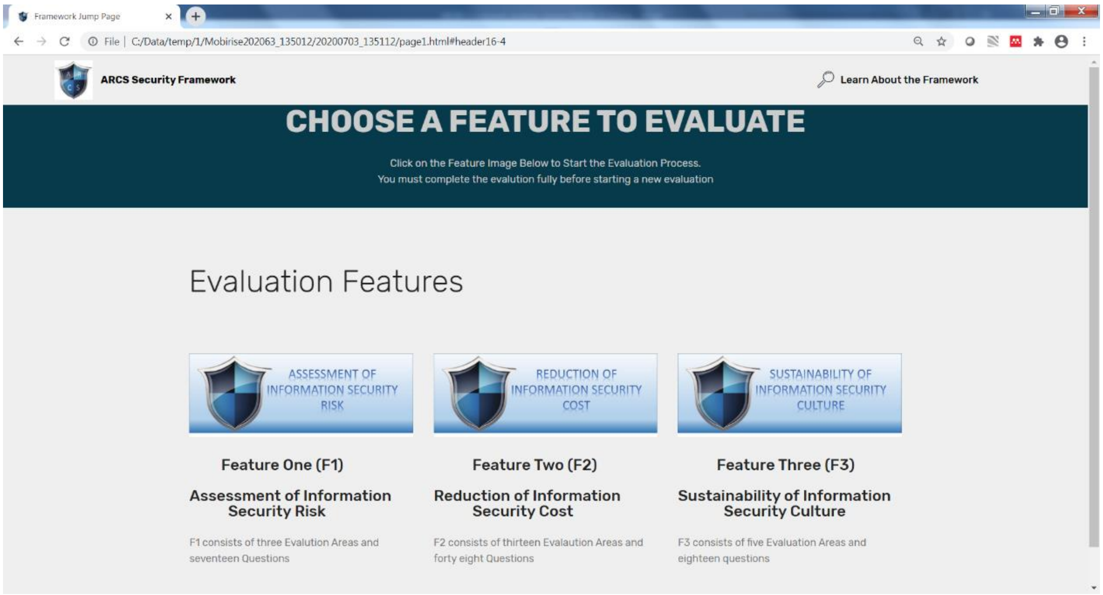
• An organisations ability to assess whether common security values and principles exist within the organisation and to what extent these are entrenched.

• An organisations ability to assess whether positive reinforcement and reward is applied for good information security behaviour.

• An organisations ability to assess whether the organisation implements common and couple security processes across the IT/IS disciplines.

Figure 6-9 Feature 3 – Information Page – Screenshot 2

The framework evaluation jump-page is depicted in Figure 6-10. On this page, the user has the opportunity to initiate the online form evaluation for any of the features.



Framework Jump Page
C:/Data/temp/1/Mobirise202063_135012/20200703_135112/page1.html#header16-4
ARCS Security Framework
Learn About the Framework

CHOOSE A FEATURE TO EVALUATE

Click on the Feature Image Below to Start the Evaluation Process.
You must complete the evalution fully before starting a new evaluation

Evaluation Features

ASSESSMENT OF INFORMATION SECURITY RISK
REDUCTION OF INFORMATION SECURITY COST
SUSTAINABILITY OF INFORMATION SECURITY CULTURE

Feature One (F1)

Assessment of Information Security Risk

F1 consists of three Evalution Areas and seventeen Questions

Feature Two (F2)

Reduction of Information Security Cost

F2 consists of thirteen Evalaution Areas and forty eight Questions

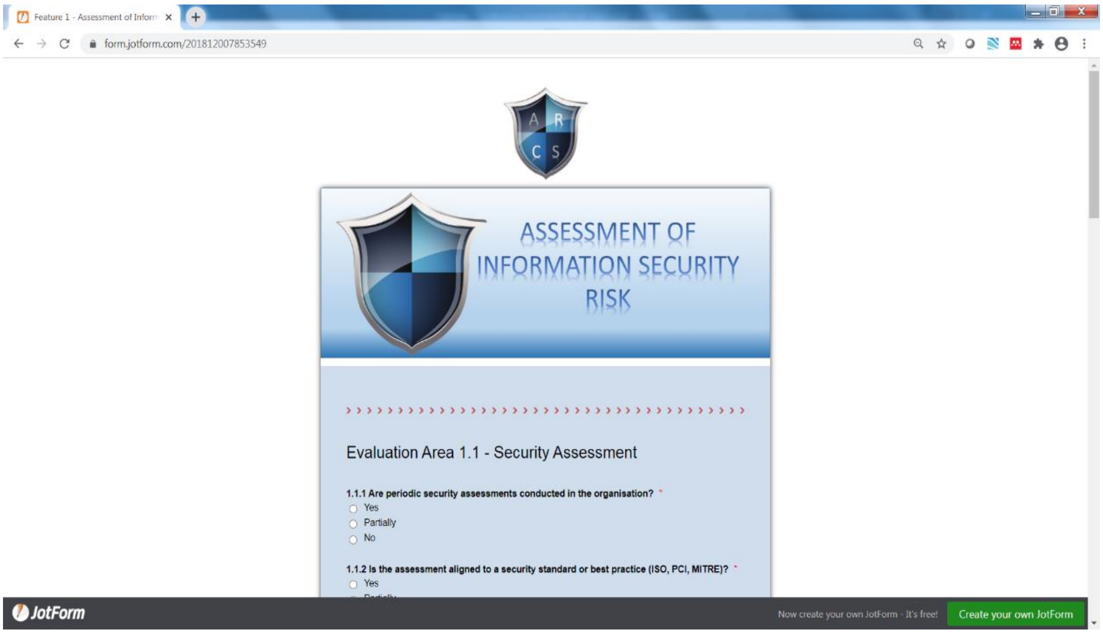
Feature Three (F3)

Sustainability of Information Security Culture

F3 consists of five Evaluation Areas and eighteen questions

Figure 6-10 Feature Evaluation Jump Page

Figures 6-11 to 6-16 depict the online forms created to evaluate each feature in an online platform called Jotform. Jotform is an online application that allows one to create custom online forms. It uses a drag-and-drop user interface to build forms with coding. Jotform can be used to create and publish forms, integrate the forms into a website and receive responses to inputs by email. The forms have the scoring logic embedded and output responses and calculations for analysis thereof are stored in an MS Excel file for evaluation and reporting.



Feature 1 - Assessment of Inform
form.jotform.com/201812007853549
A R C S
ASSESSMENT OF INFORMATION SECURITY RISK

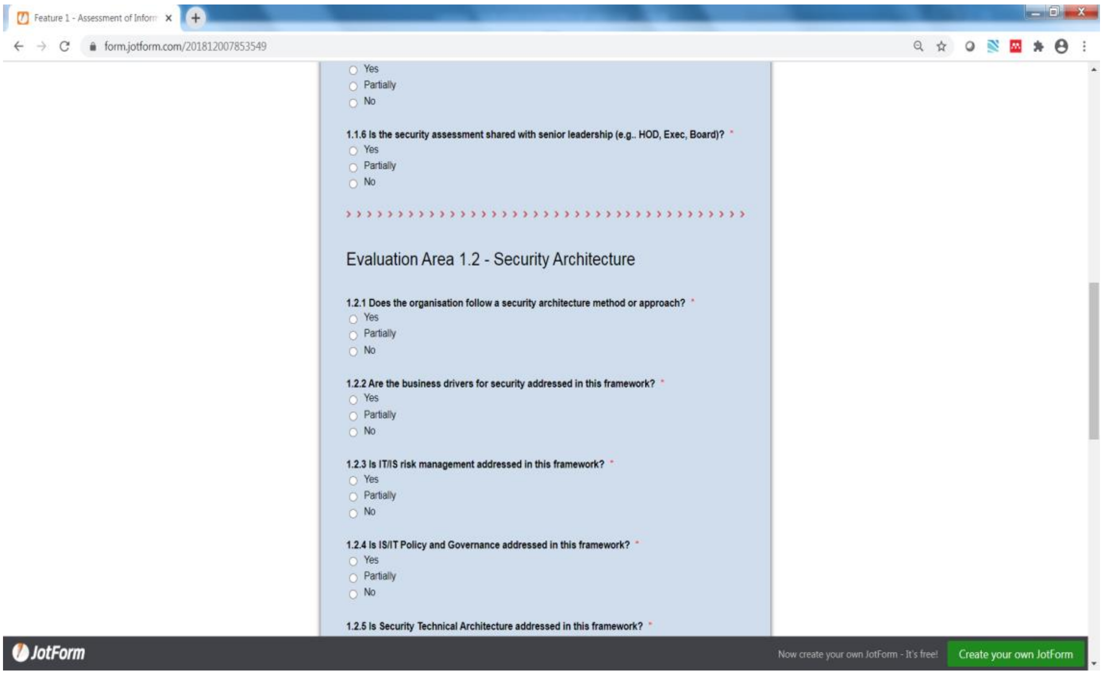
Evaluation Area 1.1 - Security Assessment

1.1.1 Are periodic security assessments conducted in the organisation? *
○ Yes
○ Partially
○ No

1.1.2 Is the assessment aligned to a security standard or best practice (ISO, PCI, MITRE)? *
○ Yes

JotForm
Now create your own JotForm - It's free!
Create your own JotForm

Figure 6-11 Feature 1 Online Form Screenshot 1


Feature 1 - Assessment of Inform
form.jotform.com/201812007853549

○ Yes
○ Partially
○ No

1.1.6 Is the security assessment shared with senior leadership (e.g.. HOD, Exec, Board)? *
○ Yes
○ Partially
○ No

› ›

Evaluation Area 1.2 - Security Architecture

1.2.1 Does the organisation follow a security architecture method or approach? *
○ Yes
○ Partially
○ No

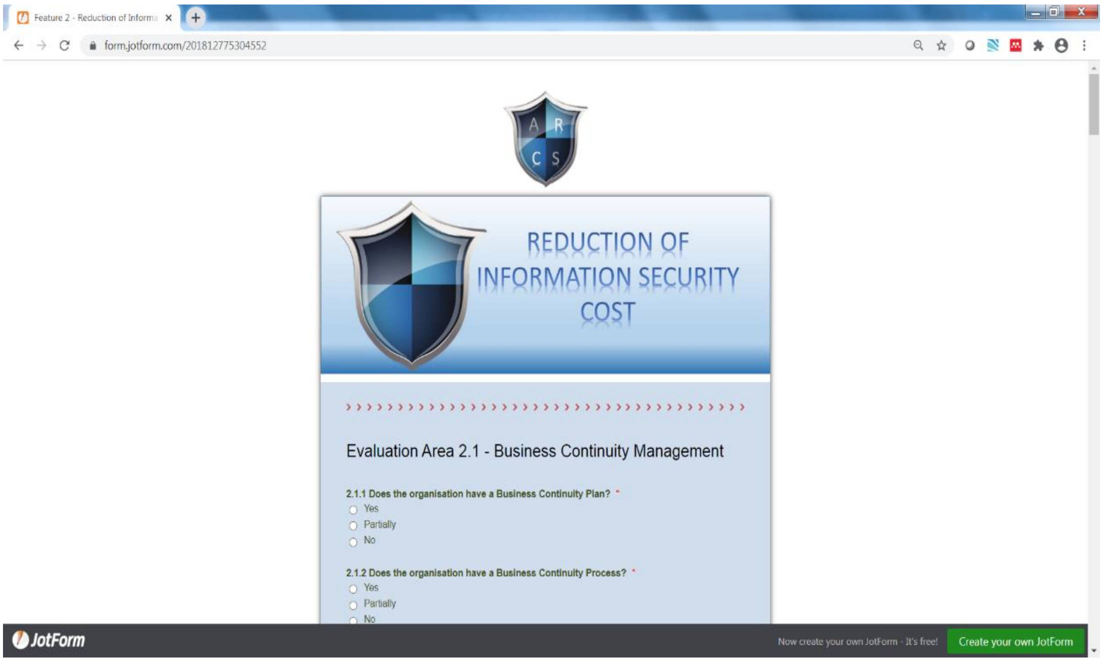
1.2.2 Are the business drivers for security addressed in this framework? *
○ Yes
○ Partially
○ No

1.2.3 Is IT/IS risk management addressed in this framework? *
○ Yes
○ Partially
○ No

1.2.4 Is IS/IT Policy and Governance addressed in this framework? *
○ Yes
○ Partially
○ No

1.2.5 Is Security Technical Architecture addressed in this framework? *

Figure 6-12 Feature 1 Online Form Screenshot 2


Feature 2 - Reduction of Informa
form.jotform.com/201812775304552
A R
C S

REDUCTION OF INFORMATION SECURITY COST

› ›

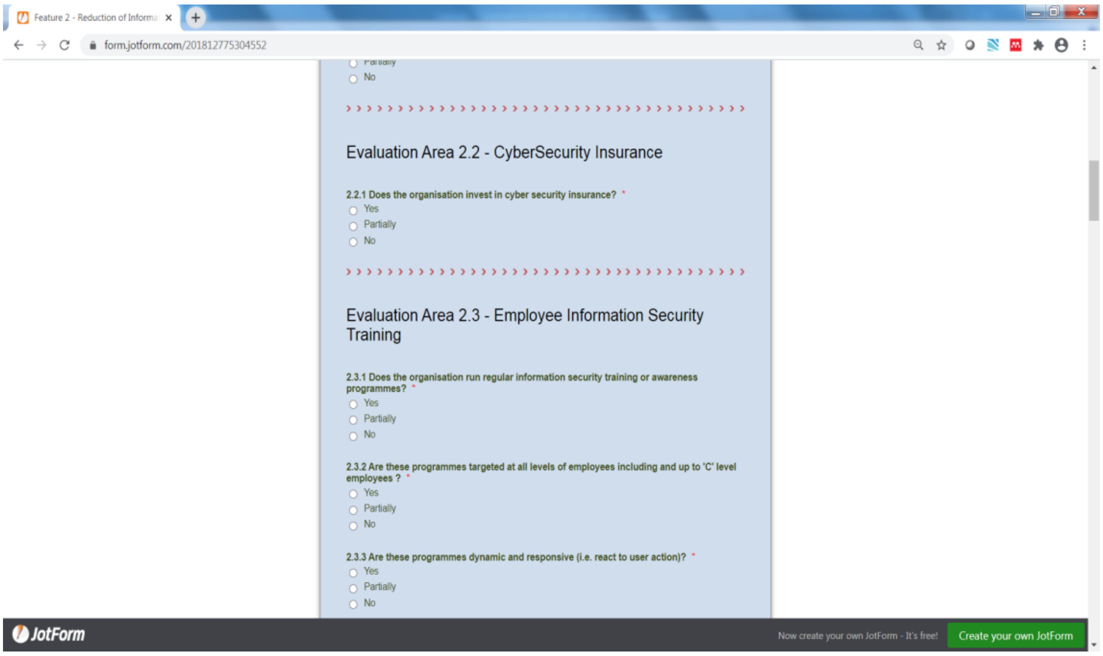
Evaluation Area 2.1 - Business Continuity Management

2.1.1 Does the organisation have a Business Continuity Plan? *
○ Yes
○ Partially
○ No

2.1.2 Does the organisation have a Business Continuity Process? *
○ Yes
○ Partially
○ No

JotForm
Now create your own JotForm - It's free!
Create your own JotForm

Figure 6-13 Feature 2 Online Form Screenshot 1


Feature 2 - Reduction of Informa
form.jotform.com/201812775304552
JotForm
Now create your own JotForm - It's free!
Create your own JotForm

○ No

Evaluation Area 2.2 - CyberSecurity Insurance

2.2.1 Does the organisation invest in cyber security insurance? *
○ Yes
○ Partially
○ No

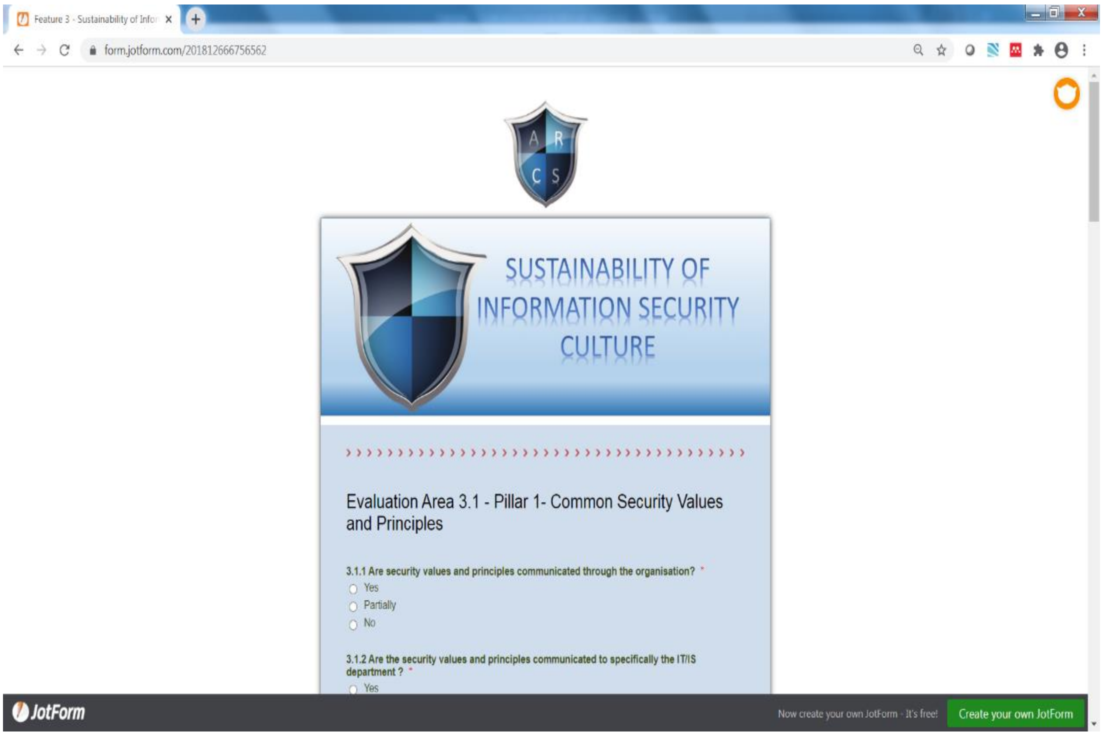
Evaluation Area 2.3 - Employee Information Security Training

2.3.1 Does the organisation run regular information security training or awareness programmes? *
○ Yes
○ Partially
○ No

2.3.2 Are these programmes targeted at all levels of employees including and up to 'C' level employees ? *
○ Yes
○ Partially
○ No

2.3.3 Are these programmes dynamic and responsive (i.e. react to user action)? *
○ Yes
○ Partially
○ No

Figure 6-14 Feature 2 Online Form Screenshot 2

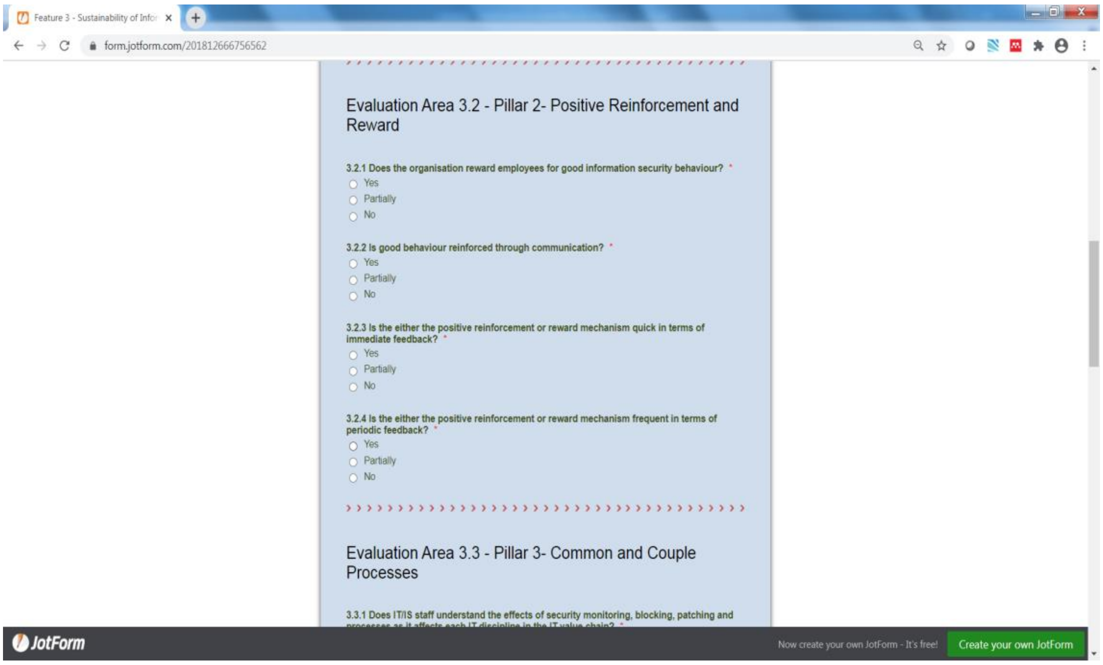

Feature 3 - Sustainability of Infor
form.jotform.com/201812666756562
A R
C S
SUSTAINABILITY OF
INFORMATION SECURITY
CULTURE
JotForm
Now create your own JotForm - It's free!
Create your own JotForm

Evaluation Area 3.1 - Pillar 1- Common Security Values and Principles

3.1.1 Are security values and principles communicated through the organisation? *
○ Yes
○ Partially
○ No

3.1.2 Are the security values and principles communicated to specifically the IT/IS department ? *
○ Yes

Figure 6-15 Feature 3 Online Form Screenshot 1



Feature 3 - Sustainability of Infor
form.jotform.com/201812666756562
JotForm
Now create your own JotForm - It's free!
Create your own JotForm

Evaluation Area 3.2 - Pillar 2- Positive Reinforcement and Reward

3.2.1 Does the organisation reward employees for good information security behaviour? *
○ Yes
○ Partially
○ No

3.2.2 Is good behaviour reinforced through communication? *
○ Yes
○ Partially
○ No

3.2.3 Is the either the positive reinforcement or reward mechanism quick in terms of immediate feedback? *
○ Yes
○ Partially
○ No

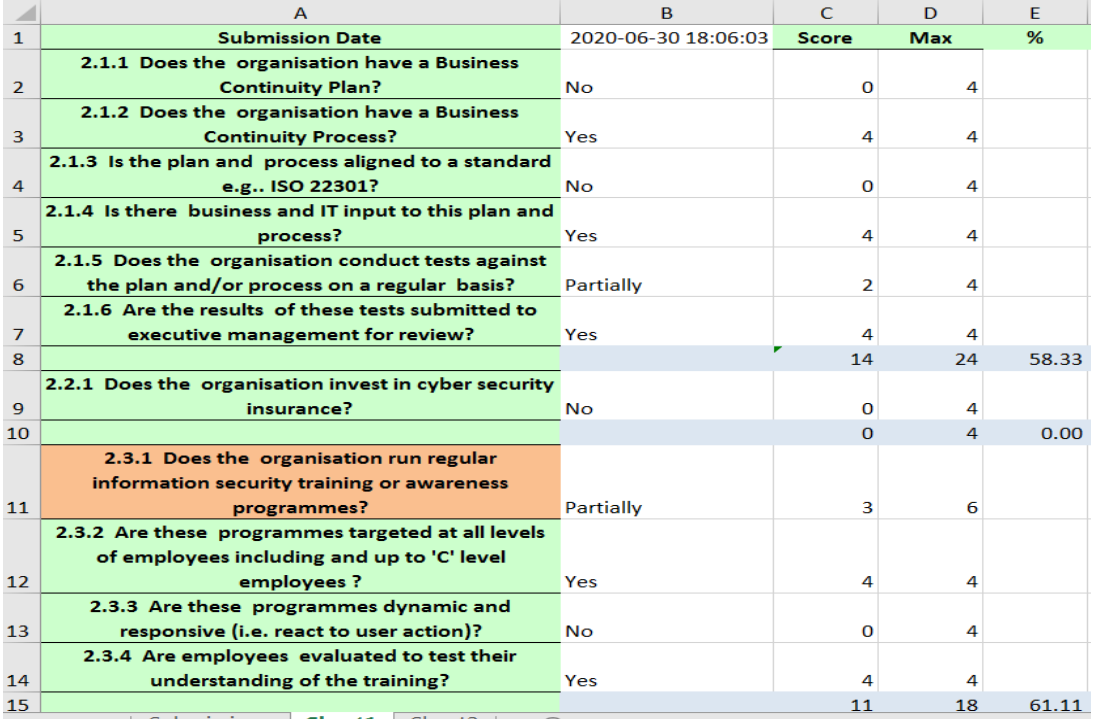
3.2.4 Is the either the positive reinforcement or reward mechanism frequent in terms of periodic feedback? *
○ Yes
○ Partially
○ No

Evaluation Area 3.3 - Pillar 3- Common and Couple Processes

3.3.1 Does IT/IS staff understand the effects of security monitoring, blocking, patching and processes as it affects each IT discipline in the IT value chain? *

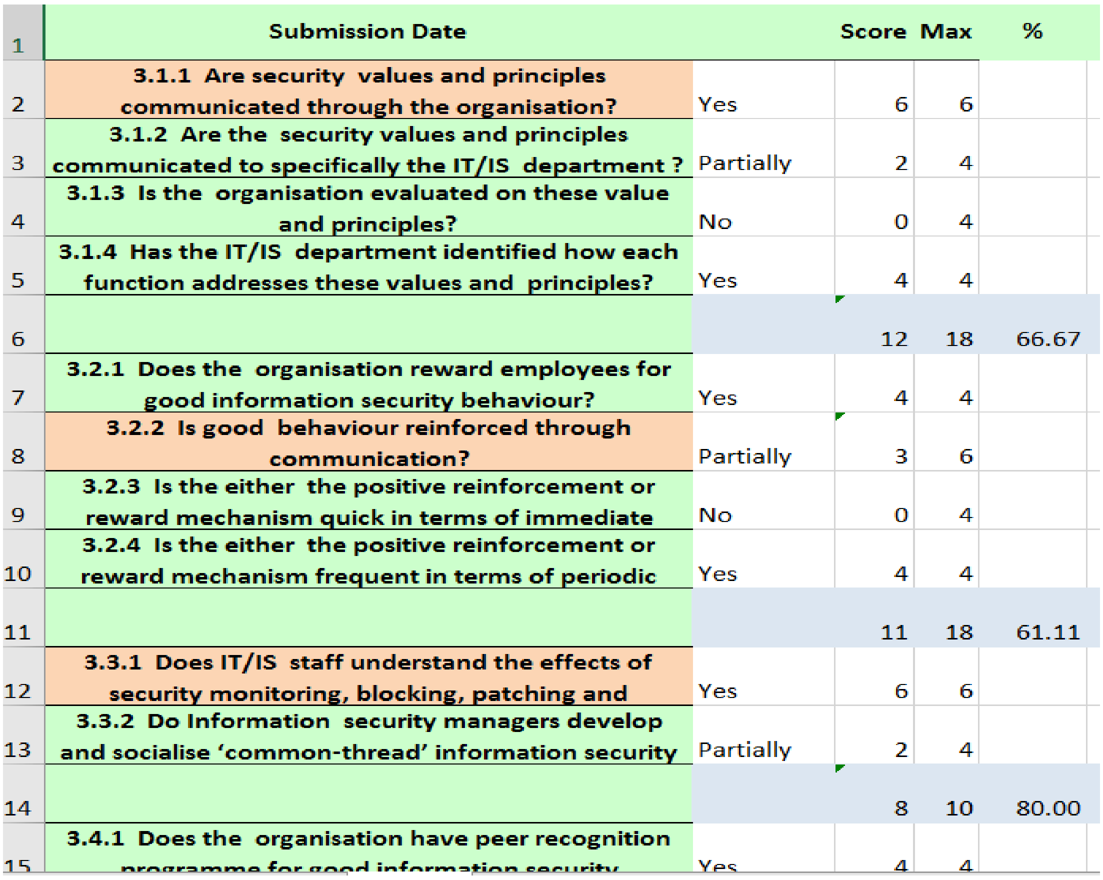
Figure 6-16 Feature 3 Online Form Screenshot 2

Figures 6-17 and 6-18 show examples of the results of assessments for specific features that are automatically populated from the Jotform application.



	A	B	C	D	E
1	Submission Date	2020-06-30 18:06:03	Score	Max	%
2	2.1.1 Does the organisation have a Business Continuity Plan?	No	0	4	
3	2.1.2 Does the organisation have a Business Continuity Process?	Yes	4	4	
4	2.1.3 Is the plan and process aligned to a standard e.g.. ISO 22301?	No	0	4	
5	2.1.4 Is there business and IT input to this plan and process?	Yes	4	4	
6	2.1.5 Does the organisation conduct tests against the plan and/or process on a regular basis?	Partially	2	4	
7	2.1.6 Are the results of these tests submitted to executive management for review?	Yes	4	4	
8			14	24	58.33
9	2.2.1 Does the organisation invest in cyber security insurance?	No	0	4	
10			0	4	0.00
11	2.3.1 Does the organisation run regular information security training or awareness programmes?	Partially	3	6	
12	2.3.2 Are these programmes targeted at all levels of employees including and up to 'C' level employees ?	Yes	4	4	
13	2.3.3 Are these programmes dynamic and responsive (i.e. react to user action)?	No	0	4	
14	2.3.4 Are employees evaluated to test their understanding of the training?	Yes	4	4	
15			11	18	61.11

Figure 6-17 Example of MS Excel output of Jotform Assessment – Feature 2



1	Submission Date		Score	Max	%
2	3.1.1 Are security values and principles communicated through the organisation?	Yes	6	6	
3	3.1.2 Are the security values and principles communicated to specifically the IT/IS department ?	Partially	2	4	
4	3.1.3 Is the organisation evaluated on these value and principles?	No	0	4	
5	3.1.4 Has the IT/IS department identified how each function addresses these values and principles?	Yes	4	4	
6			12	18	66.67
7	3.2.1 Does the organisation reward employees for good information security behaviour?	Yes	4	4	
8	3.2.2 Is good behaviour reinforced through communication?	Partially	3	6	
9	3.2.3 Is the either the positive reinforcement or reward mechanism quick in terms of immediate	No	0	4	
10	3.2.4 Is the either the positive reinforcement or reward mechanism frequent in terms of periodic	Yes	4	4	
11			11	18	61.11
12	3.3.1 Does IT/IS staff understand the effects of security monitoring, blocking, patching and	Yes	6	6	
13	3.3.2 Do Information security managers develop and socialise 'common-thread' information security	Partially	2	4	
14			8	10	80.00
15	3.4.1 Does the organisation have peer recognition programme for good information security	Yes	4	4	

Figure 6-18 Example of MS Excel output of Jotform Assessment – Feature 3

Based on the output results, spider graphs were then created to show the performance in regard to the assessment. The output charts are similar to the original created in Chapter 4; however, the enhanced graphs show more information, such as the actual scores. The graphs also depict the relative coverage against the total score out of 100 percent. Examples of outputs graphs for each feature and the overall summary are illustrated in Figures 6-19 to 6-22. The interpretation of these graphs remains the same as described in Chapter 4.

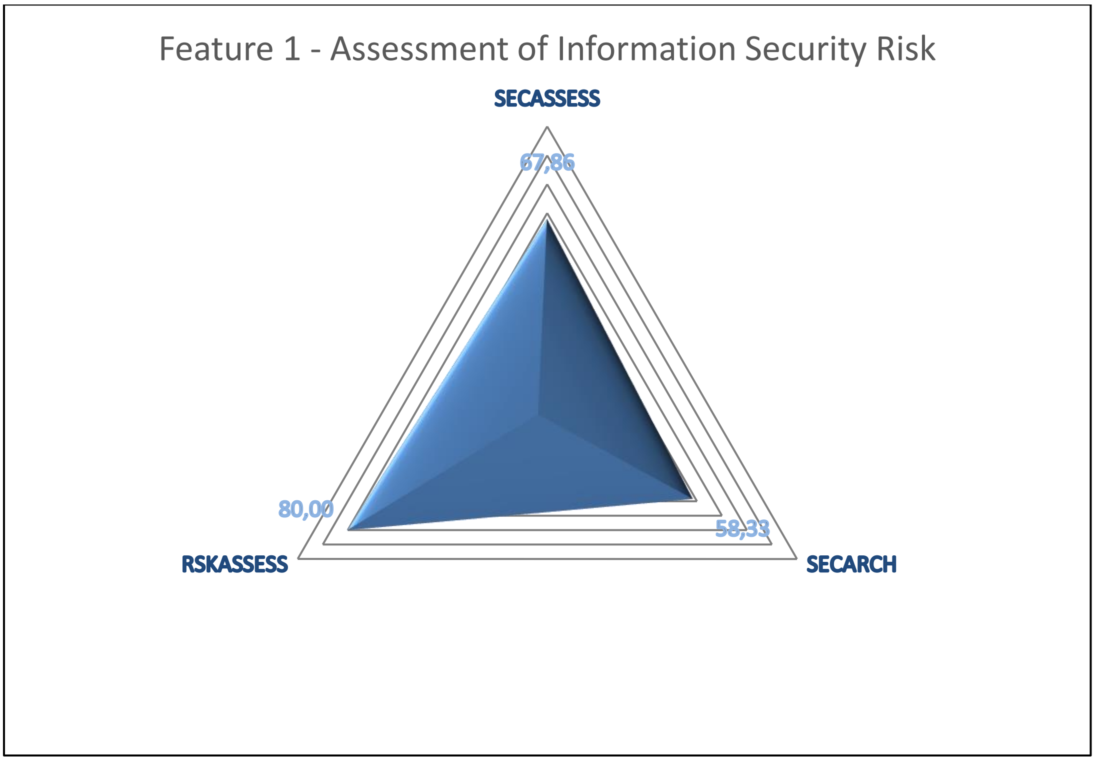


Figure 6-19 Enhanced output graph for Feature 1

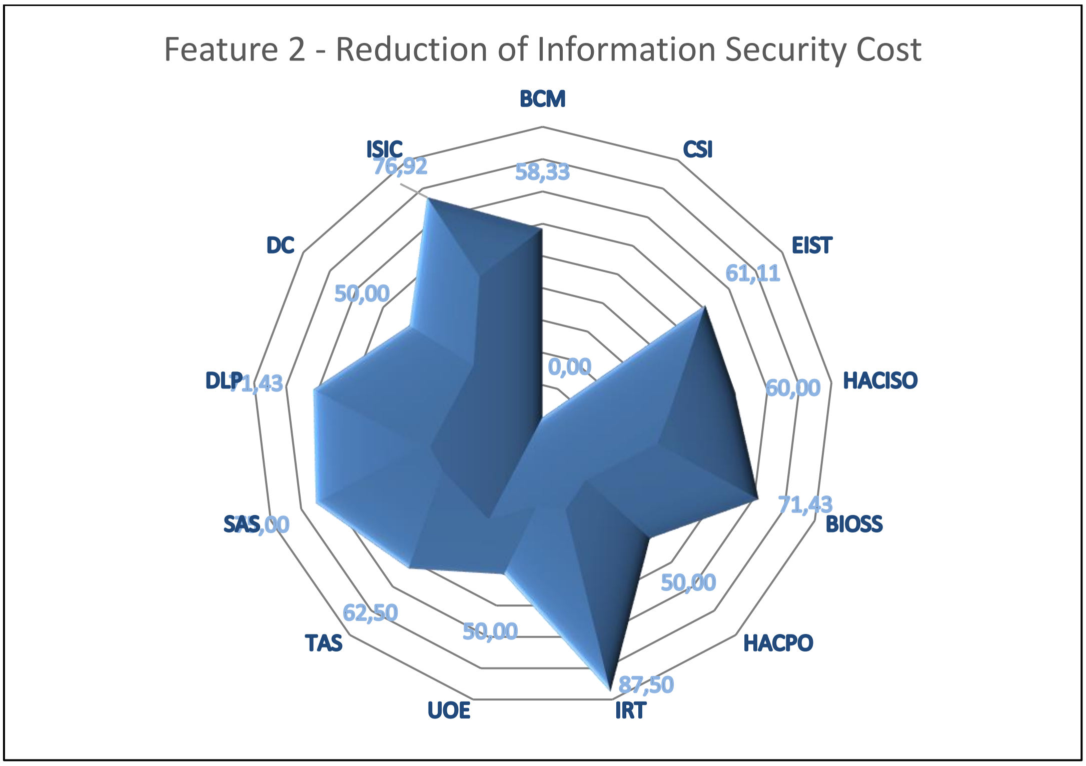


Figure 6-20 Enhanced output graph for Feature 2

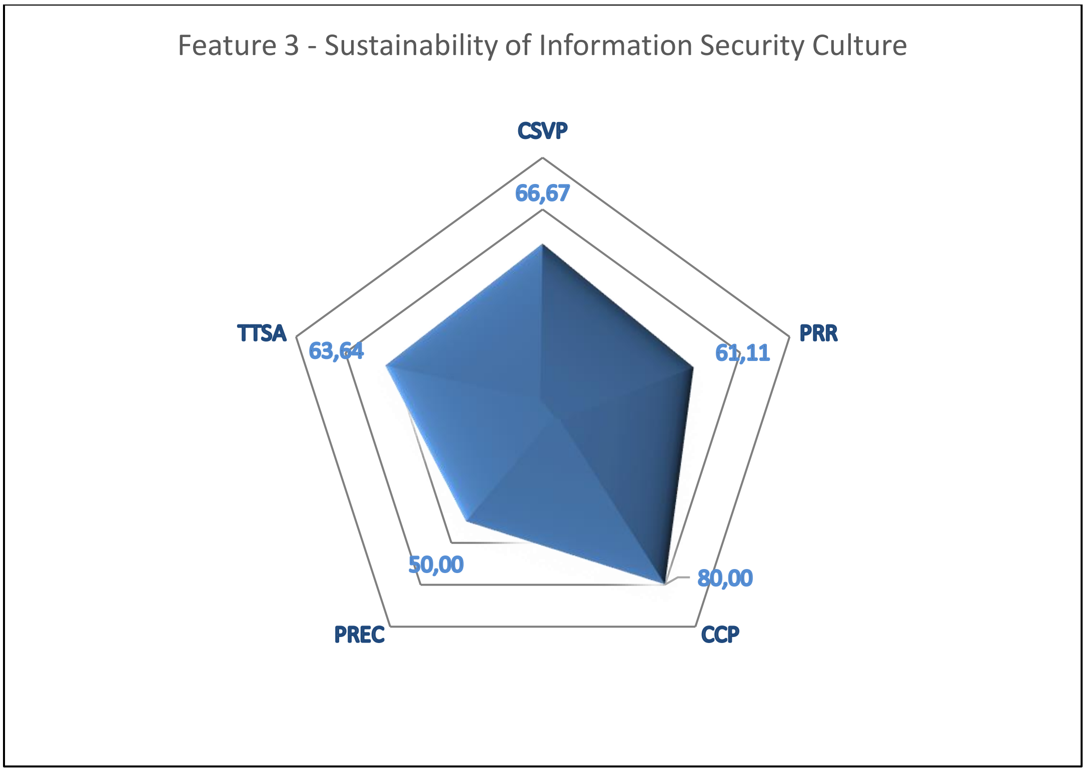


Figure 6-21 Enhanced output graph for Feature 3

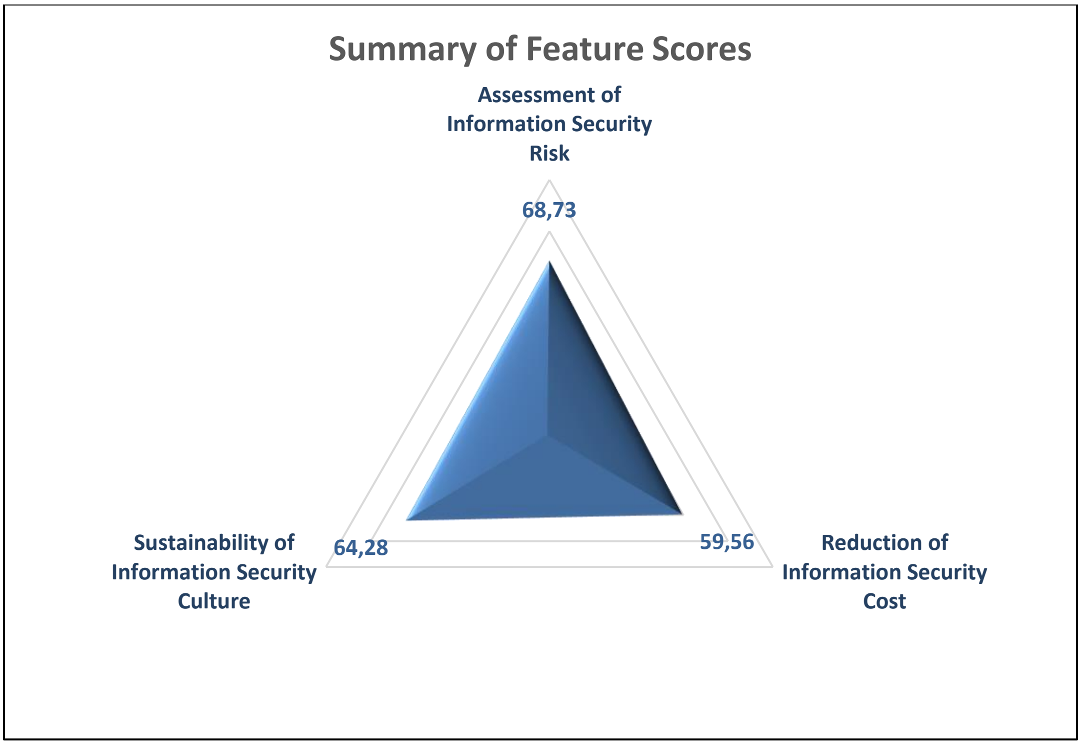


Figure 6-22 Enhanced output graph for Summary Scores of All Features

6.2 SUMMARY AND IMPLICATIONS

In this chapter, the framework and tool have been enhanced based on comments elicited from the expert’s review, noted in Chapter 5. The key improvements have been:

- Enhanced responses allowing for a “Partial” response in addition to “Yes” and “No”
- Enhanced scoring allowing for better differentiation in output scoring and improved analysis
- Creation of a website to give users more information about the framework, models and related components
- Automation of the launching of the evaluation tool
- Automation of the survey mechanism in using the evaluation tool
- Built-in logic for scoring in the automated tool
- Automated output of results from the tool
- Improved graphs with more information showing output and summary results

The improvements noted have not been tested further but may be considered for future research. The enhancements described in this chapter form the foundation for the future iteration and improvement roadmap described in Chapter 7.

Chapter 7: Further Research and Future Studies

Chapter 1 Introduction	Research Purpose, Rationale, Background and Scope of Study
Chapter 2 Literature Review	Information Security (IS), IS Assessments, IS Architecture, IS Risk Assessment, Organisational Culture, IS Culture, Motivation, Positive Reinforcement and Reward
Chapter 3 Research Methodology	Methodology and Research Design, Participants, Instruments, Procedures and Timelines, Analysis, Ethics and Limitation
Chapter 4 Security Models, Framework and Evaluation Tool	Models for Cost Reduction, Security Assessment and Information Security Cultural Improvement, The ARCS Security Framework, The ARCS Security Evaluation Tool
Chapter 5 Analysis, Results and Findings	Analysis, Results and Findings of the Demonstration of the ARCS Security Evaluation Tool
Chapter 6 Review and Update of the Evaluation Tool	Evaluation of Expert Reviews of the ARCS Security Model and the ARCS Security Evaluation Framework Update of the ARCS Security Evaluation Framework
Chapter 7 Further Research and Future Studies	Further Research and Future Studies
Chapter 8 Conclusion	Conclusion

Chapter 7: Further Research and Future Studies

In Chapter 6, a second iteration of the security framework and evaluation tool was developed in line with the iterative improvement philosophy of DSR.

In this chapter, the researcher will discuss potential future research, including improvements and enhancements to the security framework and tool. Additionally, the researcher will consider expanding the framework to encompass a more detailed evaluation of Information Security in an organisation.

Section 7.1.1 will focus on an improved framework relationship model along with an improved question model. Sections 7.1.2 and 7.1.3 discuss new features that may be included in the security framework that deal with information technology compliance as a function of securing information, as well as data privacy.

Section 7.2 proposes a technological enhancement of the security evaluation tool through a conceptual architecture for the development of the tool into a full web application.

Finally, in Section 7.3, an evaluation of the utility, quality and efficacy of the designed artefacts is conducted.

7.1 IMPLICATIONS OF STUDY AND FUTURE RESEARCH

In Chapter 5, the artefacts developed in this study were demonstrated and evaluated. The outcome of the evaluation was communicated. In Chapter 6, a second iteration of the ARCS Security Framework and Evaluation tool was developed in line with the iterative DSR process selected. Based on the scope of the study, there is potential to expand and improve the ARCS Security Framework and Evaluation Tool. The following section describes potential enhancements. It is envisaged that additional research can be conducted by practically making the changes noted and then conducting additional phases of demonstration and evaluation of the 'new' artefacts. Further research could also be conducted by selecting one or more features and expanding those to a more detailed level of questioning to meet the needs of different levels of employees, from information security managers to technical security personnel.

7.2 EXPANSION OF THE ARCS SECURITY FRAMEWORK

7.2.1. Reconfiguration of the relationship model and question model

In Chapter 4, Section 4.3, the ARCS relationship model was described and is depicted for reference in Figure 7 -1. In this model, each feature (F1, F2 and F3) is broken down into an evaluation area. Each evaluation area (E1, E2, $E_{n)}$ is given a shortened tagged description and is broken down further into questions (Q $_{n}$.1 to Q $_{n.m}$) related to that evaluation area. The questions were then developed in line with the evaluation aim of the overall evaluation goal of the information security programme.

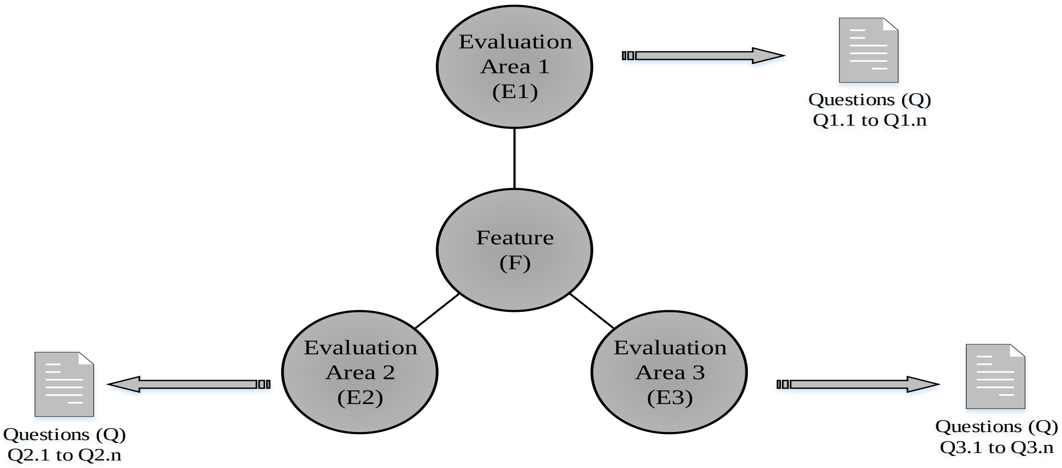

Evaluation Area 1 (E1)
Questions (Q) Q1.1 to Q1.n
Feature (F)
Evaluation Area 2 (E2)
Evaluation Area 3 (E3)
Questions (Q) Q2.1 to Q2.n
Questions (Q) Q3.1 to Q3.n

Figure 7-1 Original ARCS Security Framework Relationship Model

The framework comprised of three features established from the models developed in sections 4.1.2 and 4.1.3; twenty-one evaluation areas were created for the framework, and eighty-three questions were developed for the framework that is aligned to the evaluation areas.

In discussion with expert reviewers, it was established that the framework was positioned at a management reporting level and did not interrogate more technical aspects of information security. Furthermore, one expert reviewer advised that the evaluation areas did not cover the compliance realm as much as the information security realm. The researcher developed the framework relationship model with expansion in mind to evolve over time based on newer information security concepts, technology and processes.

The researcher would consider future studies to reconfigure the framework to expand the relationship between evaluation areas and questions to a relationship between evaluation areas and sub-evaluation areas, as noted in Figure 7-2. The researcher would also consider an expansion of the framework to include an assessment or measurement process to evaluate the organisations' ability to respond to the outcomes after using the framework and evaluation tool. This could be developed as a stand-alone ongoing organisational improvement metric.

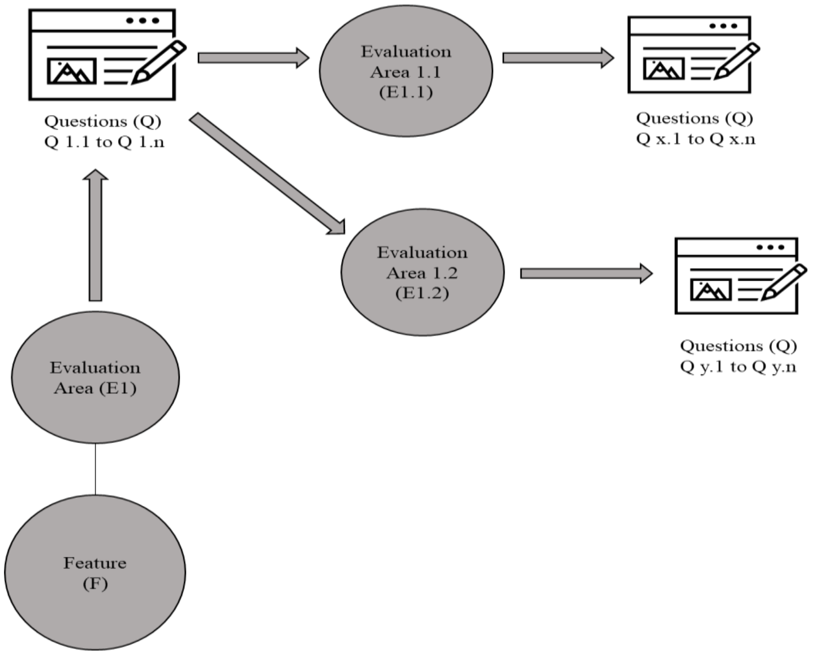


Figure 7-2 Updated Relationship Model

The question in each section or sub-section will be contextual, thus leading a user of the framework to more defined and detailed evaluations of their environments. The questions would be related as per a defined tree model, as depicted in Figure 7-3.

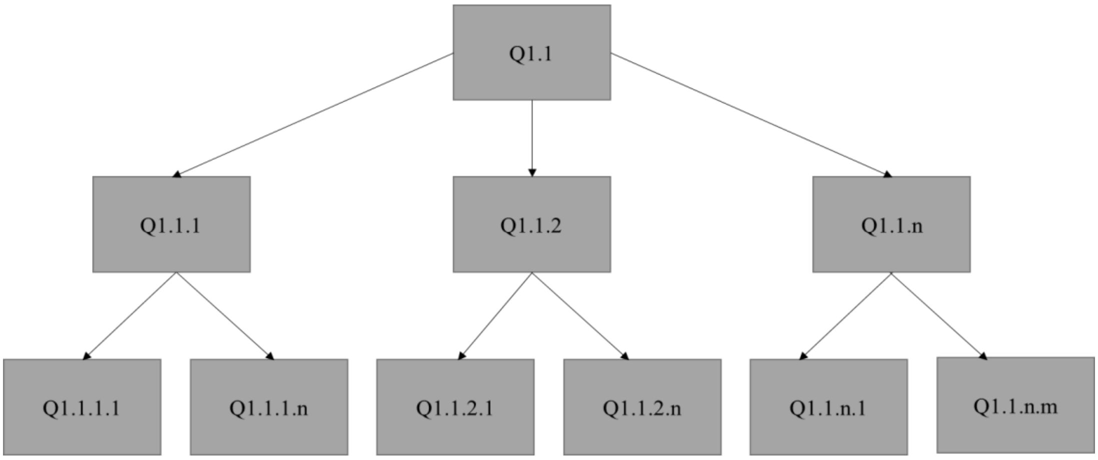


Figure 7-3 Updated Questionnaire Tree Model

Expanding the models addresses the concerns of expert reviewers in regard to bringing in more technical aspects of information security management and moving the reporting output away from just high-level management reporting to more actionable technical responses to the evaluated gaps.

7.2.2 Addition of a Compliance Feature Area

IT compliance pertains to adhering to established regulations, ensuring that products or services meet prescribed criteria stipulated by the regulated sector, and avoiding the creation of undue risks (Chatterjee and Sokol 2019). Regulatory bodies, including auditors, customers, regulators, and legislators, establish and enforce industry-specific standards, while industry participants are responsible for complying with these standards as they engage in the sector. Typically, each industry possesses a set of standards, and certain domains are subject to multiple sets of rules that may intersect or overlap (Edwards et al. 2019).

Though compliance shares similarities with information security in terms of encouraging businesses to exercise due diligence in safeguarding their digital assets, the underlying motivation diverges. Compliance primarily revolves around fulfilling the prerequisites set forth by a third party, be it a government entity, security framework, or the contractual terms stipulated by a client. Compliance frameworks define the controls and the parameters of control an organisation needs to adhere to in order to conduct business (Haqaf and Koyuncu 2018). Should an organisation aspire to operate within a jurisdiction governed by stringent privacy regulations, or within heavily regulated sectors such as healthcare or finance, or in collaboration with clients demanding elevated confidentiality standards, they are required to follow the specified guidelines and enhance their security measures accordingly. For instance, regulations like HIPAA (Herold and Beaver 2014) and Sarbanes Oxley (Kim et al. 2008) or standards like PCI-DSS (Wu et al. 2018) or ISO:27001 (Prislan and Bernik 2010), detail explicit security prerequisites that a business must satisfy to attain compliance. A prominent client might demand the implementation of exceptionally stringent security measures, exceeding what could be deemed as reasonably essential, as a condition for awarding them a contract. Meeting these goals is pivotal for success, as failure to comply could lead to erosion of customer confidence or outright legal impediments to engaging in business within the market.

Achieving compliance with a specific set of standards entails ensuring that all pertinent facets of the business mandated to adhere to those standards indeed adhere to them, and the company can substantiate this assertion (Chatterjee and Sokol 2019). Any organisation utilising technology to conduct business within a sector subject to specific regulations (or within a relevant legal jurisdiction in certain instances) must validate their compliance with those standards, lest they face potential fines or other punitive measures.

IT compliance refers to the procedure of satisfying the digital security prerequisites set forth by a third party, facilitating the conduct of business operations within a specific market or in collaboration with a particular customer (Herold and Beaver 2014).

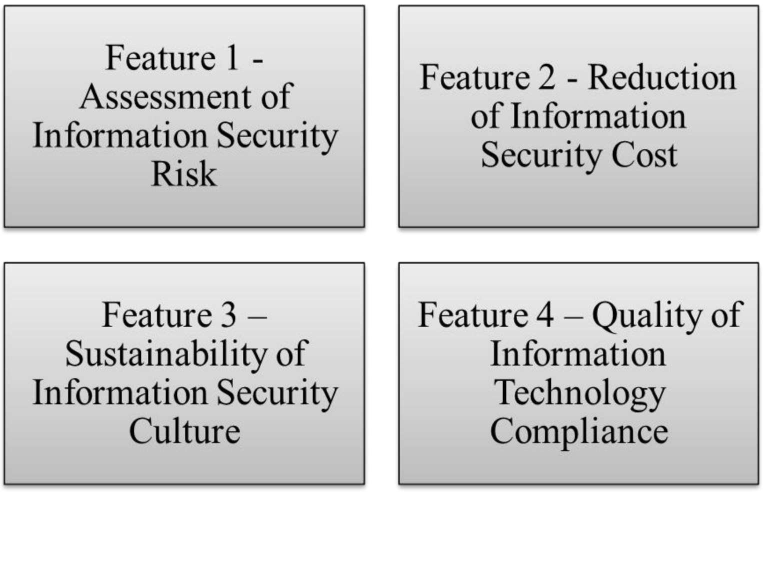

Feature 1 - Assessment of Information Security Risk
Feature 2 - Reduction of Information Security Cost
Feature 3 – Sustainability of Information Security Culture
Feature 4 – Quality of Information Technology Compliance

Figure 7-4 Updated Security Evaluation Framework including Compliance

In the context of this study, the framework developed evaluates an organisation’s adherence to a best practice or standard. Still, it does not currently evaluate the effectiveness of the organisation in implementing the controls, processing activities and related collection of supporting evidence from a compliance perspective. Therefore, the researcher considers that an expansion of the framework to assist in evaluating compliance effectiveness through the addition of a compliance feature area along with supporting evaluation areas and questions, as depicted in Figure 7-4, would be of significant value to users.

7.2.3. Data Privacy Feature

Data privacy is a subset of information security that concentrates on the proper handling of data, encompassing elements such as consent, notifications, and regulatory obligations. While the terms data security and data privacy are occasionally used interchangeably, they hold distinct attributes: data security protects data from external threats and internal breaches, while data privacy governs the practices of data gathering, sharing, and utilisation.

Data privacy concerns frequently center on matters like whether and how data are disclosed to third parties, the lawful methods of data collection or storage, and adherence to regulatory constraints such as GDPR, HIPAA, or POPIA. (Torra 2017).

Data remains as one of an organisation's most valuable resources. In the era of the data economy, businesses recognise significant worth in gathering, distributing, and utilising data. Maintaining transparency in the way companies solicit consent, adhering to their privacy policies and appropriately managing the data they have collected becomes crucial to nurturing trust and accountability among customers and partners who emphasise privacy (Martin, Borah and Palmatier 2017).

Within the technology sector, standards play a crucial role in dictating numerous facets of how companies gather, oversee, and utilise customer and consumer data. As technology's accessibility and multifaceted applications expanded, so did the potential for companies to leverage it (Wu et al. 2018). Consequently, a plethora of regulatory bodies across the globe have emerged, issuing directives that impact technology and its comprehensive applications. Furthermore, the number of countries that enacted data privacy legislation, or are currently in the process of doing so, has increased significantly in the last three to five years.

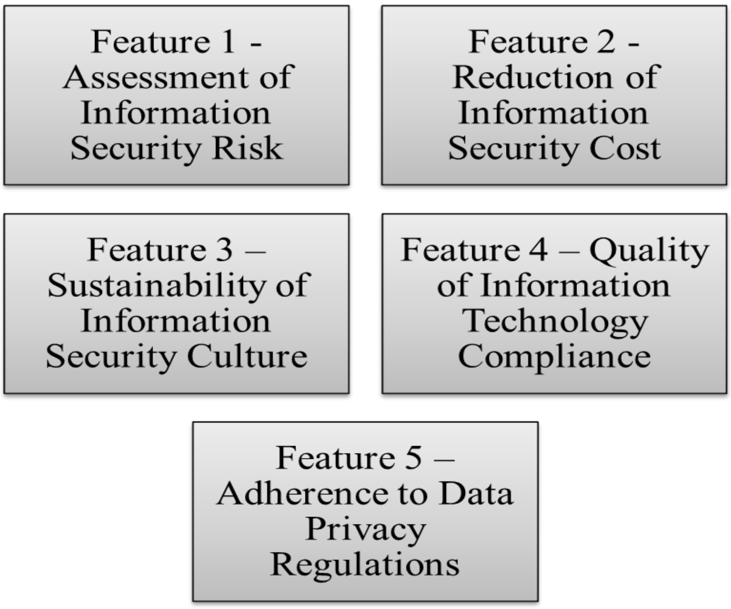

Feature 1 - Assessment of Information Security Risk
Feature 2 - Reduction of Information Security Cost
Feature 3 – Sustainability of Information Security Culture
Feature 4 – Quality of Information Technology Compliance
Feature 5 – Adherence to Data Privacy Regulations

Figure 7-5 Updated Security Evaluation Framework including Data Privacy

In the context of this study, the framework developed is limited to an organisation's effective adherence to data privacy regulations and the processes expected of an organisation to protect personal identifiable information submitted by customers, vendors and employees. Therefore, the researcher considers that an expansion of the framework to assist in evaluating Data Privacy regulatory and process alignment through the addition of a Data Privacy feature area along with supporting Evaluation areas and questions, as depicted in Figure 7-5, would be of significant value to users.

7.3 ENHANCEMENT OF THE SECURITY EVALUATION TOOL

The enhancement of the security evaluation tool was addressed in line with expert reviewers in Chapter 6. However, the researcher considers that there can be more significant improvements with further research and development. The current instantiation of the tool is not built with expansion and professional usability in mind. The tool may also not be applicable for organisation that have a limited information security capacity or capability. The tool will need to be re-developed to adhere to software development best practices for web-based applications. The application should be on single platform, tiered and architected with modularity in mind. A defined data model, along with a robust modular evaluation model must be implemented as part of the evaluation tool.

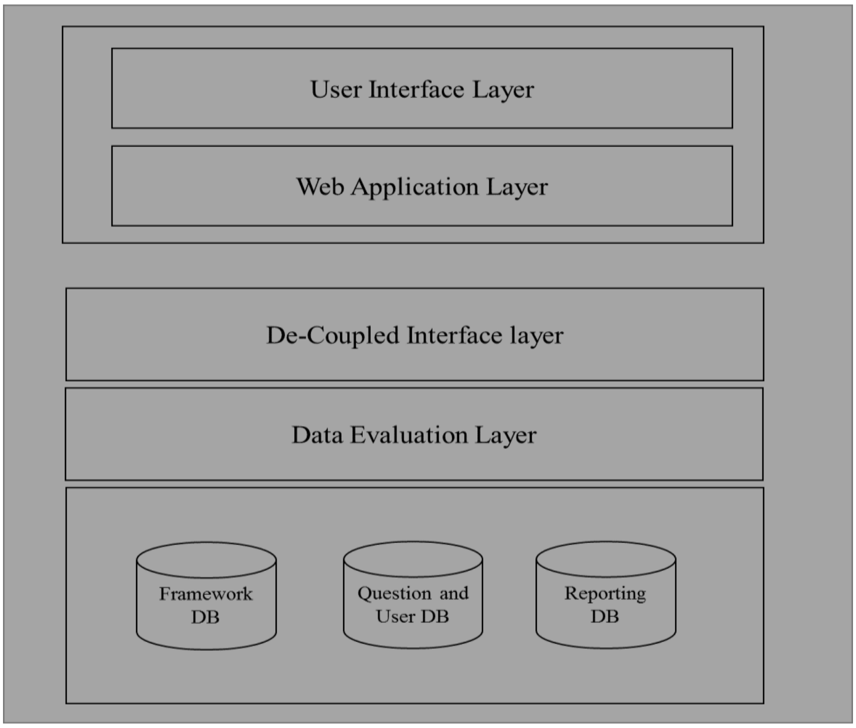


Figure 7-6 Conceptual Architecture of Improved Security Evaluation Tool

A generic architecture of the future state is described in Figure 7-6, which shows the tiered conceptual design. The application should be an easily accessible web-based tool that contains a user interface that allows the user to capture the input of the responses of the evaluation tool. The tool should use the data evaluation layer to assess inputs and create a pro-forma management report which is presented either through the user interface or through a prepared electronic document. The data layer and respective database would allow for the retention of historical data which would then allow an organisation to continuously evaluate themselves as they make relevant improvements.

7.4 DSR METHODS EVALUATION

As described in Chapter 3, Hevner et al. (2004) aligns research methods to possible artefacts created, to allow the researcher to evaluate the utility, quality and efficacy of design artefacts. Table 7-1 conducts this evaluation for the research methods used in this study.

Table 7-1 Design Evaluation Methods (Hevner et al., 2004)

Research Methods	**Artefact Used**	**Utility**	**Quality**	**Efficacy**
Observational	Field study - interviews	The semi-structured interview questionnaire was easy to use and was well understood by the participants.	The quality of the data received assisted well in conducting analysis of the artefacts.	The semi-structured interview questionnaire was effective in eliciting relevant information from participants.
Analytical	Static analysis and optimisation - expert reviews	In the initial development the researcher felt that the framework and tool developed would be easy to use. Through discussion and observation with expert reviewers it was found that the framework may need to be expanded with additional features and evaluation areas and that the tool could be improved by modernising it. These are the improvements described in Chapter 6 and 7.	Generally, the expert reviews found the quality of the framework and tool to be good.	Expert reviewers all agreed that the usage of assessment methodology and the fact that there was a supporting tool would be effective for their organisation.

Research Methods	Artefact Used	Utility	Quality	Efficacy
Experimental	Simulation – Analysis of Framework and Evaluation Tool conducted with Expert Reviewers	When describing the framework and tool and allowing expert reviewers to analyse these artefacts it was observed that the artefacts where of easy to understand and could be used in practice.	Expert reviewers felt that all artefacts presented were of a good quality.	Expert reviewers felt that Framework and Tool would be of value to their organisations.
Testing	Functional (Black Box Testing) – Framework tested through Evaluation Tool using Expert Reviewer data	All testing of the framework and tool was conducted without any glitches or misrepresentation of data.	Expert reviewers felt that the output of the tools could be better represented and also looked for better automated reporting from the tool. These concerns were addressed in Chapter 6 and 7.	Expert reviewers felt that the output results were in line with their own observations of their organisations.
Descriptive	Informed Argument – Used information gathered from	The output if the evaluation assisted the researcher in enhancing and redeveloping the framework and tool artefacts.	The data received from Expert Reviewers was of good quality and the observations assisted researcher.	The information gathered helped the researcher to develop a more effective Framework and Tool and

Research Methods	**Artefact Used**	**Utility**	**Quality**	**Efficacy**
	Expert Reviewer and researcher observation to evaluate artefacts.			assisted in developing a roadmap for future iteration. These are described in Chapter 6 and 7.

7.5 SUMMARY AND IMPLICATIONS

In this chapter, the framework and evaluation tool artefacts developed in Chapter 4 and improved in Chapter 6 are further proposed for expansion to be able to further academic and practical application of these artefacts. As described in Chapter 3, Section 3.1.2, in Drechsler and Hevner's (2006) process model the DSR process accommodates change and impact of artefacts once developed, described and evaluated. In the case of this study, through observation and expert review, the researcher noted limitations and possible enhancements to the artefacts that are beyond the scope of this study. As such, this chapter focused on those possible changes.

Chapter 8 summarises and concludes this research initiative. Outcomes of the study and its response to expected research questions and objectives are discussed.

Chapter 8: Conclusion

Chapter 1 Introduction	Research Purpose, Rationale, Background and Scope of Study
Chapter 2 Literature Review	Information Security (IS), IS Assessments, IS Architecture, IS Risk Assessment, Organisational Culture, IS Culture, Motivation, Positive Reinforcement and Reward
Chapter 3 Research Methodology	Methodology and Research Design, Participants, Instruments, Procedures and Timelines, Analysis, Ethics and Limitation
Chapter 4 Security Models, Framework and Evaluation Tool	Models for Cost Reduction, Security Assessment and Information Security Cultural Improvement, The ARCS Security Framework, The ARCS Security Evaluation Tool
Chapter 5 Analysis, Results and Findings	Analysis, Results and Findings of the Demonstration of the ARCS Security Evaluation Tool
Chapter 6 Review and Update of the Evaluation Tool	Evaluation of Expert Reviews of the ARCS Security Model and the ARCS Security Evaluation Framework Update of the ARCS Security Evaluation Framework
Chapter 7 Further Research and Future Studies	Further Research and Future Studies
Chapter 8 Conclusion	Conclusion

Chapter 8: Conclusion

This Chapter will summarise and conclude the research initiative. This research set out to answer the primary research question: *What constitutes a framework and an associated tool that evaluates an organisation regarding how the organisation assesses information security, aligns cost-reducing of information security products and services and sustains improved information security culture?*

In meeting that objective, a DSRM process was followed. The artefacts that were developed, evaluated and improved provided the key deliverables defined, regarding the primary and secondary research questions. These also lent to the researcher's understanding of the limitations of the developed artefacts, which gave input to what future studies may be undertaken.

Section 8.1 discusses the foundation of the study, the rationale and purposes of the study and the key contributions of the In Section 8.2, the researcher discusses how the problems, defined in Chapter 1, were understood and how the researcher responded to addressing those problems and the sub-research objectives defined. In Section 8.3 the artefacts developed in response to the primary and sub-research questions are summarised. Section 8.4 provides a summary of the analysis and findings and the researcher's interpretation of the comments of participants. Lastly, Section 8.5. discusses the researcher's view of the artefacts developed from the conceptual to developed stage, future research considerations and the researcher's experiences during the study.

8.1 FOUNDATION OF STUDY

The foundation of this research initiative was based on the importance of information to an organisation and therefore, the importance of protecting the related information assets. The prevalence and increase in data breaches, loss of business information, the current methods used to address the reduction of information security risk and the concept of reducing information security risk through non-technical means were key underpinnings of the value and importance of this study.

The rationale and purpose of the study were defined by the research question and sub-questions as well as the research objectives. The primary research question was: *What constitutes a framework that evaluates the information security assessment methods, the reduction of information security cost and the sustainability of information security culture?,* while the primary research objective was to: *Develop a framework and related tool that evaluates an organisation in regard to the way the organisation assesses information security, aligns to cost reducing information security products and services and sustains improved information security culture.*

Therefore, the key contributions of the study were the theoretical models related to information security risk assessment, information security cost and information security culture and the consolidated framework derived from these models in addition to the security evaluation tools implemented in line with the constructs of the framework.

8.2 UNDERSTANDING THE PROBLEM

In collecting and synthesising information related to the key constructs required to answer the research questions, the researcher conducted a critical evaluation on key topics related to the primary and secondary research questions and objectives. The key topics of review regarding information security as a concept were the importance of information security considering the proliferation and ubiquity of computing devices and the increases in data breaches and malicious threat actors. In terms of information security cost, traditional models and methods of costing information security and the limitation of these in managing information security in a new age of information security technology and threats were evaluated.

In terms of information security assessment, three topics were reviewed, namely the value, objectives and processes of assessing information security risk, implementing information security architecture and conducting traditional risk assessments in organisations. The literature reviewed showed that several individual methodologies and frameworks led to the assessment of information security risk, but no comprehensive framework considered information security cost and culture as part of its constructs. One of the key drivers in embarking on this study was the researcher own experience in leading information security teams, in that many best practices exist in the security field, but none assist in quantifying the direct relationship between evaluated risk and information security budgets.

Organisational culture and information security culture were evaluated through an overview of seminal organisational culture theory and the value, objectives and processes of information security culture in organisations. It was established that improving information security culture reduced overall information security risk and was the keystone for a sustained successful information security management programme. The researcher also observed through professional experience the impact of poorly managed information security culture and the relevance that people have in promoting, supporting and sustaining information security technology, controls and processes. Through reflection of interactions with participants it was apparent that improving information security culture is still a secondary concern to organisations in relation to technology implementation.

Lastly, an overview of motivation, positive reinforcement and reward as supporting drivers for the improvement of information security culture were also reviewed. The psychological traits and related actions supported the creation of the culture model described in Chapter 4 and substantiated Feature 3, which was a key part of the developed framework.

Based on this literature review, the basis for the key research contribution, the models and framework developed in Chapter 4, were established.

The literature evaluated effectively answered the sub-research objectives of:

- *SRO1: Determine and assess what frameworks and evaluation tools exist to assess information security in organisations.*

  To meet this objective, the researcher conducted literature reviews on the ISO 27002 risk framework, general risk management concepts, the FEAF, SABSA, COBIT for Security and Open Group Enterprise Architecture Frameworks.

- *SRO2: Evaluate frameworks and models that exist to manage information security costs.*

  To meet this objective, common information security cost models were evaluated. The process of cost evaluation was discussed and it was determined that none of the common models evaluates cost against known cost increasing or cost-reducing information security technologies and services.

- *SRO3: Assess models and evaluation tools that exist to improve information security culture.*

  To meet this objective, two information security culture frameworks were evaluated to understand how information security culture improvement could be quantified in an organisation and to understand the components that influence information security culture.

Therefore, the literature reviewed highlighted the key concepts in current frameworks, methodologies and models that supported the development of new models and the security framework described in Chapter 4.

8.3 SECURITY MODELS, FRAMEWORK AND EVALUATION TOOL

Three underpinning models related to information security risk assessment, information security cost and information security culture were developed based on the literature surveyed in Chapter 2. The researcher attempted to build on evaluated models and frameworks in order to define a unique management level reporting framework that would give insight into the evaluated environment versus the focused need of information security spending.

The models, theories and frameworks discussed in Chapter 2 effectively answered the sub-research questions of:

- *SRQ1: What frameworks and evaluation tools exist to assess information security in organisations?*
- *SRQ2: What are the common factors that influence information security costs?*
- *SRQ3: What constitutes information security culture and how can this be improved?*

The models developed in Chapter 4 set the foundation for the security evaluation framework that was developed. The first model developed focused on defining information security cost-reducing and cost-increasing factors. The model describes how cost-reducing factors can be split into social (people influenced) factors and technical factors and how these are inextricably linked by human interaction and behaviour.

The second model described how common information security assessment methods lead to selecting information security tools, technology and services but remain rooted in the need for human intervention through the implementation, management, support and administration of these.

The third model focused on five pillars that will help improve information security culture in an organisation.

Components of each of these models defined the security framework, which evaluates information security methods, information security cost and information security culture. The framework consisted of three feature areas, twenty-one evaluation areas and eighty-three questions related to the evaluation areas. The framework developed effectively answered the primary research question of:

> *What constitutes a framework and an associated tool that evaluates an organisation regarding how the organisation assesses information security, aligns cost-reducing of information security products and services and sustains improved information security culture?*

The framework was complemented by an evaluation tool. The evaluation in line with the developed framework effectively met the primary study objective of:

> *Develop a framework and related tool that evaluates an organisation regarding how the organisation assesses information security, aligns cost-reducing of information security products and services and sustains improved information security culture.*

The development and expansion of the three models, the security framework and associated tool, are the main knowledge contributions within this study. The framework allows organisations to conduct an alternative assessment to determine the organisation’s information security position. This is valuable to any organisation regardless of its size or complexity. As the framework is modular, it also allows for an organisation to extend specific focus on areas that are deemed more valuable to that organisation. Furthermore, the framework was developed with expansion and changes in the security landscape in mind. The agile nature of the framework also allows for further research and development. Additionally, this framework focuses on the one feature of information security that is not prevalently addressed in an organisation and that is information security culture. The improvement of information security culture provides tremendous long-term benefits. As was described in this study and is commonly espoused in media, human error is the most significant driver of security breaches within an organisation. The enhancement of information security culture, therefore, is key to providing longer-term protection for organisations.

The addition of a tool to apply the framework is also a significant contribution. One of the major concerns in the information security discipline in organisations today is the lack of human resource capability to conduct assessments and describe security deficiencies at a management level. Creating an application that allows an organisation to conduct an assessment internally without procuring services at a significant cost and being able to repeat this assessment will be of significant value. Through discussion with expert reviewers, the researcher established that the artefacts created as part of the research contribution in this study have value in the academic and business world.

8.4 ANALYSIS, RESULTS AND FINDINGS

In aligning to the use of the DSR methodology, the artefacts created needed to be evaluated. Therefore, expert reviewers were selected and a process of interrogation and evaluation regarding the value, completeness, impact and ease of use of the framework and tool was conducted.

Overall, the expert reviewers concurred that the framework exhibited a well-organised and comprehensible structure. A prevailing consensus emerged that the framework held significant worth for their respective organisations, proving pertinent across diverse organisational types seeking to assess information security within their domains. The expert reviewers largely perceived the framework as comprehensive, encompassing the most pivotal facets of information security. However, the reviewers also highlighted some shortcomings. They observed that there could be improved clarification of the framework's context and positioning concerning management or employee levels. Additionally, the reviewers expressed a desire for more extensive insights into the interconnections between evaluation areas and a better grasp of the rationale behind the scoring logic.

The expert reviewers responded positively to the evaluation tool. The majority of participants expressed that the output reports were in sync with their perception of the information security landscape within their respective organisations. They found the tool user-friendly and believed it to be a suitable companion to the framework. The expert reviewers perceived the tool as coherent and anticipated its relevance for implementation in their own organisational contexts.

The expert reviews defined a few opportunities for improvement of the framework and tools, which was further expanded in Chapter 6.

The outputs of the expert review supported the value statements perceived by the researcher when setting out to develop the models, framework and tools. Expert reviewers were senior people in large and medium organisations with decades of experience in the information security field. The validation received through expert review, therefore, supported that the contribution of this study was of value.

8.5 SUMMARY AND PERSONAL REFLECTION

The purpose of this study was to conduct research in information security around the key topics of information security risk assessment, information security cost and information security culture. In his own experience, the researcher has found that building a comprehensive information security programme within an organisation requires a strong understanding of these concepts to provide proactive management. The outputs of analysis towards such a programme have traditionally been technology and service based. The researcher felt that the people within the organisation have a significant role to play and set out to establish and understand that role. In doing so, research was conducted in the key topic areas that culminated in developing the security evaluation framework and the security evaluation tool. The researcher has brought together the literature, his own experiences and the review of experts to define a comprehensive framework related to the key topics and considerations for future growth and expansion of the framework and tool.

In developing the initial models and framework, the researcher was focused on allowing organisations to expose the key gaps that are faced in understanding their information security environment, within the context of established evaluation methods, methods of attack and methods of protection. The concept behind the development of the evaluation tool was for organisations to be able to evaluate themselves without continuous 3rd party consultation. This development was the key academic contribution as envisaged and outlined in Chapter 1. The further academic value of creating the framework in a modular fashion and to modernise the evaluation tool was to be able to expand these artefacts as new research was conducted in regard to threat analysis, security technology improvement and information security cost evaluation. This also fit into the research paradigm of DSR, which called for iterative improvement of artefacts, as it was established in Chapter 1 that the artefacts produced could not be refined exhaustively within the context and timeline of the study.

In Chapter 6, the researcher has identified two immediate areas of expansion of the framework and tool, which is relevant to organisational risk. The researcher expects that future research will focus on expanding the framework horizontally, by adding in newer relevant features and vertically, by refining questions and evaluation areas, so that the framework can become an evolving tool for organisational information security evaluation. Future research may also be conducted in developing a stand-alone costing model that provides organisations information on current risk levels in relation to information security cost versus future risk levels in relation to cost, based on selectable risk reduction scenarios.

In conducting this study, the researcher found that his experiences around information security in multiple organisations were similar to those organisations he evaluated and that the issues faced by senior participants were common. The researcher’s experience of being able to understand, evaluate and translate some of those concerns into artefacts that were felt to be practicably usable, was satisfying and has led to greater intrigue into how the artefacts produced could be improved and refined to help organisations support their information security journeys better.

References

Akhtar, S., Sheorey, P.A. and Bhattacharya, S., 2021. Cyber Security Solutions for Businesses in Financial Services: Challenges, Opportunities, and the Way Forward. *International Journal of Business Intelligence Research (IJBIR)*. 12(1), pp.82-97.

Almaiah, M.A., Al-Zahrani, A., Almomani, O. and Alhwaitat, A.K.. 2021. Classification of cyber security threats on mobile devices and applications. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications*. (pp. 107-123). Springer, Cham.

Alshahrani, H.M., Alotaibi, S.S., Ansari, M.T.J., Asiri, M.M., Agrawal, A., Khan, R.A., Mohsen, H. and Hilal, A.M., 2022. Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach. *Applied Sciences*. 12(12), p.5911.

Alwadain, A., Fielt, E., Korthaus, A. and Rosemann, M. 2011. Where do we find services in enterprise architectures? A comparative approach. In: *22nd Australasian Conference on Information Systems (ASIC) 2011 Proceedings*.

Anderson, J.M. 2003. Why we need a new definition of information security. *Computers and Security*. 22(4):308–313. doi.org/10.1016/S0167-4048(03)00407-3.

Arcuri, M.C., Brogi, M. and Gandolfi, G., 2018. The effect of cyber-attacks on stock returns. *Corporate Ownership & Control*. 15(2), pp.70-83.

Arnold, J., Randall, R., Patterson, F., Silvester, J., Robertson, I., Cooper, C., Burnes, B., Swailes, S., Harris, D., Axtell, C. and Den Hartog, D., 2010. Work psychology: Understanding human behaviour in the workplace. 5th ed. *Financial Times Prentice Hall*. Hoboken, New Jersey.

Asen A., Bohmayr W., Deutsche, S., Gonzalez M. 2019. Are You Spending Enough on Cybersecurity? Available from: https://www.bcg.com/publications/2019/are-you-spending-enough-cybersecurity.aspx [Accessed 26 March 2019].

Bahit, H. and Regragui, B. 2013. Risk Management for ISO27005 Descision Support. *International Journal of Innovative Research in Science, Engineering and Technology*. 2(3):530-538. Available from: https://www.rroij.com/open-access/risk-management-for-iso-27005-decision-support-.php?aid=44887 [Accessed 20 September 2022].

Bartol, K.M., Durham, C. 2000. Incentives: Theory and practice. In: *Industrial and Organizational Psychology: Linking Theory with Practice*. 2000, July 13:1–33.

Baskerville, R. 2008. What design science is not. *European Journal of Information Systems*. 17(5):441–443. doi.org/10.1057/ejis.2008.45.

Beaver, K. 2016. Best practices for an information security assessment. Available from: *https://searchsecurity.techtarget.com/tip/Best-practices-for-an-information-security-assessment [Accessed 10 October 2019].*

Becher, M., Freiling, F.C., Hoffmann, J., Holz, T., Uellenbeck, S. and Wolf, C. 2011. Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. In: *Proceedings - IEEE Symposium on Security and Privacy*. pp 96–111. doi.org/10.1109/SP.2011.29.

Berti, J. and Rogers, M. 2004. Social Engineering: The Forgotten Risk. In: *Information Security Management Handbook*. 5th ed. Boca Raton: Auerbach Publications. Florida.

Bey, Z.T. and Agyeman, M.O.. 2022. An Analysis of Cybersecurity Data Breach in The State of California. *Advanced Sciences and Technologies for Security Applications*. Presented at International Conference on Global Security, Safety and Sustainability (ICGS3) 2022.

Bluedorn, A.C. and Evered, R. 1980. Middle Range Theory and the Strategies of Theory Construction. In: *Middle Range Theory and the Study of Organizations*. Springer, Dordrecht. pp19–32. doi.org/10.1007/978-94-009-8733-3_2.

Bodin, L.D., Gordon, L.A. and Loeb, M.P. 2005. Evaluating information security investments using the Analytic hierarchy process. *Communications of the ACM*. 48(2):78–83. doi.org/10.1145/1042091.1042094.

Bojanc, R., Jerman-Blažič, B. and Tekavčič, M. 2012. Managing the investment in information security technology by use of a quantitative modeling. *Information Processing and Management*. 48(6):1031–1052. doi.org/10.1016/j.ipm.2012.01.001.

Botha, R.A., Furnell, S.M. and Clarke, N.L. 2009. From desktop to mobile: Examining the security experience. *Computers and Security*. 28(3–4):130–137. doi.org/10.1016/j.cose.2008.11.001.

Boudreau, M-C, Ariyachandra, T., Gefen, D. and Straub, D.W. 2011. Validating IS Positivist Instrumentation. In: *The Handbook of Information Systems Research*. 15–26. doi.org/10.4018/978-1-59140-144-5.ch002.

Brecht, M. and Nowey, T. 2013. A closer look at information security costs. In: *The Economics of Information Security and Privacy*. Springer Berlin Heidelberg. pp 3–24. doi.org/10.1007/978-3-642-39498-0_1.

Brown, A. 1998. *Organisational Culture*. 2nd ed. Pitman Publishing.London

Burkett, J.S. 2012. Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal*. 21(1):47–54. doi.org/10.1080/19393555.2011.629341.

Catania, A.C. 2001. Positive psychology and positive reinforcement. *American Psychologist*. 56(1):86–87. doi.org/10.1037/0003-066x.56.1.86.

Cavusoglu, H., Cavusoglu, H., Son, J.Y. and Benbasat, I. 2015. Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources. *Information and Management*. 52(4):385–400. doi.org/10.1016/j.im.2014.12.004.

Cerasoli, C.P., Nicklin, J.M. and Ford, M.T. 2014. Intrinsic motivation and extrinsic incentives jointly predict performance: A 40-year meta-analysis. *Psychological Bulletin*. 140(4):980–1008. doi.org/10.1037/a0035661.

Chatman, J.A., Caldwell, D.F., O'Reilly, C.A. and Doerr, B. 2014. Parsing organizational culture: How the norm for adaptability influences the relationship between culture consensus and financial performance in high-technology firms. *Journal of Organizational Behavior*. 35(6):785–808. doi.org/10.1002/job.1928.

Chatterjee, C. and Sokol, D. 2019. Data Security, Data Breaches, and Compliance. In: *Cambridge Handbook on Compliance*. 1st ed. Cambridge University Press. 1–17..

Chess, B. and Arkin, B. 2011. Software security in practice. *IEEE Security and Privacy*. 9(2):89–92. doi.org/10.1109/MSP.2011.40.

Chingapi, A. and Steyn, A.A., 2022. SMEs in South Africa: The Era of Adopting Mobile Payment Solutions. *In Proceedings of Sixth International Congress on Information and Communication Technology.* Springer, Singapore. pp. 429-447.

Chong, J. 2018. *How Security Technology Improves Business Operations*. Available from: https://www.securitymagazine.com/articles/89706-how-security-technology-improves-business-operations [Accessed 7 October 2019].

Cremonini, M. and Martini, P. 2005. Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA). *4th Workshop on the Economics of Information Security (WEIS)*. Boston

Davies, G., Mison, A. and Eden, P., 2022. Addressing the Skills Shortage in Cybersecurity. *In International Conference on Cyber Warfare and Security.* Vol. 17, No. 1, pp. 544-551.

Davis, S. 1984. *Managing corporate culture*. Harper Collins Publishers. New York

Deal, T. and Kennedy, A. 1982. *Corporate cultures*. Addison Wesley. Boston

Debar, H. 2019. Cybersecurity: high costs for companies. *Available from: http://theconversation.com/cybersecurity-high-costs-for-companies-110807* [Accessed 7 October 2019].

Deci, E.L., Koestner, R. and Ryan, R.M. 2001. Extrinsic rewards and intrinsic motivation in education: Reconsidered once again. *Review of Educational Research*. 71(1):1–27. doi.org/10.3102/00346543071001001.

Delmont, S. and Mason, J. 1997. Qualitative Researching. *The British Journal of Sociology*. 48(4):709. doi.org/10.2307/591613.

Demeyer, S. 2011. Research methods in computer science. In: *IEEE International Conference on Software Maintenance, ICSM*. Carroll and Swatman. p 600. doi.org/10.1109/ICSM.2011.6080841.

Detert, J.R., Schroeder, R.G. and Mauriel, J.J. 2000. A framework for linking culture and improvement initiatives in organizations. *Academy of Management Review*. 25(4):850–863. doi.org/10.5465/AMR.2000.3707740.

Dhillon, G., Torkzadeh, G. and Chang, J. 2018. Strategic planning for IS security: Designing objectives. In: *International Conference on Design Science Research in Information Systems and Technology*. Springer, Cham. pp 285–299. doi.org/10.1007/978-3-319-91800-6_19.

Drechsler, A. and Hevner, A. 2016. A four-cycle model of IS design science research:

capturing the dynamic nature of IS artifact design. In: *Parsons, J., Tuunanen, T., Venable, J. R., Helfert, M., Donnellan, B., & Kenneally, J. (eds.) Breakthroughs and Emerging Insights from Ongoing Design Science Projects: Research-in-progress papers and poster presentations from the 11th International Conference on Design Science Research in Information Systems and Technology (DESRIST) 2016. St. John, Canada,* 23-25 May. pp. 1-8

Dronov, V.Y. and Dronova, G.A., 2022. Principles of information security management system. *Journal of Physics: Conference Series.* 2182(1).

Dusan, M. 2004. The Influence of National Culture on Organizational Subcultures and Leadership Styles in Serbian Enterprises: An Empirical Analysis. *Sociologija*. 45(4).

Edwards, B., Jacobs, J. and Forrest, S. 2019. Risky Business: Assessing Security with External Measurements. *arXiv preprint arXiv:1904.11052*. Available from: http://arxiv.org/abs/1904.11052 [Accessed 6 October 2019].

Eisenberger, R. and Aselage, J. 2009. Incremental effects of reward on experienced performance pressure: Positive outcomes for intrinsic interest and creativity. *Journal of Organizational Behavior*. 30(1):95–117. doi.org/10.1002/job.543.

Elloy, D. 2012. Effects of Ability Utilization, Job Influence and Organization Commitment on Employee Empowerment: An Empirical Study. *International Journal of Management*. 29(2):627.

Eloff, M.M. and Von Solms, S.H. 2000. Information security management: An approach to combine process certification and product evaluation. *Computers and Security*. 19(8):698–709. doi.org/10.1016/S0167-4048(00)08019-6.

Enck, W., Ongtang, M. and McDaniel, P. 2009. Understanding Android Security. *IEEE Security and Privacy*. 7(1):50–57. doi.org/10.1109/MSP.2009.26.

Erdogan, G., Nguyen, P.H., Seehusen, F., Stølen, K., Hofstad, J. and Aagedal, J.Ø. 2019. An Evaluation of a Test-Driven Security Risk Analysis Approach Based on Two Industrial Case Studies. In: *Exploring Security in Software Architecture and Design*. IGI Global - Ch. 4. 69–103. doi.org/10.4018/978-1-5225-6313-6.ch004.

Everett, C. 2011. A risky business: ISO 31000 and 27005 unwrapped. *Computer Fraud and Security*. 2011(2):5–7. doi.org/10.1016/S1361-3723(11)70015-X.

Fenz, S., Heurix, J., Neubauer, T and Pechstein, F. 2014. Current challenges in information security risk management. *Information Management and Computer Security*. 22(5):410–430. doi.org/10.1108/IMCS-07-2013-0053.

Fischhoff, B. 2002. Assessing and Communicating the Risks of Terrorism. In: *Colloquim on Science and Technology Policy*. 11(12).

Ford, A., Al-Nemrat, A., Ghorashi, S.A. and Davidson, J.. 2022. The impact of GDPR infringement fines on the market value of firms. *Information & Computer Security,* (ahead-of-print).

Furnham, A. and Gunter, B. 1993. Corporate culture: definition, diagnosis and change. *International Review of Organizational Psychology*. (8):233–261.

Garbers, Y. and Konradt, U. 2014. The effect of financial incentives on performance: A quantitative review of individual and team-based financial incentives. *Journal of Occupational and Organizational Psychology*. 87(1):102–137. doi.org/10.1111/joop.12039.

García-Morales, V.J., Jiménez-Barrionuevo, M.M. and Gutiérrez-Gutiérrez, L. 2012. Transformational leadership influence on organizational performance through organizational learning and innovation. *Journal of Business Research*. 65(7):1040–1050. doi.org/10.1016/j.jbusres.2011.03.005.

Garrett, C. 2004. Developing a Security-Awareness Culture –Improving Security Decision Making. SANS Institute. *Available from: https://gisf.ngo//wp-content/uploads/2014/09/0241-Garrett-2005-Security-awareness-culture.pdf* [Accessed 27 August 2019].

Ghadi, S.A., 2021. Overview and challenges of security schemes in mobile computing. *In multi-disciplinary inter-collegiate Online Student Research Convention Changing dynamics of Covid era: new normal in society and industry.* p. 473.

Gohari, P., Ahmadloo, A., Boroujeni, M.B. and Hosseinipour, S.J. 2013. the Relationship Between Rewards and Employee Performance. *Interdisciplinary Journal of Contemporary Research in Business*. 5(3):543–570.

Goodman, S. and Harris, A. 2010. The coming African tsunami of information insecurity. *Communications of the ACM.* 53(12):24–27. doi.org/10.1145/1859204.1859215.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. 2015. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*. 06(01):24–30. doi.org/10.4236/jis.2015.61003.

Gray, G.M. and Ropeik, D.P. 2002. Dealing with the dangers of fear: The role of risk communication. *Health Affairs*. 21(6):106–116. doi.org/10.1377/hlthaff.21.6.106.

Gregor, S. 2006. The nature of theory in Information Systems. *MIS Quarterly: Management Information Systems*. 30(3):611–642. doi.org/10.2307/25148742.

Gregor, S.. and Hevner, A.R. 2013. Positioning and presenting design science research for maximum impact. *MIS Quarterly: Management Information Systems*. 37(2):337–355. doi.org/10.25300/MISQ/2013/37.2.01.

Gregor, S. and Jones, D. 2007. The Anatomy Of A Design Theory. Journal of the Association for Information Systems. 8(5). Available from: https://aisel.aisnet.org/jais/vol8/iss5/19/ [Accessed 20 September 2022].

Gunter, S. 2017. Digitally secure transformation. *ITNOW*. 59(2):12–13. doi.org/10.1093/itnow/bwx036.

Gupta, M. and Sharman, R. 2008. *Social and human elements of information security: Emerging trends and countermeasures*. doi.org/10.4018/978-1-60566-036-3.

Hampden-Turner, C. 1990. *Corporate culture: from vicious to virtuous circles*. Hutchinson. London

Haqaf, H. and Koyuncu, M. 2018. Understanding key skills for information security managers. *International Journal of Information Management*. 43:165–172. doi.org/10.1016/j.ijinfomgt.2018.07.013.

Hendijani, R., Bischak, D.P., Arvai, J. and Dugar, S. 2016. Intrinsic motivation, external reward, and their effect on overall motivation and performance. *Human Performance*. 29(4):251–274. doi.org/10.1080/08959285.2016.1157595.

Herold, R. and Beaver, K. 2014. Security Rule Requirments Overview. In: *The Practical Guide to HIPAA Privacy and Security Compliance*. Oct 20(236-259) doi.org/10.1201/b17548.

Hevner, A.R. and Chatterjee, S. 2010. Design Research in Information Systems, Intergrated Series. In: *Design Research in information Systems, Intergrated Series in Information Systems*.22(1):9-22 doi.org/10.1007/978-1-4419-5653-8_2.

Hevner, A.R., March, S.T., Park, J. and Ram, S. 2004. Design science in information systems research. *MIS Quarterly: Management Information Systems*. 28(1):75–100.

Holicza, P. and Kadëna, E.. 2018. Smart and secure? Millennials on mobile devices. *Interdisciplinary Description of Complex Systems: INDECS*. *16*(3-A), pp.376-383.

Hofstede, G. 1994. The business of international business is culture. *International Business Review*. 3(1):1–14.

Hofstede, G. 2001. *Culture's consequences: Comparing values, behaviors, institutions and organizations across nations*. 2nd ed. SAGE Publications. California

House, R. J., Hanges, P. J., Javidian, M., Dorfman, P. W. and Gupta, V. 2004. Culture, leadership, and organizations: The globe study of 62 societies. *Sage Publications*. Thousand Oaks, CA.

Howard, J.L. 2008. The Use of Non-Monetary Motivators in Small Business. *The Entrepreneurial Executive*. 13:17-19.

Huang, C., Hu, Q. and Behara, R.S. 2008. An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics*. 114(2):793–804. doi.org/10.1016/j.ijpe.2008.04.002.

Huberman, M. and Miles, M. 1994. *The qualitative researcher's companion*. 2nd ed. Thousand Oaks: SAGE Publications. California

Hübner, R. and SchÏsser, J. 2010. Monetary reward increases attentional effort in the flanker task. *Psychonomic Bulletin and Review*. 17(6):821–826. doi.org/10.3758/PBR.17.6.821.

Innerhofer-Oberperfler, F. and Breu, R. 2006. Using an enterprise architecture for IT risk management. *Information Systems Security Association*. July:1–12.

Internet Crime Complaint Centre. Internet Crime Report. 2020. Federal Bureau of Investigations. *Available from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf*

Jeong, C.Y., Lee, S.Y.T. and Lim, J.H. 2019. Information security breaches and IT security investments: Impacts on competitors. *Information and Management*. 56(5):681–695. doi.org/10.1016/j.im.2018.11.003.

Ji, W.L. and Xia, A.B. 2007. Federal enterprise architecture framework. *Jisuanji Jicheng Zhizao Xitong/Computer Integrated Manufacturing Systems, CIMS*. 13(1):57–66. Available from: https://cio-wiki.org/wiki/Federal_Enterprise_Architecture_Framework_(FEA) [Accessed 10 October 2019].

Johnson, K.E. and Stake, R.E. 1996. The Art of Case Study Research. *The Modern Language Journal*. 80(4):556. doi.org/10.2307/329758.

Johnson, R.B. and Onwuegbuzie, A.J. 2004. Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*. 33(7):14–26. doi.org/10.3102/0013189X033007014.

Kanfer, R., Chen, G. and Pritchard, R. 2008. Chapter 1: The three C's of work motivation: Content, context, and change. *Work motivation: Past, present and future*. Routledge.London

Kaspersky Lab. 2015. Cyber Security For Business – Counting the Costs, Finding the Value. *Available from : https://media.kaspersky.com/en/business-security/cybersecurity-for-business-counting-the-costs-finding-the-value.pdf*

Kaspersky Lab. 2016. Damage Control: The Cost of Security Breaches, IT Security Risks Special Report Series. *Available from: https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf*

Khalil, O.E.M. 2011. E-Government readiness: Does national culture matter? G*overnment Information Quarterly*. 28(3):388–399. doi.org/10.1016/j.giq.2010.06.011.

Kim, S., Mclean, G.N. 2014. The Impact of National Culture on Informal Learning in the Workplace. *Adult Education Quarterly*. 64(1), pp. 39-59.

Kim, N.Y., Robles, R.J., Cho, S.E., Lee, Y.S. and Kim, T.H. 2008. SOX act and IT security governance. In: *Proceedings - 2008 International Symposium on Ubiquitous Multimedia Computing, UMC 2008*. 218–221. doi.org/10.1109/UMC.2008.51.

Kosutic, D. 2017. ISO 27001 checklist: 16 steps for the implementation. *Available from:https://advisera.com/27001academy/knowledgebase/iso-27001-implementation-checklist/ [Accessed 11 September 2019].*

Kreuter, M.W. and Strecher, V.J. 1995. Changing Inaccurate Perceptions of Health Risk: Results From a Randomized Trial. *Health Psychology*. 14(1):56–63. doi.org/10.1037/0278-6133.14.1.56.

Kuhn, T. 1970. The structure of scientific revolutions. (Vol 111). *University of Chicago Press*. Chicago

Kuusisto, R. and Kuusisto, T. 2008. Information security culture as a social system: Some notes of information availability and sharing. In: *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. 77–97. doi.org/10.4018/978-1-60566-036-3.ch006.

Kwok, J., Hall, D., Paradice, D., and Courtney, J.F. 2003. Building a Theoretical Foundation for a Learning-Oriented Knowledge Management System. *Journal of Information technology Theory and Application (JITTA)*. 5(2):7

Lacohee, H., Phippen, A.D. and Furnell, S.M. 2006. Risk and restitution: Assessing how users establish online trust. *Computers and Security*. 25(7):486–493. doi.org/10.1016/j.cose.2006.09.001.

Lakatos, I. 1976. Falsification and the Methodology of Scientific Research Programmes. In: *Can Theories be Refuted?* Dordrecht: Springer Netherlands. pp 205–259. doi.org/10.1007/978-94-010-1863-0_14.

Latif, B., Mahmood, Z., Tze San, O., Mohd Said, R. and Bakhsh, A.. 2020. Coercive, normative and mimetic pressures as drivers of environmental management accounting adoption. *Sustainability*. 12(11), p.1-14.

La Polla, M., Martinelli, F. and Sgandurra, D. 2013. A survey on security for mobile devices. *IEEE Communications Surveys and Tutorials*. 15(1):446–471. doi.org/10.1109/SURV.2012.013012.00028.

Lepofsky, R. 2014. COBIT® 5 for Information Security. In: *The Manager's Guide to Web Application Security*. Chapter 8:133–145. doi.org/10.1007/978-1-4842-0148-0_10.

Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M. and Combs, B. 1978. Judged frequency of lethal events. *Journal of Experimental Psychology: Human Learning and Memory*. 4(6):551–578. doi.org/10.1037/0278-7393.4.6.551.

Linz, S.J. and Semykina, A. 2012. What Makes Workers Happy? Anticipated Rewards and Job Satisfaction. *Industrial Relations*. 51(4):811–844. doi.org/10.1111/j.1468-232X.2012.00702.x.

Lion, R. and Meertens, R.M. 2005. Security or opportunity: The influence of risk-taking tendency on risk information preference. *Journal of Risk Research*. 8(4):283–294. doi.org/10.1080/1366987042000192435.

Liu, Y. 2010. Reward Strategy in Chinese IT Industry. *International Journal of Business and Management*. 5(2):119. doi.org/10.5539/ijbm.v5n2p119.

Lord, N. 2017. *The History of Data Breaches*. Available from: https://digitalguardian.com/blog/history-data-breaches [Accessed 7 October 2019].

Lowry, P.B. and Moody, G.D. 2015. Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*. 25(5):433–463. doi.org/10.1111/isj.12043.

Malik, M.A.R, Butt, A.N. and Choi, J.N. 2015. Rewards and employee creative performance: Moderating effects of creative self-efficacy, reward importance, and locus of control. *Journal of Organizational Behavior*. 36(1):59–74. doi.org/10.1002/job.1943.

March, S.T. and Smith, G.F. 1995. Design and natural science research on information technology. *Decision Support Systems*. 15(4):251–266. doi.org/10.1016/0167-9236(94)00041-2.

Marquardt, M., Berger, N. and Loan, P. 2004. HRD in the Age of Globalization. N.Y. Basic Books.

Martin, J. and Siehl, C. 1983. Organizational culture and counterculture: An uneasy symbiosis. *Organizational Dynamics*. 12(2):52–64. doi.org/10.1016/0090-2616(83)90033-5.

Martin, K.D., Borah, A. and Palmatier, R.W. 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing*. 81(1):36–58. doi.org/10.1509/jm.15.0497.

Martins, E. and Martins, N. 2002. An organisational culture model to promote creativity and innovation. *SA Journal of Industrial Psychology*. 28(4). doi.org/10.4102/sajip.v28i4.71.

Masutha, M. and Rogerson, C.M. 2014. Small enterprise development in South Africa: The role of business incubators. *Bulletin of Geography*. 26(26):141–155. doi.org/10.2478/bog-2014-0050.

Mayer, N., Aubert, J., Grandry, E., Feltus, C., Goettelmann, E. and Wieringa, R. 2019. An integrated conceptual model for information system security risk management supported by enterprise architecture management. *Software and Systems Modeling*. 18(3):2285–2312. doi.org/10.1007/s10270-018-0661-x.

McIlwraith, A. 2016. *Information Security and Employee Behaviour*. Routledge. London doi.org/10.4324/9781315588537.

Mehmood, A., Natgunanathan, I., Xiang, Y., Hua, G. and Guo, S. 2016. Protection of big data privacy. *IEEE Access*. 4:1821–1834. doi.org/10.1109/ACCESS.2016.2558446.

Mercuri, R.T. 2003. Analyzing security costs. *Communications of the ACM*. 46(6):15–18. doi.org/10.1145/777313.777327.

Mithas, S. and Rust, R.T. 2016. How information technology strategy and investments influence firm performance: Conjecture and empirical evidence. *MIS Quarterly: Management Information Systems*. 40(1):223–245. doi.org/10.25300/MISQ/2016/40.1.10.

Mitnick, K.D. and Simon, W.L. 2003. The Art of Deception: Controlling the Human Element in Security. *John Wiley and Sons*. doi.org/0471237124.

Morgan, D. L. 1988. Focus Groups as Qualitative Research. *Sage Publications*. Newbury Park, CA.

Mukherjee, S. 2019. Overview of the Importance of Corporate Security in Business. *SSRN Electronic Journal*. July:1-16. doi.org/10.2139/ssrn.3415960.

Myers, M.D. 1997. Qualitative research in information systems. *MIS Quarterly*. 21(2):241–242.

Nachmias, D. and Nachmias, C. 1976. Research methods in the social sciences. Worth Publishers. New York

Nazarian, A., Irani, Z. and Ali, M. 2013. The Relationship between National Culture and Organisational Culture: The Case of Iranian Private Sector Organisations. *Journal* *of Economics, Business and Management*. pp 11–15. doi.org/10.7763/joebm.2013.v1.3.

Netshakhuma, N.S. 2019. Assessment of a South Africa national consultative workshop on the Protection of Personal Information Act (POPIA). *Global Knowledge, Memory and Communication*. (July, 25). doi.org/10.1108/gkmc-02-2019-0026.

Nilsen, P. 2015. Making sense of implementation theories, models and frameworks. *Implementation Science*. 10(1):1–13. doi.org/10.1186/s13012-015-0242-0.

O’Neill, P. 2004. Developing A Risk Communication Model to Encourage Community Safety from Natural Hazards. New South Wales. State Emergency Management. Australia

Offermann, P., Levina, O., Schönherr, M. and Bub, U. 2009. Outline of a design science research process. *In Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*. (pp. 1-11).

Oliver, G., 2011. Organisational Culture for Information Managers. *Chandos Publishing.* Cambridge, UK.

Oltsik, J. 2019. *The cybersecurity skills shortage is getting worse*. Available from: https://www.csoonline.com/article/3331983/the-cybersecurity-skills-shortage-is-getting-worse.html [Accessed 28 March 2019].

Orlikowski, W.J. and Iacono, C.S. 2001. Research Commentary: Desperately Seeking the “IT” in IT Research - A Call to Theorizing the IT Artifact. *Information Systems Research*. 12(2):121–134. doi.org/10.1287/isre.12.2.121.9700.

Othman, N.A.A., Norman, A.A. and Kiah, M.L.M. 2021. Information System Audit for Mobile Device Security Assessment. *In 2021 3rd International Cyber Resilience Conference (CRC).* (pp. 1-6). IEEE.

Parsons, K., Mccormac, A., Butavicius, M. and Ferguson, L. 2010. Human Factors and Information Security : Individual Culture and Security Environment. *Science And Technology*. (DSTO-TR-2484):45. doi.org/10.14722/ndss.2014.23268.

Patton, M.Q. 2002. *Qualitative research and evaluation methods*. 3rd ed. SAGE Publications. California.

Peffers, K., Tuunanen, T., Rothenberger, M.A. and Chatterjee, S. 2007. A design science research methodology for information systems research. *Journal of Management Information Systems*. 24(3):45–77. doi.org/10.2753/MIS0742-1222240302.

Peltier, T.R. and Peltier, J. 2016. Complete Guide to CISM Certification. *Auerbach Publications*. Florida doi.org/10.1201/9781420013252.

Peretz, H. and Fried, Y. 2012. National cultures, performance appraisal practices, and organizational absenteeism and turnover: A study across 21 countries. *Journal of Applied Psychology*. 97(2):448–459. doi.org/10.1037/a0026011.

Ponemon Institute. 2020. *Cost of Data Breach Study*. Available at : https://www.ibm.com/downloads/cas/AEJYBPWA#:~:text=In%20this%20year's%20study%2C%20the,477%20companies%20is%20USD5%2C703.

Prislan, K. and Bernik, I. 2010. Risk management with ISO 27000 standards in information security. *Inf. Secur*. December:58-63.

Pulkkinen, M., Naumenko, A. and Luostarinen, K. 2007. Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool. *Journal of Systems and Software*. 80(10):1607–1620. doi.org/10.1016/j.jss.2007.01.044.

Rotvold, G. How to create a security culture in your organization: a recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs. *Information Management Journal*. 42(6):32-38.

Ruighaver, A.B., Maynard, S.B. and Chang, S. 2007. Organisational security culture: Extending the end-user perspective. *Computers and Security*. 26(1):56–62. doi.org/10.1016/j.cose.2006.10.008.

SABSA Institute. 2018. *SABSA Executive Summary - The SABSA Institute*. Available from: https://sabsa.org/sabsa-executive-summary/ [Accessed 10 October 2019].

Safa, N.S., Maple, C., Watson, T. and Von Solms, R. 2018. Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security and Applications*. 40:247–257. doi.org/10.1016/j.jisa.2017.11.001.

Sarwar, A. and Khalid, A. 2011. Impact of Employee Empowerment on Employee’s

Job Satisfaction and Commitment with the Organization. *Interdiscliplinary Journal of Contemporary Research in Business*. 3(2):664–684. doi.org/10.1108/17506141111163390.

Saunders, A. and Brynjolfsson, E. 2016. Valuing information technology related intangible assets. *MIS Quarterly: Management Information Systems*. 40(1):83–110. doi.org/10.25300/MISQ/2016/40.1.04.

Schatz, D. and Bashroush, R. 2017. Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers*. 19(5):1205–1228. doi.org/10.1007/s10796-016-9648-8.

Schein, E.H. 2009. *The Corporate Culture Survival Guide*. John Wiley and Sons. New Jersey.

Schinagl, S. and Shahim, A. 2020. What do we know about information security governance?"From the basement to the boardroom": towards digital security governance. *Information & Computer Security.* 28(2):261-292. doi.org/10.1108/ICS-02-2019-0033.

Schmid, M. and Pape, S. 2019. A structured comparison of the corporate information security maturity level. In: *IFIP Advances in Information and Communication Technology*. V. 562. Springer New York LLC. 223–237. doi.org/10.1007/978-3-030-22312-0_16.

Schmittling, R. 2010. Performing a Security Risk Assessment. *ISACA Journal.* 2010,1:18 Available from: https://www.isaca.org/Journal/archives/2010/Volume-1/Pages/Performing-a-Security-Risk-Assessment1.aspx [Accessed 10 October 2019].

Scholtz, T. 2011. Articulating the business value of information security. *Technical Report.* Gartner Inc.

Schuster, J., Weatherhead, P. and Zingheim P. 2006. Pay for Performance Works: The United States Postal Service Presents a Powerful Business Case. *The Journal of Total Rewards.* 15(1):24–31.

Sherwood, J., Clark, A. and Lynas, D. 2004. Enterprise Security Architecture-SABSA. *Information Systems*. 6(4):1–27.

Shiraz, N, Rashid, M. and Riaz, A. 2011. The impact of reward and recognition programs on employee's motivation and satisfaction. *Journal of Contemporary*

Research in Business. 3(3):1428–1434.

Siponen, M. 2001. Five dimensions of information security awareness. *SIGCAS Computers and Society*. 31(2):24–29.

Siponen, M. 2002. Towards maturity of information security maturity criteria: Six lessons learned from software maturity criteria. *Information Management and Computer Security*. 10(5):210–224. doi.org/10.1108/09685220210446560.

Sonawane, P. 2008. Non-monetary Rewards: Employee Choices and Organizational Practices. *International Journal of Industrial Relations*. 44(2):256–271. doi.org/10.2307/27768195.

Soomro, Z.A., Shah, M..H and Ahmed, J. 2016. Information security management needs more holistic approach: A literature review. *International Journal of Information Management*. 36(2):215–225. doi.org/10.1016/j.ijinfomgt.2015.11.009.

Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G. and Thomas, C.B. 2018. *MITRE ATT&CK - Design and Philosophy*. Available from: https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf [Accessed 7 September 2020].

Subashini, S. and Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*. 34(1):1–11. doi.org/10.1016/j.jnca.2010.07.006.

Takemura, T. and Komatsu, A. 2013. An empirical study on information security behaviors and awareness. In: *The Economics of Information Security and Privacy*. Springer Berlin Heidelberg. 95–114. doi.org/10.1007/978-3-642-39498-0_5.

Tanimoto, S., Nagai, K., Hata, K., Hatashima, T., Sakamoto, Y. and Kanai, A. 2017. A Concept Proposal on Modeling of Security Fatigue Level. In: *2017 5th Intl Conf on Applied Computing and Information Technology/4th Intl Conf on Computational Science/Intelligence and Applied Informatics/2nd Intl Conf on Big Data, Cloud Computing, Data Science (ACIT-CSII-BCD).* pp 29-34

Targett, E. 2018. *Global Data Breaches 2018: 4.5 Billion Records Compromised Thus Far*. Available from: https://www.cbronline.com/news/global-data-breaches-2018 [Accessed 7 October 2019].

Tashi, I. 2009. Regulatory compliance and information security assurance. In:

Proceedings - International Conference on Availability, Reliability and Security, ARES 2009. 670–674. doi.org/10.1109/ARES.2009.29.

Thomson, KL, von Solms, R and Louw, L. 2006. Cultivating an organizational information security culture. *Computer Fraud and Security*. 2006(10):7–11. doi.org/10.1016/S1361-3723(06)70430-4.

Tiller, J.S. 2010. Adaptive Security Management Architecture. *Auerbach Publications*. Florida doi.org/10.1201/b10325.

Torra, V. 2017. Data Privacy: Foundations, New Developments and the Big Data Challenge. *Springer International Publishing.* Volume 28 doi.org/10.1007/978-3-319-57358-8.

Tremblay, M.C., Hevner, A.R. and Berndt, D.J., 2010. The use of focus groups in design science research. *In Design Research in Information Systems, Integrated Series on Informations Systems.* 22. pp.121-143.

Tsai, Y. 2011. Relationship between organizational culture, leadership behavior and job satisfaction. *BMC Health Services Research*. 11(1):98. doi.org/10.1186/1472-6963-11-98.

Tsatsenko, N. 2020. SME Development, economic growth and structural change: evidence from Ghana and South Africa. J*ournal of Agriculture and Environment*. 2(14). doi.org/10.23649/JAE.2020.2.14.7.

Tsiakis, T. and Stephanides, G. 2005. The economic approach of information security. *Computers and Security*. 24(2):105–108. doi.org/10.1016/j.cose.2005.02.001.

Twati, J. 2006. The influence of societal culture on the adoption of information systems: The case of Libya. In: *Internet and Information Systems in the Digital Age Challenges and Solutions - Proceedings of the 7th International Business Information Management Association Conference, IBIMA 2006*. 8(1):588–598.

US Office of Management and Budget. 2013. *Federal Enterprise Architecture Framework v2*. Available from: https://obamawhitehouse.archives.gov/omb/e-gov/FEA. [Accessed 19 May 2019]

Utzerath, J. and Dennis, R., 2021. Numbers and statistics: data and cyber breaches under the General Data Protection Regulation. *International Cybersecurity Law Review*. *2*(2), pp.339-348.

Vaishnavi, V., Kuechler, W. and Petter, S. 2004. Design Science Research in Information Systems. Available from http://www.desrist.org/design-research-in-information-systems/ [Accessed 17 December 2020]

Vaishnavi, V. and Kuechler, W. 2012. A framework for theory development in design science research: multiple perspectives. *Journal of the Association for Information Systems.* 13(6),395-423.

Van Aken, J.E. 2004. Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules. *Journal of Management Studies*. 41(2):219–246. doi.org/10.1111/j.1467-6486.2004.00430.x.

Van Muijen, J.J. and Koopman, P.L. 1994. The influence of national culture on organizational culture: A comparative study between 10 countries. *European Work and Organizational Psychologist*. 4(4):367–380. doi.org/10.1080/13594329408410496.

Van Niekerk, J.F. and Von Solms, R. 2010. Information security culture: A management perspective. *Computers and Security*. 29(4):476–486. doi.org/10.1016/j.cose.2009.10.005.

Van Slyke, C., Clary, G., Ellis, S. and Maasberg, M. 2019. Employer preferences for cybersecurity skills among information systems graduates. In: *SIGMIS-CPR 2019 - Proceedings of the 2019 Computers and People Research Conference*. Association for Computing Machinery, Inc. pp 131–134. doi.org/10.1145/3322385.3322418.

Venable, J.R. 2013. Rethinking design theory in information systems. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. LNCS. Springer, Berlin, Heidelberg. pp.136–149. doi.org/10.1007/978-3-642-38827-9_10.

Venable, J. and Baskerville, R., 2012. Eating our own cooking: Toward a more rigorous design science of research methods. *Electronic Journal of Business Research Methods*. 10(2), pp.141-153.

Venable, J., Pries-Heje, J. and Baskerville, R.. 2016. FEDS: a framework for evaluation in design science research. *European journal of information systems*. *25*(1), pp.77-89.

Verizon. 2017. *2017 Data Breach Investigation Report, 10th Edition*. Available from:

http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/. [Accessed 17 January 2019]

Wacker, J.G. 1998. A definition of theory: Research guidelines for different theory-building research methods in operations management. *Journal of Operations Management*. 16(4):361–385. doi.org/10.1016/s0272-6963(98)00019-9.

Wahe, S. and Petersen, G. 2011. Open Enterprise Security Architecture (O-ESA): A Framework and Template for Policy-driven Security. Available from: https://publications.opengroup.org/g112 [Accessed 8 May 2020].

Walsham, G. 1993. *Interpreting Information Systems in Organizations*. Wiley and Sons. Chichester doi.org/10.1177/017084069401500614.

Watkins, M. 2013. What is organizational culture? And why should we care? *Harvard Business Review*. 15(1):1-5.

Wei, L.T. and Yazdanifard, R. 2014. The impact of Positive Reinforcement on Employees' Performance in Organizations. *American Journal of Industrial and Business Management*. 4(1):9–12. doi.org/10.4236/ajibm.2014.41002.

Wei, Y., Samiee, S. and Lee, R.P. 2014. The influence of organic organizational cultures, market responsiveness, and product strategy on firm performance in an emerging market. *Journal of the Academy of Marketing Science*. 42(1):49–70. doi.org/10.1007/s11747-013-0337-6.

Wilczek, M. 2019. *Cybercrime is increasing and more costly for organizations*. Available from: https://www.cio.com/article/3386417/cybercrime-is-increasing-and-more-costly-for-organizations.html [Accessed 7 October 2019].

Winder, D. 2019. *Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019*. Available from: https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#7fe19849bd54 [Accessed 7 October 2019].

Wu, S.M., Guo, D., Wu, Y.J. and Wu, Y.C. 2018. Future development of Taiwan's smart cities from an information security perspective. *Sustainability*. 10(12):4520. doi.org/10.3390/su10124520.

Wylder, J. 2003. Strategic Information Security. *Auerbach Publications*. Florida doi.org/10.1201/9780203497081.

Yasar, A.U.H, Preuveneers, D., Berbers, Y. and Bhatti, G. 2008. Best practices for software security: An overview. In: *IEEE INMIC 2008: 12th IEEE International Multitopic Conference - Conference Proceedings*. pp 169–173. doi.org/10.1109/INMIC.2008.4777730.

Yildirim, E. 2016. The importance of information security awareness for the success of business enterprises. In: *Advances in Intelligent Systems and Computing*. Springer Verlag. 501(1):211–222. doi.org/10.1007/978-3-319-41932-9_17.

Yin, R. 2003. *Case Study Research: Design and Methods*. 3rd ed. SAGE Publications.

Florida

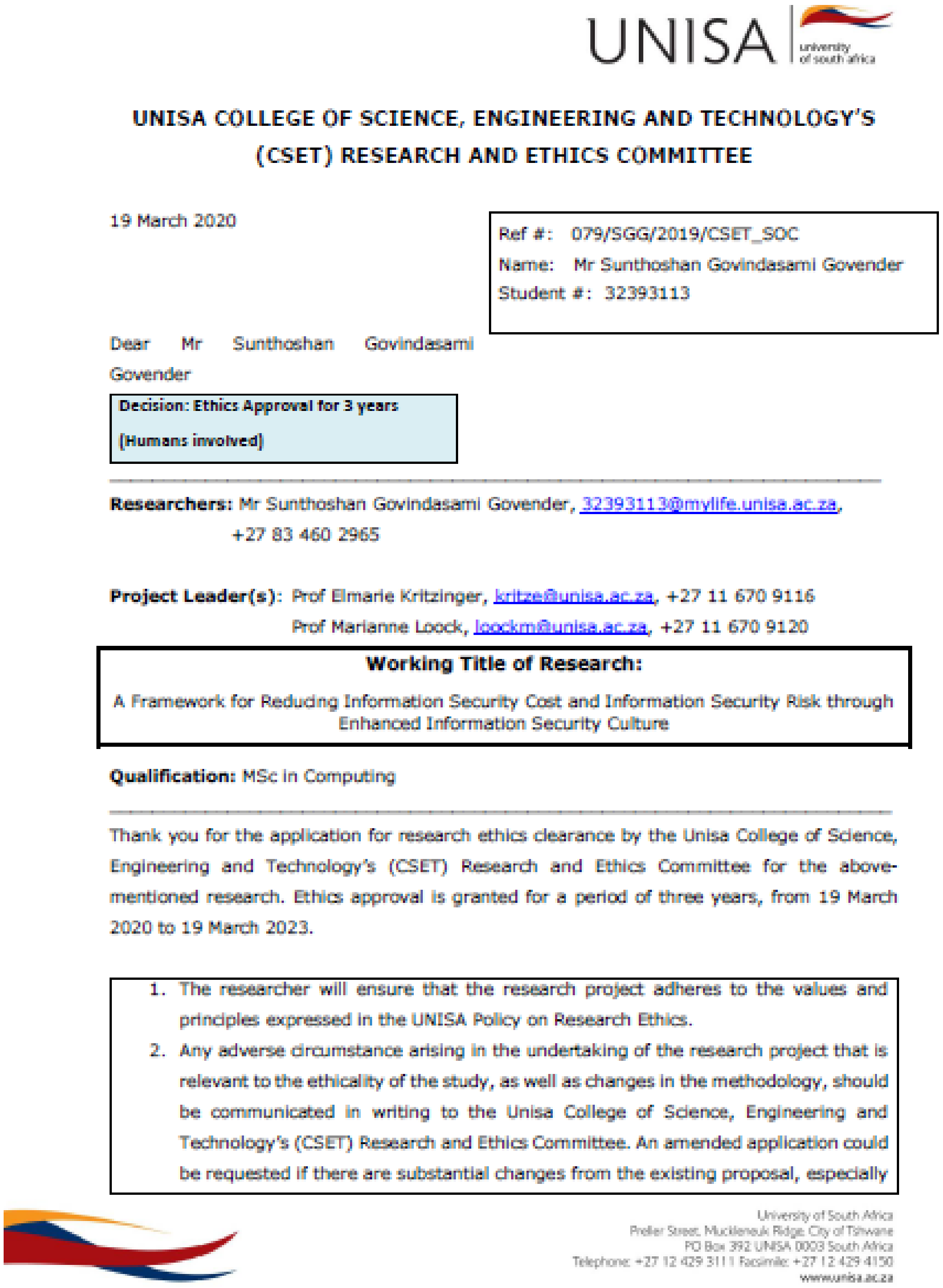
Zerlang, J. 2017. GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*. 2017(6):8–11. doi.org/10.1016/S1353-4858(17)30060-0.

Zissis, D. and Lekkas, D. 2012. Addressing cloud computing security issues. *Future Generation Computer Systems*. 28(3):583–592. doi.org/10.1016/j.future.2010.12.006.

Appendix

Appendix A

Ethical Clearance



UNISA university of south africa

UNISA COLLEGE OF SCIENCE, ENGINEERING AND TECHNOLOGY'S (CSET) RESEARCH AND ETHICS COMMITTEE

19 March 2020

Ref #: 079/SGG/2019/CSET_SOC
Name: Mr Sunthoshan Govindasami Govender
Student #: 32393113

Dear Mr Sunthoshan Govindasami Govender

Decision: Ethics Approval for 3 years
(Humans involved)

Researchers: Mr Sunthoshan Govindasami Govender, 32393113@mylife.unisa.ac.za, +27 83 460 2965

Project Leader(s): Prof Elmarie Kritzinger, kritze@unisa.ac.za, +27 11 670 9116
Prof Marianne Loock, loockm@unisa.ac.za, +27 11 670 9120

Working Title of Research:

A Framework for Reducing Information Security Cost and Information Security Risk through Enhanced Information Security Culture

Qualification: MSc in Computing

Thank you for the application for research ethics clearance by the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee for the above-mentioned research. Ethics approval is granted for a period of three years, from 19 March 2020 to 19 March 2023.

1. The researcher will ensure that the research project adheres to the values and principles expressed in the UNISA Policy on Research Ethics.
2. Any adverse circumstance arising in the undertaking of the research project that is relevant to the ethicality of the study, as well as changes in the methodology, should be communicated in writing to the Unisa College of Science, Engineering and Technology's (CSET) Research and Ethics Committee. An amended application could be requested if there are substantial changes from the existing proposal, especially

University of South Africa
Preller Street, Muckleneuk Ridge, City of Tshwane
PO Box 392 UNISA 0003 South Africa
Telephone: +27 12 429 3111 Facsimile: +27 12 429 4150
www.unisa.ac.za

Appendix B

Consent of Participants

Consent forms contain personal information. The signed consent forms can be submitted upon request if required.

Appendix C

Example of Participant Permission Letter

PERMISSION LETTER

Request for permission to conduct research at XXXXX

“An Information Security Framework for Reducing Information Security Costs and Sustaining Information Security Culture”

Date

Name
Address

Cellphone Number Email address

Dear Mr/Ms/Dr/Prof. xxxxxx,

I, ______________ am doing research with ____________, Professors in the College of Science, Engineering and Technology, towards a Ph.D. in Information Systems at the University of South Africa. We are inviting your organisation to participate in a study entitled “An Information Security Framework for Reducing Information Security Costs and Sustaining Information Security Culture”.

The aim of the study is to develop a framework and related tool that evaluates an organisation in regard to the way the organisation assesses information security, aligns to cost reducing information security products and services, and sustains improved information security culture.

Your company has been selected because the identified group for this study is limited to IT Departments in medium to large organisations where medium is defined as a company with up to five hundred employees and large is defined as companies with more than one thousand employees. Participants from these types of organisations on a senior and executive level working in Information Technology, will also be selected to act as expert reviewers in the evaluation phase of the Framework and Evaluation Tool developed. The expert reviewers must have at least 10 years of experience in the Information Security field as well.

The study will entail that the expert reviewer will be introduced to two artefacts developed. One is a Framework and the other is an Evaluation Tool based on the Framework. The details and function of the Framework and Evaluation Tool will be presented and explained to the participants by the researcher. The underlying concepts and models used to generate the Framework will be explained to the participants as well. The researcher will assist participants in using the tool to answer questions about the organisation and the researcher will then present the results to the participants. The interview for collecting data for this study will then be used to understand the validity, value and accuracy of the artefacts presented.

The benefits of this study are that the expert reviewers will be able to use a workable evaluation tool that will give them insight into the current information security state within their organisation. Specific information about their organisation will be presented back to them directly while anonymised information from other participants may be shared if requested (and allowed) to benchmark against.

The feedback procedure will entail that results of the Evaluation Tool are presented to the expert reviewers immediately after evaluation. Once information is collected from all expert reviewers, the information will be analysed and findings will be reported in a thesis that this study is the basis for. If you would like to be informed of the final research findings, please contact ____________ on _______________. The findings are accessible for six months after publication.

Yours sincerely

____

Appendix D

Example of Participant Information Sheet

PARTICIPANT INFORMATION SHEET

Ethics clearance reference number: 079/SGG/2019/CSET_SOC
Research permission reference number (if applicable):N/A

Date

Title: “An Information Security Framework for Reducing Information Security Costs and Sustaining Information Security Culture”

Dear Prospective Participant

I, __________ am doing research with ________________, Professors in the College of Science, Engineering and Technology, towards a Ph.D. in Information Systems at the University of South Africa. We are inviting you to participate in a study entitled “An Information Security Framework for Reducing Information Security Costs and Sustaining Information Security Culture” as an expert reviewer.

The aim of the study is to develop a framework and related tool that evaluates an organisation in regard to the way the organisation assesses information security, aligns to cost reducing information security products and services, and sustains improved information security culture

You have been invited to participate in this study because of your status of being on a senior or executive level working in Information Technology and because of your extensive experience in the Information Security Field.

Your contact details were obtained through our previous professional interactions. You along with approximately ten other prospective expert reviewers have been invited to participate in this study.

The nature of your participation in this study will be to act as an expert reviewer in the evaluation phase of a Framework and Evaluation Tool that has been developed as part of this study.

The study will entail that the expert reviewers will be introduced to two artefacts developed. One is a Framework and the other is an Evaluation Tool based on the Framework. The details and function of the Framework and Evaluation Tool will be presented and explained to the expert reviewers by the researcher. The underlying concepts and models used to generate the Framework will be explained to the expert reviewers as well. The researcher will assist expert reviewers in using the tool to answer questions about the organisation and the researcher will then present the results to the participants. A further interview for collecting data for this study will then be conducted to understand the validity, value and accuracy of the artefacts presented.

The interview will take approximately two hours and the audio of the interview will be recorded for validation purposes. All audio and information collected from you will be anonymised and stored in a secure storage location that is encrypted.

Your participation is wholly voluntary and there is no penalty or loss of benefit for non-participation. Participating in this study is voluntary and you are under no obligation to consent to participation.   If you do decide to take part, you will be given this information sheet to keep and be asked to sign a written consent form. You are free to withdraw at any time and without giving a reason.

The benefits of this study are that the expert reviewers will be able to use a workable evaluation tool that will give them insight into the current information security state within their organisation. Specific information about their organisation will be presented back to them directly while anonymised information from other participants may be shared if requested (and allowed) to benchmark against.

There should be no adverse effects to participating in the study. None of your personal information will be used in the study. Your only possible inconvenience may be the time that is spent participating in the study. The risk that may be foreseen in participating, may be that your personal information or that of your company is ex-filtrated from the secure storage. However all reasonable measures will be taken to make sure this does not occur, such as; not using internet based storage, using a high level encryption algorithm on the data saved, securing the storage device in a safe and anonymising all data collected.

All information you provide will be codified and you and your organisation will be referred to by pseudonyms. This will apply when information from this research is published in any way, including any publications, conference proceedings or further research.

Electronic information collected will be stored on a password protected computer, with an encrypted hard drive. Electronic copies of the interview will be stored on an external hard drive by the researcher for a minimum period of five years in a locked safe on the personal premises of the researcher for future research or academic purposes. Future use of the stored data will be subject to further Research Ethics Review and approval if applicable. No paper documentation will be kept of the interview. After the five-year period all information will be electronically shredded.

None of the participants in this study will receive any reward, payment or incentive for participating in this study.

This study has received written approval from the Research Ethics Review Committee of the School of Computing at UNISA. A copy of the approval letter can be obtained from the researcher if you so wish.

The feedback procedure will entail that results of the Evaluation Tool are presented to the participant immediately after evaluation. Once information is collected from all participants, the information will be analysed and findings will be reported in a thesis that this study is the basis for. If you would like to be informed of the final research findings, please contact ___________ on _______________. The findings are accessible for six months after publication.

Should you have concerns about the way in which the research has been conducted, you may contact _____________. Contact the research ethics chairperson of the Ethics Review Committee (ERC) ________________) if you have any ethical concerns.

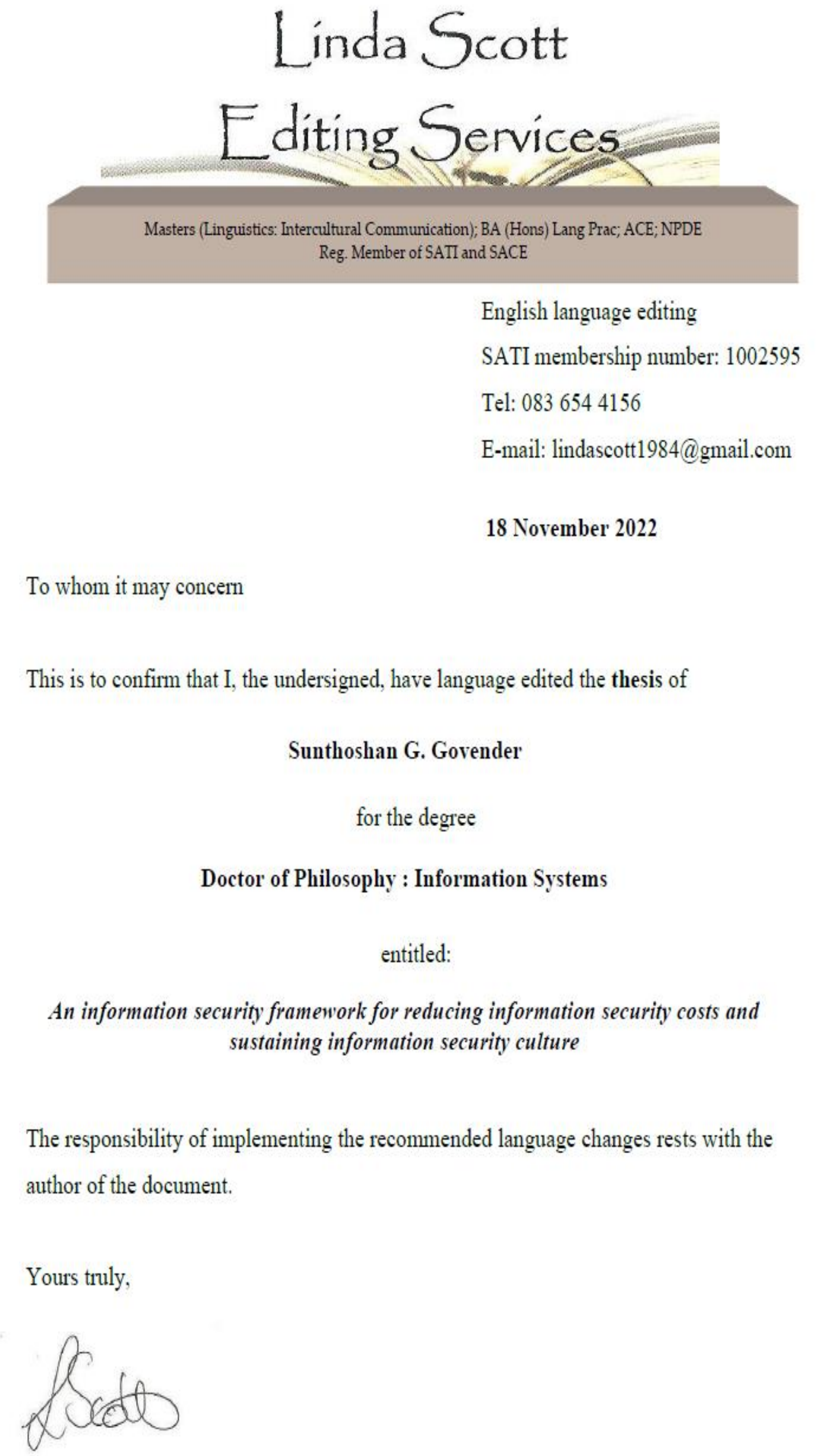
Thank you for taking time to read this information sheet and for participating in this study.

Thank you.

____

Appendix E

<u>Editing Certificate</u>



Linda Scott
Editing Services

Masters (Linguistics: Intercultural Communication); BA (Hons) Lang Prac; ACE; NPDE
Reg. Member of SATI and SACE

English language editing
SATI membership number: 1002595
Tel: 083 654 4156
E-mail: lindascott1984@gmail.com

18 November 2022

To whom it may concern

This is to confirm that I, the undersigned, have language edited the **thesis** of

Sunthoshan G. Govender

for the degree

Doctor of Philosophy : Information Systems

entitled:

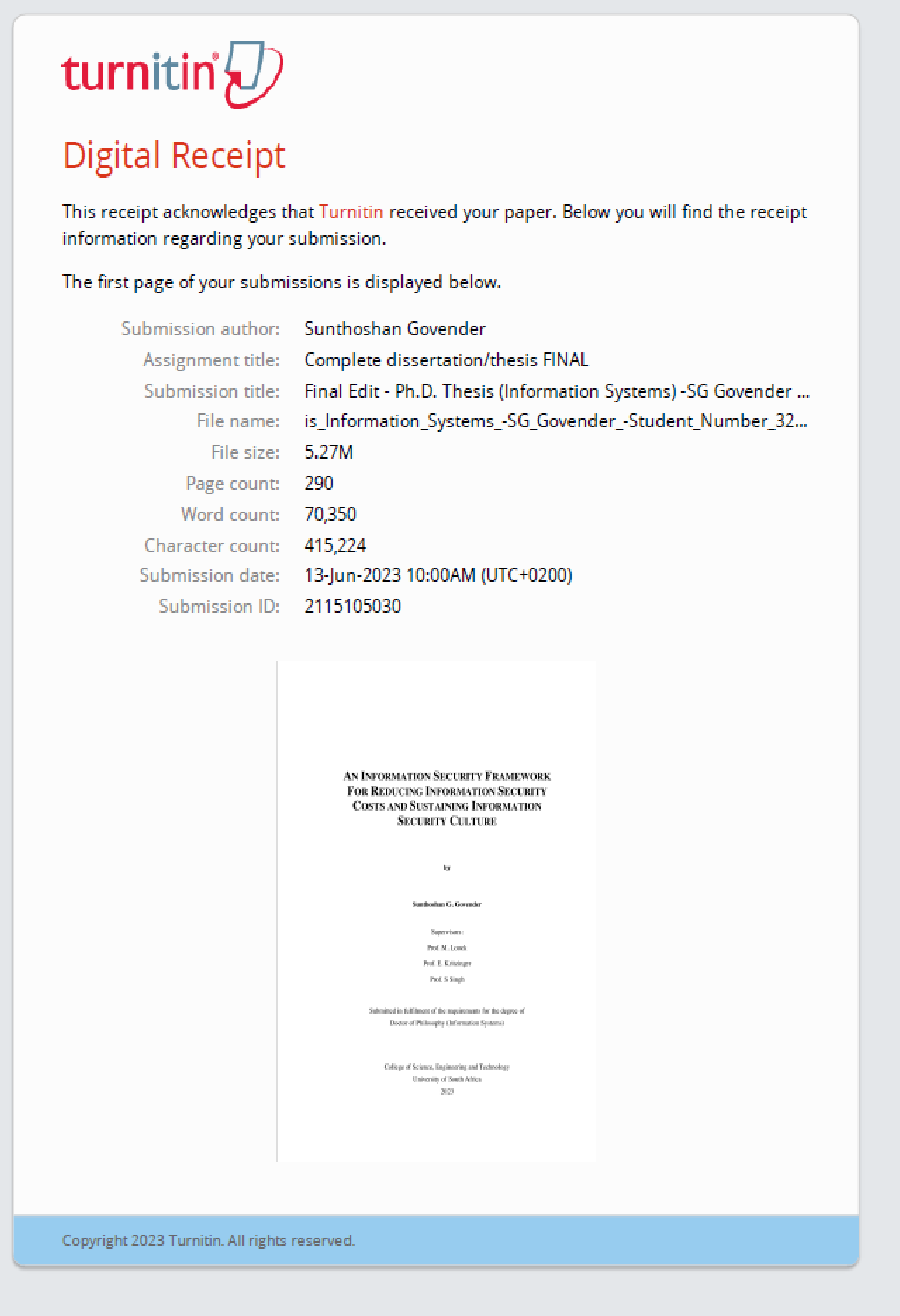
An information security framework for reducing information security costs and sustaining information security culture

The responsibility of implementing the recommended language changes rests with the author of the document.

Yours truly,

Appendix F

TurnItIn Receipt



turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Sunthoshan Govender
Assignment title:	Complete dissertation/thesis FINAL
Submission title:	Final Edit - Ph.D. Thesis (Information Systems) -SG Govender ...
File name:	is_Information_Systems_-SG_Govender_-Student_Number_32...
File size:	5.27M
Page count:	290
Word count:	70,350
Character count:	415,224
Submission date:	13-Jun-2023 10:00AM (UTC+0200)
Submission ID:	2115105030

AN INFORMATION SECURITY FRAMEWORK
FOR REDUCING INFORMATION SECURITY
COSTS AND SUSTAINING INFORMATION
SECURITY CULTURE

by

Sunthoshan G. Govender

Supervisors :

Prof. M. Loock

Prof. E. Kritzinger

Prof. S Singh

Submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy (Information Systems)

College of Science, Engineering and Technology
University of South Africa
2023

Copyright 2023 Turnitin. All rights reserved.

Appendix G

Evaluation Questions

Feature 1 – (F1) - Assessment of Information Security Risk	
Evaluation Area E1.1	**Security Assessment**
1.1.1	Are periodic security assessments conducted in the organisation?
1.1.2	Is the assessment aligned to a security standard or best practice (ISO, PCI, MITRE)?
1.1.3	Are vulnerability assessments conducted on a regular basis?
1.1.4	Is penetration testing conducted on a regular basis?
1.1.5	Are there key KPI's associated with remediation and resolution of vulnerabilities identified?
1.1.6	Is the security assessment shared with senior leadership (e.g. HOD, Exec, Board)?
Evaluation Area E1.2	**Security Architecture**
1.2.1	Does the organisation follow a security architecture method or approach?
1.2.2	Are the business drivers for security addressed in this framework?
1.2.3	Is IT/IS risk management addressed in this framework?
1.2.4	Is IS/IT Policy and Governance addressed in this framework?
1.2.5	Is Security Technical Architecture addressed in this framework?
1.2.6	Is Security Operations addressed in this framework?
Evaluation Area E1.3	**Risk Assessment**
1.3.1	Is a companywide risk management framework implemented?
1.3.2	Is there a specific IT/IS Security risk management process?
1.3.3	Are there specific IT/IS Security risk treatment KPI's defined?
1.3.4	Is the IT/IS Security risk management process integrated into IT/IS Project Management process?
1.3.5	Are IS/IT Security risks communicated to senior leadership (e.g. HOD, Exec, Board)?

Feature 2 – (F2) Reduction of Information Security Cost	
Evaluation Area E2.1	**Business Continuity Management**
2.1.1	Does the organisation have a Business Continuity Plan?
2.1.2	Does the organisation have a Business Continuity Process?
2.1.3	Is the plan and process aligned to a standard (e.g. ISO 22301)?
2.1.4	Is there business and IT input to this plan and process?
2.1.5	Does the organisation conduct tests against the plan and/or process on a regular basis?
2.1.6	Are the results of these tests submitted to executive management for review?
Evaluation Area E2.2	**Cyber Security Insurance**
2.2.1	Does the organisation invest in cyber security insurance?
Evaluation Area E2.3	**Employee Information Security Training**
2.3.1	Does the organisation run regular information security training or awareness programmes?
2.3.2	Are these programmes targeted at all levels of employees including and up to 'C' level employees?
2.3.3	Are these programmes dynamic and responsive (i.e. react to user action)?
2.3.4	Are employees evaluated to test their understanding of the training?
Evaluation Area E2.4	**Having a CISO**
2.4.1	Does the organisation have a Chief Information Security Officer (or equivalent)?
2.4.2	Does the CISO report to the board?
Evaluation Area E2.5	**Board Input on Security Spend**
2.5.1	Does the board have a view of security spend?
2.5.2	Does the board have input into security spend?
2.5.3	Is information security risk presented to the board on a regular basis?
Evaluation Area E2.6	**Having a CPO**
2.6.1	Does the organisation have a Chief Privacy Officer?
2.6.2	Does the organisation have a robust Data Privacy programme?

Evaluation Area E2.7	**Incident Response Team**
2.7.1	Does the organisation have a Security Incident Response Team?
2.7.2	Does the organisation do periodic internal penetration testing?
2.7.3	Does the organisation do periodic external penetration testing?
2.7.4	Does the organisation have defined KPI’s for the resolution of breach vectors found by the penetration testing team?
Evaluation Area E2.8	**Use of Encryption**
2.8.1	Is data at rest encrypted as a general standard?
2.8.2	Is data in motion encrypted as a general standard?
2.8.3	Are laptops, desktops and corporate cellphones encrypted as standard?
Evaluation Area E2.9	**Threat Analysis and Sharing**
2.9.1	Does the organisation conduct threat analysis activities?
2.9.2	Does the organisation employ an external company to conduct threat analysis activities?
2.9.3	Does the organisation have a threat hunting team?
2.9.4	Does the organisation actively share threat analysis information with information security forums?
Evaluation Area E2.10	**Security Analytics Services**
2.10.1	Does the organisation have a Security Operations Centre?
2.10.2	Does the organisation conduct analysis of logs and feeds from security products implemented?
2.10.3	Does the organisation conduct analysis of security logs and feeds from applications, operating systems and infrastructure implemented?
2.10.4	Does the organisation have a robust plan to address alerts and incidents that emanate from security analysis?
Evaluation Area E2.11	**Data Loss Prevention**
2.11.1	Are USB and mass storage devices blocked within the organisation?
2.11.2	Are non-sanctioned cloud sharing sites (e.g. DropBox, Google Drive, box.net etc.) blocked for usage by all users?
2.11.3	Are non-sanctioned webmail sites (e.g. Gmail, Hotmail, Yahoo Mail) blocked for usage by all users?
2.11.4	Is email monitored for data loss/leakage?
2.11.5	Are databases monitored for data loss/leakage?
2.11.6	Does the organisation have an email retention policy?

2.11.7	Does the organisation have a data retention policy?
Evaluation Area E2.12	**Data Classification**
2.12.1	Does the organisation have a Data Classification Policy?
2.12.2	Is the Data Classification Policy applied strictly?
Evaluation Area E2.13	**IS Input Costs**
2.13.1	Does the organisation evaluate costs caused by Information Security Incidents?
2.13.2	Does the organisation budget for costs caused by Information Security Incidents?
2.13.3	Does the organisation budget for costs of Information Security Measures (products, technology, services) put in place?
2.13.4	Does the organisation budget for costs of Information Security Management (people, services) put in place?
2.13.5	Does the organisation budget for costs of Information Security Risks (identified by assessment)?
2.13.6	Are these budgets evaluated and approved by senior leadership?
Feature 3 – (F3) Sustainability of Information Security Culture	
Evaluation Area E3.1	**Pillar 1- Common Security Values and Principles**
3.1.1	Are security values and principles communicated through the organisation?
3.1.2	Are the security values and principles communicated to specifically the IT/IS department?
3.1.3	Is the organisation evaluated on these value and principles?
3.1.4	Has the IT/IS department identified how each function addresses these values and principles?
Evaluation Area E3.2	**Pillar 2- Positive Reinforcement and Reward**
3.2.1	Does the organisation reward employees for good information security behaviour?
3.2.2	Is good behaviour reinforced through communication?
3.2.3	Is the either the positive reinforcement or reward mechanism quick in terms of immediate feedback?
3.2.4	Is the either the positive reinforcement or reward mechanism frequent in terms of periodic feedback?
Evaluation Area E3.3	**Pillar 3- Common and Couple Processes**
3.3.1	Does IT/IS staff understand the effects of security monitoring, blocking, patching and processes as it affects each IT discipline in the IT value chain?

3.3.2	Do Information security managers develop and socialise 'common-thread' information security processes where the impact of each IT discipline on information security is transparent?
Evaluation Area E3.4	**Pillar 4- Peer Recognition**
3.4.1	Does the organisation have peer recognition programme for good information security behaviour?
3.4.2	Is this programme led by employees rather than management?
3.4.3	Is information derived from this programme made visible to all employees?
Evaluation Area E3.5	**Pillar 5- Technical Training and Awareness of Security Issues**
3.5.1	Are security and awareness training programmes targeted at specifically IT/IS staff?
3.5.2	Is information about potential threat, breaches and information security concerns shared with employees?
3.5.3	Are security and awareness training programmes targeted at specifically senior and executive leadership?
3.5.4	Does the organisation measure the level of improvement in information security understanding of users before and after training and awareness initiatives?
3.5.5	Are remedial initiatives put in place based on training evaluations?

General Questions
ARCS Security Framework
1.What are your views on the components of the ARCS Security Framework? 2.Do you see value in the components of the Framework? 3.Are the components of the framework applicable to your organisation? 4.What are your views on the structure of the framework? 5.What are the components that you feel were not covered? 6.What improvements and/or changes can you advise on for the Framework? 7. Are there any general views or comments on the framework?
ARCS Security Evaluation Tool
1.Are outcomes of the Evaluation Tool an accurate reflection of the information security position of the organisation in its current state? 2.What are your views on the structure and application of ARCS Security Evaluation Tool?

3.Do you see the value in the Evaluation Tool with respect to the Framework developed?

4.Do you see the applicability of the implementation of the tool in your organisation?

5.What are the views on the scoring mechanism and weighting of questions?

6.What are your views on the quality and value of the output charts generated?

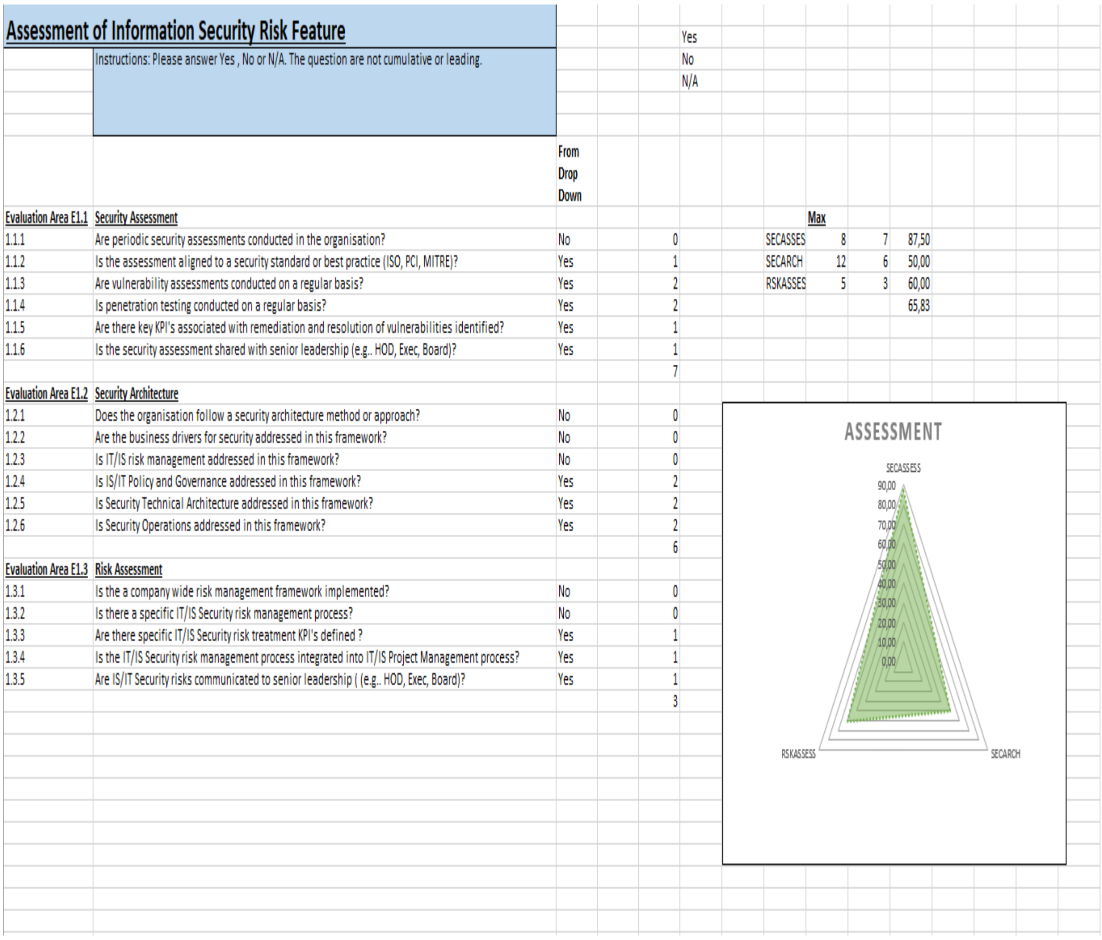
7.What improvements and/or changes can you advise on for the Evaluation Tool?

8.What are your general views or comments on the Evaluation Tool?

Appendix H

Sample Microsoft Excel Evaluation Outputs

Participant 1 – Example of Feature 1 Review



Assessment of Information Security Risk Feature

Instructions: Please answer Yes , No or N/A. The question are not cumulative or leading.

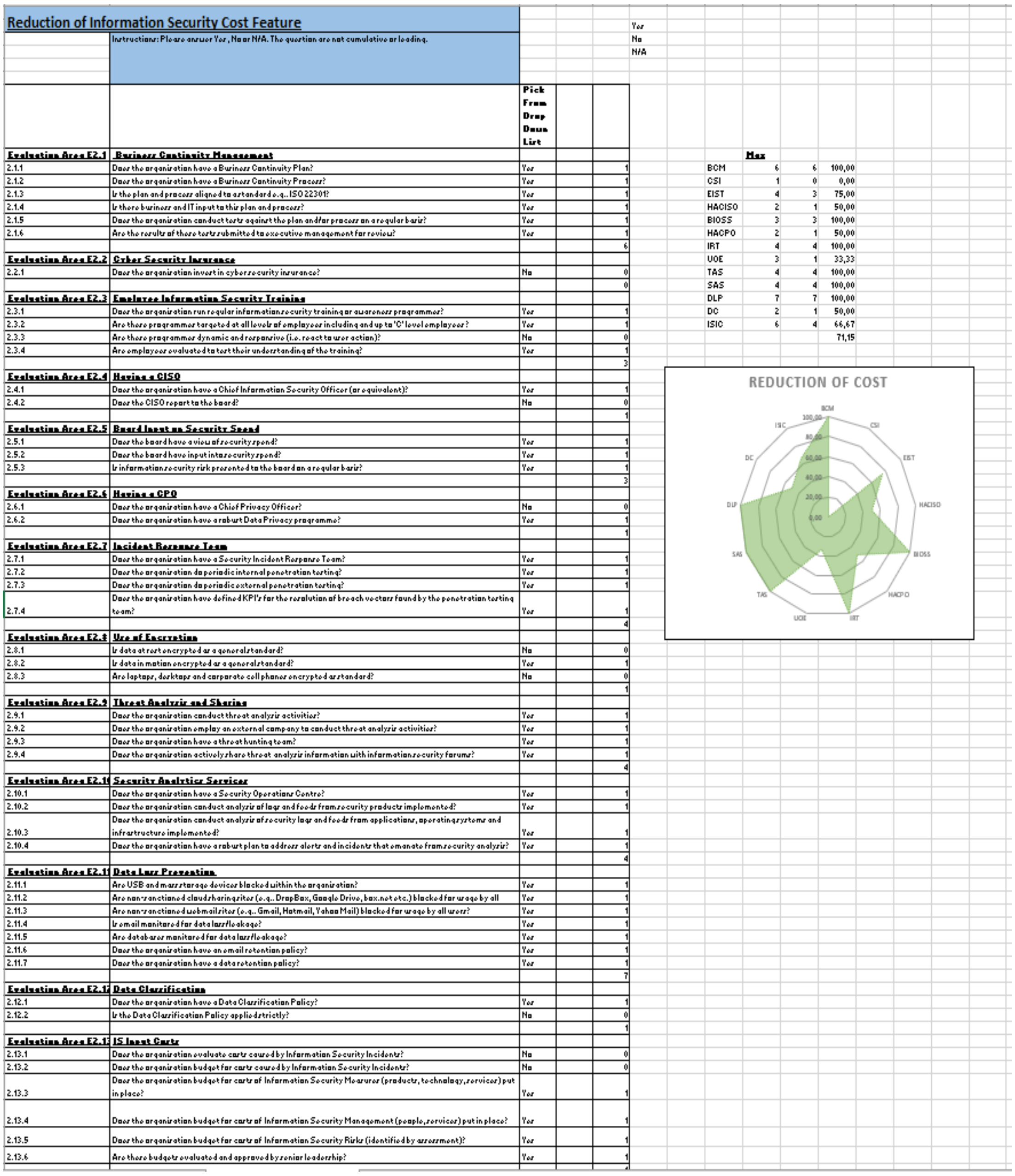
Yes
No
N/A

		From Drop Down	
Evaluation Area E1.1	**Security Assessment**		
1.1.1	Are periodic security assessments conducted in the organisation?	No	0
1.1.2	Is the assessment aligned to a security standard or best practice (ISO, PCI, MITRE)?	Yes	1
1.1.3	Are vulnerability assessments conducted on a regular basis?	Yes	2
1.1.4	Is penetration testing conducted on a regular basis?	Yes	2
1.1.5	Are there key KPI's associated with remediation and resolution of vulnerabilities identified?	Yes	1
1.1.6	Is the security assessment shared with senior leadership (e.g.. HOD, Exec, Board)?	Yes	1
			7
Evaluation Area E1.2	**Security Architecture**		
1.2.1	Does the organisation follow a security architecture method or approach?	No	0
1.2.2	Are the business drivers for security addressed in this framework?	No	0
1.2.3	Is IT/IS risk management addressed in this framework?	No	0
1.2.4	Is IS/IT Policy and Governance addressed in this framework?	Yes	2
1.2.5	Is Security Technical Architecture addressed in this framework?	Yes	2
1.2.6	Is Security Operations addressed in this framework?	Yes	2
			6
Evaluation Area E1.3	**Risk Assessment**		
1.3.1	Is the a company wide risk management framework implemented?	No	0
1.3.2	Is there a specific IT/IS Security risk management process?	No	0
1.3.3	Are there specific IT/IS Security risk treatment KPI's defined ?	Yes	1
1.3.4	Is the IT/IS Security risk management process integrated into IT/IS Project Management process?	Yes	1
1.3.5	Are IS/IT Security risks communicated to senior leadership ((e.g.. HOD, Exec, Board)?	Yes	1
			3

	Max		
SECASSES	8	7	87,50
SECARCH	12	6	50,00
RSKASSES	5	3	60,00
			65,83

ASSESSMENT

Participant 1 – Example of Feature 2 Review



Reduction of Information Security Cost Feature

Instructions: Please answer Yes , No or N/A. The question are not cumulative or leading.

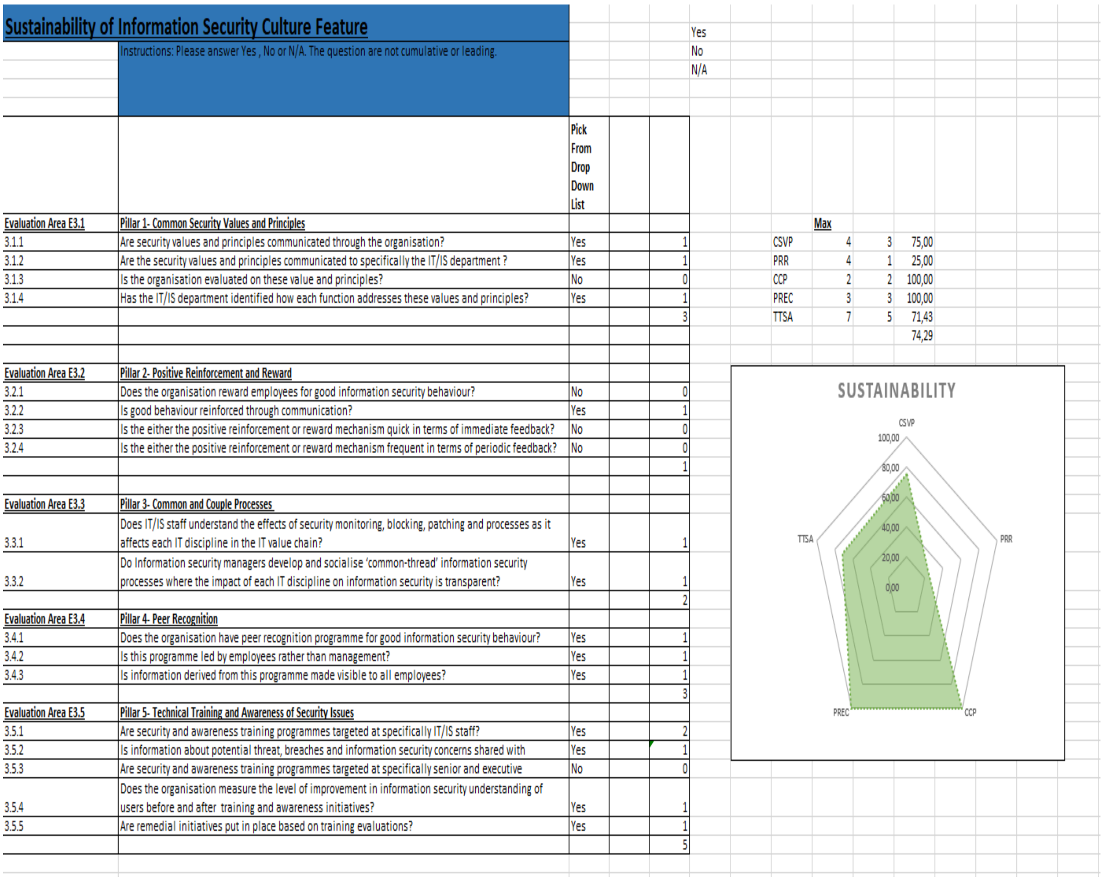
Yes
No
N/A

		Pick From Drop Down List		
Evaluation Area E2.1	**Business Continuity Management**			
2.1.1	Does the organisation have a Business Continuity Plan?	Yes		1
2.1.2	Does the organisation have a Business Continuity Process?	Yes		1
2.1.3	Is the plan and process aligned to a standard e.g.. ISO 22301?	Yes		1
2.1.4	Is there business and IT input to this plan and process?	Yes		1
2.1.5	Does the organisation conduct tests against the plan and/or process on a regular basis?	Yes		1
2.1.6	Are the results of these tests submitted to executive management for review?	Yes		1
				6
Evaluation Area E2.2	**Cyber Security Insurance**			
2.2.1	Does the organisation invest in cyber security insurance?	No		0
				0
Evaluation Area E2.3	**Employee Information Security Training**			
2.3.1	Does the organisation run regular information security training or awareness programmes?	Yes		1
2.3.2	Are there programmes targeted at all levels of employees including and up to 'C' level employees ?	Yes		1
2.3.3	Are there programmes dynamic and responsive (i.e. react to user action)?	No		0
2.3.4	Are employees evaluated to test their understanding of the training?	Yes		1
				3
Evaluation Area E2.4	**Having a CISO**			
2.4.1	Does the organisation have a Chief Information Security Officer (or equivalent)?	Yes		1
2.4.2	Does the CISO report to the board?	No		0
				1
Evaluation Area E2.5	**Board Input on Security Spend**			
2.5.1	Does the board have a view of security spend?	Yes		1
2.5.2	Does the board have input into security spend?	Yes		1
2.5.3	Is information security risk presented to the board on a regular basis?	Yes		1
				3
Evaluation Area E2.6	**Having a CPO**			
2.6.1	Does the organisation have a Chief Privacy Officer?	No		0
2.6.2	Does the organisation have a robust Data Privacy programme?	Yes		1
				1
Evaluation Area E2.7	**Incident Response Team**			
2.7.1	Does the organisation have a Security Incident Response Team?	Yes		1
2.7.2	Does the organisation do periodic internal penetration testing?	Yes		1
2.7.3	Does the organisation do periodic external penetration testing?	Yes		1
2.7.4	Does the organisation have defined KPI's for the resolution of breach vectors found by the penetration testing team?	Yes		1
				4
Evaluation Area E2.8	**Use of Encryption**			
2.8.1	Is data at rest encrypted as a general standard?	No		0
2.8.2	Is data in motion encrypted as a general standard?	Yes		1
2.8.3	Are laptops, desktops and corporate cell phones encrypted as standard?	No		0
				1
Evaluation Area E2.9	**Threat Analysis and Sharing**			
2.9.1	Does the organisation conduct threat analysis activities?	Yes		1
2.9.2	Does the organisation employ an external company to conduct threat analysis activities?	Yes		1
2.9.3	Does the organisation have a threat hunting team?	Yes		1
2.9.4	Does the organisation actively share threat analysis information with information security forums?	Yes		1
				4
Evaluation Area E2.10	**Security Analytics Services**			
2.10.1	Does the organisation have a Security Operations Centre?	Yes		1
2.10.2	Does the organisation conduct analysis of logs and feeds from security products implemented?	Yes		1
2.10.3	Does the organisation conduct analysis of security logs and feeds from applications, operating systems and infrastructure implemented?	Yes		1
2.10.4	Does the organisation have a robust plan to address alerts and incidents that emanate from security analysis?	Yes		1
				4
Evaluation Area E2.11	**Data Loss Prevention**			
2.11.1	Are USB and mass storage devices blocked within the organisation?	Yes		1
2.11.2	Are non-sanctioned cloud sharing sites (e.g.. DropBox, Google Drive, box.net etc.) blocked for usage by all	Yes		1
2.11.3	Are non-sanctioned webmail sites (e.g.. Gmail, Hotmail, Yahoo Mail) blocked for usage by all users?	Yes		1
2.11.4	Is email monitored for data loss/leakage?	Yes		1
2.11.5	Are databases monitored for data loss/leakage?	Yes		1
2.11.6	Does the organisation have an email retention policy?	Yes		1
2.11.7	Does the organisation have a data retention policy?	Yes		1
				7
Evaluation Area E2.12	**Data Classification**			
2.12.1	Does the organisation have a Data Classification Policy?	Yes		1
2.12.2	Is the Data Classification Policy applied strictly?	No		0
				1
Evaluation Area E2.13	**IS Input Costs**			
2.13.1	Does the organisation evaluate costs caused by Information Security Incidents?	No		0
2.13.2	Does the organisation budget for costs caused by Information Security Incidents?	No		0
2.13.3	Does the organisation budget for costs of Information Security Measures (products, technology, services) put in place?	Yes		1
2.13.4	Does the organisation budget for costs of Information Security Management (people, services) put in place?	Yes		1
2.13.5	Does the organisation budget for costs of Information Security Risks (identified by assessment)?	Yes		1
2.13.6	Are there budgets evaluated and approved by senior leadership?	Yes		1
				4

	Max		
BCM	6	6	100,00
CSI	1	0	0,00
EIST	4	3	75,00
HACISO	2	1	50,00
BIOSS	3	3	100,00
HACPO	2	1	50,00
IRT	4	4	100,00
UOE	3	1	33,33
TAS	4	4	100,00
SAS	4	4	100,00
DLP	7	7	100,00
DC	2	1	50,00
ISIC	6	4	66,67
			71,15

REDUCTION OF COST

Participant 2 – Example of Feature 3 Review



Sustainability of Information Security Culture Feature

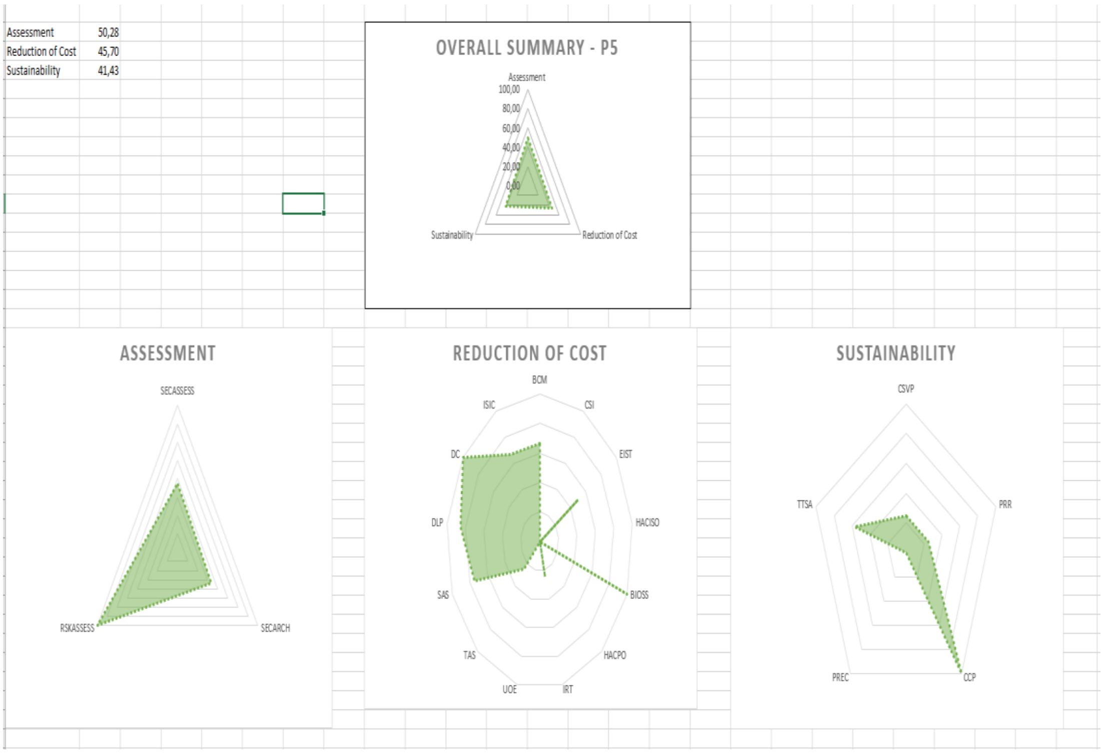
Instructions: Please answer Yes , No or N/A. The question are not cumulative or leading.

Yes
No
N/A

		Pick From Drop Down List		
Evaluation Area E3.1	Pillar 1- Common Security Values and Principles			
3.1.1	Are security values and principles communicated through the organisation?	Yes		1
3.1.2	Are the security values and principles communicated to specifically the IT/IS department ?	Yes		1
3.1.3	Is the organisation evaluated on these value and principles?	No		0
3.1.4	Has the IT/IS department identified how each function addresses these values and principles?	Yes		1
				3
Evaluation Area E3.2	Pillar 2- Positive Reinforcement and Reward			
3.2.1	Does the organisation reward employees for good information security behaviour?	No		0
3.2.2	Is good behaviour reinforced through communication?	Yes		1
3.2.3	Is the either the positive reinforcement or reward mechanism quick in terms of immediate feedback?	No		0
3.2.4	Is the either the positive reinforcement or reward mechanism frequent in terms of periodic feedback?	No		0
				1
Evaluation Area E3.3	Pillar 3- Common and Couple Processes			
3.3.1	Does IT/IS staff understand the effects of security monitoring, blocking, patching and processes as it affects each IT discipline in the IT value chain?	Yes		1
3.3.2	Do Information security managers develop and socialise 'common-thread' information security processes where the impact of each IT discipline on information security is transparent?	Yes		1
				2
Evaluation Area E3.4	Pillar 4- Peer Recognition			
3.4.1	Does the organisation have peer recognition programme for good information security behaviour?	Yes		1
3.4.2	Is this programme led by employees rather than management?	Yes		1
3.4.3	Is information derived from this programme made visible to all employees?	Yes		1
				3
Evaluation Area E3.5	Pillar 5- Technical Training and Awareness of Security Issues			
3.5.1	Are security and awareness training programmes targeted at specifically IT/IS staff?	Yes		2
3.5.2	Is information about potential threat, breaches and information security concerns shared with	Yes		1
3.5.3	Are security and awareness training programmes targeted at specifically senior and executive	No		0
3.5.4	Does the organisation measure the level of improvement in information security understanding of users before and after training and awareness initiatives?	Yes		1
3.5.5	Are remedial initiatives put in place based on training evaluations?	Yes		1
				5

	Max		
CSVP	4	3	75,00
PRR	4	1	25,00
CCP	2	2	100,00
PREC	3	3	100,00
TTSA	7	5	71,43
			74,29

Participant 5 – Example of Summary Sheet



Assessment	50,28
Reduction of Cost	45,70
Sustainability	41,43

Appendix I

Excerpts of Transcripts from Participant Interviews

The following transcripts are portions of the interviews conducted with different participants. A portion of a conversation was transcribed related to each of the three parts of the interviews with participants. The selection of these transcripts is merely to show the types of conversations that were had and were not selected based on any specific criteria.

1. Introduction Excerpt

Researcher - SG Govender
So, we're not going to have any formalities and I have to introduce you the framework and tool.
Researcher - SG Govender
We just want to get into the actual study and also not to waste any of your time.
I think what I just want to start with is to show you the models that led to the development of the framework.
So the first, the first model that I've actually published, this was about 2017 that we put this together is based on International Studies around particular factors that is that assist an organization, in reducing information security cost. The initial premise was talking about culture and values in behaviour and that sort of thing and relating traditional let's call it HR practices of organizational behaviour to information security culture and that applies to computing culture in current times and specifically information security.
Participant
OK.
Researcher - SG Govender
Right, so in studies that have been published, you find that there are certain cost reduction factors and certain products and services that will basically reduce costs from an information security perspective and certain factors that increase cost, even though they may reduce risk.
Researcher - SG Govender
I've synthesized these studies to show that there are twelve factors that actually help reduce cost and have broken them up into social factors and technical factors.
Researcher - SG Govender
The social factor part of it is something that is structural that requires people to intervene to be successful.
Researcher - SG Govender
The technical factors are products, solutions, services that an organization may put into place.
Researcher - SG Govender
However, what we are trying to establish from this entire thing is that, irrespective of putting in those products solution services, you still require people. OK, so ultimately, it's still ultimately the value of those product solution services, so comes down to the people itself and therefore their culture and behaviour.
Researcher - SG Govender

Now I think you sitting on both sides of the fence you are. You have customers and you are also dealing with internal security. Yes, yeah, so you could look at it from whichever perspective you want to look at it from. You can maybe choose a customer that you worked with or alternatively. Focus on your organization and when we're talking about these.

Participant

I think we're going to keep it internal because if you do it differently then it just makes it difficult.

Participant

So, what we do internally also gets done for customers.

Researcher - SG Govender

The next thing that was then published was to look at the methods that one would be able to get information about information security assessment in organizations.

Researcher - SG Govender

We looked at this, but what are well, the traditional ways that one does understand your organization from security perspective currently and we just grouped it into 3 factors, which is basically security assessment which is best practice evaluation, you know, like ISO 27000 or something like that or uh, NIST framework or something like that.

Researcher - SG Govender

Just a just a security assessment method or best practice. The next part being maybe a longer term consideration is security architecture so implementing some sort of framework methodology that has a longer term strategy from information security in your organization and then the last one being the standard straightforward risk assessment and what an internal audit would have done in the past and coming out with the results, finding the gap and addressing the gap, which is very much a reactive way of addressing or evaluating information security.

Researcher - SG Govender

But what we basically said is that irrespective of what your input information is you come, you'll come up with a gap and you want to address that gap. And generally, in the information security environment we come up with technology products and services, so we can put something into place to reduce risk.

Researcher - SG Govender

We buy a piece of technology or something that ought to be able to plug the gap. We don't necessarily look at it from. A from a non -technical perspective OK. But for each of those products and services that you bring in you will need to have some sort of technical factors or some implementation design configuration. And of course, all of that requires some sort of human intervention. Yeah, OK, so there are always people involved in it.

Researcher - SG Govender

OK, so from that description what we then went and said is from a culture perspective, how does one change? Purely from the information security perspective, how do you change things in your organization purely from a human perspective? So, I developed the five-pillar model.

We're talking about common security values and principles. So, the concept of here is about we have different disciplines within the environment, and each of those disciplines have a touch point in security.

Do we have a common thread amongst the different disciplines? So a patch might be a security priority, but it affects an application .It'll fix the infrastructure, fix your transmission over the network, whatever the case may be but do those people in the

different environments have the same view of information security across all disciplines, or is it something that is purely coming from a security perspective?
Positive reinforcement reward very similar to the HR part of positive reinforcement. Is this coming from a management perspective, you know to be able to say, “Does management reward people for doing the right thing?” “Do we communicate to staff and to the organization in general? “Within the organization, do all of these people know when they do something good?
The common in couple processes is yet again that that idea of making sure that as these things filtered through the environment, that people see what their value add is in this security process and the fact that they that a small breach that link or that chain can have a catastrophic effect, so making sure that people understand that as much as I may just make a small change in the system, it actually has huge impact.
The next one is peer recognition is very similar to the positive reinforcement work, but it flips it around and says as employees of the organization, you have ownership of information security and your evaluation of your peers. So, you know are there forums and environments within the organization, and it may not only be for information security, but do people or employees support other employees in their good decision making? Because what we tend to find, and that’s just a general thing from a human resource perspective, is that. Especially in certain countries, it works better when your peer tells you you’ve done better and pat you on the back rather than your manager doing so.
And then the last one being the technical training awareness of security issues and this is speaking specifically to tailored cyber security awareness for particular levels of the organization particular environments within the organization, and a specific focus on training IT staff on security, which is something that you know literature shows that is generally not done.

2. Framework Demonstration Excerpt

Researcher - SG Govender
So just to kick off straightforwardly it’s going to the assessment feature.
The assessment feature is described by these three green circles. So, the first part of this first evaluation area is about security assessment. This is in regard to best practice standards. Right, so the first question being are there periodic security assessments that are conducted in the organization?
Is the assessment aligned to security standard or best practice?
Participant
OK.
Yes, we conduct regular security assessments, so it’s linked to the NIST, and ISO best practices. But as things mature, we identify new areas. We start looking at identifying specific areas from different best practices.
Researcher - SG Govender
OK. Are vulnerability assessments and pen testing conducted on a regular basis?
Are there KPI’s associated with the remediation and resolution of issues found during those tests?
Participant
So, it’s not really done regularly. It could be higher, but we….We break it down from high, medium and low, so we focus on high priority items first. We then have a look at the medium ones.

Researcher - SG Govender
OK, so actually what I'm asking here is that you are able to categorize this from your system, but the question is that is there a set KPIs to prioritize resolution? So what we're trying to get at is that, say for example, for highs you want to be able to address it on 30 days as a basis. And mediums in 60 days. And follow a best practice rather than seeing how many highs you have and saying, how long will it take to resolve?
Participant
OK, yes yeah. So normally there are time frames are well. We identify the amount of systems that are affected. I mean they are prioritized based on the top vulnerabilities. Some might have 30 day time period, others might be a lot shorter depending on the amount of risk and so. It's about we say well which one do we need to address first, how long it's gonna take? What do we need to do? Communicate with anybody?
Researcher - SG Govender
Is that evaluated against systems?
Researcher - SG Govender
So, we categorise systems and then you work on the vulnerabilities based on system priority.
Researcher - SG Govender
Is the security assessment shared with senior leadership?
Participant
Yes
Researcher - SG Govender
The next evaluation area is around security architecture, so does the organization follow a security architecture, method or approach?
Participant
Various ones, but yes there is.
Researcher - SG Govender
Are there business drivers in your security architecture framework. Is your business risk addressed in the framework? Have you developed or have you taken from different frameworks?
Participant
We, it's developed, we developed our own system internally and it's like, well, we take it from best practices and it's based on the all sorts of requirements.
Researcher - SG Govender
The next evaluation area is around risk assessment. OK, so is there a companywide risk assessment risk management framework? Are there specific security risk management processes. And is there security risk treatment for those identified risks. Does it have a KPI defined?

3. <u>Evaluation of Framework and Tool Excerpt</u>

Researcher - SG Govender
Next step then is to basically go through a set of questions in terms of your thoughts of this entire process that we've been through what you've seen. And what you've heard. I will type as we speak. But I've got that recording so that I can look back at your responses.
Researcher - SG Govender
So just on the on the framework itself, so framework is the three features evaluation areas. The questions that came up right. So what are your views of the components?

Participant
I think it's very well constructed, it covers a lot of a large spectrum of items is that's important in data and on the information security side so I think it's well thought out. The items that it doesn't focus on is data privacy. Focused on another privacy functions as well, which I mean it's becoming a lot more evident nowadays with all the new legislation and items that comes out.

Researcher - SG Govender
Do you see value in the components that are covered so far? I mean give me a general view of it, but there's there's quite a lot that we covered in terms of concepts there, but do you see value in this?

Participant
Yes, I do. There are different areas with some questions that you've asked that I know of. The processes isn't best, it's not 100% effective, so additional work can be done and it definitely helps you to think of how do we improve on those different systems, so it is good.

Researcher - SG Govender
I think you hit the nail on the head. It is not to give you an answer, not to solve your problem. It rather is to ask some questions, to see if this was implemented in real life, what you have done and where you can improve.

Researcher - SG Govender
What is your view of the structure of the framework, so the structure being the assessment, the evaluation areas, the technical model and the feature evaluations the questions?
Could it be better?

Participant
No, I think it's good. For what it looks at you can maybe review the human features. How human interaction and communication with the two parties or maybe even combine those two or bring them closer together. It might help I think. It's coming from that process, but otherwise I think it's very good. You may want to structure just so areas are linked..

Researcher - SG Govender
You say we don't describe what? The reference model is in the back end. In terms of how these things are linked.

Participant
So they are linked it sounds.

Participant
There's nothing wrong with the way that it's set out, I'm just I was just thinking focusing on the fact that we're planning and evaluating. How it's being embedded within the organization, we focus on the physical, Umm, sections. Maybe just put it together. It's just a suggestion. It doesn't throw the whole thing off.

Participant
I think. If you go too technical it is going to be difficult to manage because all organizations don't have the same complexities, so it wouldn't be beneficial to go in to more technical detail.