A METHOD FOR IMPLEMENTING AN INFORMATION SECURITY AWARENESS CAMPAIGN WITHIN AN ORGANISATION

A Research Dissertation presented to
The Department of Information Systems

University of Cape Town

By

Juan-Marc Scrimgeour

SCRJUA001

in partial fulfilment of the requirements of the
INF5005W Information Systems Masters Dissertation Course
February 2019

Plagiarism Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.

2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this dissertation "A method for implementing an Information Security Awareness Campaign within an organisation", from the work(s) of other people has been attributed, and has been cited and referenced.

3. This dissertation "A method for implementing an Information Security Awareness Campaign within an organisation", is my own work.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

5. I acknowledge that copying someone else's assignment or essay, or part of it, is wrong, and declare that this is our own work.

6. I have not falsified or manufactured any data, and declare that all data was ethically collected

Signed by candidate

Signature: Date: 14/02/2019

Name: Juan-Marc Scrimgeour

Abstract

Research has shown that educating end-users on information security awareness plays an essential part in securing any environment. While best practice standards provide a set of minimum information security awareness controls that should be implemented, little guidance exists on how to implement these controls to ensure the effectiveness of the training.

This research set out to define and evaluate a method for implementing an Information Security Awareness Campaign within an organisation based on existing research and standards while assisting the organisation in improving their information security awareness campaign through the creation of artifacts and measurement techniques. A design science research approach guided the research to evaluate changes in the information security awareness campaign implementation method through several research cycles. The method was implemented within an organisation and evaluated based on the impact, effectiveness and results of each step as well as the feedback from participants.

The research found both positive and negative results throughout the method. Specific steps within the method proved to be lengthy, time-consuming and confusing to participants. Although many improvements can yet be made, the method was suitable as it achieved the required objective within the organisation. The research outcome provided a risk-based method with a visual representation that demonstrated the lack of awareness of specific information security awareness topics to the organisation. The results of the study not only provided value to the organisation but provided a tried and tested method for implementing an Information Security Awareness Campaign within other organisations.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Cyber-attacks are increasingly prevalent in our everyday activities, both in professional and personal lives. Companies spend a large amount of money on technologies and highly skilled resources to mitigate this risk (Daniel Ani, He, & Tiwari, 2016; McCormac, Calic, Parsons, Zwaans, Butavicius & Pattinson, 2016b; Stewart & Lacey, 2012; Yildirim, 2016). However, these resources are often insufficient to prevent an attack since the technologies are themselves often targets of attacks (Ragan, 2015). The National Institute of Standards and Technology (NIST) defines a zero-day attack as “An attack that exploits a previously unknown hardware, firmware, or software vulnerability.” (National Institute of Standards and Technology, 2019). Zero-day attacks thrive on obscurity which, without a known attack signature or strategy, remain undetected by some of the best security-related technologies.

When the flaws in these security technologies are addressed, they are vulnerable to human error, as a slight misconfiguration by Information Technology (IT) staff, could render an otherwise secure technology ineffective (Daniel Ani et al., 2016). As a result, it is becoming increasingly important to educate end-users in information security awareness practices (Daniel Ani et al., 2016; Denning, Lerner, Shostack, & Kohno, 2013; Mylonas, Kastania, & Gritzalis, 2013; Yildirim, 2016). NIST (2019) defines information security as “The protection of information and information systems from unauthorised access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability”. Information security awareness is, therefore, defined as “a learning process that sets the stage for training by changing individual and organisational attitudes to realise the importance of security and the adverse consequences of its failure.” (National Institute of Standards and Technology, 2019).

Without an effective information security awareness campaign in place, even the most secure network is vulnerable to human error which could result in a breach in cyber defences (Daniel Ani et al., 2016; Waly, Tassabehji, & Kamala, 2012). A campaign is defined by Oxford University Press (2019) as "An organised course of action to achieve a goal". An information security awareness campaign is, therefore, an organised course of action in order to improve information security awareness. An information security awareness campaign can include a variety of actions, such as marketing campaigns, promotions, gifts and training (Waly, Tassabehji, & Kamala, 2012).

As a result, end-users are targeted, since they are perceived as the weakest link in any environment (Aloul, 2012; Daniel Ani et al., 2016; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2012; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014; Waly et al., 2012). To date, research around information security awareness has focused mainly on techniques used to implement and improve on the awareness training, as well as ways to measure its impact on the environment (Arachchilage & Love, 2014; Bashorun, Worwui, & Parker, 2013; Denning et al., 2013; Gundu & Flowerday, 2012; Manifavas, Fysarakis, Rantos, & Hatzivasilis, 2014; Parsons et al., 2014)

Best-practice standards require several controls be implemented to drive a successful information security awareness campaign (BSI Group, 2013; Chaplin, Creasey, & Thathupara, 2016; Jordan, Haken, & Creasey, 2018; PCI Security Standards Council, 2016). Although these standards guide what is required, they do not guarantee an effective campaign as their focus is not on the effectiveness of the training, but instead meeting legislative and regulatory requirements. (Aloul, 2012; Daniel Ani et al., 2016; Stewart & Lacey, 2012). Additionally, while best-practice standards require the effectiveness of the campaign must be measured, evaluated, and monitored to improve and ensure its success, little guidance on how to perform or execute these measurements is provided (BSI Group, 2013; Chaplin et al., 2016; Jordan et al., 2018; PCI Security Standards Council, 2016).

1.1 Research problem

Research has shown that educating end-users on information security awareness plays an integral part in securing any environment (Daniel Ani et al., 2016; Denning et al., 2013; Mylonas et al., 2013; Yildirim, 2016). Best practice standards provide a set of minimum controls that should be implemented, however, no guidance is given on how to implement these controls to ensure the effectiveness of the training (Aloul, 2012; Daniel Ani et al., 2016; Stewart & Lacey, 2012). The field of information security awareness is popular. However, most studies focus on improving training or how to implement the training differently. There seems to be a lack of studies that focus on how to implement a campaign that meets the stringent requirements set by best practice standards. Besides, research on effectiveness measurement techniques primarily uses questionnaires as the primary means of measuring effectiveness. However, researchers in this field state that the questionnaire technique can be improved by including metrics.

1.2 Research purpose

This research sought to define and evaluate a method for implementing an information security awareness campaign within an organisation based on existing research and standards through the creation of artifacts and measurement techniques. The method used attempts to supplement the widely used questionnaire technique with risk management practices, such as those defined by the NIST (2019), “The program and supporting processes to manage information security risk to organisational operations (including mission, functions, image, reputation), organisational assets, individuals, other organisations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.” This will address the research problem by implementing and evaluating a method for providing an information security awareness campaign for an organisation that is measurable and uses risk management metrics to determine its effectiveness.

1.3 Scope of study

The study was conducted within a financial institution in South Africa over ten months in 2018 (January to October). The study focused on delivering training to a group of business units that have a similar risk profile. The target group includes staff responsible for Human Resource Management, Financial Management, Marketing, Property Acquisition and Maintenance, Risk Management Services, and Project Management. The training provided was created and administered by employees of the organisation. The training focused on one specific theme (Acceptable Usage Policy) and was delivered using a single method (E-mailers).

1.4 Outline of the study

Chapter 2 provides a review of the literature and academic studies in the field of information security awareness. The review shows that two major themes are prevalent in current studies, namely, factors that influence the effectiveness of training, and various techniques of measuring the effectiveness of training.

Chapter 3 explains and substantiates the research methodology being used, along with an overview of design science as the research paradigm. The chapter concludes with ethical considerations.

Chapter 4 provides an overview of the research process, starting with a summary of Poepjes' (2015) Information Security Awareness Capability Model. The proposed method is illustrated, and each step explained in detail.

The method's application in an organisation is presented in Chapter 5, with detailed documentation for each step.

The method is evaluated in Chapter 6, with both positive and negative results discussed throughout the method. After evaluating each step of the method, the complete method was evaluated and was found to be adequate, as it had achieved the intended objective.

The dissertation concludes in Chapter 7 with a summary and reflection of the research presented, followed by the contributions that the research has made. Finally, the limitations of the study and recommendations for future research are presented.

2 LITERATURE REVIEW

2.1 Introduction

A systematic approach to the review was undertaken to obtain a complete view of research performed within this field of study, (Boell & Cecez-Kecmanovic, 2015; Lebek, Uffen, Breitner, Neumann, & Hohler, 2013). It is important to note that there is a paucity of literature, as the information security awareness field is not widely researched (Poepjes, 2015). Of the papers analysed, a little more than half of the papers focused on measuring the effectiveness of an information security awareness campaign. Even though the balance used measuring techniques and theories, they focused on improving the knowledge of end-users or elaborating on the importance of the training.

The review firstly provides an overview of information security awareness and the methods used to provide information security awareness. The review then examines the literature whose primary focus was on improving the effectiveness of information security awareness — followed by the various techniques used in the studies to measure the effectiveness of information security awareness campaigns.

2.2 Information security awareness

It is essential to understand what information security awareness is and how it is different from training. NIST (2019) make a clear distinction between the two. Awareness focuses on bringing IT security concerns to someone's attention and making them aware in order to change their behaviour. Awareness pushes information to the end-user and is often aimed at a broad audience, using multiple methods for providing this communication. Training is a more formal process, with the end goal being to increase the end-users' knowledge and skill to improve their job performance (National Institute of Standards and Technology, 2019). Training

requires the user to be active in the process (National Institute of Standards and Technology, 2019).

Information security awareness is delivered in multiple ways, often based on the targeted end-user group. As there is no clearly defined method for delivering information security awareness, the method used changes from organisation to organisation. Industry leaders in the field provide multiple methods in implementing information security awareness, which include simulations of cyberattacks, marketing material, games, micro-learnings and training videos (Huisman, 2018). Figure **1** illustrates the awareness offerings from each of the leaders in the industry (Cofense, 2019; KnowBe4, 2019; MediaPRO, 2019; Proofpoint, 2019; Terranova, 2019), as identified in the Gartner publication "Magic Quadrant for Security Awareness Computer-Based Training" (Huisman, 2018).

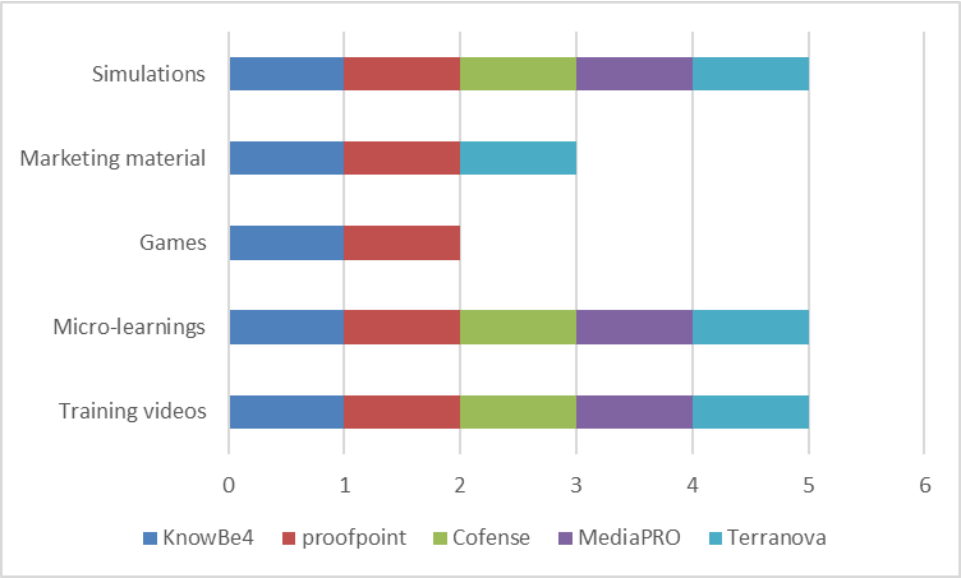


Figure 1: Awareness offering overview

Simulations, as a method for delivering training, is widely used by many of the industry leaders and requires the implementer to send fake phishing e-mails to their end-users in an attempt to not only increase their awareness but to allow the end-user to practice what they have learnt while gaining valuable data to measure the effectiveness of the training. This method widely used in research to measure

awareness effectiveness (Aloul, 2012; Young-McLear, Wyman, Benin, & Young-McLear, 2016).

Marketing materials consist of general communication techniques in the form of posters, wallpapers, infographics and e-mailers. Many of the leaders provide information security awareness themed marketing material templates (KnowBe4, 2019; MediaPRO, 2019; Proofpoint, 2019).

Games as a delivery method are not widely used, with only two of the market leaders providing them within their standard offering (Figure 1). This technique, also known as Gamification, is widely researched (Denning et al., 2013) and used by security research providers to provide free-to-play resources (Microsoft, 2013; Open Web Application Security Project, 2018).

Micro-learnings are short videos, usually between 2-5 minutes, that focus on specific information security awareness topics (Cofense, 2019; KnowBe4, 2019; MediaPRO, 2019; Proofpoint, 2019; Terranova, 2019). Training videos are longer, anywhere from 15 to 40 minutes in length, and require the end-user to test their knowledge at the end of the video by answering a series of questions (Cofense, 2019; KnowBe4, 2019; MediaPRO, 2019; Proofpoint, 2019; Terranova, 2019).

2.3 Factors influencing the effectiveness of information security awareness

Over the past five years, there have been many studies trying to identify the best way to improve on an information security awareness campaign. These studies have varied in approach from simulations (Arachchilage & Love, 2014; Aloul, 2012; Young-McLear et al., 2016) to the development of educational material (Denning et al., 2013; Pattinson, Butavicius, Parsons, McCormac, & Calic, 2017). After analysing research papers, a common thread of three common themes were found. These themes are end-user knowledge and skills, the personality of the end-user and the environment that surrounds the end-user.

2.3.1 *Knowledge and skills*

A major theme in most studies is the importance of end-users knowledge and skills around information security awareness, such as, what to do when a phishing mail is received or what to do when someone tailgates. The most common type of research was simulations aimed at proving that information security awareness is essential and could be effective. These studies performed phishing simulations on a target audience to show how end-users are unaware of underlying information security awareness themes and how these basic attacks could bypass currently implemented information security controls (Aloul, 2012; Young-McLear et al., 2016). The two assessed studies highlighted that phishing e-mails are the most common way to compromise an environment. What stood out, was that that in five years from 2012 to 2016 end-users remained susceptible to phishing attacks and that no one has found a way to instil or communicate the basics of information security awareness to end-users.

Another gap in research is that there is no defined outline of what knowledge should be shared regarding information security awareness. While some standards, such as Payment Card Industry Data Security Standard 3.2 (PCI Security Standards Council, 2016), state key focus areas for information security awareness, it is not all-encompassing and is generally focused on software developers. However, creating a database of all-encompassing information security awareness themes is not as simple as one would think, due to the level of information security awareness knowledge differing from end-user to end-user. Within the field of study, Arachchilage and Love (2014) made use of the Technology Threat Avoidance Theory to say that if an end-user perceives a threat, they will avoid it. Which, while entirely accurate, relies on the assumption that the end-user knows there is a threat, or that the end-user can correctly understand the likelihood or impact of the threat. Stewart and Lacey (2012) refer to the term as “Bounded Rationality”. Stewart and Lacey (2012) state that when an end-user faces a choice between a safe/rational or unsafe/irrational choice, the end-user will choose the safe/rational option, assuming they have sufficient

knowledge to make that choice. The end-users ability to make the rational choice is constrained (bounded) by his knowledge of the choice in front of him.

Mylonas et al. (2013) performed a study to determine end-user awareness around the information security of mobile devices. They found that many end-users made assumptions around the level of testing that is done on applications that are placed on official application repositories, such as the App Store (iPhones) and Play Store (Android). Most end-users incorrectly assume that security tests are done on all applications before being made publicly available. This assumption can result in end-users downloading malicious software from official application repositories (Mylonas et al., 2013). This is an example of how lack of knowledge regarding information security controls can lead to incorrectly identified threats in applications on official application repositories.

2.3.2 *Personality and preferences*

The second major theme was how the end-users personality could influence the effectiveness of information security awareness campaign. While various personality focused methodologies were used, the conventional methodology was the big five personality traits model. These studies prove that end-users tend to interpret, experience and perceive the importance of information security awareness differently based on an end-users personality (Kajzer, D'Arcy, Crowell, Striegel, & Van Bruggen, 2014; McCormac et al., 2016b; Pattinson, Butavicius, Ciccarellol, Lillie, Parsons, Calic & McCormac, 2018). These studies have highlighted the importance of how one communicates the content and importance of information security awareness.

A study by Denning et al. (2013) highlighted how communicating information security awareness training in unexpected ways could prove to be effective. Traditional information security awareness training is done using e-mail communications, posters and e-learnings. However, Denning et al. (2013) developed a board game that can be used to educate end-users on basic information security awareness themes. The study measured the effectiveness of the board game based on the end-users knowledge of information security

awareness themes after playing the game. While the game proved to be effective, the study focused solely on end-users currently involved with IT (Denning et al., 2013). Applying the same strategy on end-users who are not comfortable with IT terminology could prove ineffective.

How the importance of information security awareness training is communicated to various personality types can also impact the effectiveness of the training. Kajzer et al. (2014) point out that end-users generally expect to gain something out of the training. Whether it is for self-improvement, prevention of harm, or a new gadget, end-users need to benefit from doing the training. This thinking was echoed by Stewart and Lacey (2012), where they draw a comparison between information security awareness training and that of safety awareness training. The research draws a comparison between the two disciplines to leverage the maturity of the safety awareness field of study. While the study proved to be effective, the basis for the comparison appeared to be flawed. While both fields of study tend to provide the benefit of prevention of harm to the end-user, the one would have a higher value to the end-user than the other. The consequences of not adhering to safety awareness training could result in death or disability, while information security awareness training would result in losing your job or money. End-users would, therefore, obtain greater value from safety awareness, resulting in more effective training.

2.3.3 *Environment*

The final major theme is the environment that surrounds the end-user. Studies show that context is crucial in the effectiveness of information security awareness training (Tsohou et al., 2012; Waly et al., 2012; Yildirim, 2016). This aligns with standards and regulations that state that information security awareness training should be relevant to the end-users role and environment (Chaplin et al., 2016; Jordan et al., 2018; PCI Security Standards Council, 2016).

A study by Waly et al. (2012) highlights the difference in the environment in which end-users finds themselves, which can affect the effectiveness of the information security awareness training. The study found that information security awareness

training within the Health industry was more effective than that in Business or Education industries. Waly et al. (2012) found that end-users in the Health industry were performance-driven, and therefore received satisfaction from the training as it improved their knowledge and provided positive reinforcement. The exact opposite was found in the Business and Education industry, where end-users felt the training was ineffective, they picked up bad habits, and there was a lack of communication, feedback or motivation to complete the training (Waly et al., 2012). This shows that effective training in one environment does not guarantee success in another.

2.4 Measuring the effectiveness of information security awareness training

After analysing the research conducted, two primary measurement techniques were identified. These techniques were technical measures, in the form of metrics (number of reported phishing emails; incidents due to change, data leakage events, audit findings), and questionnaires or surveys, that test the knowledge of the end-users. These techniques are analysed separately in the sections to follow.

2.4.1 *Testing end-user knowledge through questionnaires and surveys*

Questionnaires are by far the most popular means of measuring the effectiveness of information security awareness campaigns with more than three-quarters of studies performed over the past years focusing on the designing and using a variation of a questionnaire to test end-user knowledge of information security awareness topics. Figure **2**: Count of measurement technique in varying study purpose illustrates the techniques used in varying studies (See Annexure 1: Literature Analysis for full breakdown).

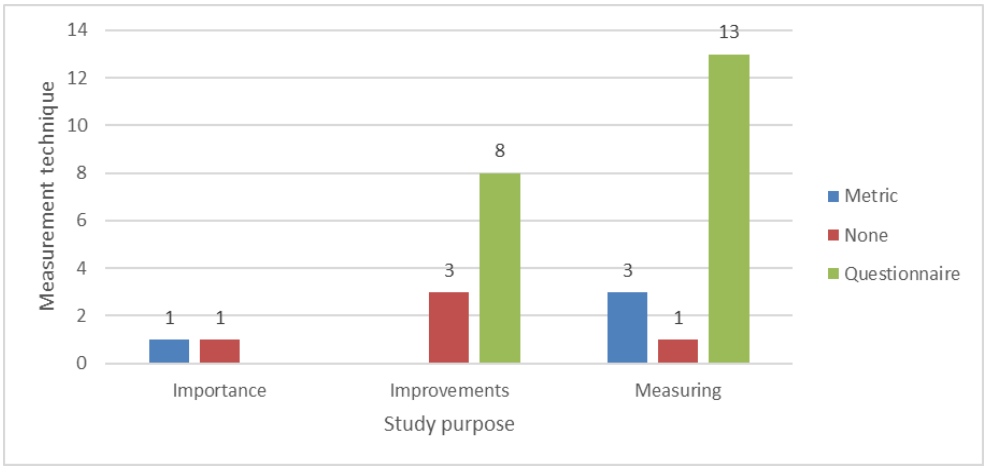


Figure 2: Count of measurement technique in varying study purpose

Few of these questionnaires are ever used again in a study, apart from the Human Aspects of Information Security Questionnaire (HAIS-Q) by Parsons et al. (2014). The questionnaire is derived from testing end-users' knowledge of information security policies and employee behaviour. The study uses this knowledge to create seven focus areas (password management, e-mail use, internet use, social networking site use, incident reporting, mobile computing, information handling), which are used to create questions to assess end-user knowledge on the topics. This results in a very long and time-consuming questionnaire.

While the HAIS-Q model has proven to be effective, the questions themselves were derived from reviewing information security policies and senior management interviews (Parsons et al., 2013). These focus areas should be grounded in research or best practice. A more defined approach is that of Poepjes (2015), who based his questions and focus areas on the ISO 27001/2 standard. Unfortunately, his study is based on the previous version of the standard, as the new standard was only released during his research period.

Additionally, Poepjes (2015) created a model that provides the implementer of an information security awareness campaign with a more structured and risk-based approach for control/topic implementation. Poepjes (2015) first collected data from IT security professionals to understand what they believe are the most critical controls within ISO 27001/2 that end-users, IT professionals and senior

management need to know. He used the data to create a benchmark value and priority list of controls. The prioritised controls are then broken down into questions, much like that of HAIS-Q, and sent to end-users, IT professionals and senior management, to test their knowledge on the controls. The data from the questionnaire (Awareness Capability) is then compared to the benchmark value (Awareness Importance) from IT security professionals, which provides the implementer of the campaign a gap analysis of expected knowledge, versus that of the groupings actual knowledge (Awareness Risk).

It is hard to criticise this approach taken by Poepjes (2015), other than the fact the standard used is out of date. Additionally, not all IT security professionals choose ISO 27001/2 as their information security framework (ISF). The implementer should rather take the theory behind the study and adapt it to their chosen ISF. Poepjes (2015) himself stated that the study could be expanded on by moving to the latest standard, as well as combing the framework with metrics indicating a change in employee behaviour.

2.4.2 *Using metrics to assess a change in end-user behaviour*

Not many studies make use of metrics to measure effectiveness, mainly because obtaining the required data from businesses has proven difficult since the owners of the data have security concerns around sharing the data (Lebek et al., 2013; Poepjes, 2015). Most studies that make use of metrics are case studies that use for simulated phishing campaigns (Aloul, 2012; Parsons, Calic, Pattinson, Butavivius, McCormac, & Zwaans, 2017; Young-McLear et al., 2016). While these studies show that end-users retain what they have learnt and have changed their behaviour, it only addressed one, albeit an important, security concern.

Rantos, Fysarakis, & Manifavas (2012) developed a set of quantitative measurements to track the effectiveness of an information security awareness training program. Their methodology is underpinned by the belief that to measure the effectiveness of an information security awareness campaign; the target audience must receive, and absorb the information. Their measurements are based on information security incidents, reports and various techniques used to

distribute information security awareness information with each technique having a hard measure to track its effectiveness. The methodology provides a weighting table that allows an organisation to adjust the weighting of each metric to align the metrics to the organisation's requirements. The goal of this methodology is to highlight a weakness in knowledge transfer, content, and the content delivery method and support structures (management support, funding, marketing, campaign management).

This methodology was expanded in 2014 to include a tool to assist in the evaluation of the measurements (Manifavas et al., 2014). The methodology itself was not expanded. The researchers demonstrated the tool in a small business of 50 employees to prove the effectiveness of the tool. The tool proved to be effective in highlighting areas for improvement.

While metrics have proven to be effective, they do not cover the same level of scope that a questionnaire can. Moreover, specifically for incident-related metrics, it is impossible to differentiate between an increase in the knowledge of end-users or a decrease in the number of attacks on the network.

2.5 Summary

While research has focused on knowledge, skill, personality, and the environment, no conclusive findings are available on how to implement an effective information security awareness campaign. Even within the themes, there is disparity and contradictions. Research shows that the knowledge and skill of the resource impact the effectiveness of information security awareness training. However, there is a divide between personality and environment which requires diverse approached. Personality-driven research recommends that training and communication should be customised to fit personality types. Environment-driven research suggests customisation of training and communications based on the environment of the end-user. One clear thing is the need for customisation of training and communications.

The effectiveness of personality-driven research is undeniable. However, it does not take the environment into account. Context is crucial in defining a feasible information security awareness campaign. Customising information security awareness training to fit varying personality types is not feasible in a large corporate environment. The implementation of information security awareness training based solely on context/environment, as stated in standards and regulations, has proven to be ineffective (Aloul, 2012; Daniel Ani et al., 2016; Stewart & Lacey, 2012). The implementation of context-aware and personality-driven information security awareness training is posited to be the most effective.

Studies show that testing end-users knowledge and metrics are useful in measuring the effectiveness of an information security awareness campaign. Although both techniques have their weak points, the questionnaire technique is more refined and well researched, while the metric approach holds promise but lacks research. However, for an all-encompassing effectiveness measurement technique, the strengths of both techniques need to be applied.

Although information security awareness is well researched, the studies focus mostly on improving training, thereby confirming its importance in an information security program, or how to implement it in a new way. Few types of research focus on measuring its effectiveness. Many of these studies are once-off and rarely expanded to further the body of knowledge. Research on measurement techniques is mainly focused on questionnaires, and as a result, questionnaires are the primary means of measuring effectiveness. However, researchers in the field state that the questionnaire technique can be improved upon by supplementing it with metrics.

3 RESEARCH METHODOLOGY

This chapter describes the philosophical stance that forms the basis of this research and the resulting research methodology. The chapter starts with a justification of ontological and epistemological approaches used in the study, followed by the research approach and research method. The chapter then guides the reader through the research process and ends with the ethical considerations of the study.

3.1 Ontology and Epistemology

Ontology refers to assumptions about the nature of reality (Saunders, Lewis, & Thornhill, 2015) and whether reality follows some order, or is ever-changing (Bhattacherjee, 2012; Saunders et al., 2015). Epistemology refers to our assumptions about knowledge (Saunders et al., 2015) and how reality is best studied and observed (Bhattacherjee, 2012).

This study supports an interpretivist view of life, which assumes that the world is complex and is continuously changed and moulded based on our interactions with each other (Saunders et al., 2015). The study adopts an interpretive epistemology for this study since it assumes that knowledge can be enriched and a better understanding of the field of study can be obtained (Saunders et al., 2015) by developing and evaluating a method for implementing an information security awareness campaign within an organisation.

3.2 Research approach

A mixed-method approach was chosen for this study, as it made use of multiple artifacts and techniques to capture data in the environment, influencing factors and sample population (Saunders et al., 2015). The artifacts and techniques were created and implemented by the study participants and therefore, cannot be considered highly structured. However, this research method, combined with an interpretivist philosophy (Saunders et al., 2015), provides a suitable approach for

the study. Data were collected in three ways. The first collection method artifacts created in Microsoft Excel to capture the responses of the IT security team in a structured manner. The second method was a questionnaire that was sent to end-users to obtain their understanding of the material given to them. The content was created from existing documents and questionnaires of the organisation. Lastly, feedback from the IT security team, concerning the model, was collected using e-mails. The IT security team was asked two questions, “In your opinion, what worked well?” and “In your opinion, what did not work well?’. Answers were returned by e-mail.

3.3 Research strategy

As the study takes place in a real-world setting and requires a close working relationship with the study participant, three potential research strategies were considered as being appropriate for the study. Namely, action research, case study and design science.

The first type investigated was action research, as the study seeks to test a theory within a real-world setting (Bhattacherjee, 2012). Of the many types of action research approaches available, canonical action research was considered as it provides an iterative process, rigorous structure and collaborative involvement of the participants with the primary goal of the study the development of the organisation and the growth in scientific knowledge (Baskerville & Wood-Harper, 1998). Action research requires the evaluation of the subject before an action is taken, the action taken, and the evaluation of the subject after the action was taken (Baskerville & Wood-Harper, 1998). This study focuses on the action itself and does not evaluate the subject before the implementation of the action.

The second strategy investigated was a case study. A case study is a point in time in-depth study within a real-world setting (Bhattacherjee, 2012; Saunders et al., 2015). While the case-study research method could provide the framework needed to conduct the study, it does not focus on the implementation and evaluation of the proposed method.

The final paradigm investigated and ultimately chosen was design science research (DSR). At the core of DSR is a problem and the development of an artifact to assist in resolving that problem (March & Smith, 1995). The second primary step is the evaluation of the artifact as an effective means for resolving the problem. Figure 3 illustrates the general design research cycle as defined by Vaishnavi & Keuchler Jr (2015), and followed in this dissertation. Problem awareness is provided in Chapter 2, with the suggestion and development presented in Chapter 4. The implementation and evaluation of the method are described in Chapter 5 and 6. The dissertation concludes in Chapter 7.

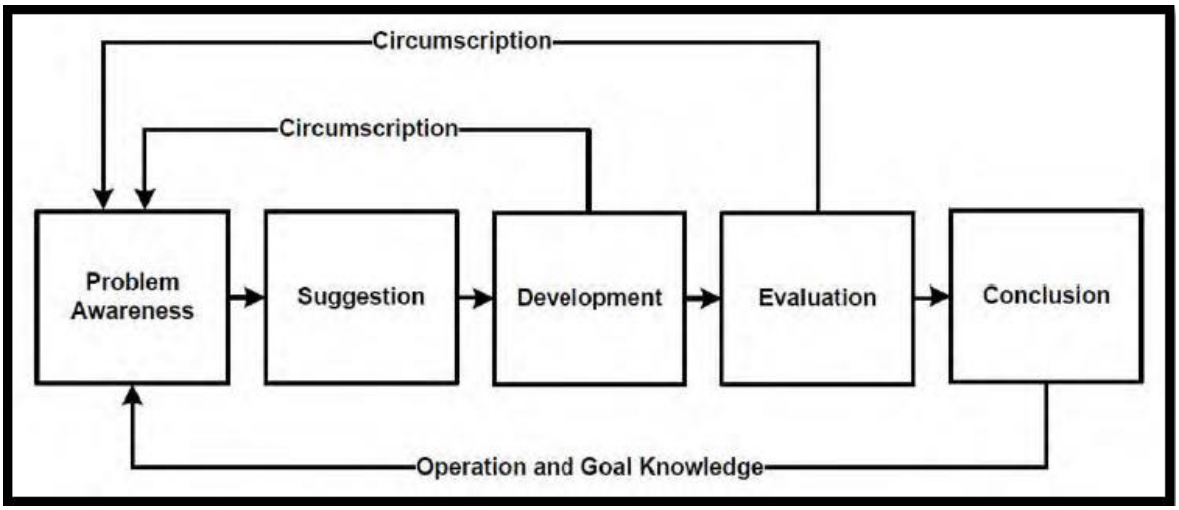


Figure 3: General design research cycle (Vaishnavi & Keuchler Jr, 2015)

March and Smith (1995) proposed four artifacts that design science research can produce, namely constructs, models, methods and instantiations. A construct is a problem defined and explained as a series of symbols and terminology (Hevner, March, Park, & Ram, 2004). Models are a grouping of statements that express a relationship between multiple constructs (March & Smith, 1995). Methods are based on constructs and models and provide a guide or process on how to arrive at a solution (March & Smith, 1995). Finally, instantiation is the final output of design science research and involves demonstrating the effectiveness of the construct, model and method (March & Smith, 1995).

This study proposes a method (artifact) for implementing an information security awareness campaign within an organisation while applying the Information Security Awareness Capability Model (ISACM) from Poepjes (2015). This is followed by evaluating the proposed method used. Design science research provided the setting required for the study, as it allowed the researcher to provide a flexible framework through which the subject of the study could assist in the study, while still conducting their business as they see fit. The learnings from the study are, therefore, more about the method used than an evaluation of the ISACM (Peopjes, 2015) or the training implemented.

3.4 Design science guidelines

Hevner et al. (2004) proposed a set of guidelines for DSR, recommending that these points are merely guidelines, not requirements, and should be used as such. Table **1**: Design science guidelines summarises these guidelines, along with how this research will cater to them.

Table 1: Design science guidelines

#	Guideline (Hevner et al., 2004)	Description	Research Overview
1	Design as an artifact	A useful artifact must be produced	A method for implementing an information security awareness campaign will be developed and evaluated.
2	Problem relevance	Research must address a problem	The research seeks to propose a method for implementing an information security awareness campaign within an organisation.
3	Design evaluation	The artifact must be tested and evaluated	Each artifact created will be tested and evaluated separately, and then lastly as a whole.
4	Research contributions	Research must provide a contribution	This will be discussed in 7.2 Research contributions.
5	Research rigour	Rigorous methods used in the construction and evaluation process of the artifact	A rigorous process for development and evaluation was used, as documented in this dissertation.

#	Guideline (Hevner et al., 2004)	Description	Research Overview
6	Design as a search process	An iterative process should be used	Each artifact created followed the same process for evaluation and testing.
7	Communication of research	Research presented coherently and understandable to a broad audience.	This dissertation seeks to meet this guideline.

3.5 Ethical considerations

Several ethical concerns were taken into consideration. The first concern was the collection or disclosure of personal information. As a result, no personal information was collected during the research. Only data that is necessary for the research was collected. The organisation asked to remain anonymous; as a result, all data collected were anonymised.

The second concern was whether or not the data can lead to the identification of an individual or definable group, as the data collected provides information on target groups defined by the organisation. This concern is reduced as these groups are defined based on the risk posture of a subset of employees by the organisation employees. Each target group is made up of multiple employees from multiple business units, across multiple regions, making identifying an individual or group from the data impossible.

The topics discussed, and controls measured are sensitive. Results from the research can indicate control weakness in employee behaviour. As a result, the organisation requested to remain anonymous.

There was a concern of influence on the participants by the researcher and the sponsor as the researcher was employed by the organisation and was directly involved in the development and implementation of an information security awareness campaign. Nevertheless, multiple business units were involved in the development and implementation of the information security awareness campaign, which dissipated any influence of the researcher.

No payments were offered to participants of the study. No racial, minority or cultural variables were used. The involvement of minors is not a concern as all participants involved with the research are employed at the organisation, and as such, are of working age.

4 METHOD DEVELOPMENT

This chapter describes a method to implement an information security awareness campaign within an organisation. The chapter starts with a summary of the Information Security Awareness Capability Model of Poepjes (2015). The chapter illustrates the method used to implement the information security awareness campaign with a description of each phase of the ISACM method.

4.1 Information Security Awareness Capability Model

ISACM (Poepjes, 2015) uses several metrics to determine what awareness campaigns need to be delivered in an information security risk environment. The metrics are Awareness Importance (AI), Awareness Capability (AC) and Awareness Risk (AR). Figure **4**: ISACM (Poepjes, 2015) illustrates the metrics within the ISACM.

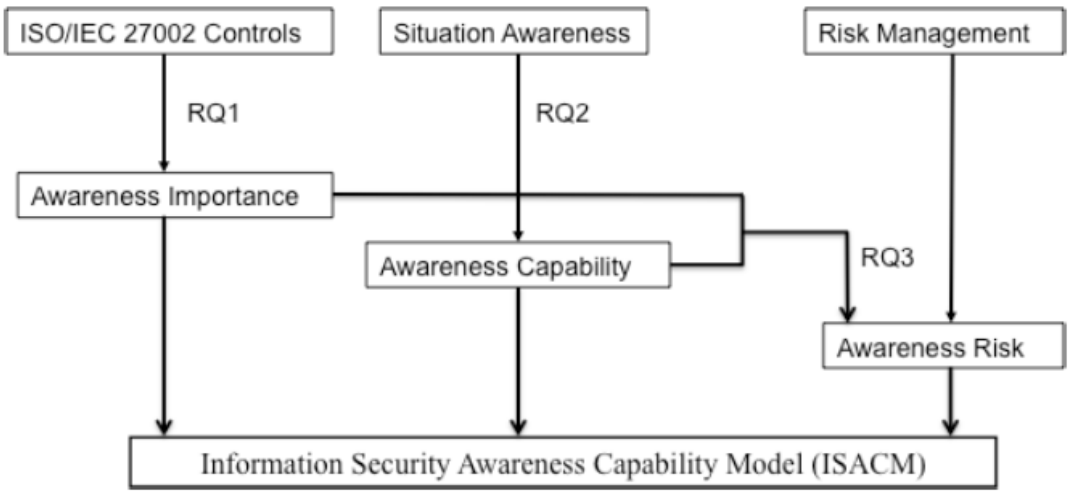


Figure 4: ISACM (Poepjes, 2015)

Awareness Importance derives from taking an information security best practice standard, extracting the controls and rating their level of importance regarding user awareness of the control within the environment. Poepjes (2015) used the ISO/IEC 27002: 2006 control framework for awareness importance.

Awareness Capability derives from surveying a random sample of the end-user base on their understanding of the various controls identified as necessary in the Awareness Importance phase. Awareness Capability can, thus, be defined as the end-users' understanding and knowledge affecting awareness controls.

Awareness Risk is calculated by applying the values obtained from Awareness Capability surveys to an awareness risk matrix. Poepjes (2015) adjusted the Standards Australia risk matrix, shown in Figure 5: Standards Australia Risk Matrix (Standards Australia/Standards New Zealand, 2009), to create an Awareness Risk matrix, as shown in Figure 6: Awareness Risk Matrix (Poepjes, 2015). The risk matrix provides an Awareness Risk rating. Awareness Risk is defined as the risk identified when comparing the users' Awareness Capability against the Awareness Importance score for each awareness control.

Likelihood						
	V	Medium	High	Very high	Very high	Very high
	IV	Medium	High	High	Very high	Very high
	III	Low	Medium	Medium	High	Very high
	II	Low	Low	Medium	Medium	High
	I	Low	Low	Low	Medium	High
		1	2	3	4	5
		Consequence				

Figure 5: Standards Australia Risk Matrix (Standards Australia/Standards New Zealand, 2009)

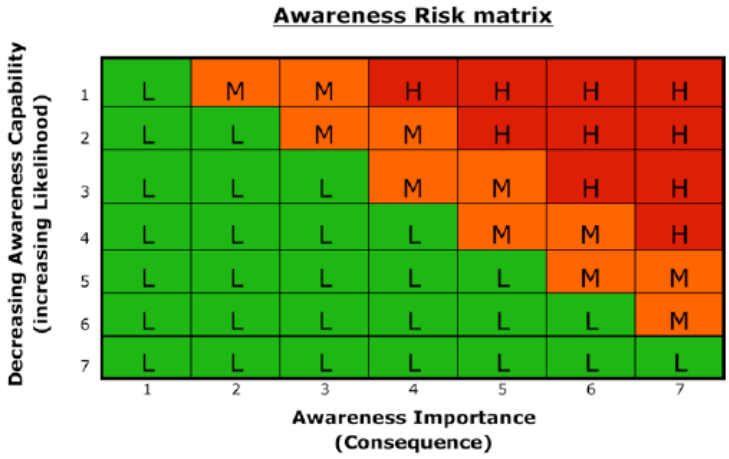


Figure 6: Awareness Risk Matrix (Poepjes, 2015)

The results of the ISACM (Poepjes, 2015) can be used to create an information security awareness campaign.

4.2 Implementation methodology

The Information Security Awareness Campaign Method (ISAC-M) depicted in Figure **7**: ISAC-M is proposed for implementing the ISACM (Poepjes, 2015). The ISAC-M method requires that the model proposed by Poepjes (2015) be adapted to the organisation environment.

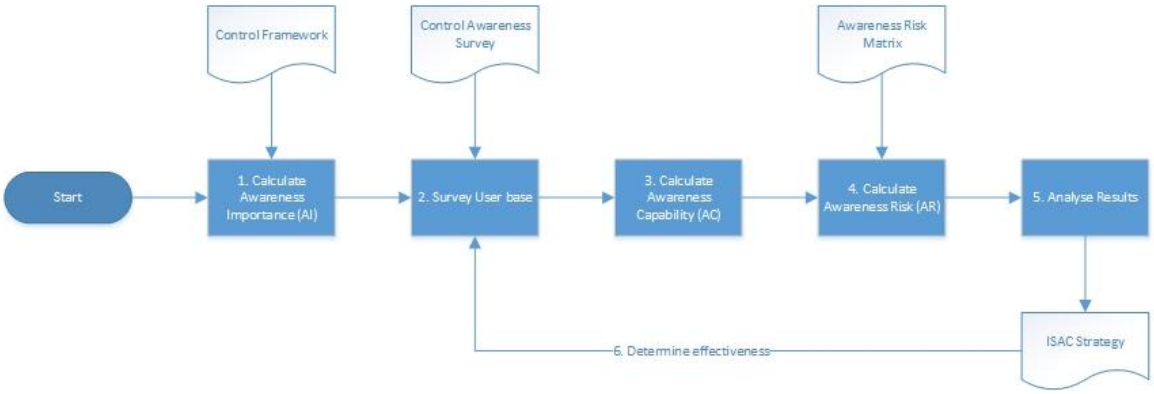


Figure 7: ISAC-M

Consequently, the following instruments need to be developed by the researcher in conjunction with the organisation personnel before starting each phase:

- Control framework – The control framework is a list of information security best practice controls. The framework must align with the ISF that the organisation use within their environment.

- Control awareness survey – The control awareness survey must be updated with a change in the control framework. At a minimum, the survey must contain questions to determine the Awareness Capability value of controls that received an Awareness Importance rating of a minimum od Moderately Important to Extremely Important.

- Awareness risk matrix – This awareness risk matrix is used to determine the Awareness Risk rating and adapted to the organisation's risk framework.

4.2.1 *Awareness Importance*

The control framework is a list of information security best practice controls which will be given to Senior Staff members of the IT security department as part of the information security awareness campaign. Each control is then rated by the IT security team to determine the Awareness Importance of each control per end-user group. The control framework incorporates the IS/cybersecurity framework of the organisation adapted from the instrument used by Poepjes (2015). NIST (2019) defines a cybersecurity framework as "a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. Includes activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes".

4.2.2 *Survey user base*

The control awareness survey is dependent on the results of the control framework. Typically, the top 10 controls that are deemed moderate to extremely important per group are used in the survey and tailored to the identified group's environment. Restricting the number of controls reduces the burden on the surveyed users. The results of the survey are used to calculate the groups' Awareness Capability.

4.2.3 *Calculate awareness capability*

The results of the survey provide an average score for each control per group. This score is used as the Awareness Capability metric. For example, for control X, a survey reports results of 10 users from group Y are 2, 3, 2, 4, 5, 2, 2, 4, 5 and 2. The scores summed, resulting in a total of 31 out of a possible 50. The

aggregated value of 31 is divided by the number of participants (10) to yield an Awareness Capability score of control X for group Y of 3.1.

4.2.4 *Calculate awareness risk*

The awareness risk matrix is applied to the organisation's environment and adapted to align with the organisation’s risk framework. This provides an awareness risk matrix that can be used to plot the Awareness Importance and Awareness Capability scores to determine the Awareness Risk for each control.

4.2.5 *Analyse results*

The Awareness Risk rating for each control is used to determine what training should be implemented in the environment per user group. The control with the highest Awareness Risk is used to compile and implement the information security awareness campaign strategy for the following training period and is then implemented by the information security team.

4.2.6 *Determine the effectiveness*

Once the training curriculum addressing the Awareness Risk has been implemented and is considered complete by the information security team, the same questionnaire that was used to measure Awareness Capability will be sent to a new sample set of users for each target group. The sample should not contain any users that were part of the original sample group. The answers from the second sample group will then compared to the awareness risk matrix. Should the user base have learnt anything from the information security awareness campaign,, their Awareness Capability score will be higher, thus, reducing the Awareness Risk score. As the Awareness Risk score of each control reduces, a new control with a higher Awareness Risk score becomes the focus for the next information security awareness campaign period.

5 APPLICATION OF THE ISAC-M

This chapter discusses the implementation of the implementation method for an information security awareness campaign within an organisation. The chapter provides a brief overview of the organisation, stating the organisation's requirements and key role players. The chapter then describes each step of the method and state how it is applied within the organisation.

5.1 Organisation overview

The organisation was required by regulation to implement information security awareness within their environment. The information security awareness campaign objective was to transform the behaviour of staff to be more security-minded. The organisation opted to align themselves with international best practices, for which they chose the Information Security Forums Standards of Good Practice (SoGP) (Chaplin et al., 2016) as their primary Information Security Framework. The responsibility of implementing training within the organisation was given to the IT security department. Within the IT security department, there were multiple security teams, including IS, cybersecurity and access control. The information security team were assigned the responsibility for implementing an information security awareness campaign on behalf of the IT security department, overseen by senior members of various teams within the IT security department who formed part of the information security awareness campaign stakeholder group. The following controls derived from best practice standards were nominated as the control objectives required from the information security awareness campaign:

- The information security awareness campaign must provide awareness and training on information risk and IS, as well as legislative and regulatory requirements of employees.

- Information security awareness training must be compulsory and conducted on an on-going basis, from date of hire and, where relevant, on transfer to a new role.
- Information security awareness training must be applicable and aligned to the end-users environment.
- All developers, testers and architects of IT solutions must attend secure development training that applies to their role.
- The information security awareness campaign must make use of multiple methods of communication for promotion and training.
- The information security awareness campaign must be endorsed by senior management and executives.
- The responsibility of the information security awareness campaign has been assigned to, and executed by the information security team, with support from the human resources employee education and marketing departments.
- The information security awareness campaign must be updated to ensure relevance and alignment to organisation requirements.
- The information security awareness campaign must be driven using a risk-based approach to ensure the relevance of training.
- The effectiveness of the information security awareness campaign must be regularly evaluated and monitored.
- The information security awareness campaign must provide relevant guidance, tools and techniques to equip staff in their environment.
- Both successful and failed security incidents should be communicated to the staff.

- The information security awareness campaign must be linked to staff performance objectives.

The organisation was required by their board of directors to deploy at least four topics per year, allowing topics to be deployed every three months at a minimum. The training was deployed in multiple ways at the organisation according to the level of training or awareness the information security team needed to implement. For structured e-learning style training, the information security team made use of a Learning Management System (LMS), which deployed the training to the end-user and tracked their progress. E-learnings were either sourced from an external supplier who is an expert on the topic or created internally by the human resource employee education department. The information security team played the role of the Subject Matter Expert (SME).

For information security topic awareness, the information security team made use of the organisation's marketing department. The marketing department provided multiple platforms on which to communicate and advertise the awareness campaign, as well as design and copyright services that ensured a single organisation style for both design and communications. External suppliers were used on occasion for design work, with a senior member of the marketing department approving the work performed by the external supplier. The information security team made use of diverse communication and advertising platforms including; Desktop Wallpapers, A4 and A3 posters in break-away areas, posts and infographics on the organisation internal social media page, e-mailers, flyers, gifts, and prizes.

5.2 Awareness importance

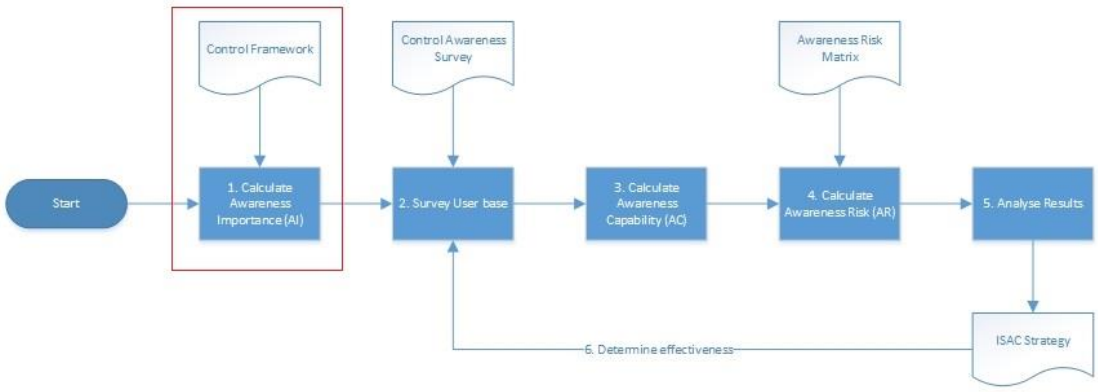
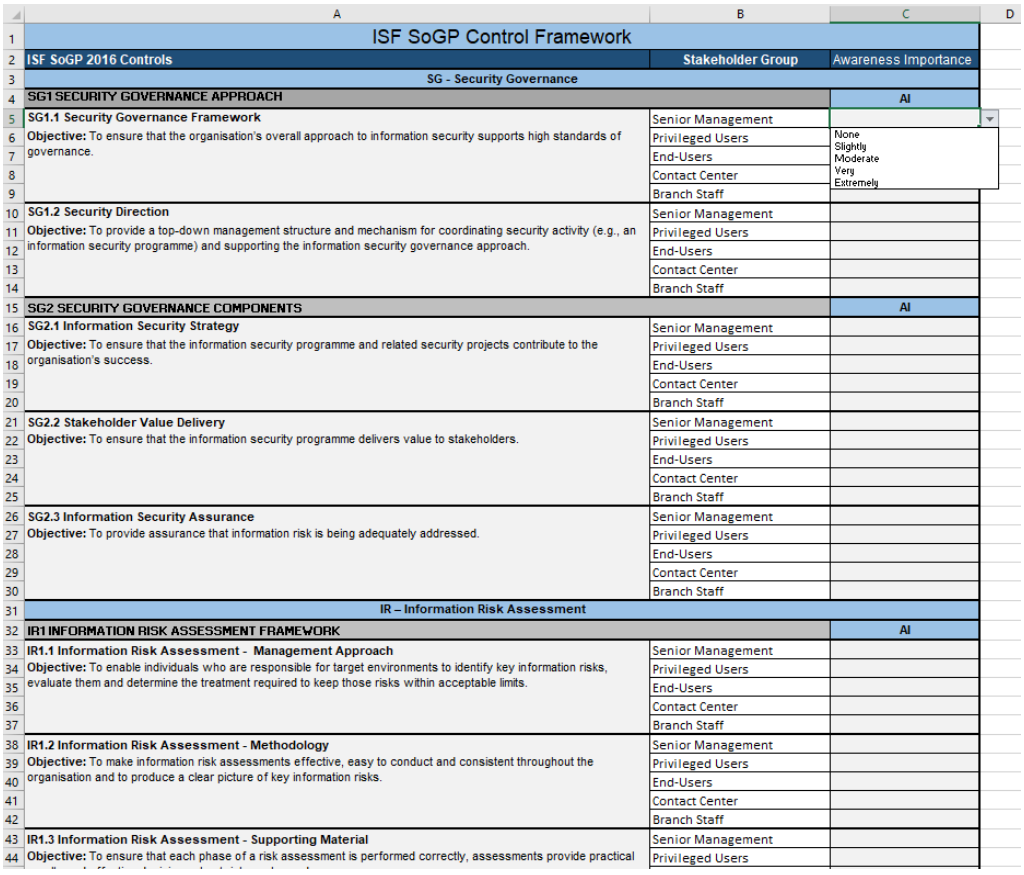


Figure 8: ISAC-M – Step 1

The control framework to measure Awareness Importance was a list of information security best practice controls which were given to senior staff members of the IT security department as stakeholders in the information security awareness campaign. The control framework aligned to the 2016 version of the SoGP (Chaplin et al., 2016), as the 2018 version (Jordan et al., 2018) was not published until later in the year. The instrument is an adaptation of the instrument used by Poepjes (2015).



	A	B	C	D
1	ISF SoGP Control Framework			
2	ISF SoGP 2016 Controls	Stakeholder Group	Awareness Importance	
3	SG - Security Governance			
4	SG1 SECURITY GOVERNANCE APPROACH		AI	
5	SG1.1 Security Governance Framework	Senior Management		
6	Objective: To ensure that the organisation's overall approach to information security supports high standards of governance.	Privileged Users		
7		End-Users		
8		Contact Center		
9		Branch Staff		
10	SG1.2 Security Direction	Senior Management		
11	Objective: To provide a top-down management structure and mechanism for coordinating security activity (e.g., an information security programme) and supporting the information security governance approach.	Privileged Users		
12		End-Users		
13		Contact Center		
14		Branch Staff		
15	SG2 SECURITY GOVERNANCE COMPONENTS		AI	
16	SG2.1 Information Security Strategy	Senior Management		
17	Objective: To ensure that the information security programme and related security projects contribute to the organisation's success.	Privileged Users		
18		End-Users		
19		Contact Center		
20		Branch Staff		
21	SG2.2 Stakeholder Value Delivery	Senior Management		
22	Objective: To ensure that the information security programme delivers value to stakeholders.	Privileged Users		
23		End-Users		
24		Contact Center		
25		Branch Staff		
26	SG2.3 Information Security Assurance	Senior Management		
27	Objective: To provide assurance that information risk is being adequately addressed.	Privileged Users		
28		End-Users		
29		Contact Center		
30		Branch Staff		
31	IR – Information Risk Assessment			
32	IR1 INFORMATION RISK ASSESSMENT FRAMEWORK		AI	
33	IR1.1 Information Risk Assessment - Management Approach	Senior Management		
34	Objective: To enable individuals who are responsible for target environments to identify key information risks, evaluate them and determine the treatment required to keep those risks within acceptable limits.	Privileged Users		
35		End-Users		
36		Contact Center		
37		Branch Staff		
38	IR1.2 Information Risk Assessment - Methodology	Senior Management		
39	Objective: To make information risk assessments effective, easy to conduct and consistent throughout the organisation and to produce a clear picture of key information risks.	Privileged Users		
40		End-Users		
41		Contact Center		
42		Branch Staff		
43	IR1.3 Information Risk Assessment - Supporting Material	Senior Management		
44	Objective: To ensure that each phase of a risk assessment is performed correctly, assessments provide practical	Privileged Users		

Figure 9: Control Framework

Figure **9**: Control Framework demonstrates the spreadsheet that was used to workshop Awareness Importance with key stakeholders.

- Column A provides the category (Security Governance), area (Security Governance Approach), topic (Security Governance Framework) and control objective (Objective) with the accompanying SoGP 2016 reference keys (Chaplin et al., 2016).

- Colum B comprises the target groups as defined by the organisation. These groups were defined by the information security personnel from the organisation.

    1. Senior management included executive management and senior leadership. The organisation included the personal assistants of these high-profile employees in this group.

2. Privileged users were users with administrative rights within the environment. Whether on their local machine (Laptops, Desktops) or Server/System side. These users were mostly IT personnel with a significant developer presence.

3. End-Users were general staff typically situated at head office. They consist of staff in departments such as finance, human resources and marketing. Most of these staff used laptops and could work remotely.

4. Contact centre staff used fixed PCs/Desktops and were not able to work remotely. Additionally, the functionality of these devices was limited. However, the information accessed by these staff members was considered highly confidential.

5. Branch staff used devices that were restricted even further. They were the primary source of the data captured within the environment, and monitoring of their behaviour was limited.

- Column C provides a drop-down list for the stakeholder to rate the Awareness Importance of the control stated in Column A, for the group in Column B. Awareness Importance was rated on a 1 to 5 ordinal scale, with 5 being the highest level of importance. These numbers were presented in a drop-down list with the following values:

  1. None – Not important
  2. Slightly – Slightly important
  3. Moderate – Moderately important
  4. Very – Very important
  5. Extremely – Extremely important

Data for the control framework was collected by the researcher, with assistance from the information security team. The target audience for the control framework were senior members of the IT security department who were stakeholders in the information security awareness campaign. By answering the control framework, these senior members provided the information security team with their

understanding of what training is vital for each target group (senior management, branch staff, privileged users, contact centre and end-users).

The data was collected by sending the control framework to each senior IT security department team member with instructions on how to complete it. Each senior IT security department team member was given two weeks to complete the task. After three months of project prioritisation sessions, the control framework was completed by all senior IT security department team members.

The tables below highlight the top 6 topics for each target group. All scores are high on the awareness risk matrix. A table is expanded in Annexure 2: ISF SoGP Control Objectives (Chaplin et al., 2016).

Table 2: Awareness Importance for Senior Management

SoGP 2016 Controls	Average Score
SM1.2 Acceptable Use Policies	4.5
PM1.1 Employment Life Cycle	4.5
PM2.2 Security Awareness Messages	4.5
IM2.2 Sensitive Physical Information	4.5
TS1.6 Information Leakage Protection	4.5
BC1.1 Business Continuity Strategy	4.5

The Awareness Importance score for senior management was similar across topics, with less than 0.1 difference between the topic scores. Most of the senior IT security staff appeared to agree on what topics were critical for senior management to know.

Table 3: Awareness Importance for Branch Staff

SoGP 2016 Controls	Average Score
IM2.2 Sensitive Physical Information	4.2
SM1.2 Acceptable Use Policies	3.8
IM1.2 Information Privacy	3.7
IM1.1 Information Classification and Handling	3.3
SA2.3 Customer Connections	3.3
IM2.1 Document Management	3.0

The Awareness Importance score for branch staff showed a clear separation in priority, with at least a 0.1 difference in score.

Table 4: Awareness Importance for Privileged Users

SoGP 2016 Controls	Average Score
PA2.1 Mobile Device Configuration	4.8
PA2.2 Enterprise Mobility Management	4.8
PA2.3 Mobile Device Connectivity	4.8
SD2.5 System Testing	4.8
SY1.2 Server Configuration	4.8
TS2.2 Cryptographic Key Management	4.8

The Awareness Importance score for senior management was similar across topics, with less than 0.1 difference between the topic scores. Most of the senior IT security staff appeared to agree on what topics were important for privileged users.

Table 5: Awareness Importance for Contact Centre

SoGP 2016 Controls	Average Score
IM2.2 Sensitive Physical Information	4.0
SM1.2 Acceptable Use Policies	3.8
IM1.1 Information Classification and Handling	3.5
NC2.2 Instant Messaging	3.5
NC2.3 Voice over IP (VoIP) Networks	3.5
IM1.2 Information Privacy	3.3

The Awareness Importance score for contact centre showed a clear separation in priority, with a small grouping of topics with a 3.5 score.

Table 6: Awareness Importance for End-Users

SoGP 2016 Controls	Average Score
PA2.5 Portable Storage Devices	4.3
SM1.2 Acceptable Use Policies	4.2
BA2.2 Protection of Spreadsheets	4.2
PA2.4 Employee-owned Devices	4.0
PM2.2 Security Awareness Messages	3.8
IM1.1 Information Classification and Handling	3.8

The Awareness Importance score for end-users showed a clear separation in priority, with two groupings of topics of 4.2 and 3.8.

5.3 Survey user base

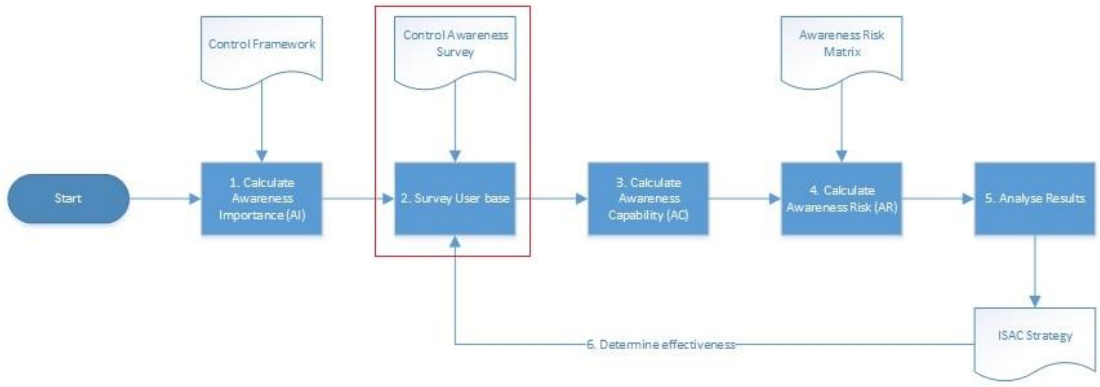


Figure 10: ISAC-M - Step 2

While the information security team were waiting for responses to their Awareness Importance control framework, the information security team started working on creating questions for the Awareness Capability questionnaire based on each topic within the SoGP (Chaplin et al., 2016). The information security team were provided with several artifacts to assist in crafting these questions that included, HAIS-Q (Parsons et al., 2014); Questionnaire guidelines; and the Awareness Importance control framework for formatting. The information security team first attempted to create Likert style questions for each topic within SoGP (Chaplin et al., 2016), which proved to be far more challenging than they expected. Much like

the questionnaire in HAIS-Q (Parsons et al., 2014), theme-specific questions are easily incorporated into Likert style questions. However, the topics presented in SoGP (Chaplin et al., 2016) were far more complex and did not allow for a Likert scale format of “strongly agree” to “strongly disagree”.

The information security team, therefore, decided to create questions that were aimed at current processes and procedures in the environment that related to the SoGP (Chaplin et al., 2016) controls. During this process, several changes occurred within the information security team, including a restructuring of the IT security department, the resignation of an information security team member assigned to developing the Awareness Capability questionnaire, and the hiring of several employees who were included in the information security team responsible for the Awareness Capability questionnaire and the implementation of the information security awareness campaign. This resulted in several delays and necessitated a rework of the questionnaire. During the disruptions within the department, the Awareness Importance data were finalised, and the department was forced to relook at their priorities and decided on the way forward. The IT security department management team rallied to analyse the results and decided on the way forward. Due to several security-related incidents and projects throughout the environment, several information security awareness topics had to be implemented as a matter of urgency. This conflicted with the topics that were identified in the Awareness Importance results. The organisation, therefore, decided to use the Awareness Importance results to define the topic for a specific target group, namely, the end-user group. Training for the remaining target groups was deferred until a more appropriate time. While this was not ideal, the risk of not performing the required training for the target groups was far too significant to ignore.

Immediately after being informed of the training decision, the information security team creating the Awareness Capability questionnaire focused on preparing the questions required for measuring the Awareness Capability of the top 10 topics (from 132) (Chaplin et al., 2016) for the end-user target group. This reduced the work significantly, and while a large amount of already completed work was no

longer required, the information security team agreed it was the best way forward. The information security team created five questions for each topic. Each question had one correct answer and three incorrect answers. The number of correct answers would, therefore, provide the information security team with the Awareness Capability score of each control for each completed questionnaire.

The information security team used the Sample Size Calculator on Survey Monkey to determine their sample size. Their total population was 749 users, which at a confidence level of 95% and a Margin of Error of 5%, resulted in a sample size of 255 users. The information security team then placed the full population into an Excel spreadsheet and created a column titled User Number. Consecutive numbers were generated for each row for the entire population, creating a unique number for each user within the population. The information security team then used RANDOM.ORG to create a list of randomly generated numbers between 1 to 749. The first 255 numbers were pasted into an Excel sheet, and a VLOOKUP formula was used to map the random number to a user to create a list of sample users for the questionnaire.

The questionnaire was populated on Survey Monkey, and e-mails sent to the sample users with a link to the survey. The sample users were given two weeks to complete the survey. After one week, the information security team found that responses were slow, and a follow-up reminder mail was sent to the sample users. The questionnaire was automatically closed by Survey Monkey after two weeks and results were sent to the information security team. A total of 47 out of 255 users completed the questionnaire. The information security team felt that this was sufficient to proceed to the next step.

5.4 Calculate awareness capability

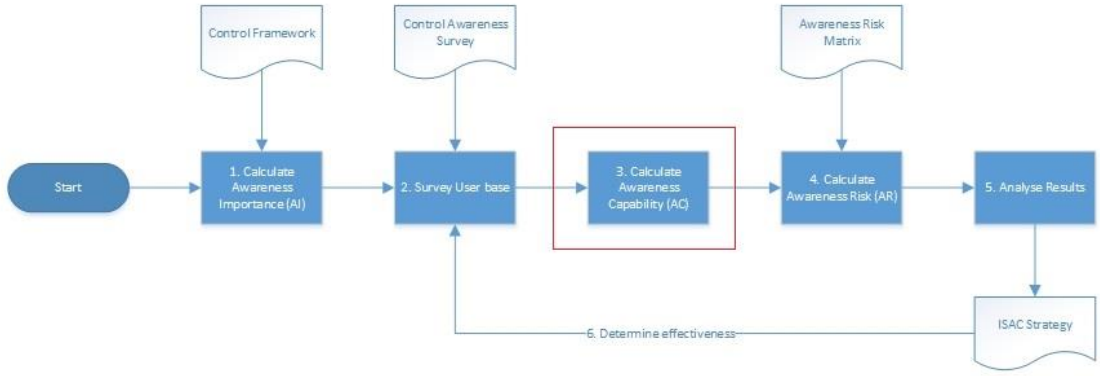


Figure 11: ISAC-M - Step 3

Table **7**: Awareness Capability for End-Users shows the average score received from the questionnaires. The scores ranged from 0 to 5. A score of 5 signified that the users answered all questions correctly and 0 meant that the user did not answer any of the questions correctly for that topic. The results revealed that the end-user target group was unfamiliar with the security controls within their day to day working environment, including information classification and handling and the processes and procedures defined in the Acceptable Use Policies.

Table 7: Awareness Capability for End-Users

SoGP 2016 Controls	Average Score
IM1.1 Information Classification and Handling	1.7
SM1.2 Acceptable Use Policies	1.9
BA2.2 Protection of Spreadsheets	2.4
PA1.2 Office Equipment	2.4
PA2.4 Employee-owned Devices	2.7
PA2.3 Mobile Device Connectivity	3.1
IM2.2 Sensitive Physical Information	3.2
PM2.2 Security Awareness Messages	3.2
IM1.2 Information Privacy	3.4
PA2.5 Portable Storage Devices	3.5

The scores in Table 6 and 7 were then mapped to the awareness risk matrix to determine the Awareness Risk score for each control.

5.5 Calculate awareness risk

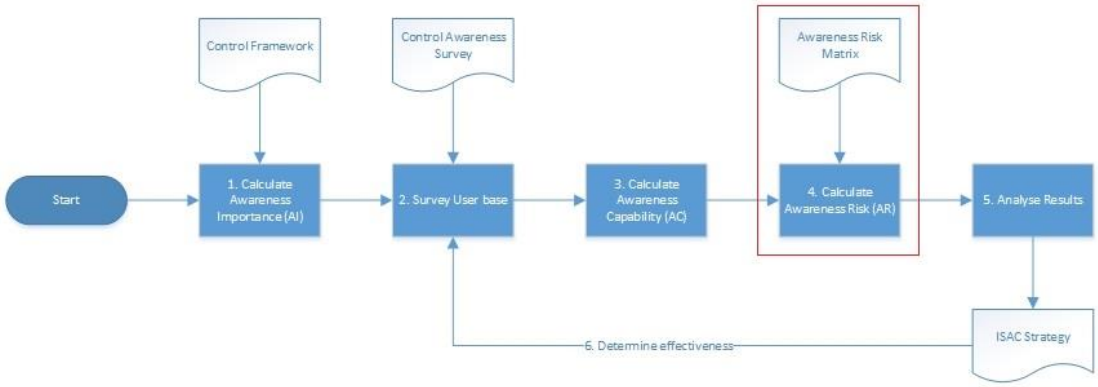


Figure 12: ISAC-M - Step 4

The awareness risk matrix applied the model by Poepjes (2015) to the organisation's environment. The organisation makes use of an organisation-wide risk framework that was developed by the risk management business unit and approved by the board of directors. The risk matrix used in Poepjes (2015) was then adapted to align with the organisation's risk framework. Figure **13**: Organisation Risk Matrix is a representation of the Risk Matrix applied to the organisation. As can be seen in the image, impact holds a higher value than likelihood, as the organisation sees any impact within the short term (3 years) as being significant enough to warrant attention.

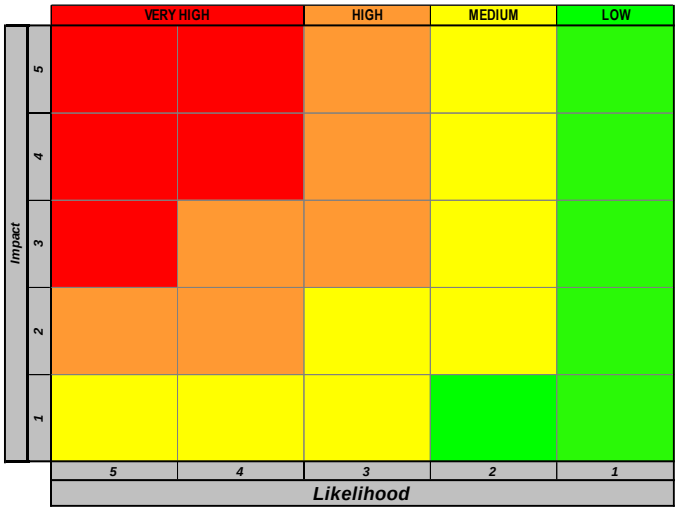


Figure 13: Organisation Risk Matrix

The strategy applied by Poepjes (2015) was then applied to this matrix. Poepjes (2015) supplemented likelihood with Awareness Capability and impact with Awareness Importance. The result is shown in the Awareness Risk Matrix in Figure **14**: Awareness Risk Matrix. The matrix was approved by the organisation stakeholders responsible for the development and implementation of the information security awareness campaign.

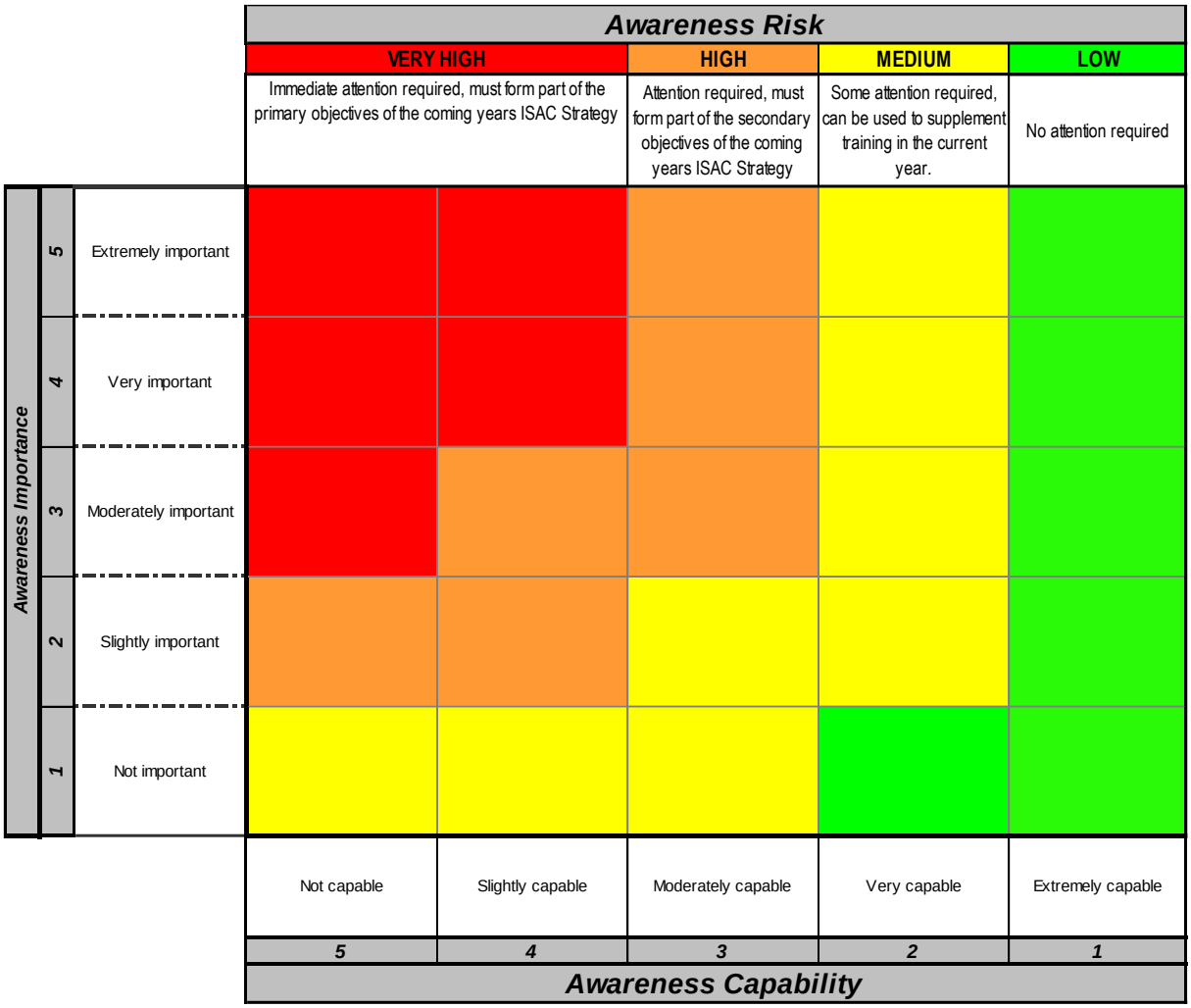


Figure 14: Awareness Risk Matrix

The result of mapping aggregated scores for Awareness Importance, and Awareness Capability for each grouping was the Awareness Risk rating for each control. The following ratings were defined to guide the information security awareness campaign strategy:

- Very High - Immediate attention required, must form part of the primary objectives of the coming year's information security awareness campaign strategy.
- High – Attention required must form part of the secondary objectives of the coming year's information security awareness campaign strategy.

- Medium – Some attention required can be used to supplement training in the current year.
- Low - No attention required

The Awareness Importance and Awareness Capability scores for the end-user target group were then mapped to the awareness risk matrix. Table **8**: End-User Awareness Risk Scoring and Figure **15**: End-User Awareness Risk mapping demonstrate the Awareness Importance and Awareness Capability mapping. The Awareness Capability score is inverted in order to map to the risk matrix. This was done by taking the highest rating and subtracting the current score. For example, “IM1.1 Information Classification and Handling” received an Awareness Capability score of 1.7, this is subtracted from the highest risk rating of 5, to give the risk matrix Awareness Capability mapping of 3.3.

Table 8: End-User Awareness Risk Scoring

SoGP 2016 Controls	AI	AC	AR
IM1.1 Information Classification and Handling	3.8	3.3	Very High
SM1.2 Acceptable Use Policies	4.2	3.1	Very High
BA2.2 Protection of Spreadsheets	4.2	2.6	High
PA1.2 Office Equipment	3.8	2.6	High
PA2.4 Employee-owned Devices	4.0	2.3	High
PA2.3 Mobile Device Connectivity	3.8	1.9	Medium
IM2.2 Sensitive Physical Information	3.8	1.8	Medium
PM2.2 Security Awareness Messages	3.8	1.8	Medium
IM1.2 Information Privacy	3.8	1.6	Medium
PA2.5 Portable Storage Devices	4.3	1.5	Medium

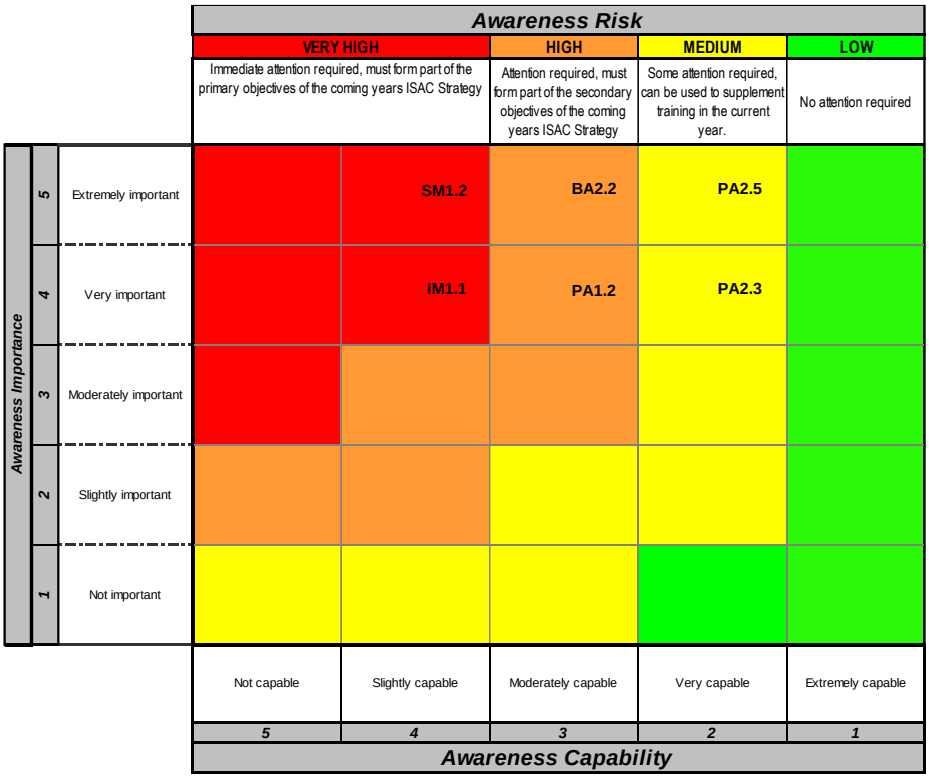


Figure 15: End-User Awareness Risk mapping

5.6 Analyse results

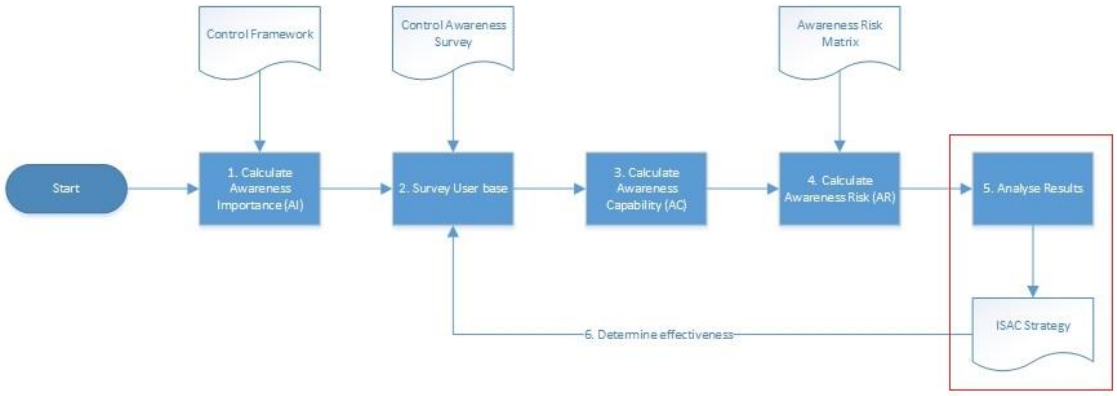


Figure 16: ISAC-M - Step 5

The results from mapping the Awareness Importance and Awareness Capability score showed that the most substantial Awareness Risk score came from the topic “SM1.2 Acceptable Use Policies” (Figure **15**: End-User Awareness Risk

mapping). The information security team agreed that this did reflect what they have suspected for a while and would use the topic for the information security awareness campaign for the end-user target group. The information security team then started on building an information security awareness campaign strategy in order to increase the end-users awareness of Acceptable Use Policies controls within the environment. The information security team had multiple discussions with vendors and departments in order to determine the best way to deliver training for this topic. Due to the topic being organisation specific, generic e-learning programs from vendors proved to be inadequate. Recommendations from the human resources employee education department within the organisation required creating a lengthy and complicated, custom-built, e-learning tool. This tool was deemed inadequate, as the information security team knew from prior training efforts, that lengthy e-learning programs did not have a high completion rate.

The information security team decided to focus on n e-mailer and marketing campaign in order to educate the end-users on the topic. The overall theme from the training was “Protect the family”, with posters and desktop backgrounds designed and created by an organisation vendor. The marketing material was used to instil a sense of responsibility in employees and alert them of pending training initiatives. The information security team then created a series of e-mailers that were sent out every two weeks for eight weeks, each tackling a different section of the Acceptable Use Policies. The e-mailers carried a similar design to that of the marketing material, with the content limited to a few short paragraphs. Unfortunately, examples of the material could not be illustrated, as the design and content of the material would negate the requested anonymity of the organisation.

5.7 Determine the effectiveness

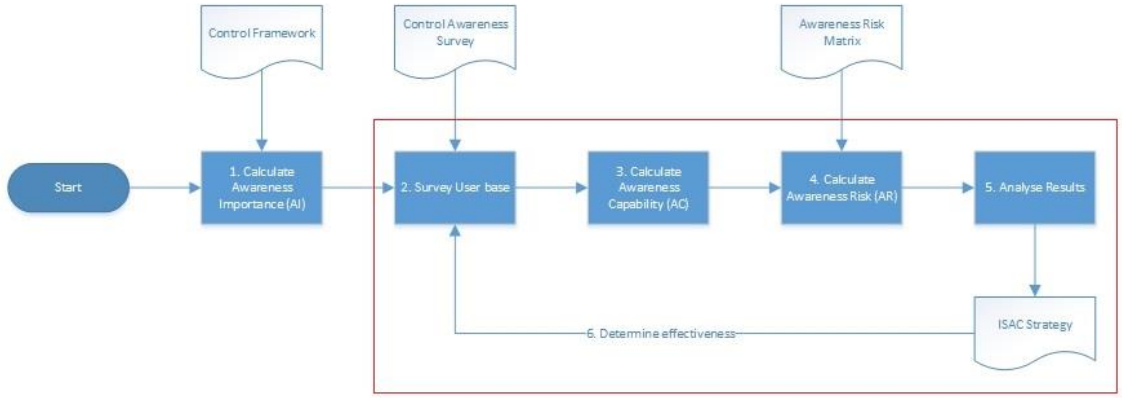


Figure 17: ISAC-M - Step 6

Once the information security team had deployed the training to their satisfaction, the questionnaire and email used in “5.3 Survey user base” was sent to a further 255 respondents. Respondents were given three weeks to complete the survey with a reminder e-mail sent a week before the final closure date. A total of 36 out of 255 users completed the questionnaire. The information security team felt that this was sufficient to proceed to the next step.

Table **9**: Average score before and after training shows the average score received from the questionnaire for before and after the training. The score ranged from 0 to 5. A score of 5, meant that the users answered all questions correctly and 0, meant that the users answer none of the questions correctly for that topic. The results showed a slight increase in the user’s knowledge of the security controls within their day to day working environment.

Table 9: Average score before and after training

SoGP 2016 Controls	Average Score Before Training	Average Score After Training
SM1.2 Acceptable Use Policies	1.9	2.5

The original Awareness Importance and post-training Awareness Capability score for the end-user target group were mapped to the awareness risk matrix. Figure **18**: Awareness Capability move after training illustrates the Awareness Importance and Awareness Capability mapping for before and after training. The Awareness Capability score was inverted for mapping to the risk matrix. This was done by taking the highest rating and subtracting the current score. There was a clear move of Awareness Capability to the right, decreasing the Awareness Risk from very high risk to high risk.

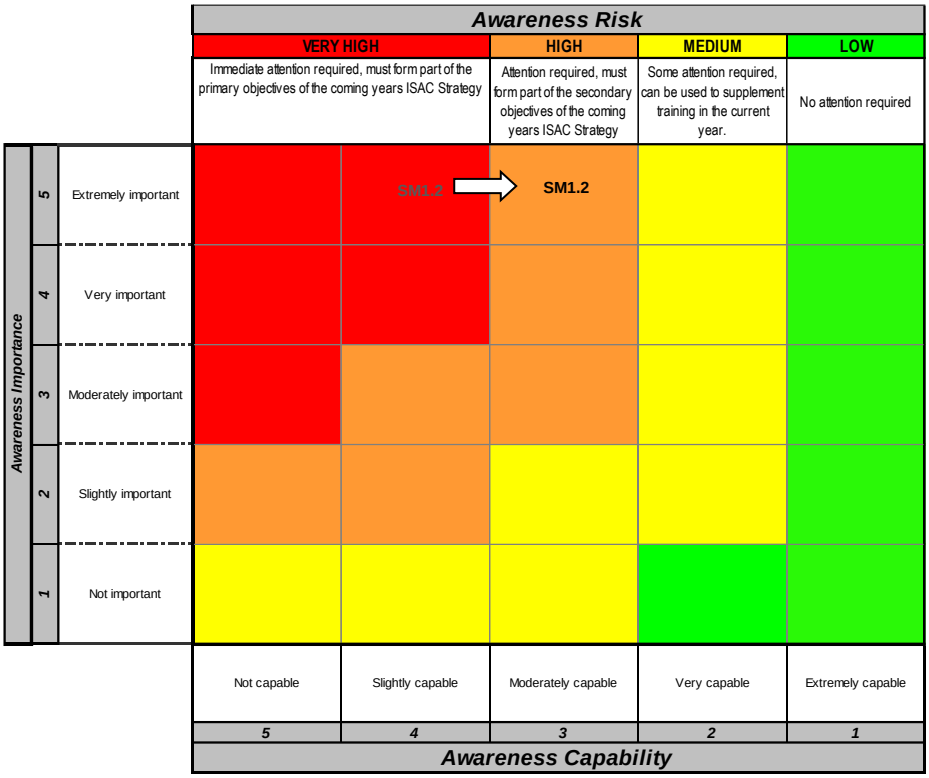


Figure 18: Awareness Capability move after training

5.8 Summary

The implementation of the ISAC-M took ten months, from the development of the control framework to measuring the effectiveness of the information security awareness campaign. This appeared excessive as it resulted in an information security awareness campaign that lasted only three months and produced a marginal reduction of an Awareness Risk score from very high to high. However,

many of the artifacts created were reuseable and refined for future implementations within the organisation. Reusing the artifacts can reduce the time taken should the organisation use the ISAC-M again. Chapter 6 will evaluates each step of the ISAC-M.

6 EVALUATING THE ISAC-M

This chapter evaluates each step of the proposed method based on the implementation discussed in Chapter 5. The chapter concludes with a summary and evaluation of the complete method. Each step within the method has a colour rating. The colours red, amber, green represent the steps in the method that worked well (green), worked with limitations (amber) and those that need critical attention (red). Comments from the IT security team members are used to substantiate the observations.

6.1 Awareness importance

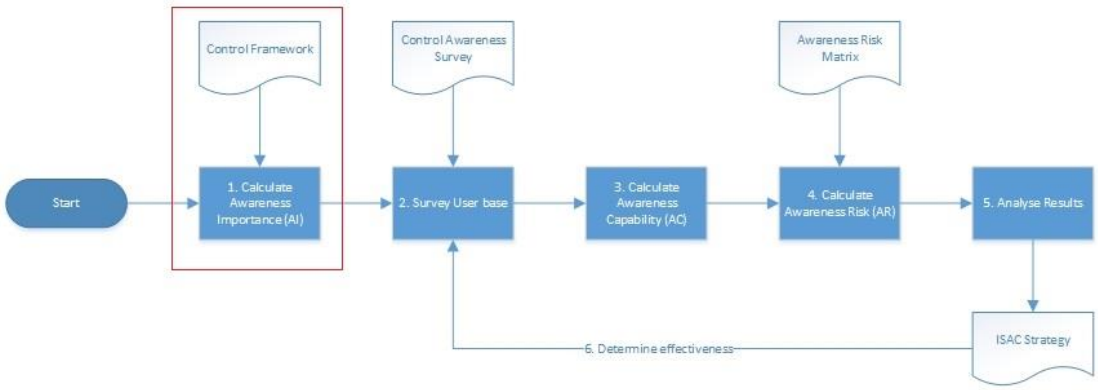


Figure 19: ISAC-M - Step 1

6.1.1 *The control framework*

Using the organisation's ISF proved to be useful. The IT security staff were familiar with the topics and controls within the framework with only one of the six staff stating that they were unfamiliar with the content (Figure 20). However, some of the participants found it challenging to interpret controls within the context of specific groupings (Figure 20). All the same, most of the controls within the framework were implemented.

The translation of the ISF standard into a questionnaire was detailed and comprehensive (Figure **21**: Positive comments on AI) although determining Awareness Importance proved to be difficult Each staff member interpreted the importance and impact of each control differently, as can be seen in Figure 20. Additionally, the length of the control framework proved to be a challenge and resulted in slow response rates due to the amount of time required to complete the Awareness Importance rating survey. One participant stated, *"Although comprehensive, it was long and therefore tedious to complete"*.

There seemed to be a difference of opinion about the grouping of stakeholder groups. One participant stated that *"The one thing that really worked well was using the ISF framework to map out areas that needs to be addressed in the different classes of users. Identifying the user classes and applying what is relatable for them from the ISF framework ensures that all the areas are covered for the correct audience."* Another participant stated that the groupings were inaccurate, *"There should only be a grouping of three user categories – Senior Management, Privileged users and End-Users. I think although only certain controls might be applicable to certain environments or grouping of users in a certain ORG (organisation) structure it is imperative that the business users as a whole should be made aware of all kinds of risks and attacks a business might face."*

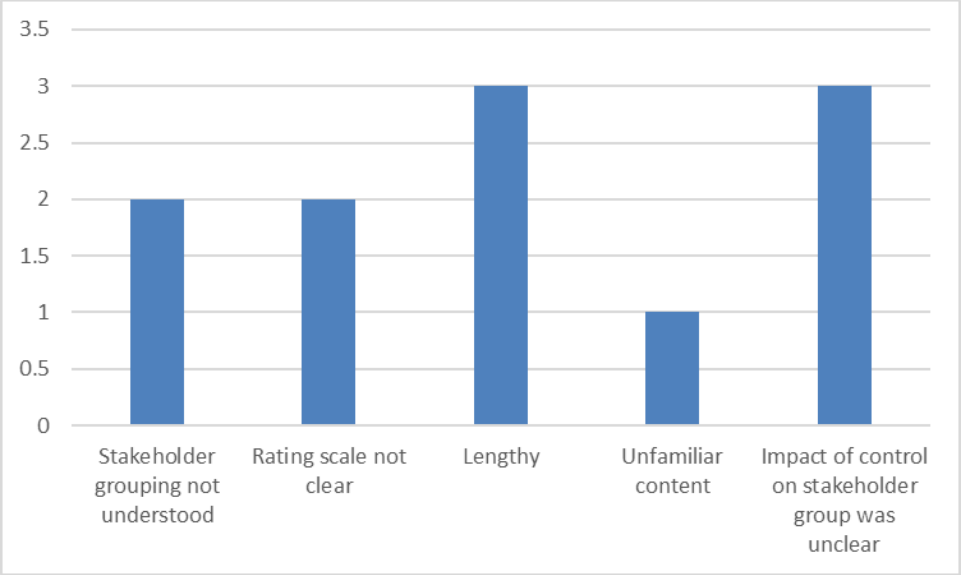


Figure 20: Negative comments on AI

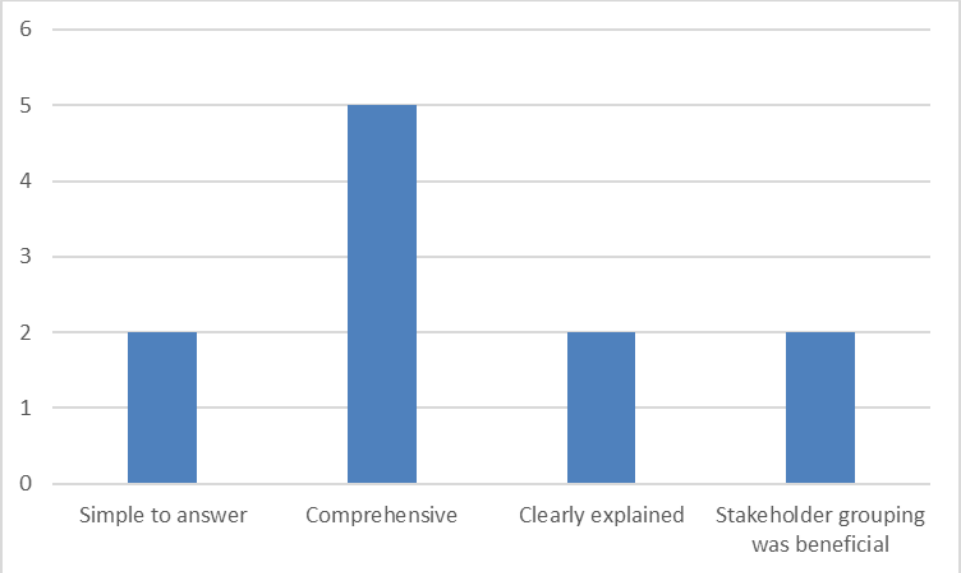


Figure 21: Positive comments on AI

6.1.2 *Awareness importance scores*

Notable points from the Awareness Importance scores are indicated and summarised in

Table 10: Awareness Importance Scores and Figure **22**: Awareness Importance scores for the top 21 controls. Privileged Users received the highest Awareness

Importance score of 4.8. This shows the IT security departments focus on the importance of educating privileged users. Senior management received the second-highest score (4.5). Except for privileged users, all other target groups focussed chiefly on data protection related controls. The most common control, appearing in 4 of the five groups, was Acceptable Use Policies. Sensitive physical information and information classification and handling where the next most common, appearing in 3 of the five groups. The control with the highest total score (16.3) was Acceptable Use Policies. Sensitive physical information (12.7) and information classification and handling (10.6) followed at second and third most significant.

Table 10: Awareness Importance Scores

	Senior Management	Branch Staff	Privileged Users	Contact Center	End-Users
BA2.2 Protection of Spreadsheets					4.2
BC1.1 Business Continuity Strategy	4.5				
IM1.1 Information Classification and Handling		3.3		3.5	3.8
IM1.2 Information Privacy		3.7		3.3	
IM2.1 Document Management		3			
IM2.2 Sensitive Physical Information	4.5	4.2		4	
NC2.2 Instant Messaging				3.5	
NC2.3 Voice over IP (VoIP) Networks				3.5	
PA2.1 Mobile Device Configuration			4.8		
PA2.2 Enterprise Mobility Management			4.8		
PA2.3 Mobile Device Connectivity			4.8		
PA2.4 Employee-owned Devices					4
PA2.5 Portable Storage Devices					4.3
PM1.1 Employment Life Cycle	4.5				
PM2.2 Security Awareness Messages	4.5				3.8
SA2.3 Customer Connections		3.3			
SD2.5 System Testing			4.8		
SM1.2 Acceptable Use Policies	4.5	3.8		3.8	4.2
SY1.2 Server Configuration			4.8		
TS1.6 Information Leakage Protection	4.5				
TS2.2 Cryptographic Key Management			4.8		

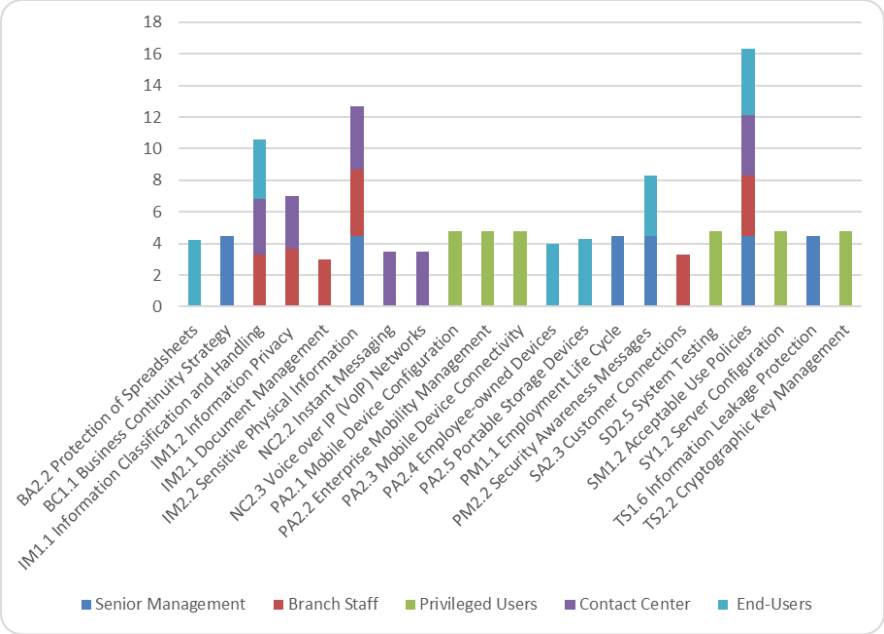


Figure 22: Awareness Importance scores for the top 21 controls

6.1.3 *Awareness Importance summary*

Even though the creation of the control framework from the organisation's chosen ISF was successful, and the resulting scores provided the intended view and benefit, issues were observed. The size of the framework resulted in a lengthy template, which took time to complete. With the SoGP (Chaplin et al., 2016) being updated every two years, the control framework would need to be updated at least every two years. However, the Awareness Importance responses must be done more frequently since the risk profile of groupings may change based on new technologies or risks in the environment.

Additionally, participants had varying degrees of understanding about the SoGP (Chaplin et al., 2016) controls. While the information security team believed that all IT security department team members were familiar with the standard, some participants struggled to understand the control, how one control differentiates from another, and how the control changes and applies according to the stakeholder group.

A suggestion for improving this step would be to map the information security awareness control groups to the ISF. For example, controls such as data protection controls were grouped by the respondents and received similar Awareness Importance scores. This would allow for a natural grouping of controls under an information security control named Data Protection. This control could represent all data protection controls, allowing for one control to supplement many of the smaller controls. This will not only shorten the length of the control framework but allow for more control variety within the various information security awareness campaigns throughout the year. Additionally, this will provide a single information security awareness campaign with multiple topics with each information security control broken into smaller ISF controls, and make it easier to incorporate other ISFs to the proposed method. The grouped controls would also allow for a more generic definition of each control, making it easier for participants unfamiliar with the ISF of the organisation to answer the control framework.

As the control framework worked but could use improvement, it is highlighted in amber in Figure **23**: ISAC-M - Step 1 evaluation. Calculate Awareness Importance is highlighted as green, as the step works well but is highly dependent on the control framework input. An improvement in the control framework could improve the results of the Awareness Importance calculation.

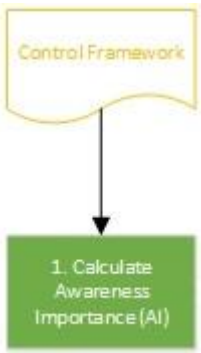


Figure 23: ISAC-M - Step 1 evaluation

6.2 Survey user base

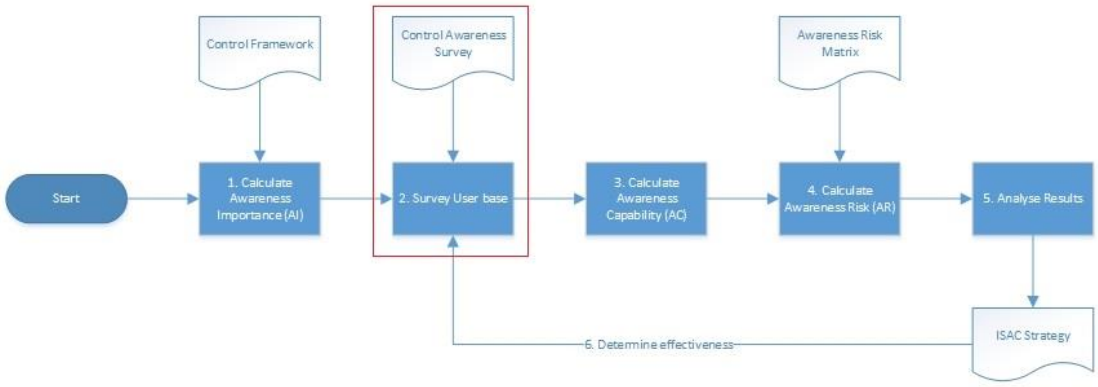


Figure 24: ISAC-M - Step 2

6.2.1 *Control awareness survey*

Using the results from the Awareness Importance questionnaire to build a questionnaire targeting the end-users proved challenging. The mapping of the ISF controls to general information security awareness questions or previously used questions from academic papers was almost impossible. This resulted in the information security team having to create the questions, as opposed to relying on past research. While the time taken to build this questionnaire took far longer than expected, the resulting questions can be used again with minimal rework. The more focused approach of using the controls that were deemed significant from the Awareness Importance scores proved to be the correct method, as creating questions from the control framework would have taken significantly longer.

6.2.2 *Surveying the user base*

While the method used to survey the user base was not perfect, it was reflective of standard practices within the organisation. Using the tools and methods the information security team were familiar with, allowed for a quick transition from creating questions to the sample user base receiving the questions. Although the information security team was happy with the low number of respondents, from a

reliability and validity perspective, there were concerns for the ability to extrapolate a view that could statistically represent the group.

The questions were easily understood by the target group, and the information security team felt the results accurately represented the environment. One participant stated, *"Looking at what did not work well, I will be speculating a bit and scraping the bottom of the barrel here. The amount [sic] of questions posed to the users might have been just that little too much."* This may have been the reason for the small number of respondents.

6.2.3 *Survey user base summary*

While this step was plagued with several difficulties and outside factors experienced by the information security team, the team obtained results with which they were comfortable. The disruptions experienced in the department reduced the amount of time available to the information security team, resulting in this step getting less attention than it deserves. The questions were questionable as no testing was done on their reliability. However, the survey's was easily understood by the participants.

A suggestion for improving this step would be to collate questions used in earlier studies and relate them to the high-level control groups suggested in 6.1.3. This will increase the reliability of the questions and may reduce the number of questions, which could increase the number of responses. Additionally, a different survey mechanism might increase the number of respondents, for example, a physical survey handed out after meetings or a reward for completing the survey.

As the reliability of the questions is questionable, it is highlighted as red in Figure **25**: ISAC-M - Step 2 evaluation. Survey User Base is highlighted as amber since the techniques used to survey the user base can be improved in order to gain a higher response rate. Improving these two steps will significantly improve the reliability of the data.

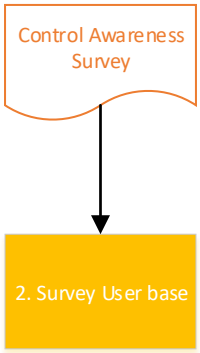


Figure 25: ISAC-M - Step 2 evaluation

6.3 Calculate awareness capability

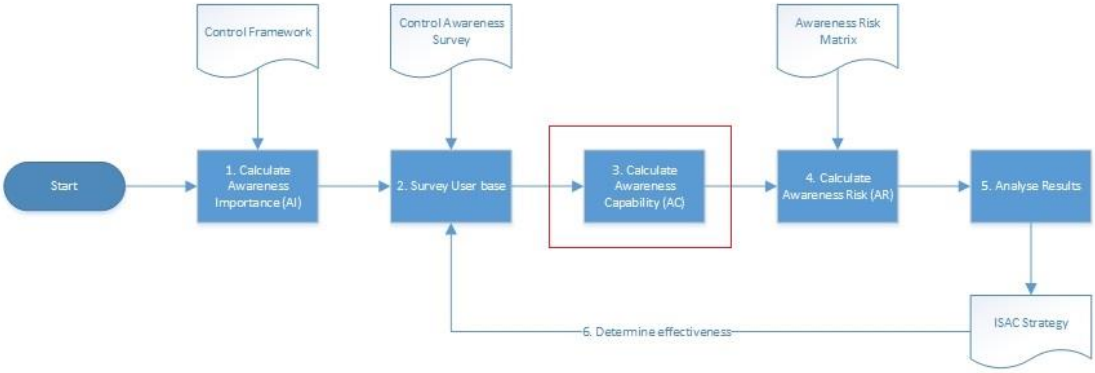


Figure 26: ISAC-M - Step 3

6.3.1 *Calculating awareness capability*

Calculating the Awareness Capability score from the survey results was easily performed by the information security team. The information security team felt the results were a true reflection of the environment with one member of the information security team stating, *"The one thing that really worked well was using the ISF framework to map out areas that needs to be addressed in the different classes of users. Identifying the user classes and applying what is relatable for them from the ISF framework, ensures that all the areas are covered for the correct audience."*

6.3.2 *Calculate awareness capability summary*

This step worked well and was implemented without any issues. As a result, this step has been highlighted as green in Figure **27**: ISAC-M - Step 3 evaluation. However, an improvement in the previous steps could increase the accuracy and reliability of this step.

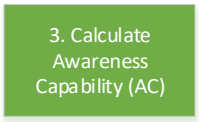


Figure 27: ISAC-M - Step 3 evaluation

6.4 Calculate awareness risk

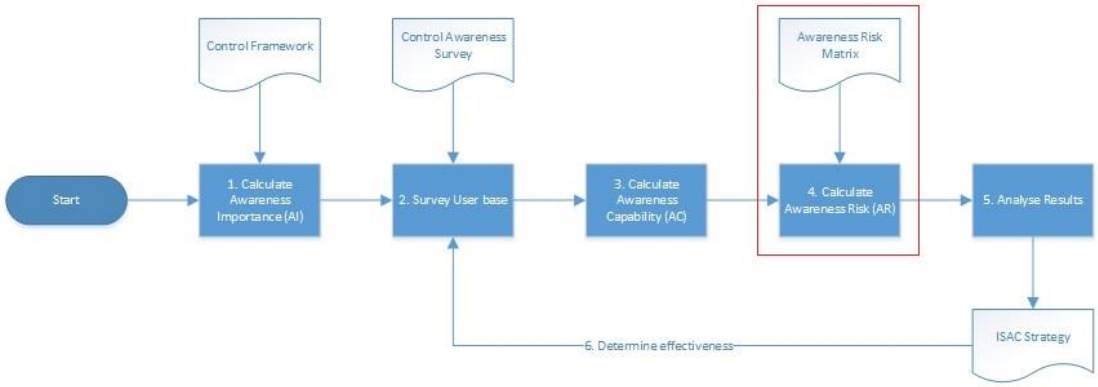


Figure 28: ISAC-M - Step 4

6.4.1 *The Awareness Risk Matrix*

The information security team adjusted the organisation's risk matrix to create an awareness risk matrix. Their understanding of both risk management practices and how the impact and likelihood mapped to importance and capability came easily to them, making the development of the awareness risk matrix a quick and efficient task.

6.4.2 *Calculating Awareness Risk*

The plotting of the results of the Awareness Importance and Awareness Capability questionnaire provided a very effective means of illustrating the Awareness Risk within the environment. Unfortunately, the 5x5 risk matrix resulted in groups of Awareness Risks, requiring the information security team to revert to the raw data to determine the highest Awareness Risk. Additionally, the awareness risk matrix required the original Awareness Capability score to be inverted in order to map to the awareness risk matrix. While this did not affect the results of the Awareness Risk score, it was an unnecessary complication in an otherwise well-developed step.

6.4.3 *Calculate Awareness Risk summary*

Even with the small complications, such as inverting the Awareness Capability score and reviewing the raw data to determine the highest risk between similarly scored controls, this step worked well. The information security team appreciated the visual representation of the Awareness Risk within the environment. As with other risks in their environment, it allowed them to demonstrate risks to a broader audience in an easy to understand format. As a result, both steps have been highlighted as green in Figure **29**: ISAC-M - Step 4 evaluatio.

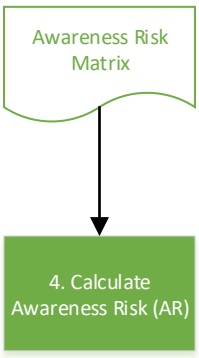


Figure 29: ISAC-M - Step 4 evaluation

6.5 Analyse results

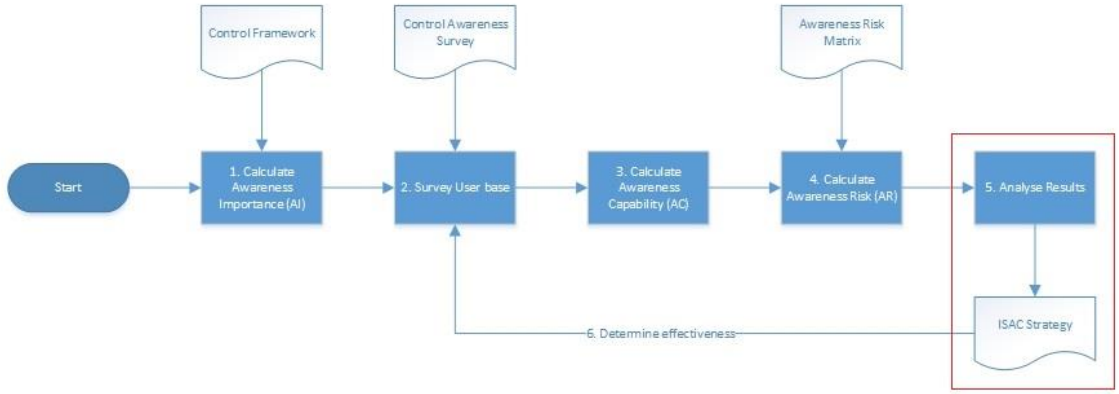


Figure 30: ISAC-M - Step 5

6.5.1 *Analysing the results*

The visual representation of the Awareness Risk within the environment made identifying the required training very easy. The information security team felt that it was a true reflection of the current environment, with one member of the information security team stating, *"One could gain a true direction for awareness training within an organisation".*

6.5.2 *Building the information security awareness campaign strategy*

This step proved to be challenging due to the nature of the topic chosen. As the topic focused on Acceptable Use Policies, the training needed to be customised to the local environment making it impossible to use generic training from a third party irrespective of how proficient they are in the topic. This required the information security team to develop their content and decide on the method to deploy the training. While the content was straightforward for the team to come by since it was derived from company policy, deciding on the method to deploy the training was not as easy. The chosen method was a series of e-mails supported by a marketing campaign.

6.5.3 *Analyse results summary*

Although this step went smoothly for the information security team, there were concerns regarding the method used to deploy the training. While e-mailers are a valid mechanism for deploying awareness training, the choice was based on information security team opinions and experience and not based on research data. The information security team could benefit from previous research, such as that done by Pattinson et al. (2018), to determine the best method of training for the diverse end-users.

As the results of the Awareness Risk scoring was easy to determine, analysing results is highlighted as green in Figure **31**: ISAC-M - Step 5 evaluation. Information security awareness campaign strategy, however, is highlighted as amber since the information security team believed it was appropriate and that it met their requirements, even though the training method was questionable.

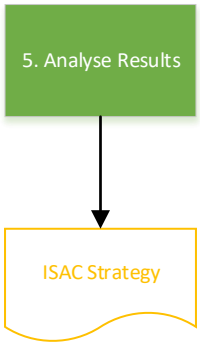


Figure 31: ISAC-M - Step 5 evaluation

6.6 Determine the effectiveness

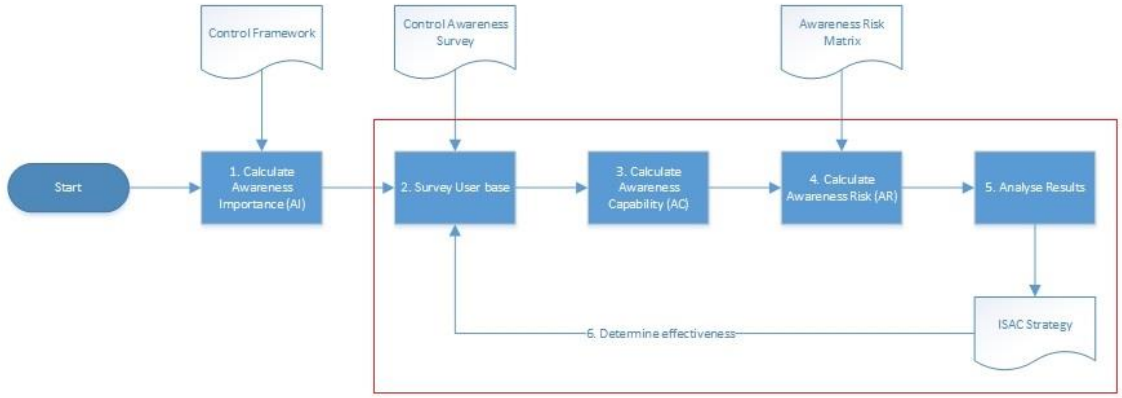


Figure 32: ISAC-M - Step 6

6.6.1 *Re-performing steps 2 to 4*

Re-performing the survey, as well as calculating the new Awareness Capability and Awareness Risk scores, was done significantly faster than many of the other steps. The artifacts created at the start of the method made this step particularly efficient.

6.6.2 *Analysing the results*

The reduction of the Awareness Capability of the target group from very high to high proved to be any practical illustration of the effectiveness of the implemented training. The information security team believed that, although the method used to train the staff was not the most effective, the downward move was an accurate view of the effectiveness of the information security awareness campaign, and they were therefore pleased with the results.

6.6.3 *Determine effectiveness summary*

This step was plagued by weaknesses experienced throughout the method. Several of the data collection points required improvement and refinement in order to improve the accuracy of determining whether the information security awareness campaign was effective or not. Despite the questions around the accuracy of some data points, the method did prove valuable to the information security team, and as a result, determining effectiveness is highlighted as amber in Figure **33**: ISAC-M - Step 6 evaluation.

Figure 33: ISAC-M - Step 6 evaluation

6.7 ISAC-M evaluation summary

Figure **34**: ISAC-M evaluation illustrates the evaluation of the complete method used in the study. The colours represent the steps in the method that worked well (green), worked but with weaknesses (amber) and those that need some serious attention (red). As can be seen in Figure 34, most of the method worked as intended, although some data collection points need refinement in order to improve the accuracy and reliability of the results.

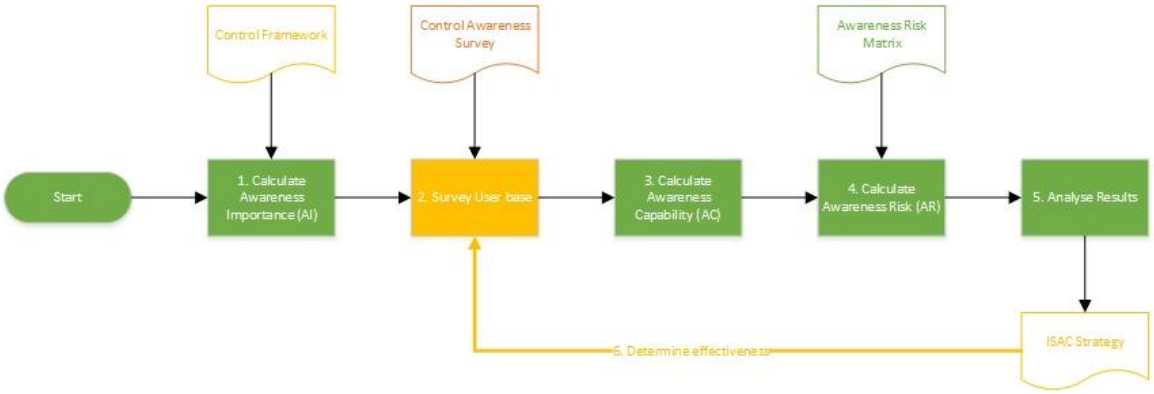


Figure 34: ISAC-M evaluation

By refining the control framework in the first phase of the method, the time taken to collect data and maintain these artifacts can be significantly reduced, resulting in a faster process and less of a burden on participants in collecting both Awareness Importance and Awareness Capability data.

The information security team should make use of tried and tested questions to improve the reliability of the control awareness survey or enlist the expertise and experience of industry subject matter experts to develop and refine the questions. Additionally, subject matter experts can be used to assist in finding the optimal method for deploying training to the various groups of users.

7 CONCLUSION

To conclude the research, the general design cycle by Vaishnavi & Keuchler Jr (2015), depicted in Figure 3, is used to guide a summary through the DRS process.

The primary objective of this study was to define and test a method for implementing an information security awareness campaign within an organisation. The dissertation established *problem awareness* by providing an overview of the problem it seeks to address, followed by a review of current literature and academic studies in the field of information security awareness. The review showed that two major themes were prevalent in current studies, namely factors that influence the effectiveness of training and techniques of measuring the effectiveness of training. However, no studies attempt to provide a method for implementing information security awareness.

The dissertation *suggested* a means for resolving this paucity by proposing the implementation of the ISAC-M to deploy an information security awareness campaign, using prior research as its foundation. The *development* of the ISAC-M is presented, with each step and artifact within the ISAC-M explained. The ISAC-M was implemented within an organisation with detailed results and documentation for each step of the method.

Finally, the study *evaluated* the ISAC-M, with both positive and negative results observed in using the method. After evaluating each step of the method, an evaluation was done on the entire method, and although many improvements can be made, it was found to be adequate as it achieved the required objective in the organisation.

The following sections *conclude* the study by reflecting on the study and highlighting the contributions it has made to the field of study, the limitations of the study and recommendations for future research.

7.1 Research reflections

7.1.1 *Methodological reflection*

The interpretivist stance proved to be the correct choice as its flexibility allowed the organisation to conduct their business and change priorities without impacting the research from achieving its objective. The multi-method approach was practical, as it helped substantiate and validate many of the opinions expressed by the organisation staff members during the study.

The design science research paradigm was suitable for the research in its current context; however, an action research approach with more significant change throughout the target groups within the organisation and a longer time frame to observe changes could have provided higher value. A canonical action research approach would provide the study with an iterative process, rigorous structure and allow collaborative involvement from participants (Baskerville & Wood-Harper, 1998). As action research requires the evaluation of the subject before an action is taken, an action being taken, followed by the evaluation of the subject after the action was taken (Baskerville & Wood-Harper, 1998), a larger time frame for study would be required.

The ISACM (Poepjes, 2015) was found to be effective; however, the results could be more reliable if the organisation staff used academic research to create the artifacts used in the study. For example, HAIS-Q (Parsons et al., 2014) that have been substantiated in multiple studies (McCormac, Calic, Parsons, Zwaans, Butavicius, & Pattinson, 2016; Parsons et al., 2017) and provides questions with greater integrity and validity. A simple factor analysis on the questions used in Awareness Importance would have allowed the organisation staff to adjust the questions before sending to the target group, thereby providing more integrity to the results obtained.

7.1.2 *Substantive reflection*

Other than the fact that the research makes use of the framework by Poepjes (2015), the research is similar to those discussed in the literature review. The context of the organisational environment provided a substantial impact on the research, as echoed in other studies (Tsohou et al., 2012; Waly et al., 2012; Yildirim, 2016). This can be seen in the Awareness Capability artifact where answers and opinions varied based in the organisation staff member. Also, the organisation adjusts training to the target groups based on their risk profile. This not only validates the interpretivist stance of the study but elaborates on the difficulties experienced by many studies due to the complexity of working within a real-world setting (Tsohou et al., 2012; Waly et al., 2012; Yildirim, 2016).

Despite the study collecting and creating many metrics, the data is still based on the results from questionnaires. This is the primary means of obtaining data and is reflected in many studies (McCormac et al., 2016a; 2016b; Parsons et al., 2017; Parsons et al., 2014). Collecting data in other ways has proven difficult for researchers (Lebek et al., 2013; Poepjes, 2015).

7.2 Research contributions

This study proposes and tests a method for implementing an information security awareness campaign within an organisation. The implementation of this method within the organisation is documented in detail, showing not only the positives and negatives of the method but how it impacted the environment and how the environment impacted the method. The study evaluated each step in the method, highlighting and showing the need for several research streams within the information security awareness field of study. Additionally, the study contributes to the validation of the study by Poepjes (2015).

For the organisation, the study highlighted several awareness risks within their environment that were previously only assumed. The visual representation of the awareness risk matrix provided the information security team with the view needed to target training material for specific groups. The organisation now has

the artifacts, method and knowledge to grow the implementation of the ISAC-M within their organisation.

This study differentiated itself from other studies in that it relied on the organisation interaction and incorporated the organisation inputs, such as the organisation ISF and the organisation risk management framework and matrix.

7.3 Limitations and recommendations for further research

This method was implemented at a single organisation, and results are therefore unique to the organisation. While the organisation comes from a highly regulated industry, which requires conformance to many controls, their environment is unique, both in their systems in their environment and the information security controls they implement. The interpretivist methodology assumes that the knowledge gained is a product of the environment in which it was conducted. Testing this method in multiple environments could yield different results that may assist in improving the proposed method.

The organisation has a year-long information security awareness campaign strategy, comprising quarterly strategies. This study was undertaken over ten months but only focused on the planning and implementation of one quarter. Additionally, the organisation divides its quarterly strategies based on the risk profile of target groups in the environment. Due to compliance requirements (legislative and regulatory) and risks prevalent in the environment, the ISAC-M was used on a single trial group that was considered by the organisation as posing a low risk of negative impact to the business. The implementation of this method over an extended period would provide the opportunity to not only collect more data for analyses but improve and evolve the method.

All artifacts were developed, approved and executed by the organisation staff. No analysis was performed on the questions within the questionnaires. Additionally, the content and mechanisms used to deliver the training were decided on by the organisation staff. While the organisation staff were sure of its effectiveness as a training delivery method, there is no evidence to validate their assumption, other

than their experience in the field and knowledge of the environment. The accuracy of this data can be improved by making use of validated artifacts and questionnaires from previous studies.

Survey results and samples were limited in size as the organisation could not wait for a more significant number of respondents. Instead of waiting for a specific number of responses, a hard deadline was used to determine when sampling would be complete. As a result, the results from Awareness Capability may not be a wholly accurate reflection of the environment. Additionally, The Standards of Good Practice (Chaplin et al., 2016) was updated in the second quarter of 2018 (Jordan et al., 2018). While no controls were removed from the standard in the new edition, some controls were separated from existing controls and expanded upon to create new controls. The control framework artifact for this dissertation was created using the 2016 standard only. By simplifying the control framework to incorporate similar controls to more comprehensive controls that map back to the ISF, the burden on the end-user answering survey questions can be lessened, and the impact of changing controls reduced.

Within the field of information security awareness training, there is still much research to do around measuring the effectiveness of information security awareness campaigns. Further research should measure the effectiveness of the methodology used to conduct the training and how this impacts the effectiveness of the information security awareness campaign. Additionally, the incorporation of metrics, such as phishing simulation results and other user behaviour metrics, could prove useful; however, more research is required on what those metrics should be.

In summary, this research can be expanded upon by incorporating metrics, measuring training techniques individually, refining artifacts, conducting the study over a more extended period in order to observe the results of the implementation over time, and conducting the study in multiple environments.

REFERENCES

Aloul, F. A. (2012). The Need for Effective Information Security Awareness. *Journal of Advances in Information Technology, 3*(3), 176-183.

Arachchilage, N. A., & Love, S. (2014). Security Awareness Of Computer Users: A Phishing Threat Avoidance Perspective. *Computers in Human Behavior, 38(1)*, 304-312.

Bashorun, A., Worwui, A., & Parker, D. (2013). Information Security: To Determine Its Level Of Awareness In An Organization. *Paper presented at 2013 7th International Conference on Application of Information and Communication Technologies.* DOI:10.1109/ICAICT.2013.6722704

Baskerville, R., & Wood-Harper, A. T. (1998). Diversity in Information Systems Action Research Methods. *European Journal of Information Systems, 7(1)*, 90-107.

Bhattacherjee, A. (2012). Social Science Research: Principles, Methods, and Practices. *USF Tampa Bay Open Access Textbooks, Book 3*. Retrieved from http://scholarcommons.usf.edu/oa_textbooks/3

Boell, S. K., & Cecez-Kecmanovic, D. (2015). Debates and Perspectives On being 'systematic' in literature reviews in IS. *Journal of Information Technology, 30 (1)*, 161-173.

BSI Group. (2013). *BS ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security controls* (2nd ed.). Geneva: BSI Standards Limited.

Chaplin, M., Creasey, J., & Thathupara, S. (2016). *The Standard Of Good Practice For Information Security 2016.* Information Security Forum Limited.

Cofense. (2019). *Cofense LMS*. Retrieved February 10, 2019, from Cofense.com: https://cofense.com/lms/

Daniel Ani, U. P., He, H. M., & Tiwari, A. (2016). Human Capability Evaluation Approach For Cyber Security In Critical Industrial Infrastructure. In D. Nicholson (Ed.), *Advances in human factors in cybersecurity. 501*, pp. 169-182. Florida: Springer International Publishing.

Da Veiga, A., & Martins, N. (2015). Improving The Information Security Culture Through Monitoring And Implementation Actions Illustrated Through A Case Study. *Computers & Security, 49(1)*, 162-176.

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). Control-Alt-Hack: The Design And Evaluation Of A Card Game For Computer Security Awareness And Education. *CCS '13 Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security* (pp. 915-928). Berlin: ACM.

Gundu, T., & Flowerday, S. V. (2012). The Enemy Within: A Behavioural Intention Model And An Information Security Awareness Process. *Information Security for South Africa (ISSA).* Johannesburg: Information Security for South Africa (ISSA). DOI:10.1109/ISSA.2012.6320437

Hevner, A. R., March, S., Park, J., & Ram, S. (2004). Design Science In Information Systems Research. *MIS Quarterly, 28*(1), 75-105.

Huisman, J. (2018). *Magic Quadrant for Security Awareness Computer-Based Training.* Retrieved February 10, 2019, from Garter.com: https://www.gartner.com/doc/reprints?id=1-5S45SXS&ct=181113&st=sb

Jordan, A., Haken, G., & Creasey, J. (2018). *The Standard of Good Practice for Information Security 2018.* United Kingdom: Information Security Forum.

Kajzer, M., D'Arcy, J., Crowell, C. R., Striegel, A., & Van Bruggen, D. (2014). An Exploratory Investigation Of Message-Person Congruence In Information Security Awareness Campaigns. *Computers & Security, 43(1)*, 64-79.

KnowBe4. (2019). *Overview of KnowBe4 Training Modules*. Retrieved February 10, 2019, from KnowBe5: https://www.knowbe4.com/knowbe4-training-modules-overview/

Kocamustafaogullari, M. (2013). A Prototype For Assessment Of Information Security Awareness And Implementation Level. (Doctoral Thesis, Cankaya University Graduate School of Natural Applied Sciences, Mathematics and Computer Science, Turkey).

Labuschagne, W. A., & Eloff, M. (2014). European Conference on Cyber Warfare and Security. *Paper presented at European Conference on Cyber Warfare and Security*, (pp. 125-132).

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013). Employees' Information Security Awareness and Behavior: A Literature Review. *Paper presented at Hawaii International Conference on System Sciences (HICSS).* Wailea: IEEE. DOI:10.1109/HICSS.2013.192

Majid, A., Hasmanizam, Abdul Majid, M., Izham Ibrahim, M., Safawati Wan Manan, W. N., & Ramiza Ramli, M. (2015). Investigation of Security Awareness on e-Learning System Among Lecturers and Students in Higher Education Institution. *Paper presented at International Conference on Computer, Communication, and Control Technology (I4CT 2015),* (pp. 216-220). Kuching: IEEE.

Mäkitalo, H. (2017). Measuring Users' Level Of Information Security Awareness – Research And Development Of Sample Questions (Master thesis, University of Jyväskylä, Finland).

Manifavas, C., Fysarakis, K., Rantos, K., & Hatzivasilis, G. (2014). DSAPE – Dynamic Security Awareness Program Evaluation. In T. Tryfonas, & I. Askoxylakis (Ed.), *Paper presented at HAS: International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 259-269). Heraklion: Springer.

March, S. T., & Smith, G. F. (1995). Design And Natural Science Research On Information Technology. *Decision Support Systems, 15(1)*, 251-266.

McCormac, A., Calic, D., Parsons, K., Zwaans, T., Butavicius, M., & Pattinson, M. (2016a). Test-Retest Reliability And Internal Consistency Of The Human Aspects Of Information Security Questionnaire (HAIS-Q). *Paper presented at Australasian Conference on Information Systems*, (pp. 1-10). Wollongong.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2016b). Individual Differences And Information Security Awareness. *Computers in Human Behavior, 69(1)*, 151-156.

MediaPRO. (2019). *LearningLAB Adaptive*. Retrieved February 10, 2019, from MediaPro.com: https://www.mediapro.com/adaptive-security-awareness-program/

Microsoft. (2013). *Elevation of Privilege (EoP) Threat Modeling Card Game*, 1. Retrieved February 10, 2019, from Microsoft.com: https://www.microsoft.com/en-za/download/details.aspx?id=20303

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the Smartphone User? Security Awareness in Smartphone Platforms. *Computers and Security, 34(1)*, 47-66.

National Institute of Standards and Technology. (2019). *Glossary*. Retrieved February 10, 2019, from Computer Security Resource Center: https://csrc.nist.gov/glossary/term/zero-day-attack

Ndung'u, R. M. (2014). Information Security Awareness Measuring Model - A Case Study Of Nairobi Stock Exchange Systems. (Masters thesis, University of Nairobi School of Computing and Informatics, Kenya).

Open Web Application Security Project. (2018). *OWASP Cornucopia*. Retrieved February 10, 2019, from OWASP.org: https://www.owasp.org/index.php/OWASP_Cornucopia

Oxford University Press. (2019). *British & World English > campaign*. (Oxford University Press) Retrieved February 3, 2019, from Oxford Living Dictionaries: https://en.oxforddictionaries.com/definition/campaign

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2013). The Development Of The Human Aspects Of Information Security Questionnaire (HAIS-Q). *24th Australasian Conference on Information Systems 4-6 Dec 2013*, (pp. 1-11). Melbourne.

Parsons, K., Calic, D., Pattinson, M., Butavivius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66 (1)*, 40-51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining Employee Awareness Using The Human Aspects Of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42 (1)*, 165-179.

Pattinson, M., Butavicius, M., Ciccarellol, B., Lillie, M., Parsons, K., Calic, D., & McCormac, A. (2018). Adapting Cyber-Security Training to Your Employees. In N. L. Clarke, & S. M. Furnell (Ed.), *Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance* (pp. 67-79). Dundee: University of Plymouth.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2017). Managing Information Security Awareness At An Australian Bank: A Comparative Study. *Information & Computer Security, 25*(2), 181-189. DOI:10.1108/ICS-03-2017-0017

PCI Security Standards Council. (2016). *Payment Card Industry (PCI) Data Security Standard Requirements And Security Assessment Procedures* (3.2 ed.). PCI Security Standards Council, LLC.

Plachkinova, M., & Andres, S. (2015). Improving Information Security Training: An Intercultural Perspective. *PACIS 2015 Proceedings. 167.* AIS Electronic Library (AISeL).

Poepjes, R. (2015). The Development And Evaluation Of An Information Security Awareness Capability Model: Linking Iso/Iec 27002 Controls With Awareness

Importance, Capability And Risk. (Doctoral thesis, The University of Southern Queensland Faculty of Business, Education, Laws and Arts School of Management and Enterprise, Australia).

Proofpoint. (2019). *Security Education Platform*. Retrieved February 10, 2019, from Proofpoint Security Awareness Training: https://www.wombatsecurity.com/security-education

Ragan, S. (2015). *Researcher Discloses Zero-Day Vulnerability In FireEye*. Retrieved from CSO Online: http://www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in-fireeye.html

Rantos, K., Fysarakis, K., & Manifavas, C. (2012). How Effective Is Your Security Awareness Program? An Evaluation Methodology. *Information Security Journal: A Global Perspective, 21*(6), 328-345. DOI:10.1080/19393555.2012.747234

Saunders, M. N., Lewis, P., & Thornhill, A. (2015). *Research Methods for Business Students* (7th ed.). Essex, United Kingdom: Pearson Education Limited.

Silva, L., Menezes, S., & Costa, A. P. (2012). A Model For Evaluating Information Security With A Focus On The User. *MCIS 2012 Proceedings. 25.* AIS Electronic Library (AISeL).

Standards Australia/Standards New Zealand. (2009). SA/SNZ HB 436:2013 Risk Management Guidelines - Companion To As/Nzs Iso 31000:2009. Standards Australia/Standards New Zealand. Retrieved from http://www.standards.org.au

Stewart, G., & Lacey, D. (2012). Death By A Thousand Facts Criticising The Technocratic Approach To Information Security Awareness. *Information Management & Computer Security, 20*(1), 29-38.

Terranova. (2019). *Cyber Security Awareness Training*. Retrieved February 10, 2019, from Terranova Security: htttps://terranovasecurity.com/cyber-security-awareness/

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing Trajectories Of Information Security Awareness. *Information Technology & People, 25*(3), 327-352.

Vaishnavi, V. K., & Keuchler Jr, W. (2015). *Design Science Research Methods and Patterns: Innovating Information and Communication Technology.* Boca Raton, Florida: CRC Press.

Waly, N., Tassabehji, R., & Kamala, M. (2012). Improving Organisational Information Security Management: The Impact of Training and Awareness. *Paper presented at 2012 IEEE 14th International Conference on High Performance Computing and Communications* (pp. 1270-1275). Liverpool: IEEE .

Yildirim, E. (2016). The Importance Of Information Security Awareness For The Success Of Business Enterprises. In D. Nicholson (Ed.), *Advances in human factors in cybersecurity. 501*, pp. 211-222. Florida: Springer International Publishing.

Young-McLear, K., Wyman, G., Benin, J., & Young-McLear, Y. (2016). A White Hat Approach To Identifying Gaps Between Cybersecurity Education And Training: A Social Engineering Case Study. In D. Nicholson (Ed.), *Advances in human factors in cybersecurity. 501*, pp. 229-237. Florida: Springer International Publishing.

ANNEXURE 1: LITERATURE ANALYSIS

This annexure provides a summary of the information security awareness research that was reviewed in the development of this dissertation.

Literature	Citations	Focus of Study	Level of Analysis	Measure
Aloul, 2012	39	Importance	Mixed	Metric
Arachchilage & Love, 2014	53	Improvements	Mixed	Questionnaire
Bashorun et al., 2013	2	Measuring	Professionals	Questionnaire
Da Veiga, & Martins, 2015	32	Measuring	Professionals	Questionnaire
Daniel Ani et al., 2016	0	Measuring	Theoretical	Questionnaire
Denning et al., 2013	31	Improvements	Students	Questionnaire
Gundu & Flowerday, 2012	0	Improvements	Professionals	Questionnaire
Kajzer et al., 2014	22	Improvements	Mixed	Questionnaire
Kocamustafaogullari, 2013	1	Measuring	Professionals	Questionnaire
Labuschagne & Eloff, 2014	5	Improvements	Students	Questionnaire
Lebek et al., 2013	38	Improvements	Theoretical	N/A
Majid, Majid, Ibrahim, Manan, & Ramli, 2015	0	Measuring	Students	Questionnaire
Makitalo, 2017	0	Measuring	Theoretical	Questionnaire
Manifavas et al., 2014	0	Measuring	Professionals	Metric
McCormac et al., 2016a	4	Measuring	Professionals	Questionnaire
McCormac et al., 2016b	1	Measuring	Professionals	Questionnaire
Mylonas et al., 2013	160	Improvements	Mixed	Questionnaire
Ndung'u, 2014	0	Measuring	Professionals	Questionnaire
Parsons et al., 2017	2	Measuring	Students	Questionnaire
Parsons et al., 2013	54	Measuring	Theoretical	Questionnaire
Pattinson et al., 2017	1	Measuring	Professionals	Questionnaire
Plachkinova & Andres, 2015	0	Improvements	Professionals	Questionnaire
Poepjes, 2015	1	Measuring	Professionals	Questionnaire
Rantos et al., 2012	11	Measuring	Theoretical	Metric
Silva, Menezes, & Costa, 2012	1	Measuring	Theoretical	Metric
Stewart & Lacey, 2012	26	Improvements	Theoretical	N/A
Tsohou et al., 2012	21	Improvements	Professionals	N/A
Waly et al., 2012	21	Improvements	Professionals	Questionnaire
Yildirim, 2016	0	Importance	Theoretical	N/A
Young-McLear et al., 2016	1	Measuring	Students	N/A

ANNEXURE 2: ISF SOGP CONTROL OBJECTIVES (CHAPLIN ET AL., 2016)

This annexure provides a summary of the 21 ISF SoGP control objectives, as defined within Chaplin et al. (2016), which were deemed significant during the collection of the Awareness Importance score.

Control	Objective
BA2.2 Protection of Spreadsheets	To assure the accuracy of information processed by critical spreadsheets, and protect that information from disclosure to unauthorised individuals.
BC1.1 Business Continuity Strategy	To align business continuity goals with the organisation's business goals, provide resilience against disruption and minimise impact to the organisation in the event of a disaster or emergency.
IM1.1 Information Classification and Handling	To ensure that information is protected in line with its assigned level of classification.
IM1.2 Information Privacy	To prevent information about individuals being used in an inappropriate manner, and ensure compliance with legal and regulatory requirements for information privacy.
IM2.1 Document Management	To protect information contained in documents in accordance with legal requirements, ensure critical information remains available when required, preserve the integrity of critical information and protect sensitive information from unauthorised disclosure.
IM2.2 Sensitive Physical Information	To protect sensitive physical information in accordance with information security and regulatory requirements, preserve the integrity of sensitive physical information and protect it from unauthorised disclosure.
NC2.2 Instant Messaging	To ensure that instant messaging services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.
NC2.3 Voice over IP (VoIP) Networks	To ensure the availability of VoIP networks, and protect the confidentiality and integrity of sensitive information (e.g., the content of telephone calls) in transit.
PA2.1 Mobile Device Configuration	To ensure mobile devices do not compromise the security of information stored on them or processed by them, and prevent unauthorised access to information in the event they are lost or stolen.
PA2.2 Enterprise Mobility Management	To ensure that critical and sensitive information handled by staff working with smartphones and tablets is adequately protected.
PA2.3 Mobile Device Connectivity	To ensure mobile devices are protected against unauthorised access and to prevent the unauthorised disclosure of information.
PA2.4 Employee-owned Devices	To ensure that critical and sensitive business information handled on employee-owned devices receives the same level of protection as that typically provided for corporate-owned devices.
PA2.5 Portable Storage Devices	To ensure that sensitive information stored on portable storage devices is protected from unauthorised disclosure.
PM1.1 Employment Life Cycle	To ensure that employees are equipped with the skills, knowledge and tools to support the organisation's values and adhere to information security policies.
PM2.2 Security Awareness Messages	To ensure individuals remain aware of the importance and need for information security on an ongoing basis, and maintain a security-positive culture throughout the organisation.
SA2.3 Customer Connections	To protect the confidentiality, integrity and availability of sensitive or critical information relating to either the organisation or the customer.
SD2.5 System Testing	To ensure systems function as intended, meet predefined security requirements and do not compromise information security.
SM1.2 Acceptable Use Policies	To provide clear direction on how individuals are expected to use technology that is used to handle the organisation's information.
SY1.2 Server Configuration	To ensure servers operate as intended and do not compromise the security of computer installations or other environments.
TS1.6 Information Leakage Protection	To identify sensitive information that may be at risk of unauthorised disclosure and detect if sensitive information is disclosed to unauthorised individuals or systems.
TS2.2 Cryptographic Key Management	To ensure that cryptographic keys are not compromised (e.g., through loss, corruption or disclosure), thereby exposing critical or sensitive information to attack.