The development and evaluation of an Information Security Awareness Capability Model: Linking ISO/IEC 27002 controls with Awareness Importance, Capability and Risk.

Submitted in fulfilment of the requirements
of the degree of
Doctor of Philosophy

School of Management and Enterprise
Faculty of Business, Education, Laws and Arts
The University of Southern Queensland

Robert Poepjes

Master of Information Systems (University of Southern Queensland, 2004)
Graduate Diploma of Applied Finance & Investment
(Securities Institute of Australia, 2000)
Bachelor of Business (Economics) (Edith Cowan University, 1996)
CISM (2004), CISA (2005)
(Information Systems Audit and Control Association)

2015

ABSTRACT

This research examines the role that awareness has on the effectiveness of information security within an organisation. There is a lack of understanding as to what is an appropriate level of awareness for information security controls across an organisation. Without understanding the required awareness importance and demonstrated awareness capability, an organisation may not be able to determine whether a lack of knowledge poses information security related risks.

This study refers to Awareness Importance as how important awareness is, or how influential awareness is, in the success of a process or control. For example, when crossing a busy street it would be important to be aware of oncoming traffic before crossing. This study also refers to Awareness Capability as how aware or capable a person is when faced with a decision. It relates to the comprehension of a current situation and, for example, before a person crosses a street, are they aware or capable of comprehending the situation of the oncoming traffic? This capability will influence how successful the street crossing would be. Awareness Risk is the gap that results from the required amount of awareness (Awareness Importance) being greater than that actually being displayed (Awareness Capability.

This research is motivated by the primary question of "to what extent does the relationship between awareness importance and awareness capability predict the risks associated with an organisation's current state of information security awareness of their information security controls?" This study suggests that by identifying the potential risks posed by any awareness gap, it is likely that improvements to the capability and posture of information security in organisations could be achieved.

There is little empirical research on how awareness influences the effectiveness of information security controls. Furthermore, scant research has been conducted on how successful or effective these education and training programs are on organisational awareness. Moreover, do they raise the perception, comprehension and decision-making of individuals and organisations in relation to potential threats? In bridging this literature gap, this current research builds and tests a theoretical framework and model that combines aspects of ISO/IEC 27002 standard with theories of situation awareness and risk management. The resultant model is an information security awareness capability model (ISACM).

In the first phase of this research, survey data was collected from information security professionals in order to establish a benchmark *Awareness Importance* rating for each of the 39 main security categories and their associated control objectives in the ISO/IEC 27002 standard. These ratings, established for three stakeholder groups (IT staff, senior management, end users) within organisations, formed the first component of this study's ISACM. In the second phase survey, situation awareness theory guided the development of an *Awareness Capability* instrument to capture the second component of ISACM. This instrument was used to survey two separate populations to measure awareness capability of end users against the top 10 security categories of Awareness Importance determined in phase one. Phase two survey data was used to calculate the third component of the ISACM, *Awareness Risk* - the gap between required awareness (Importance) and demonstrated awareness (Capability).

This research extends existing literature by contributing an approach and empirical model for measuring the required importance and capability of information security awareness within an organisation, thus identifying potential information security risks. The key findings illustrate that the required importance of awareness of information security controls differs from control to control, and differs depending on which stakeholder is involved. Finally, the study's model calculates *Awareness Risk*, allowing organisations to establish where awareness is sufficient; as well as where awareness is lacking and likely to present risks.

The researcher concludes that the model developed will assist organisations in identifying awareness gaps and associated risks for specific information security control objectives across an organisation. ISACM will provide a better understanding of the level of information security awareness that exists in an organisation and where risks exist due to lower than desirable levels of awareness of information security controls. This will subsequently allow organisations to invest in the appropriate areas where unacceptable levels of risk exist.

CERTIFICATION OF DISSERTATION

The work presented in this thesis is, to the best of my knowledge and belief, original except as otherwise indicated in the text. I hereby declare that I have not submitted this material, in whole or in part, for a degree at this or any other institution.

Signed:
Robert Poepjes
Date: 01 November 2015

Signed: M Lane
Dr Michael Lane (principal supervisor)
Date: 01 November 2015

Signed:
Associate Professor Jianming Yong (associate supervisor)
Date: 01 November 2015

ACKNOWLEDGEMENTS

My deepest and most sincere gratitude is owed to Dr Michael Lane for his limitless guidance, patience, encouragement and insight throughout the duration of my doctoral studies. Michael's commitment and belief in the research I was undertaking has been immense and it is to a great degree that I thank him for helping me get to the finish line. Michael's ability to provide me with academic and subject matter guidance will be life lasting for me, and his enormous capacity to help me is very much appreciated. Thank you Michael.

I would also like to thank Chris O'Reilly for her final proof read of my thesis and her suggested grammatical changes.

Finally, I would also like to thank my wife Michele, who not only displayed boundless understanding and patience with my studies, but kept me going by continuing to study herself and helped me see this through to the end. Thank you for all your support ShellBell.

Table of Contents

List of Figures

List of Tables

1.0 Introduction

The purpose of this chapter is to introduce the research problem that provided the motivation for conducting this PhD research. Firstly, the research questions posed to provide answers to the research problem are outlined. The theoretical and conceptual model and methodological approach that underpinned this research are outlined and described. This chapter concludes by describing the structure of the dissertation in terms of the content of subsequent chapters and provides a summary of the key definitions used in this dissertation and the delineation of scope of this research. Figure 1-1 below outlines the structure of this chapter.

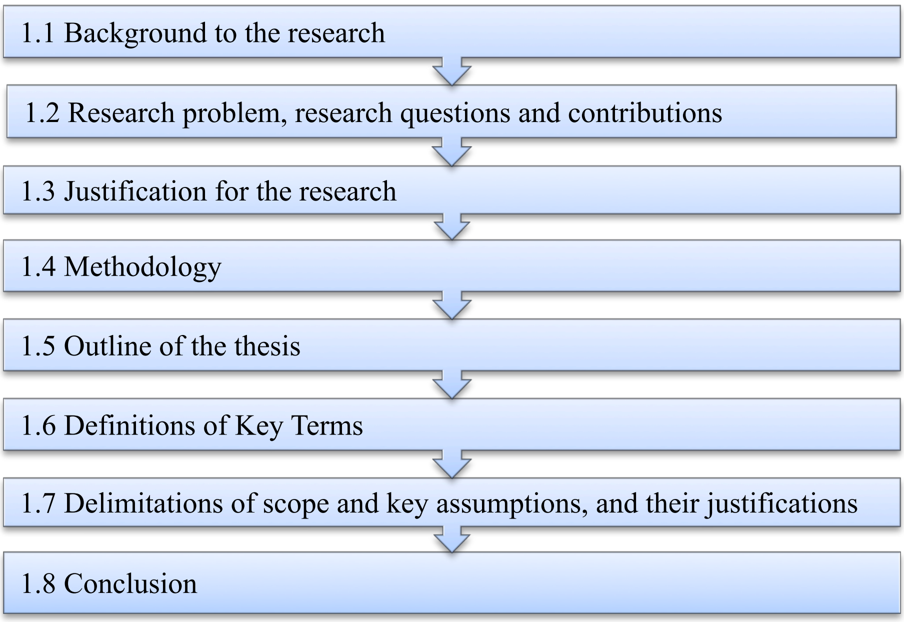

1.1 Background to the research
1.2 Research problem, research questions and contributions
1.3 Justification for the research
1.4 Methodology
1.5 Outline of the thesis
1.6 Definitions of Key Terms
1.7 Delimitations of scope and key assumptions, and their justifications
1.8 Conclusion

Figure 1-1 Structure of Chapter 1

This research is based in the field of information security and, in particular, information security awareness. However, to adequately provide a detailed insight into information security awareness, this research examines and builds on a number of parent theories that were used to develop the theoretical and conceptual model and methodological approach that underpins and guides how this research was conducted. These are Information Security, Situation Awareness, Capability Measurements, and Risk Management. This introduction chapter provides a high level overview of these parent theories and their relationship to information security awareness.

1.1 Background to the research

The need for improved information security has received increased attention since the late 1990s when substantial disruption to organisational computing services was caused by computer viruses such as Code Red and Melissa. Information security threats have continued to evolve and diversify and ‘hackers have been continuously innovative in developing polymorphic phishing vectors’ (Nagunwa 2014, p. 72) since those earlier days. Threats now faced by individuals and the organisations they work for include email threats (Aslam & Aziz 2015), identity theft (Australian Government 2014; Edwards 2014; He et al. 2014), and the Nigerian scam and data leakage (Patil & Prasanthi 2013; US Government & Lew 2010). Insider threats 'pose significant challenges to any organisation' (Sarkar 2010; Zeadally et al. 2012, p. 183), and threats to critical infrastructure (Bronk 2015; Popa 2013) pose increasing risks to organisations and society in general.

In a recent survey focused on the global state of information security, PriceWaterhouseCoopers (2012, p. 16) found that 'as mobile devices, social media, and the cloud computing services become commonplace both inside the enterprise and out, technology adoption is moving faster than security'. These changes in technology and its usage present a new wave of emerging information security threats, and yet we continue to find employees falling victim to well-used threat and exploitation techniques. In their report on email security awareness, Ipsos Public Affairs (2010, p. 24) found 'three in five users (58%) on average say that their computer has been affected by a virus'.

Information security threats continue to evolve. Old threats that first emerged via emails have now progressed to death threats via mobile phones (News.Com.au 2012) to anyone receiving a text message and not paying the stated ransom. These threats continue to manifest themselves in many different ways, include phishing emails requesting 'customers' to provide passwords to bank accounts, or to advance money in order to gain greater returns - such as the Nigerian scam (Australian Securities and Investment Commission (ASIC) 2008). In their latest *Cyber Crime & Security* survey report (Australian Government 2013a, p. 22), Cert Australia found that '56% of organisations did identify one or more cyber security incident in the previous 12 months'. The main incidents included targeted emails, virus or worm infections, Trojan or rootkit malware, theft of mobile devices, and unauthorised access.

Employees and people in general continue to fall victim to the same techniques applied many years ago. Vulnerabilities in computer software continue to provide virus, spam and phishing writers with a supply of victims, which poses a significant risk to organisations. Some believe that these vulnerabilities 'are the root cause of computer security problems' (Liu et al. 2012, p. 152). Savirimuthu and Savirimuthu (2007, p. 443) relate that 'software vendors wait for vulnerabilities to be discovered'; that this is really 'reactive approaches'; and that 'the bad guys scramble to open new holes'. Protection against, and cleaning up in relation to vulnerabilities such as a virus or phishing attack has been an ongoing significant cost and disruption to organisations, and is causing considerable annoyance to the general public.

The emergence of cloud computing does not lessen the risks of computer vulnerabilities. Research has found (Chou 2013, p. 79) that breaches to data security in cloud services 'are also increasing every year due to hackers who are always trying to exploit the security vulnerabilities'. Also poor management of computer access within organisations leaves organisations vulnerable to employees, as well as ex-employees having more access than is required. Data leakage has been widely communicated through the trials and tribulations of Wikileaks. This leakage could be 'inadvertent or intentional leakage of knowledge by disgruntled employees which could occur easily in an increasingly networked society' (Ahmad, Bosua & Scheepers 2014, p. 28). Awareness of information security is a mainstream issue for society, governments and organisations.

The emergence of identity theft and financial fraud from phishing is causing similar concerns to those experienced during the early years of viruses in the late 1990s and early 2000s. The results of a Australian Bureau of Statistics survey on personal fraud (Australian Bureau of Statistics (ABS) 2011) reported 702,100 victims of identity theft, an increase of 499,500 victims since the 2007 survey, although changes to how this survey was conducted (2007 versus 2011) makes directly comparing the two figures difficult. It is unclear whether the increase is a result of more victims or just a greater level of awareness of the problem and consequent increase in reporting incidents. Society's reliance on information technology for Internet banking, share trading, instant messaging, blogging and social networking, as well as critical infrastructure's use of information technology, provides a perfect attack vector.

Information security controls are the rules and regulations capable of preventing or minimising the impact of such attacks (Hove et al. 2014; Narain Singh, Gupta & Ojha 2014; Siponen & Willison 2009). Knowledge of these controls, through information security awareness, can provide a strong level of defence for organisations. This knowledge includes awareness of a new virus or phishing attack, awareness of identity theft, and what controls can minimise the likelihood and impact of these threats. Understanding how awareness influences the importance, capability and effectiveness of information security controls is important. It provides insight and a challenge for the development of models incorporating measures of importance and capability by linking information security control methodologies and awareness.

There is a large body of literature that describes what to include in an information security awareness program. Literature such as *Information Security Awareness: Local government and Internet service providers* (European Network and Information Security Agency (ENISA) 2007) and *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (National Institute of Standards and Technology [NIST], Souppaya & Scarfone 2013) are examples of government or industry-body provided information on information security awareness. There is, however, scant information on how awareness influences the effectiveness of the information security controls and little is documented about how capable or effective these awareness programs are, and whether they raise the perception, comprehension and decision making of individuals and organisations in relation to potential information security threats.

The Government's *Inquiry into Cyber Crime* (Australian Government 2010, p. 59) took submissions from the Australian Computer Society who argued that 'Australians seem to be aware of, and are taking precautions against, old cyber crime threats but are not aware of, or taking steps against, new and emerging cyber crime threats'. As technology continues to permeate more and more aspects of our lives, and the organisations we work for, and technologies such as cloud computing become common place, daily activities contribute to both the reporting of further information security breaches (Chou 2013), as well as to the knowledge of the subject. This increase includes the use of social media, the growth of data and data leakage, technology improvements adding significant computing power to devices (e.g. smart phones, iPad-like devices [tablets]), increased online purchasing, and critical infrastructure relying on computer automation. These increases lead to society and organisations needing to become more technology risk aware (Arabo & Pranggono 2013; Imgraben, Engelbrecht & Choo 2014).

1.2 Research problem, research questions and contributions

The problem addressed in this research is:

> *How can the relationship between the awareness of information security controls and the levels of awareness capability displayed by employees be measured to inform an organisation of the risks and consequences of any insufficient awareness capability of their employees?*

By determining the appropriate level of awareness for information security controls for an organisation's employees, and how an organisation can assess awareness capability of these employees for information security controls, the level of risk faced by an organisation as a result of the level of awareness capability that exists in its workforce can be determined and action taken to reduce that risk. These levels of awareness capability and awareness risk are captured in an information security awareness capability model developed in this research. The basis of this model are the main security categories and their associated control objectives, which are drawn from the international information security standard ISO/IEC 27002 (Standards Australia/Standards New Zealand 2006b). This current research examines awareness in terms of its importance in supporting the objectives of these security categories and controls, and how capable stakeholders in an organisation are in being able to demonstrate their awareness.

Situation awareness theory (Endsley & Garland 2000; Webb et al. 2014) and risk management theory (NSW Government 2012; Standards Australia/Standards New Zealand 2009b) provide a theoretical basis for the conceptual model of information security awareness capability developed in this research. This research determines desired levels of awareness and what levels of awareness are obtained in relation to information security controls in an organisation. The gap between desired and obtained is presented as a risk measurement for the information security control.

The main objective of this research is the development and evaluation of a theoretical and conceptual model with practical applications in assisting organisations in measuring the information security awareness capability of its workforce. This will allow organisations to identify the resultant risks that may exist because of less than desirable levels of awareness capability. This model is based on rating how important awareness is for information security controls in the ISO/IEC 27002 standard, and determining how to measure the awareness capability of three key stakeholders in relation to those controls in order to measure gaps (risks) between desired and measured awareness. The theoretical and conceptual model developed in this research is underpinned by situation awareness theory (Howard & Cambria 2013; Kokar & Endsley 2012) and risk management theory (Mejias 2012; Standards Australia/Standards New Zealand 2009b; Xiaosong et al. 2009) and is termed the Information Security Awareness Capability Model (ISACM).

A key reason for undertaking this research is to link information security awareness and the theory of Situation Awareness (SA). Whilst initially aimed at pilot behaviours, SA is an emerging field for information security. The awareness capability instrument developed for this study is based on approaches used previously in measuring SA (Breton & Rousseau 2003; Endsley, Sollenberger & Stein 2000; Muñiz et al. 1998). Some practices of assessing information security awareness only assess how aware someone is at a very shallow level (European Network and Information Security Agency (ENISA) & PricewaterhouseCoopers 2007; Talib, Clarke & Furnell 2010). This could provide an organisation with a false sense of security that employees have high levels of information security awareness. The approach of this current study uses SA, which is a cognitive information processing theory based on a hierarchy of levels of understanding for evaluating awareness capability. Such an approach allows organisations to test for awareness capability at a much deeper level in its employees.

1.2.1 Research Questions

The general research question seeks to examine how the relationship between awareness importance and awareness capability predicts awareness risk. The general research question and specific research questions are stated below in Table 1-1.

Table 1-1: General Research Questions and Specific Research Questions

General Research Question	To what extent does the relationship between awareness importance and awareness capability predict the awareness risk associated with an organisation's current state of information security awareness of their information security controls?
RQ1:	What is the appropriate level of awareness importance of the main controls of the ISO/IEC 27002 Information Security Standard in terms of three stakeholder groups (IT staff, senior management, end users)?
RQ2:	How can the awareness capability of these three stakeholder groups be measured, based on situation awareness theory?
RQ3:	How can resultant awareness risk evidenced from insufficient awareness capability (in comparison to awareness importance) be combined into a risk management model that will assist organisations in measuring and managing information security awareness risk?

In answering the first research question RQ1, this study examined the range of information security controls described by the ISO/IEC 27002 standard and rated the importance that awareness plays for each of the 39 main security categories and their associated control objectives. This was done by examining each of the 39 main security categories and their associated control objectives and developing relevant questions designed to establish awareness importance baseline levels for each of them. These questions were presented to information security experts to determine the appropriate level of awareness importance for three key stakeholder groups.

In answering the second research question RQ2, this research used situation awareness theory to help determine a suitable measure for Awareness Capability. Situation awareness theory is a cognitive information-processing theory that categorises the levels of situation awareness - from perception through to comprehension and, finally, through to projection (Endsley & Garland 2000; Tadda

& Salerno 2010; Webb et al. 2014). Situation awareness theory is playing an emerging role in understanding cyber situational awareness. And, finally, in answering the third research question RQ3, this research examined how, by comparing the Awareness Importance and Awareness Capability, an Awareness Risk measure can be derived. This measure provides an insight into gaps in the information security awareness posture that may exist within organisations.

1.2.2 Contributions

This research contributes to a number of fields of study including information security, information security awareness, and situation awareness. Firstly, it extends the existing literature in these fields by contributing an approach for measuring the importance of awareness, the capability of an organisation's information security awareness, and risks that result from the gap between the desired level of awareness and the awareness capability that exists in an organisation's workforce. The main contribution from this research is the development and evaluation of an information systems artefact: Information Security Awareness Capability Model (ISACM). This research provides the following specific contributions, which are summarised below:

- Development of an instrument to determine the Awareness Importance ratings for the 39 main security categories and their associated control objectives from the AS/NZS ISO/IEC 27002:2006 standard.
- Awareness Importance ratings for the 39 main security categories and their associated control objectives from the AS/NZS ISO/IEC 27002:2006 standard. This was determined for the three organisational stakeholder groups; IT staff, senior management, and end users.
- Awareness Capability assessment instrument, developed to test the top 10 (based on awareness importance) main security categories and their associated controls. This was demonstrated for the end user stakeholder group for two population groups: one general population to provide a baseline; and a specific population.
- Awareness Risk measure, based on the gaps between awareness importance and awareness capability.
- Evaluation of Awareness Capability and Awareness Risk in a general population sample to establish a baseline and the demonstration of the ISACM through the evaluation of Awareness Capability and resultant Awareness Risk in a specific organisation.

The development of the ISACM, including the three measures of Awareness Importance, Awareness Capability and Awareness Risk have been described in detail in this dissertation. This will allow organisations to utilise the ISACM according to their specific needs. This current research is focused on the development and evaluation of a theoretical and conceptual model for determining the level of information security awareness capability that exists in an organisation's workforce and the resultant awareness risk that may exist. The ISACM model and approach developed and evaluated in this research provides a sound foundation for other researchers and practitioners interested in evaluating awareness capability to build upon in future research on information security awareness.

This development will allow for other researchers to build on the findings of this research, and further test and refine the ISACM in a number of different organisational contexts. Future research could also extend this research and ISACM by incorporating awareness aspects into broader research on information technology or information security. This current research, through the development of the ISACM, is contributing to a better understanding on how to measure and improve the organisation's capability in information security awareness.

Effectively managing information security is a key challenge for many organisations. Section 1.1 above highlighted many of the threats that organisations face today, ranging from damaged caused by computer virus infections, through to emerging cyber criminal activities. Organisations that are unable to implement suitable information security controls, by understanding the risks associated with these threats, will be at a distinct competitive disadvantage to those organisations that implement the necessary risk based measures.

This research provides a practical way to measure awareness risk in a manner that can be incorporated into an organisation's broader risk management program. The benefits to organisations in this approach is that rather than assessing information security risks as a stand-alone issue that is an 'information technology (IT) department issue', the organisation can compare information security awareness risk alongside other risks that impact on an organisation. Incorporating awareness risk with other organisational risks will allow an organisation to make an informed choice as to the priority of any risk remediation activities required to address information security risks.

With the focus of this study being on three different stakeholder groups (IT staff, senior management, and end users), the research is not only focused on the technical aspects of information security or those employees normally associated with being responsible for information security within an organisation. By developing ISACM to incorporate the three stakeholder groups, this covers the broad range of participants within an organisation, all of whom have a role to play in ensuring that information security controls are effective. Awareness capability, the researcher believes, plays a critical role in organisations achieving an appropriate level of information security.

Implementing information security, like other management and control aspects of technology, comes at a price. The key findings from PricewaterhouseCoopers *Global State of Information Security Survey 2014* (PricewaterhouseCoopers 2013) found 'an evolved approach to security also requires the support of top executives and an adequate budget that is aligned with business needs'. As impacts of information security incidents increase, more will be expected of the information security management function within organisations. This current research provides a theoretical and practical approach that will allow organisations to determine and monitor awareness capability in their workforce and manage their information security awareness risks and information security budget in a more efficient and targeted manner, particularly where information security awareness is involved.

1.3 Justification for the research

Despite the increased growth in information security incidents, identity theft, online fraud and information theft, the budget expenditure in organisations on awareness is low. Findings from the latest *Global State of Information Security survey 2015* (PriceWaterhouseCoopers 2014) show that 'despite elevated concerns, our survey found that global IS budgets actually decreased 4% compared with 2013. In fact, security spending as a percentage of IT budget has stalled at 4% or less for the past five years'. This is similar to 2007 when '61% of organisations surveyed allocated 5 percent or less of their overall IT budget to information security', and 'less than 1 percent of their security dollars on awareness programs' (Richardson, p. 8). This appears to represent an underinvestment in information security awareness. The same survey had 50% of respondents flagging that this represented too little expenditure, and that awareness was the only area in which so many respondents felt too little was being spent.

Information security can be difficult to promote because of competing information technology budgets priorities, but it requires senior management support (McFadzean, Ezingeard & Birchall 2007, pp. 623-5; Narain Singh, Gupta & Ojha 2014; Tejay & Barton 2013). A PriceWaterhouseCoopers survey (2014) found 'only 40% of respondents say their Board is involved in security budget decisions'. This is likely to lead to difficulties in achieving suitable funding for information security. This lack of senior management involvement was a prime motivation for this current research to develop and evaluate an approach for measuring the importance and capability of information security awareness. Being able to present a strong business case for information security will help in gaining senior management support.

Any improvements in awareness could lead to an improvement in the capability and posture of information security in an organisation (Maqousi, Balikhina & Mackay 2013; Sannicolas-Rocca, Schooley & Spears 2014; Shahri, Ismail & Rahim 2013). Hagen, et al. (2008, p. 380) suggest there are 'beneficial effects of a security awareness programme'. AlAboodi (2006, p. 3) stresses that 'proper security awareness leads to the correct practice of any security control'. In relation to information security awareness training effectiveness, Shaw et al. (2009, p. 95) identified 'three levels of security awareness: perception, comprehension and projection' and suggested ways that may help educators deliver more effective training. They also suggest that 'the chance of committing human errors can be lowered as the base of users who are more aware of security risks is expanded'.

1.3.1 The Importance of the Study

Awareness of information security is seen as key for both organisations and individuals. Knapp et al. (2006, p. 1) support this view and suggest that 'information security is a critical issue threatening organizations worldwide' and that '…the need to protect information is more paramount than ever before'. They also suggest that '…everyone must agree that security is important and each person has a critical role in promoting a security-aware culture'. Understanding how to measure and improve awareness is a key factor. Organisations must proactively look at information security as something for all to be concerned with - not just IT staff. The use of three stakeholder groups in this current study acknowledges this importance.

Information security is becoming a key enabler to many organisations. It can help to facilitate the sharing of knowledge and information in an effective an efficient manner. It is crucial in providing customer confidence in transaction-based organisations such as banking, and is playing an increasing more important role in the health sector as more and more aspects of health care involve the use of computers and electronic information. Awareness of information security is a key enabler to determining the suitable balance between the protection and sharing of information.

Gartner et al. (2005, p. 2) suggests an 'information security awareness training program is a tool that all companies, regardless of size, need to implement. Without one, serious IT risks may be overlooked'. Other researchers (e.g. Talib, Clarke & Furnell 2010) found that those undertaking awareness training 'are more aware of a greater variety of security issues'. Awareness is a positive influence on achieving sound information security protection (Kim 2013; Sannicolas-Rocca, Schooley & Spears 2014; Talib, Clarke & Furnell 2010); and doing so in an efficient and effective manner is likely to improve information security overall and reduce or slow the increase in the currently observed financial losses to organisations and individuals due to information security incidents.

The Information Security Awareness Capability Model (ISACM) developed and evaluated in this research will help organisations with measuring information security awareness capability and identifying the resultant awareness risks that may exist in their organisation. ISACM provides theoretically based and practical techniques for helping organisations to improve information security effectiveness and capability within those organisations.

1.4 Methodology

This study adopts a theoretical framework combining information security control objectives presented by the International Organization for Standardization (ISO/IEC 27000 series) with theories of situation awareness and risk management. Combining these is appropriate because ISO/IEC 27002 provides a widely-accepted international standard for information security controls; situation awareness provides a relevant framework for assessing and measuring awareness capability; and risk management theory describes consequences of a mismatch between the importance of control objectives and the level or capability being demonstrated. The ISO/IEC 27002 framework, situation awareness theory, and risk management theory are covered in detail in Chapters 2, 3 and 4.

In order to see how these models, frameworks and approaches, and specific research questions interact; Figure 1-2 below depicts the overall theoretical framework that underpins this research. Figure 1-2 highlights the order and relationships of the supporting research questions (RQ1, RQ2 and RQ3) posed, and how the answers to these research questions are combined to form the overall model of the Information Security Awareness Capability Model (ISACM).

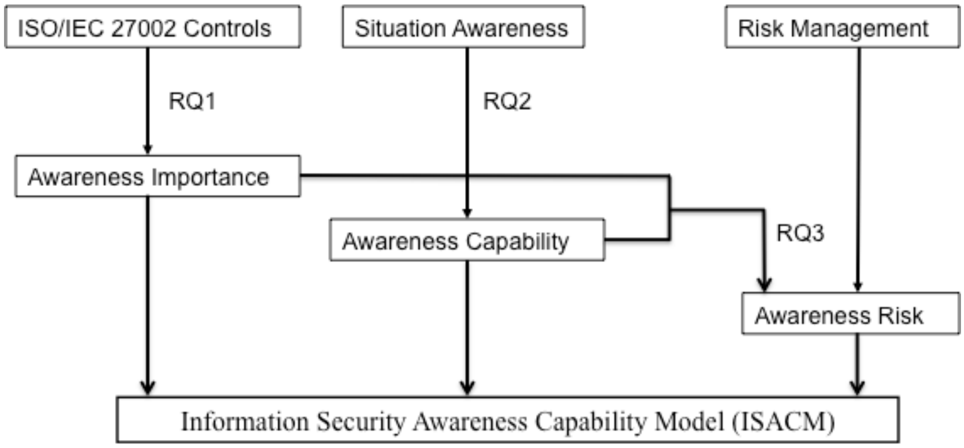


Figure 1-2: Model incorporating ISO/IEC 27002, Awareness Importance, Awareness Capability, and Awareness Risk

1.5 Outline of the thesis

Chapter 1 provides an overall introduction to this thesis, including the research problem investigated and motivation for undertaking this research. The specific research questions that address and provide answers to the research problem are outlined. The justification as to why this research is important is provided. A high level view of the methodology used in this research is provided, and formal definitions are provided for the key terms used throughout this thesis. This chapter provides the reader with an overall view of what is included within the thesis. This first chapter also provides a description of what the contribution of this research will be, as well as justification for why this research is worthwhile.

Chapter 2 provides a detailed review of the key parent theories: information security, situation awareness and risk management in terms of current literature. It begins with a discussion on the current state of information security, including a detailed description of the international information security standards ISO/IEC 27002. This standard - and in particular the 39 main security categories and their associated control objectives - provides a critical basis and context for the development and evaluation of the Information Security Awareness Capability Model in this research. The current state of information security awareness is then described, including its importance to organisations. The main aspects of the measurement of information security awareness are included in this discussion.

A detailed description of situation awareness (SA) is provided, including how SA is measured and how it relates to this research. A discussion is provided on how risk is measured in relation to the awareness risk component of the ISACM. The literature review chapter concludes with the development of the theoretical and conceptual framework that guided the development and evaluation of the ISACM and the literature support for the three research questions which underpin the ISACM.

Chapter 3 describes and justifies the philosophical stance adopted for this research and the methodology paradigm employed in this research. Overall based on the philosophical assumptions of this study in relation to ontology, epistemology and methodology, the functional positivism paradigm best fits the philosophical beliefs of this researcher. A quantitative approach using online surveys was an appropriate research method for this study. Justification is also provided for the research methodology that has been used. A detailed description of the overall research design deployed in this research is provided. The research design and procedures used for phase 1 of this study are described. Phase 1 includes the development of the structure of the overall information security awareness capability model (ISACM) that provided the key measures for this research. These measures are awareness importance, awareness capability and awareness risk.

Chapter 3 also describes how the measurement instrument for awareness importance was developed. The measurement of awareness importance was undertaken for the 39 main security categories and their associated control objectives from the ISO/IEC 27002 standard for each of three key stakeholder groups (IT staff, senior management, end users). An online survey was used to target the most appropriate respondents for rating awareness importance. Information security, IT audit and IT risk professionals were considered the most appropriate persons to be surveyed to rate awareness importance, given their knowledge and expertise in information security. Phase 1 results were used to influence the design of the awareness capability instrument developed in phase 2.

Chapter 4 is the second methodology chapter and builds upon Chapter 3. This chapter describes and justifies the research design and procedures used for phase 2 of the research. The approach used to develop the awareness capability and awareness risk measures is described. The awareness capability instrument is based on situation awareness theory. A survey was developed based on the awareness capability instrument to capture awareness capability of end users for the security categories and their associated control objectives which had been rated by IT security professionals in the phase 1 survey as having the highest levels of awareness importance for end users in organisations. The awareness capability instrument was evaluated in a survey of two population groups of end users. A general population obtained from a survey panel was used to provide a baseline for awareness capability for end users. The awareness capability of an end user population in a specific organisation was evaluated against the general population awareness capability baseline.

A description is provided of how the awareness risk measure was calculated from the results of the phase 1 survey and phase 2 surveys. The researcher adapted a traditional risk matrix heat map to illustrate how the awareness risk measures for the two survey populations in phase 2 would be presented. The chapter concludes with a description of how the researcher ensured that the surveys in phase 1 and phase 2 of this research were conducted in an ethical manner in accordance with the University of Southern Queensland's Human Research Ethics Policy.

Chapter 5 presents the results from the analyses of data collected in the phase 1 and phase 2 surveys. It describes how the results of statistical analysis of the phase 1 survey data were used to determine the *awareness importance* rating for each of the 39 main security categories and their associated control objectives in the ISO/IEC 27002 standard. A breakdown of the awareness importance ratings for each of the three stakeholder groups provides a useful and vital comparison for organisations to consider for their information security awareness programs. A heat map of the results provides an efficient way of comparing results between the stakeholder groups in relation to the desired awareness importance.

Chapter 5 also presents the results of the statistical analysis of phase 2 survey data and how this was used to determine the *awareness capability* scores for one stakeholder group, end users. The data was collected from two separate populations of end users: one was a baseline survey panel of a general population of employees who utilise computers in their work, whilst the second population was staff from an Australian university. Detailed analysis of these results allowed for a comparison between both populations in terms of their awareness capability. In particular, the analysis allowed for an examination of the phase 2 survey results in terms of the survey respondents' cognitive information processing levels, Level 1 perception, Level 2 comprehension and Level 3 projection of situation awareness (SA) theory as a way of evaluating their awareness capability. The *awareness risk* measure for the end users stakeholder group of both populations was calculated from awareness importance and awareness capability and compared between these two population groups. The risk ratings that were obtained for each of the top 10 (base on awareness importance) main security categories and their associated control objectives were described. The results of an in-depth analysis of the two highest rated awareness risks are presented to conclude this chapter.

Chapter 6 discusses key findings from the data analysis reported on in Chapter 5 from the phase 1 and phase 2 surveys. The discussion of the key findings provides answers to this study's research questions and emphasise the relationship between the key findings of this study and the relevant literature. In particular, the chapter firstly discusses the awareness importance ratings that were derived in phase 1 and assesses them in terms of the three stakeholder groups. Commentary is then provided on the measured ratings in terms of what ratings were expected for these stakeholders, and any impacts that may result where there were deviations in the measured ratings compared to the expected ratings. These outcomes were intertwined with relevant literature to assist with clarifying the measured results.

Secondly, the awareness capability scores and the resultant awareness risk ratings for both of the populations surveyed in phase 2 were examined. These awareness risk measures are presented in a commonly used risk management heat map for ease of interpretation. Finally, the chapter provides an approach for analysing the awareness capability responses in greater details that will allow organisations to determine exactly where awareness capability is lacking and subsequently resulting in unwanted risk. This will also assist organisations in determining which information security control categories the organisation should target their information security awareness program towards.

Chapter 7 is the final chapter in this thesis and includes overall conclusions and implications of this research. It provides a high-level summary of this study in terms of the research problem, the general research question, the three specific research questions investigated and tested in this research, as well as the methodological approach used. Chapter 7 also discusses the key contributions that this research has made for theory and practice and the implications of this research for current and future research and practice. The limitations of this study are also acknowledged and suggestions provided for future research in this area of study.

1.6 Definitions of Key Terms

There are definitions developed and used within this thesis that are a key aspect of this research. Definitions adopted by researchers may have differing meanings, so defining these terms enables them to be properly positioned for this research. These key terms include *Awareness Importance*, which refers to how important awareness is, or how influential awareness is, in the success of a process or control. Endsley (1999, p. 1) found situation awareness theory to be ‘particularly critical to effective functioning’ for air traffic control and control rooms. Awareness importance is described in more depth throughout this thesis and likened to ‘perception of elements’ in any situation. For example, in simple terms, when crossing a busy street it would be important to be aware of oncoming traffic before crossing. Awareness Importance would be considered high in such a situation. Compare this to driving a car, where knowing how fuel enters the engine pistons is not important in order to drive the car. Awareness Importance of having detailed knowledge of engine function in this case would be considered low for the end users (drivers), but high for specialist roles such as automobile mechanic.

Awareness Capability refers to how aware or capable a person is when faced with a decision. Capability is highlighted by Siponen (2002, p. 212) in terms of how it is ‘used to determine and improve the maturity of software processes with the help of five maturity levels’. It relates to the comprehension of a current situation and is measured by the levels of awareness as detailed in situation awareness theory (Endsley 2015). For example, before a person crosses a street, are they aware or capable of comprehending the situation of the oncoming traffic? This capability will influence how successful the street crossing would be.

Awareness Risk is the gap that results from the required amount of awareness (Awareness Importance) being greater than that actually being displayed (Awareness Capability). Slack (1994, p. 60) suggests that ‘the use of a “gap-based” approach which compares importance with performance should be used in implicitly setting improvement priorities’. Awareness risk is likened to the projection of future status. In the example of crossing the street, a high level of awareness about the current traffic is required, however, a young child may exhibit a low level of awareness or capability at that particular time. This results in a high level of awareness risk (possibly being struck by oncoming traffic) as a result of the mismatch between the two measures of awareness importance and awareness capability.

This current research targets three key stakeholder groups within an organisation. They are the *IT staff* (including information security officers) responsible for developing and managing information systems, *senior management* (such as C class officers and other key decision makers) whose support of information security is crucial, and *end users* (who are the main users of the information systems). Note that although IT staff and senior management are also end users, the focus in this research is on capturing the functional job role they play in terms of influencing security awareness.

Finally, this research draws heavily upon the international information security standard ISO/IEC 27002. It is beneficial to describe the structure and some of key terminology used in the standard in order to show the interaction that these element of the standard have with each other. The terminology used within the ISO/IEC 27002 standard is also used extensively within this thesis. The key terms are **bolded** and have been described below.

Terminology used within the ISO/IEC 27002 standard
It should be noted that the version of the standard used throughout this study was the AS/NZS ISO/IEC 27002:2006 standard. This research began whilst the 2006 version was still current, and that it would have been impractical to rework it partway through on the basis of the newly issued version of the standard.

The standard used within this research contains 11 security control clauses collectively containing a total of 39 main security categories. The hierarchy is:
Security control clause – The standard contains 11 of these and they are the primary 'dividers' of the various topics of information security.

> **Main security categories** – The standard contains 39 of these and they form the main areas of security that are covered within the standard, such as *Equipment security*, *User Responsibilities*, etc.
>
> > **Control objective** – One for each main security category, such as '*To ensure that information receives an appropriate level of protection*'.
> >
> > > **Controls** – one or more for each of the control objectives.
> > > **Implementation guidance** - supports control implementation.
> > > **Other information** - provides general assistance.

1.7 Delimitations of scope and key assumptions, and their justifications

This research's primary focus is to solve the problem of how the relationship between the awareness of information security controls and the levels of awareness capability displayed by employees can be measured to inform an organisation of the risks and consequences of any insufficient awareness capability of their employees. The ISACM helps to solve this problem. The model has been scrutinised by industry experts, and tested for one stakeholder group, end users, but until there has been significant additional scrutiny and use of the model, it remains a model that will require adaptation.

The first component of the ISACM, awareness importance, was constructed around the 39 main security categories and associated control objectives in the ISO/IEC 27002 Standard. The ISO/IEC 27002 standard includes many more detailed controls that support these 39 main security categories and their associated control objectives. Whilst it would be possible to extend the awareness importance rating to include all of these detailed controls and sub-controls, the practicality of doing so would have been difficult to achieve within the scope of this thesis.

The second component of the ISACM, awareness capability, was only developed and tested to cover the top 10 of the 39 main security categories and their associated control objectives based on their awareness importance ratings. Additionally, it was only tested for the end users stakeholder group. Extending the awareness capability instrument to include the other 29 main security controls and their associated control objectives, and testing all of these for all three stakeholder groups would have resulted in a significant amount of additional work that was beyond the scope and time constraints of this thesis. The researcher was, however, able to significantly develop and test all elements of the ISACM.

1.8 Conclusion

This chapter laid the foundations for the thesis. It introduced the research problem and research questions. The research was then justified and key definitions were presented. The methodology was briefly described and justified, a structure of the thesis was provided, and the limitations were outlined. Based on these foundations, the next chapter, the literature review Chapter 2, provides a detailed analysis of the supporting parent theories and relevant literature, which underpin the development of the theoretical and conceptual ISACM.

2.0 Research Issues

2.1 Introduction

The purpose of this chapter is to provide a detailed review of the key parent literature and theories: information security, situation awareness and risk management, with a particular focus on their relationship with information security awareness. A review of the relevant literature provides the justification for the theoretical and conceptual model Information Security Awareness Capability Model (ISACM), which is developed and evaluated in this research. Figure 2-1 below outlines the structure of this chapter.

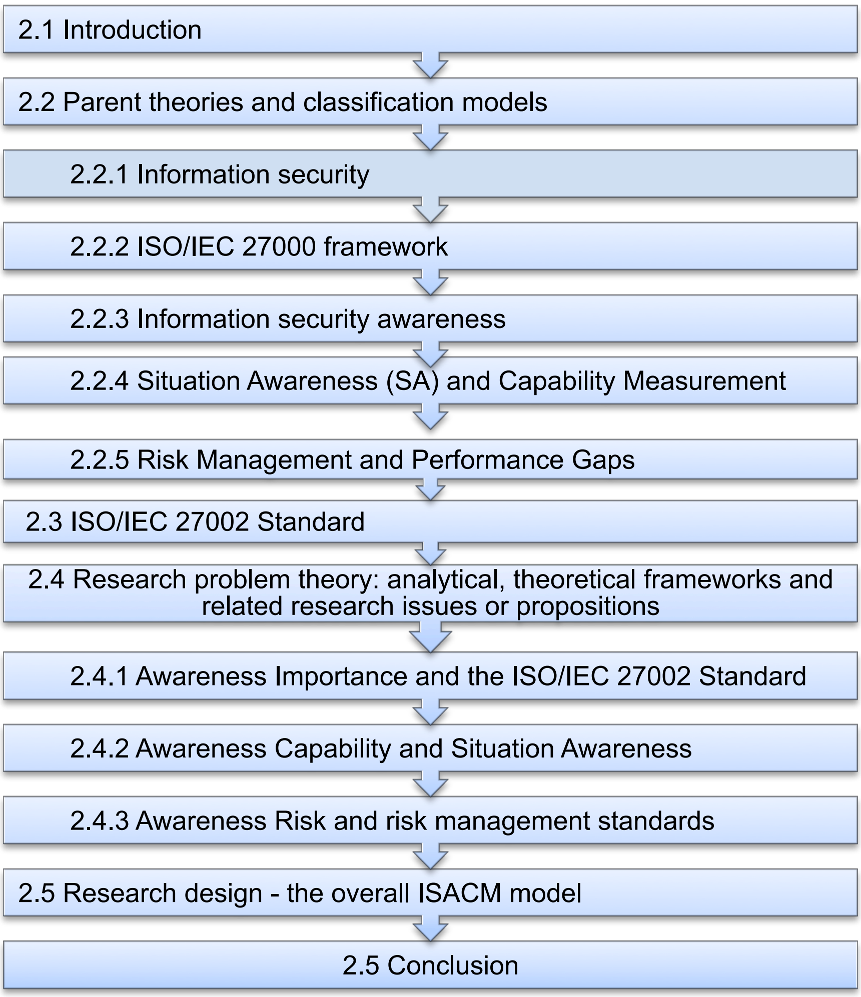

2.1 Introduction
2.2 Parent theories and classification models
2.2.1 Information security
2.2.2 ISO/IEC 27000 framework
2.2.3 Information security awareness
2.2.4 Situation Awareness (SA) and Capability Measurement
2.2.5 Risk Management and Performance Gaps
2.3 ISO/IEC 27002 Standard
2.4 Research problem theory: analytical, theoretical frameworks and related research issues or propositions
2.4.1 Awareness Importance and the ISO/IEC 27002 Standard
2.4.2 Awareness Capability and Situation Awareness
2.4.3 Awareness Risk and risk management standards
2.5 Research design - the overall ISACM model
2.5 Conclusion

Figure 2-1 Structure of Chapter 2

The foundation of this research is in the field of information security and, in particular, that of information security awareness. However, to provide a detailed insight into information security awareness this research examines and builds on a number of parent theories: information security, situation awareness and capability measurements, and risk management. This chapter examines these parent theories with a particular focus on their relationship with information security awareness.

2.2 Parent theories and classification models

This section looks into the major theories that will guide the overall research. Below is a classification model that will assist with following the sequence of this chapter.

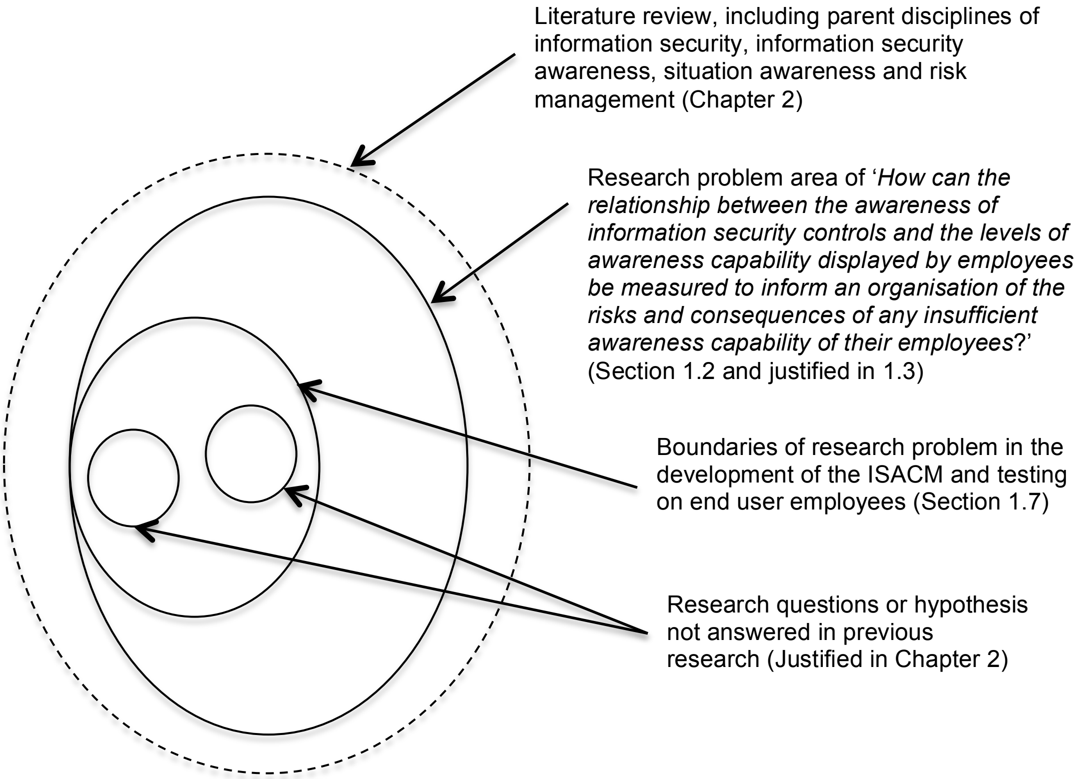

Literature review, including parent disciplines of information security, information security awareness, situation awareness and risk management (Chapter 2)
Research problem area of '*How can the relationship between the awareness of information security controls and the levels of awareness capability displayed by employees be measured to inform an organisation of the risks and consequences of any insufficient awareness capability of their employees*?' (Section 1.2 and justified in 1.3)
Boundaries of research problem in the development of the ISACM and testing on end user employees (Section 1.7)
Research questions or hypothesis not answered in previous research (Justified in Chapter 2)

Figure 2-2 Relationship between the parent theories and research problem theory, and between the research problem and the research issues or propositions

2.2.1 Information security

Information security was once the realm of technical experts. In her article on *Embedding security: when technology is no longer enough*, Everett (2010, p. 7) recalls comments from Bupa's information security manager where he suggests striving for security that 'is not just seen as a geeky thing from the IT department but is something that belongs to everyone'. Supporting this idea of moving on from 'geeks running security', Dell's former director of global information security and compliance, whilst talking about having the right people to implement security successfully, said 'I can go hire geek after geek after geek to do penetration testing or application assurance, but if there is no business acumen there, I do not know how much value that provides' (Johnson & Goetz 2007, p. 20). Technology knowledge and skills are no longer enough to provide suitable levels of information security controls (Hu et al. 2012; Narain Singh, Gupta & Ojha 2014).

Traditionally, information security was something information technology (IT) departments looked after, and in that IT department it was often an individual or small group of information security professionals who controlled 'IT security stuff'. It was also seen purely as a cost. Early attempts as captured in a 1995 conference on information security (Murray) included a presentation titled "Security should pay: it should not cost". Focused research such as "Balanced Integration of Information

Security into Business Management" (Anttila, Kajava & RaunoVaronen 2004), "Senior Executives Commitment to Information Security - from Motivation to Responsibility" (Kajava et al. 2006), and "Embedding Information Security into the Organization" (Johnson & Goetz 2007) helped highlight that information security was not an issue purely the domain of an organisation's information technology staff.

In more recent times it has been the advent of publicity generated by Wikileaks (US Government & Lew 2010) that has helped to reinforce this message that information security is not purely a concern of IT professionals. In an article highlighting the impact that Wikileaks has had on information security, Parkinson (2011, p. 25) says it is 'important to get senior managers to value security'; and for information security to be effective it needs 'leadership and guidance from the top'. It is not just about the IT department anymore, Wikileaks-related reporting certainly had non-IT department people sitting up and talking about information security. Events since then, such as leaked celebrity nude photos and hacked celebrity voicemail accounts have reinforced this message.

Widespread use of information technology

Information technology has permeated every aspect of society. Society uses it for seeking information via the Internet (Moghe et al. 2014), for improving outcomes in the healthcare sector (Patil & Patil 2014), for purchasing items online (Venkatesh, Thong & Xu 2012), for ones banking (Safeena, Kammani & Date 2014) and to communicate (Hetling, Watson & Horgan 2014). Educational institutions are increasingly using technology in their curriculum. Chai, Bagchi-Sen et al. (2006) highlight the 'need to provide more information security education opportunities to students as well as chances for students to be exposed to information security issues' such as phishing attempts or social media hacks. It is not just about teaching students how to use IT, but how to be safe and secure whilst using information technology.

The growth and prevalence of social media applications such as Facebook and Twitter has increased the information security focus. Identity theft is now impacting on all age groups using social media and IT in general (Kirk 2014; Seda 2014). Gray and Christiansen (2010, p. 17) describe how adolescences generally lack awareness about 'protecting their privacy online' or 'future implications of creating a digital footprint'. Clearly, raising information security awareness would be beneficial to people in general. The elderly, many of whom may have no previous exposure to IT are now embracing computing (Ramon-Jeronimo, Peral-Peral & Arenas-Gaitan 2013). Some may only use computers for email and Facebook to communicate with grandchildren, but even that presents information security challenges.

Spam and phishing emails are foreign to many of the elderly, many of whom grew up in a time of physical mail with its associated markings that show where and whom the mail came from. There was minimal fake physical mail sent, particularly to individuals, and when it occurred it did not occur on a mass scale. Now, as the elderly move across to the electronic age, they would therefore naturally assume that 'if it says the email is from Bill Gates then it must be from him'.

A case study examining *Uses of Internet and mobile technology in health systems for the elderly* (Lam & Chung 2010, p. 40) found that 'levels of computer anxiety decreased and levels of efficacy increasing after training'. Various seniors-related organisations conduct computer related training and include details of information security and associated risks. One such association (Australian Seniors Computer Clubs Association [ASCCA] 2013) assists clubs to educate seniors in using computer technology. They also provide seniors with computer club starter kits, promote *National Cyber Security Awareness Week* and provide links to web sites (Australian Government 2013b) focused on helping people stay safe whilst online.

Businesses and educational organisations use technology in ever-increasing ways. This explosion of use of technology has also attracted a criminal element. Moore (2010, p. 104) relates that 'one key way in which malicious parties capitalise on Internet insecurity is by committing online identity theft', as well as the growth in industrial cyber espionage. Moore's paper is 'designed to raise awareness of cyber security issues and assign responsibility for action'. Their article goes beyond technical solutions and looks at the economic consequences. Coupled with increasing use of social media, and the availability of personal information on the Internet, criminal activities such as identity theft and the subsequent financial gains associated with this is increasing.

Increased online transaction activity has seen increased identity theft (Lai, Li & Hsieh 2012, p. 353) occurring 'in any industry such as general business, educational institutions, government/military, healthcare, and banking/credit/financial services'. A recent Australian government survey (Australian Government 2014, p. 46) found that 'identity crime continues to be of serious concern to a large number of Australians, with around two-thirds of survey respondents expressing concern about becoming a victim of identity crime in the next 12 months.'

Information security now in the mainstream

Information security now forms part of the everyday vocabulary. Major banks provide targeted information security information for their customers. The Commonwealth Bank of Australia has a dedicated web page on security and privacy (Commonwealth Bank of Australia 2015). HSBC, one of the biggest banks in the world (HSBC Holdings 2015) also include a dedicated web page on online security. In fact, the majority of financial institutions provide their online customers with this level of information with the aim of raising the awareness of their customers in relation to information security. This is primarily done because it is in the bank's own interest, but it also provides a valuable customer service, and many regulators of financial institutions would demand this of the banks.

Facebook has a dedicated page (Facebook 2015) that allows topics on security to be published. One such topic (McCarthy, Watson & Weldon-Siviy 2012) on Facebook security is for young adults, parents, and educators. Information security awareness is presented for mainstream computer users and not just the traditional IT-savvy person. As newer forms of social media have emerged over the last few years, the need for raising awareness has also increased. 'Increasing security awareness should be a concern of all companies, and indications of these technical-based dangers should be included in all social media guidelines' (Oehri & Teufel 2012, p. 3).

Many of these newer forms of social media support the sharing of photos, and we have seen much media coverage about how these photos are being hacked (SMH 2014). This is not just an issue for celebrities. Behavioural changes are needed as to what and how things are posted, and more awareness needs to be provided. In a recent survey of security risks of mobile social media, it was reported that ‘cyber attacks targeting mobile social media are rapidly increasing and becoming increasingly sophisticated, targeted, and serious’ (He 2013, p. 393).

The information security messages today are not vastly different to those that have been promoted by the IT profession for the last two decades. Looking back at an article titled *Protecting Information: Effective security controls* (Wright), this 1994 perspective advocated that ‘information security must originate from the top’. It also suggests that ‘employees pose the greatest challenge to information security’ and in terms of access control ‘this type of control restricts information access according to the sensitivity of the information and the level of trust associated with the user’.

Current information security messages still call for the need to limit access to information (Rajagopal et al. 2014); the need for protecting and changing passwords regularly (Parsons et al. 2014); IT departments to harden their IT systems (European Network and Information Security Agency (ENISA) et al. 2012); organisations and individuals to deploy virus protection (Maqousi, Balikhina & Mackay 2013); and for organisations to obtain senior management support for information security activities. These are not new messages and all remain relevant today. What is changing though is the audience that these messages are being targeted towards, and the attack vectors that are being used to exploit information security vulnerabilities. The embrace of social media by the general public, and the resultant high profile stolen Twitter and Facebook accounts of celebrities, highlights the issue of information security to the general public in very real terms that they can relate to.

A 2013 warning of 250,000 Twitter accounts being hacked in the UK (Sawer 2013) is just one of many such reports appearing in the mainstream media highlighting the information security risks associated with using social media. These news stories are no longer restricted to the technical pages of computer magazines and journals and are increasingly making the front pages of mass media publications. Also in 2013 was the reported theft of some 2 million ‘user credentials from Web sites such as Facebook, Google, Yahoo, Twitter and LinkedIn’ (Tsukayama 2013). Whilst events associated with Wikileaks have played their part in raising awareness, recent reports of stolen nude photos of female celebrities (SMH 2014) attributed to hackers have continued to reinforce the risks associated with using social networking sites such as Facebook to computer users in general. The reporting in the mass media of the theft of banking credentials and other financially-motivated identity theft adds to the awareness being raised with the public in general.

A memorandum titled *WikiLeaks - Mishandling of Classified Information* (US Government & Lew 2010) sent to the Heads of Executive Departments and Agencies in the US reinforced the need to ‘establish a security assessment team’ and to ‘review the agency’s implementation of procedures for safeguarding classified information’. Further instructions in that memorandum required agencies to ‘ensure that users do not have broader access than is necessary’ and, finally, to ‘restricting usage of, and removable media capabilities from, classified government computer networks’. None of these messages, or the weaknesses they target, are new.

A US Government report titled *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* by the Honourable Stephen Horn (2000, p. 2) highlighted 'significant weaknesses in each of the 24 agencies'. These Federal Agencies 'were not fully aware of the information security risks' and the report concluded 'poor security program management and poor administration of available control techniques' were the primary cause for security breaches. Perhaps the more recent 2010 memorandum, *WikiLeaks - Mishandling of Classified Information*, and the audience (Heads of departments rather that IT security professionals) indicates a shift of focus away from IT staff and more towards senior management.

The information security profession has grown over the last 5-10 years with professional certifications such as ISACA's (Information Systems Audit and Control Association [ISACA] 2015) Certified Information Security Manager (CISM), Certified Information Security Auditor (CISA), the more technically-focused Certified Information System Security Professional (CISSP) offered by the International Information Systems Security Certification Consortium (ISC)^2 (2015), and SABSA (Sherwood Applied Business Security Architecture [SABSA] 2015). Those offered by ISACA have more than a technical focus and reach out to the IT audit and IT risk communities. Furthermore, we see many universities increasingly specialising in the provision of information security focused courses and programs. In relation to the top 10 universities in Australia, some of the courses offered include:

- Information Security Management at the University of Sydney
- Information Security at the University of Queensland
- Intelligence and Security at the Australian National University
- Master of Networks and Security at Monash University
- Cyber security at the University of New South Wales
- Digital forensics at the University of Western Australia

Whilst there are controls available to assist good information security practices, and the technology to implement these controls continues to improve, awareness of information security appears to continue to lag. For example, in the health sector researchers have concluded that 'the largest security threat facing health organizations is the insecure behavior of its own IS users' and that 'there is a lack of frameworks for the security of health information systems which are based on the security culture and the security awareness of users' (Shahri, Ismail & Rahim 2013).

Research has been conducted in order to understand 'why mainstream information security awareness techniques have failed to evolve at the same rate as automated technical security controls'. Stewart and Lacey (2012) found that using a technical expert in the field of information security to inform their audience what they believe they should know has its failings. They suggest that it is not enough to focus solely on the 'what' behaviours, but they must also understand the 'why'. This is where the *awareness importance* rating of this current research can better target awareness that is relevant to a particular stakeholder. This research includes three key stakeholder groups: IT staff, senior management, and end users.

Technical controls are become cheaper and more readily available to the non-technical audience. For example, controls for data backup are very cheap and do not require an IT professional to implement. A 2 TB external backup device with the software to perform the backup and encrypt the data is available for around $100. However, these controls are not always implemented and organisations continue to lose precious data. The *Disaster Recovery Survey 2012 for the Middle East, Turkey and Morocco* (VansonBourne) found some 'organisations who only recognised that their backup/disaster recovery procedures/technologies were insufficient for their needs once they had experienced a data loss'. This indicates a lack of awareness or relevance of information security from those particular organisations.

Puhakainen and Siponen (2010, p. 774) suggest providing 'IS security training, calls for the use of learning tasks that are of personal relevance to the learners'. From a guidance and best practice perspective for managing information security, the key international standards provide a suitable starting point for most organisations. Details of these standards are covered in the section below. ISACA (Information Systems Audit and Control Association [ISACA] et al. 2011, p. 37) in their book *Creating a Security Culture* suggest that the ISO/IEC 27000 series of international standards 'do represent a framework and a lexicon for security that are accepted internationally and must be respected even if not always observed'.

2.2.2 ISO/IEC 27000 framework

To provide a solid anchor point for measuring and evaluating information security awareness in terms of the risks that poor awareness in employees may pose to organisations, it is important to utilise a well-regarded framework for information security itself. The International Organisation for Standardization provides such a framework. According to the ISO/IEC 27001 standard (Standards Australia/Standards New Zealand 2006a), the standards in the ISO/IEC 27000 stream 'specify the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS (information security management systems) within the context of the organisation's overall business risk'. However, support by organisational senior management is also vital (Hu et al. 2012; Narain Singh, Gupta & Ojha 2014). They bear the ultimate responsibility for information security and the 'information security policy represents the position of senior management toward information security, and sets the tone for the entire organization' (Kajava et al. 2006, p. 1520).

Ramirez (2006, p. 1) suggests that some of the main problems for security projects in the 1980s and 1990s was 'the absence of security awareness and senior management support'. He also suggests 'ISO 27001 presents a new opportunity to articulate the information security policy to all the business areas and define a company wide framework'. The ISO/IEC 27000 stream of standards, and in particular ISO/IEC 27002 'is the choice of many enterprises for developing security programs' (Srinivasan 2012, p. 127). A 2013 survey of management system standard certifications showed that 22,293 ISO 27001 certifications were issued in 2013, representing a growth of 14% on the previous year (International Organization for Standardization (ISO) 2013). The adoption of this series of information security standards by organisations (as demonstrated by the high levels of certification), and the international recognition of this standard were key reasons for selecting this standard for use within this research.

This current research has used these standards as a reference point of security control objectives that organisations should have implemented or at least considered. An importance rating of awareness is determined, as well as a method on how to measure employees' awareness capability of those controls. These aspects are further described below in the section on situation awareness. With the focus of the ISO/IEC 27000 stream of information security standards being the organisation, this research limits the analysis of stakeholders to those existing within an organisation. This does not mean that other participants outside of the organisation such as suppliers, customers, general public, etc. are not important from an information security perspective, but information security in relation to these other participants is covered within the family of ISO/IEC 27000 standards. For example, *External Parties* is not a stakeholder but is addressed by one of the 39 main security categories and their associated control objectives in the ISO/IEC 27002 standard.

It is important that those stakeholders within the organisation be assessed in terms of information security of the organisation. A simple example may assist with clarifying the exclusion of any external party as stakeholders as part of the scope of this research. Many banks provide guidance and terms and conditions to their customers in relation to online usage, selection of passwords and PINs, etc. The main focus of this guidance and terms and conditions of use in relation to online banking services is not to protect the banks' overall information security, but is primarily aimed at protecting the customer. The bank would have already taken into account (including via security controls for external parties) the 'threat' that a customer (or other external party) could pose to their systems and they would have implemented suitable controls. It is the assessment of the organisation's internal stakeholders (IT staff, senior management, end users) rather than the external parties that is the focus of this current research.

2.2.2.1 How aspects of ISO/IEC 27002 help contribute to better security

This research targets three key stakeholder groups within an organisation. They are the IT staff (including information security officers) responsible for developing and managing information systems, senior management (such as C class officers) who are the key decision makers within an organisation and whose support of information security is crucial, and end users who are the main consumers of these information systems. The ISO/IEC 27002 standard covers a code of practice for information security management, including a detailed level of best practices that organisations should at least consider, although the applicability of these best practices will vary for every organisation.

The detailed information and guidance on implementing information security holistically in an organisation contained within these standards not only provides what (information security policy, procedures and controls) should be considered for the organisation, but it also describes why these are important. This 'why' factor is important for determining whether an information security control is applicable to a particular organisation. In information security practices, it is often the 'why' explanation that is missing. ISO/IEC 27002 can help address this information gap for organisations endeavouring to implement effective security practices.

Information security standards also form the foundations for many professional services organisations to use when undertaking information security audit and consulting services to many of the largest organisations in the world (KPMG Australia 2015; PriceWaterhouseCoopers 2014). Much of the development of the ISO/IEC 27000 information security standards is occurring with the assistance of ISACA, and their information security expert members. ISACA is 'an independent, nonprofit, global association. ISACA engage in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems' (Information Systems Audit and Control Association [ISACA] 2015). As of 2015, ISACA have 115,000 constituents in 180 countries. These members undertake IT audits and information security consulting reviews of organisations (often as employees of professional services organisations such as KPMG), utilizing standards such as ISO/IEC 27002.

There is an expectation that the controls in these information security standards have been considered, and either deployed or that there is suitable reasoning as to why they are not needed in a particular organisation. In a joint exercise by the IT Governance Institute and the UK Office of Government Commerce, and made available by ISACA (the primary organisation providing IT audit certification and guidance to auditors), they brought together a number of technology related international standards. Their reasoning for doing so included 'increasingly, the use of standards and best practices, such as ITIL, CobiT and ISO/IEC 27002, is being driven by business requirements for improved performance, value transparency and increased control over IT activities' (IT Governance Institute (ITGI) 2008).

The 11 security control clauses covered in the ISO/IEC 27002 standard are listed in Table 2-1 below, whilst section 2.3 discusses in depth the key aspects of these 11 security control clauses and identifies points of importance for organisations in terms of information security awareness. The three stakeholder groups are discussed in turn for each of these 11 security control clauses in relation to what is important from an information security awareness perspective for each stakeholder group.

Table 2-1 Eleven security control clauses of ISO/IEC 27002

1. Security Policy
2. Organisation of Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems, Acquisition, Development and Maintenance
9. Information Security Incident Management
10. Business Continuity Management
11. Compliance

2.2.3 Information security awareness

Before analysing the role that awareness plays within the discipline of information security, it is important to describe awareness as a concept. In her book on awareness, Nunn (1995) equates awareness with consciousness. Vaneechoutte (2000, p. 437) suggests that 'consciousness might be better understood by considering it as a special form of awareness'. Other sources, including Wikipedia (2011), suggest awareness contain aspects such as 'ability to perceive' and 'conscious of events' when they describe awareness. Other definitions (Cambridge Dictionaries Online 2011) include 'understanding of a situation', knowledge that something exists, or understanding of a situation or subject at the present time based on information or experience.

There are also various synonyms for awareness such as comprehension, perception, alertness, understanding and recognition. Writers using these terms can often be seen as referring to awareness. Therefore, when assessing an employee who requires 'a good understanding of something', this could be seen as implying that the employee is required to have sufficient awareness of a particular thing. The terms awareness importance, awareness capability and awareness risk are developed in this research and have been defined earlier in section 1.6 on page 13. The relevance of these three key terms is described further in this chapter. The scope of awareness within this research is in terms of how it relations to awareness of aspects of information security. In particular, the importance that awareness has in terms of understanding information security controls, how a person's capability of this awareness can be measures, and the risk to an organisation when the required level of awareness of information security controls is not demonstrated.

There is a large body of published literature (a selection is shown below in Table 2-2) that describes various aspects of information security awareness. The topics range from methodologies on designing an awareness program through to guidelines that can be used to provide the awareness, and governance aspects of information security. The amount of available literature provided a high degree of confidence that there is a sufficient existing knowledge available as a base to support this research.

Table 2-2: Information Security Awareness related Literature

Key Topics	Article Title	Authors
Awareness	Prototypes for assessing information security awareness	(Kruger & Kearney 2006)
Awareness	The impact of information richness on information security awareness training effectiveness	(Shaw et al. 2009)
Awareness	Information security awareness: Beyond new user orientation	(Tompkins 2008)
Awareness	A security standards' framework to facilitate best practices' awareness and conformity	(TsohouKokolakis, et al. 2010)
Awareness	An Effective Method for Information Security Awareness Raising Initiatives	(Maqousi, Balikhina & Mackay 2013)
Awareness Guidelines	The new users' guide: How to raise information security awareness	(European Network and Information Security Agency (ENISA) et al. 2008)
Awareness Methodology	Design theory for information security awareness	(Puhakainen 2006)
Awareness Methodology	An Effective Method for Information Security Awareness Raising Initiatives	(Maqousi, Balikhina & Mackay 2013)
Certification	Formal information security certifications	(Information Systems Audit and Control Association [ISACA] 2015)
Security Culture	Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness	(Herath & Rao 2009)

Key Topics	Article Title	Authors
Security Culture	Information security culture – validation of an assessment instrument	(Veiga, Martins & Eloff 2007)
Security Culture	A cross-cultural investigation of situational information security awareness programs	(Chen, Medlin & Shaw 2008)
Security Culture	A framework and assessment instrument for information security culture	(Da Veiga & Eloff 2010)
Security Culture	Security Culture and Security Awareness as the Basic Factors for Security Effectiveness in Health Information Systems	(Shahri, Ismail & Rahim 2013)
Security Culture	Information security culture: A management perspective	(Van Niekerk & Von Solms 2010)
Security Awareness Guidelines	59 approaches to Information security awareness	(Puhakainen 2006)
Security Governance	In a 'trusting' environment, everyone is responsible for information security	(Williams 2008a)
Security Governance	Information security governance: A risk assessment approach to health information systems protection	(Williams 2013)
Security Awareness Guidelines	Employees' Information Security Awareness and Behavior: A Literature Review	(Lebek et al. 2013)
Security Awareness Guidelines	Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study	(Albrechtsen & Hovden 2010)
Security Awareness Guidelines	The new users guide: How to raise information security awareness	(European Network and Information Security Agency (ENISA) 2010)
Industry Perspectives	Information Security Solved: Economics of IT Conference 2006	(Gartner & Wagner 2006)
Industry Perspectives	IT security needs makeover: experts	(Dearne 2008a)
Measures	Measuring user satisfaction with information security practices	(Montesdioca & Maçada 2015)
Measures	2010 MAAWG Email Security Awareness and Usage Report	(Ipsos Public Affairs 2010)
Measures	Assessing insider threats to information security using technical, behavioural and organisational measures	(Sarkar 2010)
Measures	Using Shared Priorities to Measure Shared Situation Awareness	(Höglund, Berggren & Nählinder 2009)
Methodology	Security Maturity Models	(Chege 2007)
Methodology	A methodology for security assurance-driven system development	(Vivas, Agudo & López 2010)
Methodology	How Effective Is Your Security Awareness Program? An Evaluation Methodology	(Rantos, Fysarakis & Manifavas 2012)
Methodology	A New Data Classification Methodology to Enhance Utility Data Security	(Rajagopal et al. 2014)
Practices	Application of CMM to medical security capability	(Williams 2008b)
Practices	Streamline ISO/IEC 27001 Implementation: Reducing the Time and Effort Required for Compliance	(Ramirez 2006)
Survey	Online users lack security skills	(Dearne 2008b)
Training	The Department of Health and Human Services Information Systems Security Awareness Training	(US Government 2014)
Vendors	IT vendor views on information security	(Microsoft 2008)

2.2.3.1 Importance of information security awareness to organisations

Information security awareness was highlighted (Tsohou, Angeliki et al. 2008, p. 271) as being important 'for information security effectiveness'. Siponen (2000, p.

31) says information security awareness is 'where users in an organisation are aware of – ideally committed to – their security mission'. He uses a behavioural science framework approach and suggests empirical studies need to consider the validity of the persuasion framework presented. The Australian Attorney-General's Department (2007, p. 3) also promotes information security awareness. They suggest that one of the seven basic principles of information security requires understanding and commitment. In particular, they suggest that 'awareness and understanding within the organisation' helps to support the culture of security within an organisation.

Information security is one priority for the *Australian Research Council Centre of Excellence in Policing and Security via National Research Priorities - Safeguarding Australia* (Australian Research Council [ARC] 2007, p. 2) emphasising 'personal identification, information protection and the integrity of security systems are fundamental towards ensuring the national security of Australia'. Specific research into evaluating security awareness (Drevin, Kruger & Steyn 2007, p. 36) suggest 'security awareness is important to being able to reduce error, theft, fraud, and misuse of computer assets'. These researchers conclude a robust information security culture cannot 'develop and grow in a company without awareness programs'. They suggest a value-focused approach to developing and delivering security awareness, but it does not present guidance on how to measure these programs.

Kruger, Drevin and Steyn (2010, p. 316) examined whether it is possible to assess information security awareness on the basis that there is a dependence on humans and that 'to protect information assets necessitates an information security awareness program'. This is required in order to raise awareness around individual's information security responsibilities. Further research (Shaw et al. 2009, p. 92) showed that 'information security awareness is becoming an important issue to anyone using the Internet' and these researchers believe that in order to reduce losses, it is important for organisations to prioritise information security awareness.

2.2.3.2 Conducting information security awareness training

There is much advice in the existing literature related to what to include in security awareness programs. One such literature is from the SANS Institute (2015) titled *Securing the Human*. Much of the available literature is commercially produced and aimed at selling organisations either an information security awareness kit or offering consultancy for conducting the awareness training. There is also non-commercially focused literature available including research by Desman (2002) who presents an overall approach to building an information security awareness program.

The National Institute of Standards and Technology (NIST) web site (2015) contains often-quoted IT guidelines and standards literature, as well as material about information security and awareness (Wilson & Hash 2003, p. 36) that highlights 'formal evaluation and feedback mechanisms are critical components of any security awareness, training, and education program'. It describes an approach in terms of using questionnaires and evaluation forms, focus groups, and selective interviews. It has a practitioner focus and includes background information and resources on the measurement and evaluation of information security awareness in terms of framework and approach. Abawajy, Thatcher et al. (2008, p. 473) highlight awareness programs have not been designed or delivered taking into account 'effects of weakness of will and lack of commitment of the stakeholders'. Additional literature (Tsohou, Aggeliki et al. 2008, p. 207) attempts to gain 'a better understanding of the reasons why security awareness practice remains an unsolved problem'. Not all awareness programs are effective, and more research is needed to determine why they fail. Without a mechanism to measure success, it is difficult to determine what is effective and what works.

2.2.3.3 Measuring information security awareness

Siponen and Kajava (1998) suggest measurement of information security awareness can be approached from two angles. Organisations should measure, verify and validate the formal part - as well as look at the content of the programs to determine their effectiveness. Results of security education should be measured to verify they meet their goals. Yngström and Björck (1999, p. 18) suggest that by measuring the impact of security education and training, one is trying to 'measure the resulting change in human behaviour and its impact on the organisation'. This view supports the focus of this research on the human behaviour aspects of situation awareness.

The Information Warfare Site (IWS) (2008) provides material describing information security measures, together with details on how to deliver information security awareness. Wright (2006, p. 1), in *Measuring the Effectiveness of Security*, does not focus on information security awareness, but he does relate how measurement (controls effectiveness) and ISO/IEC 27001 are linked and how the standard calls for a 'requirement to measure the effectiveness of selected controls'. This ISO/IEC 27001 standard (and supporting standard ISO/IEC 27002) provides a large volume of support material, audit programs and consultants' reports linking information security controls with approaches on assessing the effectiveness of that control. This provides support material for developing a model to measure the capability and effectiveness of security awareness based on control objectives awareness.

A key resource for this research is the international standards ISO/IEC 27000 series on information security. The ISO/IEC 27000 standards framework was discussed earlier, whilst the details on how information security awareness will be measured is discussed in the methodology chapters of this thesis. Situation awareness and risk management theory complete the trio of theories that provide a theoretical basis for the conceptual model of the ISACM. These aspects are covered in sections 2.2.4 and 2.2.5. In their literature on an assessment instrument for information security culture, Da Veiga and Eloff (2010, p. 205) describe their *Information Security Culture Framework (ISCF)* and how it 'is used as the input to develop an assessment instrument for assessing the information security culture in an organisation'.

Whilst higher levels of information security awareness should lead to more effective actions by employees in an organisation, measurements of the relationships between information security awareness and actions taken towards improving information security are sparse. Choi, Kim et al. (2008, p. 495) found 'although it may seem intuitive that higher MISA (managerial information security awareness) leads to more MATIS (managerial actions toward information security), empirical studies that investigate the relationship are conspicuously absent'. A measurement mechanism is therefore required.

2.2.4 Situation Awareness (SA) and Capability Measurement

With the major focus of this research being on awareness, it is important to look at theories of how humans acquire and manage awareness. Many of these theories stem from human factors and cognitive theories. Curts et al. (2002, p. 39) suggest that the OODA (observe, orient, decide and act) loop, and cognitive hierarchy may be relevant in understanding how humans acquire knowledge and then act. Another theory is the Shewhart or Deming Cycle of Plan-Do-Check-Act (PDCA) that describes a cyclical approach to undertaking tasks.

An area of study of human factors is described by Endsley and Garland (2000, pp. 5-8) as Situation Awareness (SA). They relate a definition of SA as '…the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future'. It is about being aware of information or cues in your environment, and then determining what might happen next, or what will happen if you take a certain course of action. Much of the early focus on SA was on pilots in the aviation industry and in the military and, in particular, problems with SA are quoted (Endsley & Robertson 2001) as having been accountable for 88% of pilot errors that involved human error. SA appears to be a suitable theory of understanding information security awareness in an organisational context (James et al. 2013; Kokar & Endsley 2012; Sim, Liginlal & Khansa 2012; Webb et al. 2014).

SA provides a theoretical framework that could be applicable to information security awareness, as many information security incidents or events are the result of human errors. For example, people are aware of computer viruses, but still many people readily click on unknown links and attachments due to a lack of situational awareness of the risks associated with them. Although theories such as OODA and PDCA present a suitable foundation for analysing how humans undertake learning, SA provides an extensive theory and associated model. SA begins with aspects of awareness, can be used to analyse and measure goals and decision tasks, and attempts to predict future states. SA is a multi-level model encompassing *perceptions* of cues or information at the *Level 1* stage; focuses on *comprehension* aspects of current situations at the *Level 2* stage; and attempts to *project* or forecast future situations in the *Level 3* stage (Howard & Cambria 2013; Webb et al. 2014). It has linkages to information security awareness that forms a key part of this research.

In 2008, it was suggested (Wickens 2008, p. 397) that 'during the past 15 years, the concept of situation awareness has entered the mainstream of human factors'. Much of the initial focus of SA was its application to aircraft pilots and the military (Masys 2005; Matthews & Beal 2002; Strater et al. 2001; Uhlarik & Comerford 2002), and how awareness of their situation influenced their decision-making. Subsequently researchers have expanded that view and described how SA may be applicable in other fields. In their article on the public's preparedness for natural disasters, Ravitz, Shyu et al. (2010) describe how a system could 'integrate meteorological data…with the aim of improving…by increasing their situational awareness due to such natural threats'. Additionally, a 2012 description of using SA derived from Twitter to assist with crisis management (Cameron et al. 2012) shows its expanding usage in emergency management (YinKarimi, et al. 2012; YinLampert, et al. 2012).

Tomaszewski (2011, p. 87) purports that a ‘lack of situation awareness is a recurring problem in disaster management’. Perhaps a lack of situation awareness may also be a recurring problem for information security incidents? Regarding the everyday activity of driving a car, a 2010 article (Johannsdottir & Herdman, p. 665) describes how current research is looking at techniques to ‘play a role in supporting a driver’s SA for traffic in the forward view’. SA is increasingly being used in many non-military/air force disciplines (James et al. 2013).

This research examines the role that SA can play in information security awareness. More relevant to this thesis is the application of SA to technology fields, and in particular information security. For example, in their article on *Internet Situation Awareness*, Hesse and Pohlmann (2008, p. 8) state that SA will help ‘to improve the stability and trustworthiness of the Internet, raise awareness for critical processes or components of the Internet, and find out more about the Internet and its users in order to better cater to their needs and service demands’. Similarly, in their article related to network intrusion detection systems, Folorunso, Taofiki, et al. (2010, p. 246) describe how to ‘increase situation awareness for users needing to synthesize large amounts of intrusive data and make critical decisions under time pressure’.

Cyber Situational Awareness (Jajodia et al. (2010)) presents recent developments in SA research in relation to information security. It aims to ‘establish the state of the art in the cyber situational awareness field to set the course for future research’ and covers a variety of computer and network security research topics. Tadda and Salerno’s (Jajodia et al., p. 20) presents a SA reference model that builds upon Endsley and Garland’s model (2000) containing three levels of SA: Perception, Comprehension and Projection (Endsley & Garland 2000, p. 6), but provides two additional levels (levels 0 and level 4). Many of these enhancements could have applications to information security awareness. Not only does this model provide a source of knowledge in terms of situation awareness as an information-processing model, but the associated measurement tools could assist with the development of an instrument for measuring SA as it applies to information security awareness. In examining the applicability of SA as a theoretical framework for measuring information security awareness, it is worthwhile to examine the general definitions that make up the original three levels of SA. This examination is outlined below.

2.2.4.1 Level 1 situation awareness - perception

Definitions for perception include ‘the ability to see, hear, or become aware of something through the senses’ (Oxford Dictionaries 2015c) and ‘the way you think about or understand someone or something, the ability to understand or notice something easily, the way that you notice or understand something using one of your senses’ (Merriam-Webster Dictionary 2015d). Perception has links to awareness and understanding and implies some knowledge or ability to gain that knowledge. In an information security awareness context, it could imply that ‘I know there is something about attachments of unsolicited emails that could be risky, but that is as much as I know’. It could equate to a low level of knowledge. Early literature on SA suggests that the first step required to achieve SA is ‘to perceive the status, attributes, and dynamics of relevant elements in the environment’ (Endsley 1995, p. 36). It is this that provides an initial insight and is categorised as Level 1 SA. So perception is part of the journey towards SA, but not the full story.

2.2.4.2 Level 2 situation awareness - comprehension

Definitions for comprehension include ‘the ability to understand something’ (Oxford Dictionaries 2015b) and ‘ability to understand, the act or action of grasping with the intellect’ (Merriam-Webster Dictionary 2015c). Comprehension suggests a greater level of understanding than that described by perception. In an information security awareness context, it could imply that ‘not only do I know that attachments of unsolicited emails could be risky, but I know that the attachment may contain malware code’. It could equate to understanding significantly more about the situation (when compared to a general level of perception), and enough to influence actions that may be taken. Early literature on SA suggests that ‘Level 2 SA goes beyond simply being aware of the elements that are present to include an understanding of the significance of those elements’ (Endsley 1995, p. 37). There is comprehension of the situation.

2.2.4.3 Level 3 situation awareness - projection

Definitions for projection include ‘estimate or forecast of a future situation based on a study of present trends’ (Oxford Dictionaries 2015a) and ‘what might happen in the future based on what is happening now’ (Merriam-Webster Dictionary 2015b). Projection suggests a deep understanding of what is likely to happen, given what has been perceived and comprehended about a particular situation.

From an information security awareness perspective, and continuing with the comprehension example described above, ‘not only do I know attachments of unsolicited emails could be risky, and I also know that the attachment may contain malware code, but I also know that if I open that attachment then it may infect my computer, steal my identity, and probably result in financial theft’. It equates to being able to predict what is likely to happen next. Early literature on SA suggest that this third and highest level of SA provides ‘the ability to project the future actions of the elements in the environment, based on an understanding and comprehension of those elements at least in the very near term’ (Endsley 1995, p. 37).

2.2.4.4 Measuring situation awareness

Table 2-3 below summarises previous key literature that discusses different approaches to measuring situation awareness. This literature on the measurement of situation awareness provides the foundation to support the development of a specific measurement tool for this current research. The literature listed in Table 2-3 below highlights the previous measurement of situation awareness and identifies the lack of previous empirical research, which has measured situation awareness of information security risks. Hence, the measurement of situation awareness of information security risks is an important topic worthy of more investigation.

Table 2-3: Situation Awareness measurement literature

Article Topic	Authors
Cyber Situational Awareness: Issues and Research	(Jajodia et al. 2010)
Cyber-Physical Situation Awareness and Decision Support	(James et al. 2013)
A methodology for measuring team situational awareness: Situational Awareness Linked Indicators Adapted To Novel Tasks (SALIANT)	(Muñiz et al. 1998)
Situation Awareness Analysis and Measurement	(Endsley & Garland

Article Topic	**Authors**
	2000)
Situation Awareness Measurement: A review of applicability for C4i environments	(Salmon et al. 2005)
The Development of Situation Awareness Measures in ATM Systems	(European Organisation for the Safety of Air Navigation 2003)
Situation Awareness Misconceptions and Misunderstandings	(Endsley 2015)
Situation Awareness: A review of the concept and its measurement	(Breton & Rousseau 2003, p. 19)
Assessing Situation Awareness in Field Training Exercises	(Matthews & Beal 2002)
A situation awareness model for information security risk management	(Webb et al. 2014)
Behavioural Situation Awareness Measures and the Use of Decision Support Tools in Exercise Prowling Pegasus	(Kardos 2003)
Measuring Performance of Cyber Situation Awareness Systems	(Tadda 2008)
Measuring and Predicting Shared Situation Awareness in Teams	(Saner et al. 2009)
Using Shared Priorities to Measure Shared Situation Awareness	(Höglund, Berggren & Nählinder 2009)
Measuring Situation Awareness in Complex Systems - Comparison of measure study	(Salmon et al. 2008)
Measurement of individual and Team situation awareness: A critical evaluation of the available metrics and tools and their applicability to command and control environments	(Breton, Tremblay & Banbury 2007)

Measurements of SA revolve around the three SA levels: perception, comprehension and projection. Measurement of SA aims to determine where in the spectrum of SA levels a person's awareness is. Is their perception of the situation appropriate, are they able to fully comprehend the situation, and are they able to project what is likely to happen? The three levels of situation awareness relates to how capable a person is able to deal with a situation. SA provides a theoretical framework for determining the level of information security awareness capability of an individual for a specific situation. The next section provides an overview of capability measures.

2.2.4.5 Capability measurements

The next major parent literature relevant to this research is capability measurement - which plays a key role in being able to determine the awareness capability component of the ISACM. The discussion on situation awareness above provides one aspect, including a number of approaches on how to measure situation awareness. Expanding upon this, an examination of capability measurement models provides valuable insight into how to approach measuring awareness capability. This is important in this current research for determining if the current level of information security awareness being displayed is appropriate for an individual, given their particular stakeholder role within an organisation.

Williams (2008b) proposes 'the capability maturity model (CMM), to meet the needs of medical information security practice'. An examination of the applicability of this model will assist this current research. In a 2004 article on knowledge-based decision making (Kaner & Karni, p. 244), a decision making capability maturity model is presented with the view that 'facilitates the determination of key elements of current and potential decision making capabilities and identification of the knowledge management issues most critical to decision quality'. Siponen and Willison (2009, p. 268) suggest 'SSE-CMM was intended to be used in certificating the maturity level of an organisation's IS security processes'. Many of these maturity models look at attaching a maturity level to security processes within an organisation. One such model that focuses on secure e-government services (Karokola, Kowalski & Yngström 2011, p. 8) proposes the following levels described in Table 2-4 below.

Table 2-4: Karokola's Proposed Information Security Maturity Model

Level	Description
Level 1 (undefined)	meant for organizations with low information security targets in a low security risk environment – where process metrics are not compulsory. Security policies may be available. Adequate user awareness is necessary. Security risk reduction from technical and non-technical security threats occur.
Level 2 (defined):	meant for organizations with normal information security targets in a normal security risk environment. Process metrics may be used but not compulsory. At this level, security policies including awareness, visions, and strategies are reviewed and updated. More security risk reduction from technical and non-technical security threats occurs. Information security is slowly imbedded into the organizational culture.
Level 3 (managed):	meant for organizations with high information security targets in a normal or high security risk environment. Also, high-risk reduction from technical and non-technical security threats occurs. At this level process metrics may be used. In addition, security policies including awareness, visions, and strategies are regularly reviewed and updated.
Level 4 (controlled):	meant for organizations with higher information security targets in a normal or higher security risk environment. Highest security risk reduction from technical and non-technical security threats occurs. Uses of process metrics are compulsory. Information security is embedded into the culture of the organization. Additionally, Security policies, awareness, visions, and strategies are regularly reviewed and updated.
Level 5 (optimized):	meant for organizations with higher information security targets in higher security risk environments. Highest security risk reduction from technical and non-technical security threats occurs. Uses of process metrics are compulsory. Similar to the previous maturity level – security policies, awareness, visions, and strategies are regularly reviewed and updated. Information security is embedded into the culture of the organization.

Each of the capability maturity levels in Table 2-4 refers to 'awareness', but testing of that awareness is subjective and not captured within these CMM type models. Phrases such as 'displays adequate user awareness' leaves the determination of the displayed awareness capability up to the reviewer. Thus, an awareness capability measurement instrument would benefit such models. The previous discussion on SA and the tiered approach it takes could assist with developing a measure of awareness capability. Whether these models use the term capability, or knowledge management, or other organisational specific terms, they all relate to the ability to perform (and re-perform) a task based on more than just guess work or luck.

The element that most of these maturity models have in common is a scaling approach to measure maturity or capability of a process or knowledge state. They are generally presented as five distinct and upwardly maturing levels. Properties such as maturity and repeatability feature heavily in description of these maturity models. For this current research, the three levels of situation awareness theory as a cognitive and hierarchical information-processing model provides a valuable means for measuring awareness capability (Howard & Cambria 2013; Webb et al. 2014).

2.2.5 Risk management and performance gaps

Awareness risk is the third measure of the ISACM. In broad terms it is the risk that materialises when there is a gap between the required amount of awareness (as captured by the awareness importance rating) assigned to a particular situation (and in this research the situational context of an information security control objective) and the awareness capability being displayed in that situation by an individual (as captured by the awareness capability measure). Where there is a shortfall between the required level of information security awareness (importance) and the level of information security awareness being displayed (capability) by an individual for a specific situation, an awareness risk is said to exist. It is where importance is not matched by performance.

Al-Hakim (2007, p. 168) describes how Importance-Performance Grid Analysis (IPGA) (introduced by Martilla & James 1977) can provide a means for determining the 'decisive' factor. That is, it satisfies two conditions; it has a strong importance rating and it has a significant performance-importance gap. Al-Hakim relates that the grid measurement points, perception of performance and importance can be reduced to a tabular form. This could provide a suitable mechanism for capturing the measurements. He suggests '…a gap between the perceived performance and the expected importance of a dimension may provide some indication as to whether the dimension is effectively implemented'. Similar to IPGA, risk management literature provides an approach for combining elements such as likelihood and impact to form a risk measure.

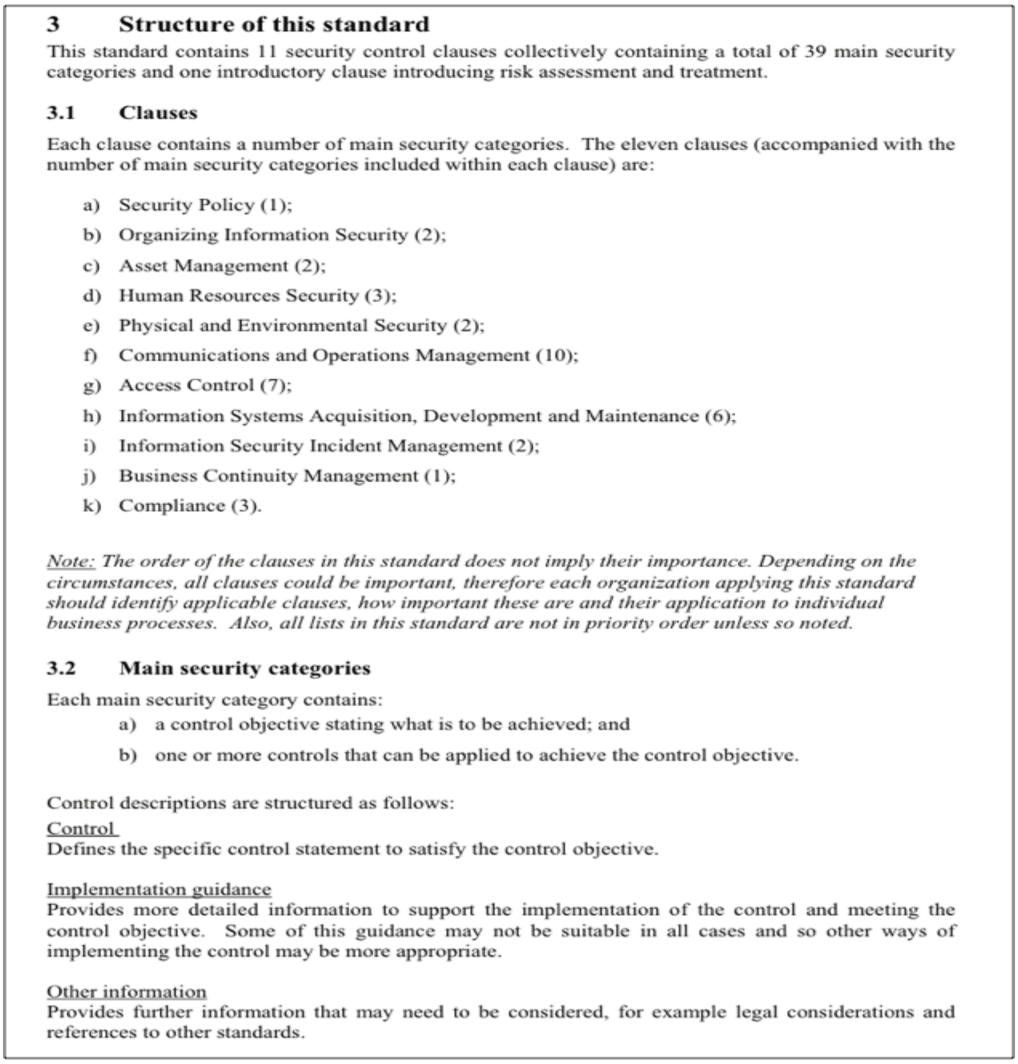
The Australian and New Zealand standard on Risk Management, AS/NZS 4360:2004, (Sai Global 2004) provides guidance on risk management. Also ISO/IEC 27005 (International Organization for Standardization (ISO) 2008) is an emerging standard for information security risk assessments which describes a grid representation (on a 5 by 5 scale) to arrive at a risk measurement for information security. *Information Security Risk Management* (Calder & Watkins 2007) examines risk management in terms of ISO/IEC 27001 and provide in-depth information on measuring impact and likelihood, as well as discussions on risk treatment and the selection of controls. This current research takes a simplified approach to awareness risk. It is the resultant gap or shortfall from the required to the demonstrated awareness that may exist in a situation for an information security event.

Baracaldo and Joshi (2013, p. 239) describe risk (in relation to access control) as 'the likelihood of a hazardous situation and its consequences if it occurs. The likelihood of occurrence can be reduced through the implementation of controls and mechanisms in the system that aims to mitigate threats'. Foreseeing this (through comprehension and projection) relates to higher levels of SA. They describe the risk exposure following the implementation of appropriate controls as the residual risk, which is ideally the level of risk an organisation is willing to accept. If unacceptable, then additional controls would be put in place.

This current research describes the gap as awareness risk, which could be addressed by increasing the level of awareness capability being demonstrated (through additional training and education), or shifting the awareness importance rating to a lower level, possibly by removing the need to know about something (e.g. by implementing additional automated controls). For example, complex password rules force an end user to choose a complex password (otherwise they cannot change their password), thus having reduced the awareness importance requirement of the end user that they should voluntarily choose a strong password.

2.3 ISO/IEC 27002 Standard

This section discusses in depth the ISO/IEC 27002 standard in terms of key aspects of these 11 security control clauses and identifies points of importance to organisations in terms of information security awareness. The three stakeholder groups: IT staff, senior management and end users are discussed in turn within each of these 11 security control clauses, as determining the appropriate level (importance) of information security awareness for each stakeholder group was the foundation of the ISACM in this research. To gain better insight into the ISO/IEC 27002 standard, the standard's structure has been reproduced in Figure 2-3 below.



3 Structure of this standard

This standard contains 11 security control clauses collectively containing a total of 39 main security categories and one introductory clause introducing risk assessment and treatment.

3.1 Clauses

Each clause contains a number of main security categories. The eleven clauses (accompanied with the number of main security categories included within each clause) are:

a) Security Policy (1);
b) Organizing Information Security (2);
c) Asset Management (2);
d) Human Resources Security (3);
e) Physical and Environmental Security (2);
f) Communications and Operations Management (10);
g) Access Control (7);
h) Information Systems Acquisition, Development and Maintenance (6);
i) Information Security Incident Management (2);
j) Business Continuity Management (1);
k) Compliance (3).

Note: The order of the clauses in this standard does not imply their importance. Depending on the circumstances, all clauses could be important, therefore each organization applying this standard should identify applicable clauses, how important these are and their application to individual business processes. Also, all lists in this standard are not in priority order unless so noted.

3.2 Main security categories

Each main security category contains:

a) a control objective stating what is to be achieved; and
b) one or more controls that can be applied to achieve the control objective.

Control descriptions are structured as follows:

Control
Defines the specific control statement to satisfy the control objective.

Implementation guidance
Provides more detailed information to support the implementation of the control and meeting the control objective. Some of this guidance may not be suitable in all cases and so other ways of implementing the control may be more appropriate.

Other information
Provides further information that may need to be considered, for example legal considerations and references to other standards.

Figure 2-3 Structure of the ISO/IEC 27002 Standard

2.3.1 Security Policy

This security policy section of the ISO/IEC 27002 (Standards Australia/Standards New Zealand 2006b, p. 7) standard aims to 'provide management direction and support for information security' and 'should be communicated throughout the organisation in a form that is relevant, accessible and understandable'. The policy should state the overall aims of information security, why it is important, and how it supports the organisation's goals. It should also include details of the roles and responsibilities of those involved in information security management, and importantly, 'rules' that end users and people managers should comply with.

D'Arcy et al. (2009, p. 83) support the notion that 'a security policy defines rules and guidelines for the proper use of organisational IS resources (i.e. acceptable use guidelines)'. Therefore it is likely that an information security policy is supported by related documents such as *Acceptable Use of Technology* and technical information security standards. Security policies are the cornerstone of an information security program and play a critical role in raising information security awareness in an organisation (Bayuk 2009). Acceptance and a willingness to follow security rules and regulations outlined by an organisation are key to strengthening information security and clearly an awareness of these rules and regulation plays a vital role (Bulgurcu, Cavusoglu & Benbasat 2010, p. 253).

The security policy and acceptable use policy should provide details of the objectives of the organisation in terms of securing information and will often outline the management strategy. It should also cover the possible consequences of a failure to comply with a policy. In many cases, policies form part of the contractual arrangement between employer and employee (such as confidentiality obligations). The lack of an information security policy could provide an employee with a simple excuse to say, 'I was not aware' or 'I did not know I was not allowed to do that'.

Whilst policies often highlight what you should not do, there is a need to include what you are allowed to do, or how you should do it. Policies supplemented with guiding principles and examples that help clarify the intent of the policy are more likely to be understood and followed than those without. In a *CIO Online* article on *How to write an information security policy* (Bayuk 2009, p. 2), it was suggested that 'policy should be reserved for mandates. Alternative implementation strategies can be stated as a responsibility, standard, process, procedure, or guideline. This allows for innovation and flexibility at the department level while still maintaining firm security objectives at the policy level'. The supplementary documents that are suggested to consider include technology standards, processes, procedures and guidelines. Providing awareness training for these policies is a key enabler to achieving awareness of the policy aims, as well as compliance.

Without suitable training and awareness, enforcement of policies may be difficult. Employees could claim they were either unaware of the policy or did not understand what it meant. Difficulties associated with information security policies include:

- They do not always align to the business objectives of the organisation;
- They contain general statements, or worse, they contain statements that are impossible to comply with (i.e. strictly for business purposes);

- It can be difficult to track and measure compliance against an information security policy;
- It can be used as an excuse by IT departments or business unit management to simply say ‘but the policy says so…’ when a genuine reason cannot be found or easily stated;
- They are not always well-supported by training or awareness programs; and
- They should be reinforced annually, but also revisited and adjusted to include what the current norm is, or to keep up with technology changes.

Awareness can be a key enabler for communicating the messages and intent of these policies, as well as aiding with achieving compliance. Organisations that just publish policies without raising awareness of their existence or explaining what the policy is intended to do (such as help the organisation protect data, or prevent identity theft), risk not gaining employee buy-in and will find compliance and adherence to the policy difficult to achieve. Bulgurcu et al. (2010, p. 542) found that ‘security awareness can directly and indirectly alter employees belief sets about compliance with the information security policy’. They also found that ‘creating a security-aware culture within the organization will improve information security’. Al-Omari et al. (2012, p. 3323) are developing models for improving compliance with information security policies (ISP) and believe that ‘information security awareness likely plays a major role in shaping user compliance behavior with ISPs’.

Security policies can be difficult to enforce and there is a reliance on people choosing to abide with organisational policies. When end users are aware that information security policies exist, and that they can protect the organisation as well as the end users, and what the consequences of violating aspects of those security policies are, then end users may be less likely to engage in the misuse of IT within their organisation (D'Arcy, Hovav & Galletta 2009, p. 92). All three stakeholders (IT staff, senior management, and end users) need a certain level of awareness of security policies. Below is a summary of the relevance that awareness plays for each of these stakeholders in relation to security policies.

Senior management plays a crucial role in the ownership and support of information security policies (Holmberg & Sundström 2012; Tejay & Barton 2013), therefore, awareness of the intent of information security and an understanding of the assignment of information security management roles and responsibilities is vital. Senior management cast a long shadow and ‘the espoused values can be seen as the “visible” contribution of the organization’s management towards the organisation’s culture’ (Van Niekerk & Von Solms 2010). A 2006 empirical study (Knapp et al.) found that support by senior management played a significant role in determining the security culture and policy compliance within an organisation.

Senior management’s influence and ownership over information security policies is a key factor in the success of these policies. Senior management should also be aware of the need for ensuring that policies are regularly reviewed, both by internal staff and external experts. Senior management are also often answerable to audit and risk committees within their organisation, and any adverse information security-related audit findings would ultimately require senior management’s attention. This is particularly relevant for public reporting organisations and boards.

IT staff provide much of the day-to-day management and enforcement of the elements contained within the information security policies, often through a dedicated information security team. These staff usually advise on the initial creation of the information security policies, and advise when changes may be required. These staff are required to understand how to translate between the non-technical business requirements of the organisation contained in the policy and the technical nature of information security measures that need to be implemented. For example, senior management's business requirement may be to 'only provide data to external organisations by sending that data in a secure manner'. This would require IT staff to translate (usually into a policy supporting standard or procedure) that, for example, all data transmissions would be conducted in a certain technical manner (such as using HTTP over SSL) using encryption (triple DES) as a technical control.

Finally, the end user must be aware of the information security policies, be aware of the intent behind the policies statements, be aware of how it will protect them and their organisation, and be aware of how they will be able to comply with the information security policies. The end users should also be aware of the consequences should they choose not to comply. A study on information security policy compliance (Bulgurcu, Cavusoglu & Benbasat 2010, p. 524) found the end user (employee) is the 'weakest link in information security' but can also play a key role in an organisation that is trying to 'reduce risk related to information security'.

Furthermore, they found that the information security policy was a 'statement of the roles and responsibilities of the employees'. To that extent the information security policy becomes a set of rules and regulations that would guide and compel end users in terms of how they should behave, what they would and would not be allowed to do (i.e. take data home on an unencrypted USB device), and consequences in the event of a deliberate breach of the information security policy.

There is an abundance of existing literature highlighting that many security risks that organisations face are internal within an organisation and often have greater impact in comparison to the more external risks (Hu et al. 2012; Parsons et al. 2014; Siponen & Vance 2010). Raising the information security awareness of employees (and the information security policies they must comply with) is a proactive way for organisation to deal with these risks that can arise internally.

To provide necessary awareness, organisations should complement the information security policy with a set of guiding principles to help explain to employees why a specific element is included within the policy and how to comply. Siponen (2000) reinforces this message suggesting that employees should not be satisfied with answers such as 'this is our policy'. Recent research into compliance challenges with information security policies also highlight the importance of explaining new policies and 'the important roles that managers have in promoting new policies, and that consideration should be given as to how these new policies are introduced and explained to employees' (Lowry & Moody 2013, p. 3006).

Consequence of poor awareness of Security Policy

Some key consequences of poor awareness include:

- Lack of clarity of what the overall aim of information security is within an organisation.

- Lack of senior management support for information security.
- Lack of enforceability of the information security policy within an organisation.

2.3.2 Organisation of Information Security

This section of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 9) describes how information security should be organised (structurally and resource wise) and managed within an organisation. There is a strong emphasis on management support within the organisation for information security. Whilst enhancing the amount of information security awareness to all employees is unquestioned, it is 'raising the awareness level of senior management' that is also seen as a key to the success of improving information security (Kajava et al. 2006, p. 1519). The 'tone at the top' plays a vital role in promoting and holding staff accountable for good security practices (Tejay & Barton 2013). In their global state of information security survey (PricewaterhouseCoopers 2013, p. 4), it was found that 'it is essential that security is a foundational component of the business strategy, one that is championed by the CEO and board, and adequately funded'.

Structure of information security management

Organisations are adopting different structural approaches in how they manage information security. In a study published in 2007 (Johnson & Goetz, p. 20), more than half the participants said that 'the security group's organisational structure is in flux and seems to undergo frequent change'. Some organisations have gone down the path of outsourcing the management (but not the accountability) of information security and some have stuck with the originally adopted centralised approach, usually locating information security staff within their IT department.

Some organisations are embracing a decentralised structure where various roles of information security management exist within business units. These roles include role based access control (RBAC) management (Baracaldo & Joshi 2013). This decentralisation approach to management of information security would suggest that a greater emphasis be placed on training and ensuring that awareness of information security is also provided as this decentralisation is implemented. Peltier (2005, p. 45), in his article on implementing an information security awareness program, highlighted this decentralisation and suggested that structurally there is a need for 'requiring each business unit to establish an information security coordinator'. He suggests that one of the tasks of an information security coordinator would be to 'present awareness sessions to their specific organisation'.

Skill level requirements

The formal skill levels of information security professionals have become easier to assess in recent times, with numerous certifications formally available for information security professionals. This allows for independent verification of the skills they have achieved, and the ability for these employees to be able to demonstrate their level of competence. Recruitment managers and human resource departments would need awareness of these aspects, and of the need for the current skills required for effectively managing information security in organisations.

Organisations such as SANS Institute (2013) have developed skills assessment instruments for information security to allow organisations to ‘rapidly and accurately assess the skill levels of job applicants and benchmark applicants against each other’. Specialist IT recruitment and compliance recruitment personnel are also being engaged or employed by human resources recruitment organisations to assist companies with this specialised recruitment of people with the necessary information security skills.

The tradition of promoting your best and brightest technical information security person does not necessarily result in an information security manager with good business acumen, or someone who is respected by other areas of the business. Indeed, in some cases the person being promoted, whilst wanting to earn more money and gain a more prestigious job title, often wishes to stay heavily involved in what they know, that of technical information security. In an article published in *Computerworld*, (2012, p. 1) Paul Glen describes how moving from a technical role into a management role is effectively a change in career, and not always one that ends well. He found ‘a large percentage of engineers who try management don't like it. Too often, they choose to leave the organization rather than suffer the public humiliation of a "demotion" or perceived failure’.

Many organisations also engage external contractors with specialist information security skills, as and when required. This is done rather than permanently hire very costly technical human resources that, if not constantly challenged at their technical skill level, are likely to become bored and leave. These external contractors may be required at key timeframes, including the implementation of a new technology (such as two factor authentication or deployment of IAMs) or after a serious information security incident. Engaging with external organisations and tapping into their knowledge is also a vital source of expertise. In their report on information security awareness initiatives, ENISA (2007) found 21% of organisations used external expertise for their security awareness training.

Senior management also engage external organisations to review the effectiveness of the overall information security management function. This is often achieved using internal and external audit functions, particularly using some of the Big 4 accounting firms. For example, KPMG Australia (2015) offer cyber security risk management services where they ‘are helping business and government move beyond uncertainty to a position of strategic advantage’. A final but key aspect of this portion of the ISO/IEC 27002 standard is specifically stated in the standard’s guidance section as ‘initiate plans and programs to maintain information security awareness’. Below is a summary of the relevance awareness plays for each of these stakeholders.

Senior management must be aware of the organisation’s need for information security. A recent study on how external influences motivate senior management to commit to information system security found ‘senior management commitment is important to achieving effective information system security (ISS) in organizations, and is a prerequisite for effective development, implementation, and compliance with ISS’ (Kayworth & Whitten 2010; Tejay & Barton 2013).

Some researchers (e.g. Chang & Ho 2006, p. 347) suggest that information security is ‘primarily a management issue’. So senior management need to demonstrate commitment to information security, understand how to allocate the necessary information security roles across the organisation, and remove organisational barriers to allow for an organisational wide and coordinated approach to information security. Senior management also need to ensure aspects such as confidentiality agreements and external reviews of the information security functions are implemented. The need to bring in outside assistance or involve external organisations as and when required also needs to be recognised and supported by senior management.

Where an external party is involved in managing an information processing facility, senior management should ensure that their organisation's security requirements continue to be met. Big 4 accounting firm Deloitte (2012) contributed an article to *CIO Journal* regarding outsourcing risks and suggest 'CIOs can ask for the service provider's SSAE16/SOC (formerly known as SAS 70) reports, in which an external auditor describes, evaluates, and issues an opinion on the service provider's security and data protection controls'. Gartner et al. (2010) suggest that these types of external reviews 'provide a very high degree of assurance' in terms of the management of an information processing facility by a service provider.

In research looking into the security risks in service offshoring and outsourcing (Nassimbeni, Sartor & Dus 2012, p. 424), the authors found that in the literature they reviewed that the issue 'still presents a deep lack of knowledge on the combination of technical, managerial, and legal protection tools in managing data and knowledge security risks' within some of these service providers. Senior management are often the drivers in the negotiations where outsourcing is involved and 'can make informed, risk-based decisions' in terms of acceptable risks, including information security risks, associated with the outsourcing. Senior management must ensure appropriate measures are included within contractual agreements (Herath & Rao 2009, p. 22). But accountability for information security cannot be outsourced. ENISA, in their article on *Cloud Computing: Benefits, risks and recommendations for information security* (European Network and Information Security Agency (ENISA) et al. 2012, p. 8), suggest that 'ultimately, you can outsource responsibility but you cannot outsource accountability'.

IT staff, especially information security staff, form the organisational structure for managing information security. They are often asked to provide 'governance, policy development, and consultancy-type functions' (Johnson & Goetz 2007, p. 18). In terms of determining organisational structures and managing information security, the responsibility often resides with the chief information security officer (CISO) or information security manager. A 2011 survey found a substantial change in reporting lines, away from the chief information officer (CIO) 'in favour of the company's senior business decision-makers' (PricewaterhouseCoopers 2010, p. 34).

The management of information security is coming under greater influence from business matters rather than purely technical IT matters. The Sherwood Applied Business Security Architecture (SABSA) (Samaras et al. 2014) methodology uses a business driven approach and SABSA asserts that it (Burkett 2012, p. 48) 'brings information security professionals the arsenal they need to become business security solution providers instead of the business operations inhibitors they have been portrayed to be'. Additionally, SABSA is an enabler of business and for 'organizations that realize business and security are now inseparable, just as business and technology, they will also understand the need to incorporate information security at every layer of the enterprise'.

In their article on business process-based information security risk assessment, Khanmohammadi and Houmb (2010, p. 205) presented a new approach for risk assessment 'based on business goals and the processes supporting these goals'. They argue that 'measuring the risk for processes of organization is an efficient way forward'. IT staff perform information security related tasks as set out by senior management. Therefore, IT staff must firstly have an understanding of what management's requirements are, as well as a deep understanding of the technology aspects of those requirements. Whilst IT staff provide guidance to senior management in terms of what technology aspects should be used to provide effective information security, increasingly IT staff need to understand the organisational impacts of their technological recommendations. Information security must not become a barrier to undertaking business, but rather it should be designed so that organisations 'remain within its risk appetite' (Australian Prudential Regulatory Authority (APRA) 2010, p. 8) as established by senior management.

End users would not typically play an important role in terms of this aspect of the ISO/IEC 27002 standard and would, therefore, not require significant awareness. Their involvement is covered in other aspects of the ISO/IEC 27002 standard.

Consequence of poor awareness of Organisation of Information Security

Some key consequences of poor awareness include:

- Inappropriate/ineffective information security resource structure established.
- Lack of senior management commitment to information security.
- Information security not properly managed.

2.3.3 Asset Management

Within the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 19) there is a fairly simple message in terms of asset management. There is a requirement for assets to be accounted for, for all assets to have a nominated owner, and for that owner to determine and state what controls should exist for the assets. This parallels with the requirements that most non-IT assets also have within an organisations. Gartner et al. (2005) support this view by stressing that 'users of IT assets must know their responsibility in protecting these assets'.

Most managers within an organisation would be suitably familiar with physical items such as a computer or a vehicle being an asset and what types of controls would be suitable to provide physical protection. However, the concept of information or a database also being classed as an asset that needs a specific owner and needs suitable protective controls may be foreign to many non-technology managers. This view is reinforced by Huang et al. (2006, p. 244) who suggest that 'information is an asset of value to an organization and consequently needs to be suitably protected'. Whether it is called data or information, its protection within an organisation is crucial (Burdon, Lane & von Nessen 2012; Rajagopal et al. 2014).

The leakage of information referred to as Wikileaks prompted a strong reaction from the Office of the US President (US Government & Lew 2010) reminding heads of executive departments and agencies that 'any unauthorized disclosure of classified information is a violation of our law and compromises our national security'. Information as a critical asset has now hit the mainstream. But as has been experienced during the Wikileaks events, identifying an owner of a particular piece of information can be extremely difficult. This is particularly so when information is used by multiple business units within an organisation. For example, is customer information in a bank owned by the marketing department, or the retail bank, or the products group? Equally difficult, and some would say impossible, is then protecting a single piece of information that exists within a broader information record such as a customer's mobile phone number.

In his article titled *Securing Information Assets*, Desouza (2009, p.38) suggests that damage can be caused to organisations 'through malicious and/or unintentional compromises of information assets'. This could involve a malicious act such as modification or deletion of information, physical damage to computing equipment, or it could involve employees with legitimate access to information who accidently declassify that information by moving or copying it to a place where many more (unauthorised) people have access to it. Measures can be implemented that make copying and disseminating information more difficult, but these measures also make the legitimate use of that information more difficult to achieve at a reasonable cost.

Placing a value on a piece of information (in order to determine what controls should be used to protect it) is also a difficult task. The person creating the information may not understand the value of that information, or the value of that information could change over time, particularly as the piece of information may progress from highly confidential through to publicly-available purely as a function of time. Awareness as to what is an asset, who should (or does) own that asset, and what practical controls should be employed to protect that asset is vital if organisations are to look after their assets properly. Moreover, this responsibility should not just reside with a person titled with a job called 'Asset Manager' (Everett 2011b; Rajagopal et al. 2014).

In relation to technology-related assets (including information), it is no longer acceptable to say, 'that is for the IT department to worry about'. This view is akin to saying that your car mechanic is responsible for your car, when you as the primary user can determine how safe and secure your car is. It is through usage that many assets may move from being properly protected to being left open to exploitation. The Wikileaks experience should be a timely reminder of the damage that can be caused to an organisation's reputation. Awareness across all three key stakeholder groups (senior management, IT staff, end users) is required in order to achieve appropriate asset identification, ownership and protection. Below is a summary of the relevance *awareness* plays for each of these three stakeholder groups.

Senior management should understand that information is an 'increasingly important asset' (AlAboodi 2006, p. 1) which can impact on organisational success. As well as recognising the value of information, 'securing information assets should be an enabler, not a suppressor, of business value' (Desouza 2009, p. 40). Strategic advantage can be gained by innovating in the use of information security. A case study on cloud security (Shi 2013, p. 42) found 'information security in cloud computing is used as a case study to introduce the concept of capturing strategic competences'. Management need to understand the importance of defining informational assets (via some inventory); and determining and defining how these assets will be stored, transmitted, secured and accessed by authorised people. This involves identification of the ownership of information assets as well as the classification of these assets so that protection levels applied are appropriate. Senior management must champion the vital need for ensuring employees understand their 'responsibility in securing information assets' (Veiga, Martins & Eloff 2007, p. 148).

IT staff are often involved in constructing and maintaining technology asset inventories. These responsibilities are documented in international standards such as Cobit, IT Infrastructure Library (ITIL) and ISO/IEC 27002 (IT Governance Institute (ITGI) 2008, p. 53) and include 'periodic review of configuration integrity' and 'configuration procedures to support logging of all changes in a configuration database'. Much of this process uses a configuration management database (CMDB) which is described by Sharifi, Ayat and Sahibudin (2008, p. 736) as 'a database that contains all relevant information about the components of the information system used in an organisation's IT services and the relationship between those components'.

The CMDB can be built in a semi-automated manner, however, where some manual intervention is required, such as documenting who is an asset owner or the 'value' of the asset to the organisation, IT staff need to work closely with the true owners of the asset. Too often IT organisation will assume ownership (or be forced to as a default option) of these assets because it is difficult to find the true owner. IT organisations must resist assuming full ownership of assets on behalf of the true business owners.

IT staff play the major role in implementing controls over the technology assets. They need to understand that the true owners of the assets must establish the access requirements and provide ongoing approval and review functions for those who has access to these assets. IT staff would then provide the technical mechanism (access control lists, AD groups, IAMs, etc.) of how the protection and access is enforced.

End users are often the primary users of these technology assets, whether that is purely the information or data they work with, or whether it is the technology they use to interact with that information. This means that they are also the most likely to put these assets at risk because of the frequent usage (Rajagopal et al. 2014; Siponen, Mahmood & Pahnila 2009). End users must therefore understand the classification (value) of these assets so that these assets are protected and managed in an appropriately secure manner. Technology controls can only go so far in providing this protection. For example, information assets could be accidently made available to unintended people simply by an authorised user of that information asset copying or saving that asset to a place not appropriately protected. This could allow unintended and unauthorised people the ability to access it.

End user employees are often the main creators of new information assets. They need to understand how new information should be classified so that the protection determined by the information owner (not the creator) is applied. This protection of technology assets starts with the need to inventory technology assets, to identify true owners (which is often a difficult task) of these assets, determine the worth of these assets, and then determine who should have access to these assets. End users can be the greatest enablers of asset protection and assist the owners (via proper classification and ownership), but they are also the weakest link through inattention, through assuming someone else will look after the asset, and they can often undo (accidently or intentionally) the protection put in place.

Consequence of poor awareness of Asset Management

Some key consequences of poor awareness include:

- Assets not easily identified.
- Assets not properly protected.
- Disclosure of sensitive information due to lack of appropriate classification.

2.3.4 Human Resources Security

This aspect of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 23) is another that is not specific or restricted to information security employees, but it does play an important influencing role in information security management. From a general employment perspective, anyone employed by an organisation (employees, contractors and third party users) needs to be aware of their responsibilities, including information security responsibilities (D'Arcy & Greene 2014; Parsons et al. 2014; Puhakainen & Siponen 2010). These people should be screened prior to employment, they should sign confidentiality agreements, and they should be made aware of their security responsibilities. The ISO/IEC 27002 standard suggests this includes complying with information security policies, protecting information assets, executing required security tasks (such as regularly changing passwords), and reporting security incidents.

Those specifically employed in information security roles, according to the US Department of Homeland Security (US Department of Homeland Security 2007, p. 17), should ‘ensure that position sensitivity is established prior to the interview process and that appropriate background screening and suitability requirements are identified for each position’. Managers have a particularly important role to play in terms of those employees reporting to them. They must ensure that these employees understand and follow their information security responsibilities, and these managers must ensure that any computer-related access given to their employees is fit for purpose and duly authorised (Boersma 2012; Narain Singh, Gupta & Ojha 2014).

Providing more access than is required to perform your job tasks is a difficult problem to detect. Rarely will someone complain about having too much access, but they will immediately raise concerns if they do not have the appropriate access to undertake their job role (Baracaldo & Joshi 2013; Everett 2011a). Where outsourcing arrangements exist, similar diligence is required in terms of security responsibilities of the employees of the outsourcer. In his article on assessing insider threats to information security, Sarkar (2010, p. 118) suggests that ‘security threats associated with outsourcing include sensitive or confidential information not being properly protected and unauthorized parties gaining access to private files’.

The practice of employing ‘ethical hackers’ must also be approached with caution (Danish Jamil & Khan 2011). Pike (2013, p. 67) believes that ‘teaching offensive hacking skills increases risk to society by drawing students toward criminal acts’. The activities of the ethical hacker could be seen as being illegal unless formal agreements have been properly drawn up. If the infrastructure being hacked does not belong to the organisation (such as the public telephone network), then depending on what is being tested and what potential vulnerabilities are being exploited, authorities could take legal action.

Many organisations use ethical hacking to test vulnerabilities in their own systems (Liu et al. 2012). Organisations must be aware they are creating a situation where they have a person that not only has the knowledge to break into their systems, but also has been encouraged to try and break into those systems. In an article focused on insider threats, Sarkar (2010, p. 113) asserts internal staff with legitimate access to information and systems have intimate knowledge and ‘any attack by these insiders can be very difficult and challenging to detect’. Employees could be paid large sums of money to commit fraud and steal company information, which may present an easier avenue for criminal elements to use rather than hacking into an organisation.

Finally, a significant concern in terms of managing human resources is the employee termination process, which many organisations have great difficulty achieving in a timely manner. The Information Systems Audit Report (Western Australian Auditor General 2013, p. 34) reported that ‘of 11 active network users belonging to former employees, six of them had logged in to the network after their termination date’. A 2009 data breach investigation report (Verizon Business RISK Team 2009, p. 47) describes how ‘several breaches in the last year were the result of malicious activity on the part of a recently terminated (or notified) employee’. Whilst they provide abundant guidance on managing the employee termination process, they suggest that most importantly organisations should ‘establish a process for quickly disabling user accounts and removal of all access permissions’.

There are often audit reports of small and large organisations that continue to highlight the timely termination of ex-employee access as an ongoing issue (Western Australian Auditor General 2013; Zeadally et al. 2012). Management in particular need to have a greater awareness of the risks associated with employees and ex-employees having access to information and systems that may no longer be required or justified. Below is a summary of the relevance awareness plays for each of these stakeholders.

Senior management has an important role to play in terms of establishing the overall lifecycle of employment (pre, during and termination) and, in particular, those aspects that have an impact on information security. Senior management should establish policies so that prior to employment, human resource professionals conduct ‘employee screening to establish past employments and other background details’ (Sarkar 2010, p.126). The use of social medial is also playing an important role in this as highlighted in a recent online article titled *Is Your Social Media Usage a Red Flag for Employers & Recruiters* (Jeffries 2014, p. 2). This article highlighted employers being put off by ‘negative comments a candidate has made on social media, particularly comments about previous employers’. Management should also establish conditions of employment that clearly outline the responsibilities of staff in terms of information security (including social media) behaviours.

During the tenure of employment, management need to support the provision of information security awareness programs, as well as any specific job tasks that need to be undertaken in terms of information security. For IT security staff, IT management would provide very detailed roles and responsibilities for these staff members. Staff termination would require management to emphasis the urgency by which terminated staff must have their access rights to company information and systems removed. This is particularly important for immediate dismissals. Removal of access rights still remains a problem within many organisations. In their recent information systems audit report, the Western Australian Auditor General (2013, p. 20) provided a recommendation to 'review user accounts to ensure that privileges and user access is appropriate at all times including accounts affected by termination or change of employment'.

IT staff often provide a mechanism for monitoring and reporting in terms of how employees are complying with their information security responsibilities (Al-Omari, El-Gayar & Deokar 2012; Hu et al. 2012). Where the organisation sets acceptable use of technology policies, it is a usual practice that IT staff would monitor and report on breaches to these policies. IT staff also provide much of the information security awareness to new starters and would also raise emerging information security issues (i.e. social media) that would need to be incorporated into awareness or acceptable usage policies for an organisation.

Government authorities such as the Australian Prudential Regulatory Authority (APRA) are quite prescriptive in terms of what organisations (in this case regulated financial institutions in Australia) would typically be required to have in place. Many of these requirements (i.e. IT system patch management, capacity management, change management) would be implemented by an organisation's IT staff.

For end users**,** APRA suggests employees would 'typically be required to periodically sign-off on information security policies as part of the terms and conditions of employment or contractual agreements' (Australian Prudential Regulatory Authority (APRA) 2010, p.12). Furthermore, APRA specify the need for regulated institutions to ensure 'removal of access rights whenever there is a change in role or responsibility, and on cessation of employment'.

It is the end user's responsibility to understand the employment conditions they are obliged to follow, including those related to their responsibilities once they have ceased employment. These responsibilities often relate to confidentiality of information that they would have had access to whilst being employed. End users need to understand their obligations, including attending information security awareness sessions and keeping abreast of changes to information security policies as organisational risks within their organisation change.

Consequence of poor awareness of Human Resources Security

Some key consequences of poor awareness include:

- Employees behaving in a risky manner (in terms of IT usage) because they are unaware of their responsibilities.
- Terminated employees retaining access to systems after they leave.
- New (unsuitable) employees not adequately screened prior to employment.

2.3.5 Physical and Environmental Security

Physical security in relation to the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 29) is not just about protecting the monetary value of the physical assets. The functions they perform and the information stored on those assets are typically more valuable than the physical asset. Australian governmental advice (Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) 2007, p. 2) to CEOs and board of directors in relation to protecting enterprise information was that these senior managers are 'ultimately responsible for protecting both physical and electronic from unauthorised access or damage'. The physical protection and the environmental facilities used to house information processing assets must be commensurate with the value of the whole asset, including the information stored on the asset and the function that assets plays in the day-to-day functioning of an organisation.

The availability of the information and technology assets to allow the continued processing capabilities of an organisation is a key aspect. Imagine a bank or an airline not having their IT systems available to process customer transactions (Craw 2014; Zolkos 2015). Recent natural events including floods, fires and earthquakes has highlighted various aspects of environmental security that need to be understood. Not only is an organisation's existing business location impacted, but also other supportive utilities (power, water, phone) including mobile phone towers are impacted. In the 2011 Queensland floods (Hutchinson 2011), the major telecommunications supplier, Telstra, declared '262 ADSL and telephone exchanges unsafe' immediately after significant flooding. This significantly impacted telecommunication services to many individuals and organisations.

Terrorist attacks and disruptions to facilities located in other countries are also factors that can impact on the availability of IT assets (Brotherton & Dietz 2014; Stanciu, Pana & Bran 2010). Distinct physical boundaries of an organisation are disappearing. Additionally, with the reduction of the physical size of technology assets (i.e. servers, storage devices), these technology assets are at times now being located in non-data centre quality locations. Environmental controls may not be as good as traditionally was the case, and the whole processing environment could be easily stolen, as was the case in 2003. The Australian Broadcasting Commission (ABC) reported (Yaxley) to an Australian parliamentary committee that 'two file servers were stolen last week from a customs building at the Sydney International Airport'. The decreased size and portability of these assets makes this type of event possible. And security around data communications facilities and data communication links is a growing problem that organisations need to be aware of.

The Payment Card Industry (PCI) Data Security Standard (DSS) (PCI Security Standards Council 2010) specify as one of their requirements that an organisation needs to 'restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines'. They call for access to the telecommunication links to be appropriately restricted in order to ensure the security of data transmission is not compromised.

The physical nature of data communications is changing as wireless communications is being more widely adopted (Imgraben, Engelbrecht & Choo 2014; National

Institute of Standards and Technology [NIST], Souppaya & Scarfone 2013). Physically possessing (or protection of) all of the communications links is difficult. Different approaches to secure communications are required and an appetite to invest in this newer technology and protection methods will be required. Awareness by senior management of emerging risks in telecommunications, as well as by IT staff, will be required. Adding to this complexity is the expanding workplace boundaries, which now includes many employees working from home or remotely from locations not controlled or secured by the employer.

Disposal of assets and cleansing of equipment also presents challenges to organisations. These challenges were highlighted in 2010 by incidents in the US where recycled photocopiers were disposed of by one organisation but purchased by someone else (Rand 2010). However, these photocopiers still had the data from the original organisation easily available, including medical and police records. This type of problem is compounded by the increased use of so-called Transient Storage Devices (TSDs) such as USB devices, mobile phones and their ever-increasing data storage capacity. An article describing security threats and mitigating risks with these TSDs (Tetmeyer & Saiedian 2010, p. 47) highlights that ‘the small size and increasing capacity of TSDs make data loss/leakage easy to carry out’. Large amounts of corporate data can be easily leaked or stolen.

Finally, this area of the ISO /IEC 27002 standard also deals with equipment maintenance. During the Global Financial Crisis (GFC), organisations may have cut back on spending for the maintenance of their information systems. This could have led to underinvestment in maintenance and possibly medium term failures of assets. For example, an analysis (Campello, Graham & Harvey 2010, p. 471) of the effect of spending on technology following on from the GFC suggests that ‘the average constrained firm in the U.S. planned to dramatically reduce employment (by 11%), technology spending (by 22%)’. Below is a summary of the relevance that awareness has for each of these stakeholders in terms of physical and environmental security.

With CEOs and Boards of Directors being ‘ultimately responsible for protecting enterprise information assets (both physical and electronic)’ (Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) 2007, p. 2), senior management have a clear responsibility to set the requirements for adequate physical and environmental security. They need to understand what levels of protection are required in terms of who should have physical access, when that access should be available, and what level of monitoring and logging of access should occur. Incidentally, this also mirrors their responsibility for logical (applications and data) access. The available controls could range from a simple physical key system, right through to complex biometric access controls.

In terms of physical and environment controls for information processing assets, senior management would rely upon specialist advice, either from their own IT staff or from specialist organisations. Environment controls such as air-conditioning, stable electrical supply, and guaranteed redundant supply of other utility services are vital for the protection and non-stop delivery of information processing environments. Recent natural disasters have highlighted the importance of environment (power, air-conditioning) security. As reported in the *Sydney Morning Herald* (Smolaks 2015), Australia’s second largest ISP, iiNet, was forced to shut down servers when the outside temperature in Perth reach 44.4 C and they experienced failures in both their main and backup air conditioners. This impacted many customers who were critical that the company failed in 'investing enough into backup and redundancy measures – after all, iiNet were operating this data center in one of the warmest regions of the world', being Perth.

IT staff play a key role when it comes to physical protection of information processing facilities. Management of these facilities form part of the responsibilities of IT staff, whether this is managed in-house within an organisation, or as part of an outsourced data centre agreement. IT staff (such as data centre management staff) should understand the special requirements needed to protect (both physically and environmentally) information processing equipment. They also often manage who has physical access to these areas. Maintenance activities, in terms of environmental protection, are also an important area in which IT staff play a primary role.

There is little involvement required from end users in terms of physical and environmental security, which is more related to complying with physical controls and directives that have been put in place, and to ensure they do not weaken these controls through poor behaviour such as sharing access codes/passes, propping open security doors for physical access, or other poor practices. However, as equipment gets physically smaller, and this equipment becomes more co-located in normal work areas, end users may be called upon to provide controls over this equipment.

Consequence of poor awareness of Physical & Environmental Security

Some key consequences of poor awareness include:

- IT systems may be rendered unavailable because of inadequate environmental (power, air conditioning, water) facilities.
- IT equipment may be stolen or damaged due to inadequate physical controls.
- Telecommunications traffic may be 'listened into' and information stolen if physical access to telecommunication links is not properly secured.

2.3.6 Communications and Operations Management

Within the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 37), this section relates to the ongoing and secure operation of information processing facilities, such as data centres, server rooms, media storage, and data and voice communications cabinets. Much of this involves technical practices and procedures, and although this is a mature area for many organisations, audit findings continue to see a lack of documented procedures. The Western Australian Auditor General (2010, p. 32) found that documented policies and procedures 'for how changes are to be made' were often lacking and where transaction processes were involved, problems arose where 'segregation of duties was not in place to mitigate the risk of unauthorised or inappropriate transactions'.

This lack of formalised procedures can lead to inconsistent or incomplete practices, poor change management procedures and, in some cases, a lack of segregation of duties (Gundu & Flowerday 2012; Western Australian Auditor General 2013). Often IT operational staff hold the 'keys to the castle' and have the ability to inadvertently operate the information processing facilities in an undesirable manner by not following the stated procedures or policies. These operational management processes include key functions such as capacity planning and change management.

Events in the Australian Banking sector have highlighted the adverse impact on customers (Zappone 2011) when overnight processing of transactions suffer some form of error. Whether this is due to inadequate capacity of systems, or changes that have not been fully tested before being implemented, the impact is not just of interest to IT staff. It impacts the whole organisation, including significant reputational risk, and highlights the need for senior management to be more aware of how their information processing facilities are being managed.

This awareness by senior management is arguably more important when processing facilities are outsourced. This outsourcing may simply introduce a third party provider that adds one layer of complexity, however, if the outsourcing is done domestically then the outsourcer is still easily contactable and issue resolution may be fairly easily achieved. However, the situation could be more complex to resolve if the outsourcer and the information processing facilities reside in another country, in a different time zone or under the jurisdiction of another legal and political system, and may be subjected to riskier geopolitical events (Nassimbeni, Sartor & Dus 2012; Sá-Soares, Soares & Arnaud 2014).

Big 4 accounting firm Deloitte (2012) suggests that when outsourcing information technology, organisations need to ask questions such as ‘what are your IT service providers business continuity plans’? Also can they continue their operations in the event that ‘their core infrastructure or business is impacted by a natural disaster, or a threat to the electrical grid, or geo-political upheaval, or other crisis’? An American paper manufacturer, Rock-Tena, recounts on IT outsourcing that when outsourcing ‘to a vendor, especially one located half way around the globe, this has its challenges’ and in particular ‘moving ahead with a lack of familiarity and with geographically dispersed teams, creates risk’ (Cady 2005, p. 53).

Other areas within this section of the ISO/IEC 27002 standard relate to control of malicious code (i.e. virus), data back-up, network security management, exchange of information and many other aspects that make up the effective running of an information processing environment. Business unit management need to understand these areas and not be solely reliant on IT staff. Complicating operational management of information security is the trend of cost cutting by organisations that continue to put pressure on all budgets, including those of IT (Schneiderman 2013). Operational management within IT may be seen as being mature and suitable for cost cutting. This is not always the case, particularly if the operational procedures and practices are not as mature as expected. External assessments of frameworks such as Information Technology Infrastructure Library (ITIL) (Ittersum et al. 2004) and formal assessment against the capabilities can help provide senior management with a greater level of comfort as to the maturity of their organisation’s IT practices.

Below is a summary of the relevance *awareness* plays for each of these stakeholders. This section of the ISO/IEC 27002 standard is made up of numerous aspects that have varying levels of reliance on the three different stakeholder groups. Because of the significant number of aspects that make up this section of the standard, these have been presented in a tabular format. These different aspects are listed and briefly described in terms of their information security awareness importance in Table 2-5 for senior management, Table 2-6 for IT staff, and Table 2-7 for end users.

Table 2-5 Senior management awareness aspects of communications and operations management

Aspect	Senior management Awareness Importance for Communications and Operations Management
Operational procedures and responsibilities	Typical role in mandating policy and controls.
Third party service delivery management	Significant role in contractual arrangements and mandating the need to monitor third parties.
System planning and acceptance	They provide the business priorities and importance factors.
Protection against malicious and mobile code	Supportive role in providing suitable 'tone at the top' in terms of support for technical controls that may not be popular (i.e. the restriction of administration rights on end user PCs) with end users.
Back-up	Key stakeholders for this area. It is very much about business requirements where back-ups are critical, rather than just the technical aspects of how the information is backed up. Senior management must specify their risk tolerance in terms of how frequently backups should occur and how far back the organisation should be able to recover from.
Network security management	Main involvement is in terms of business arrangements with external service providers.
Media handling	Must understand risks to the organisation of not doing this properly. Must ensure policies are established, provide funding to allow for technology controls to be established, and they need to promote good practices and outline consequences of compliance failures.
Exchange of information	Provide 'the tone at the top'. Establish policies that mandate the use of controls (i.e. encryption) or manual procedures (i.e. data retention periods, contractual requirements for data exchange) or data classifications.
Electronic commerce services	Provide the authorisation and policy aspects of electronic commerce services.
Monitoring	Important role to ensure that there is suitable monitoring and logging in place, particularly as a control for monitoring activities by IT staff.

Table 2-6 IT staff awareness aspects of communications and operations management

Aspect	IT staff Awareness Importance for Communications and Operations Management
Operational procedures and responsibilities	IT staff are the primary owners and operators of these procedures and require high levels of awareness.
Third party service delivery management	IT staff are best positioned to understand what services should be delivered by third parties. They are often charged with monitoring these service provisions.
System planning and acceptance	Many aspects are controlled and monitored/measured by IT staff.
Protection against malicious and mobile code	They play a key role in terms of understanding what technical controls to implement to provide suitable protection, and monitoring of issues.
Back-up	Undertake a number of aspects associated with back-up management, including implementing the controls.
Network security management	This is very much an area that relies on strong technical awareness from IT staff in terms of security controls needed for

Aspect	IT staff Awareness Importance for Communications and Operations Management
	network services. Often a specialist individual or team look after this.
Media handling	Many of the controls around removable media; including access control for users, managing their movement in and out of the organisation, and storage management falls upon IT staff. Their involvement and knowledge is very important.
Exchange of information	Awareness of techniques to protect, prevent unauthorised interception, copying, modification, destruction, re-routing or denial of electronic messages or data. Protection to prevent damage from malicious code that may be transmitted. High levels of awareness required for encryption technology.
Electronic commerce services	Key role in the technologies and techniques required to provide protection over the transaction processing of electronic commerce. Highly relevant for the banking and finance sector, as well as the retail sector.
Monitoring	A very heavy focus on IT awareness, in terms of how to enable and protect logging and monitoring, and how to utilise the resulting information.

Table 2-7 End user awareness aspects of communications and operations management

Aspect	End user Awareness Importance for Communications and Operations Management
Operational procedures and responsibilities	Perform a role in terms of owning the business activities that are subject to change management, segregation of duties, and testing and development.
Third party service delivery management	Typical involvement will be quite low.
System planning and acceptance	An important role in terms of business activities that drive IT capacity requirements. They also play a major role in user testing of new systems.
Protection against malicious/mobile code	Need awareness of where and how malicious threats may be encountered, and how they can be avoided.
Back-up	They have an important role to play, given that much of the backed up data is created/managed by them. An important role to play in Business Continuity Management (BCM).
Network security management	Very little knowledge or involvement needed from the end user.
Media handling	Involvement in movements of (key) information via USBs, CD/DVD. They need to understand that removable media should be made unrecoverable (i.e. the organisations process of how to do that), in the event of loss of media.
Exchange of information	Understanding that exchanges of information can be (maliciously or accidently) interfered with. Understand the different sensitivities of data they are transmitting, and that they play a role in ensuring safe transmission of data because not all aspects of the process are automated. This also includes the physical transfer of data (including the use of couriers), as well as the correct identification of the intended recipient.
Electronic commerce services	Play a role in terms of the business controls around electronic commerce.
Monitoring	A low level of awareness in general for end users, except for the area of exceptions for access attempts.

Consequence of poor awareness of Communications & Operations Management

Some key consequences of poor awareness include:

- IT environments may not be operated properly or consistently.
- IT staff may perform tasks in breach of 'separation of duties' principles.
- Exchange of information may be mishandled and data could be lost or stolen.

2.3.7 Access Control

Within the ISO/IEC 27002 standard, this section (Standards Australia/Standards New Zealand 2006b, p. 60) relates to access to information, including processing facilities used to house the information. Access control continues to be a challenging issue for many organisations to manage (Baracaldo & Joshi 2013; Ponemon Institute 2010). Techniques for managing this access are often referred to as Identity and Access Management (IAM). IAM relates to setting up a person's identity when they join an organisation, ensuring that the person only has the appropriate access to information and systems as deemed necessary by their job role, and that the access is modified when the person changes role, or is removed once the person leaves the organisation.

In her article on *Identity and Access Management: the second wave*, Everett (2011a, p. 12) rightly points out that past approaches saw IAMs as purely a technology issue and 'even if access rights were correct at the time that they were assigned, modifications to roles or organisational structure can mean that they go out of date quickly'. Kho (2009, p. 21) suggest IAMs 'consists of verification and authorization'. And this is not just a focus area for IT departments. In his article on access management, Young (2004, p. 5) suggest that 'Human Resources (HR) can play a vital role in the enablement of effective employee IAM'. Because the hiring, moving and firing of employees and contracts has some level of HR involvement, this is often an appropriate capture point for IAM services.

With the growth of social media sites, online email accounts, shopping carts, and other sites that require you to have a logon-id, an emerging issue is that end users (and some IT staff) will often use similar passwords for their private access (such as to Google mail), as they will for their work access. In 2013, Ofcom, the independent regulator and competition authority for the UK communications industries, conducted a survey of UK adults (UK Office of Communications (Ofcom) 2013) and found that 'more than half (55%) of adult internet users admit they use the same password for most, if not all, websites'. It is therefore possible that should a person's private logon account become compromised, and the password obtained, that the person's work related access might be targeted and also compromised. Awareness seems to be a key defence.

Qureshi, Younus et al. (2009, p. 11) support this concern and suggest 'password recognition should be considered as a process and exploitation of human senses' and it should not just be addressable in organisations as a technical issue. Most organisations have numerous information systems many that have their own security systems where users must be defined. Being able to define a person just once (referred to as single sign-on) and have that person gain access to all systems and data they require still remains the holy grail for most organisations (Acar, Belenkiy

& Küpçü 2013; Spoorthi V & Sekaran 2014). Whilst there is much literature defining approaches to single sign-on, much of it is reliant on the particular technology that an organisation is using.

The more mixed the environment, the more likely that any single sign-on solution would be a custom built (and expensive) solution (Acar, Belenkiy & Küpçü 2013; Spoorthi V & Sekaran 2014). Without use of single sign-on technology, or effective IAMs controls, staff may be defined with access rights to systems they do not need, or retain system access after someone has left the organisation. But even when the access is correctly set up, the danger in an employee moving or copying information from one security zone (that is restricted) to another security zone (say a server when everyone has general access to) remains a potential problem. Whilst there is very little literature that highlights this as a major problem, the simple act of an employee saving a confidential document into a more public area of storage does occur.

Extending this problem to include employees taking data home to use on their personal PCs and the problem could become worse (Ahmad, Bosua & Scheepers 2014; Connelly et al. 2011; Patil & Prasanthi 2013). Previous discussions highlighted the risks of data being transported on unsecured USB devices. Senior management need to be aware of these risks associated with their organisation's data being used at employee homes and other locations outside of the control of their organisation. Complicating these problems is the need for employees to have to remember multiple access accounts (referred to as logon ids) and multiple passwords. These employees also have to remember the many logon ids and account names they have in their private life, (Facebook, Twitter, eBay, etc.).

Furthermore, delays in getting correct access established, particularly for new employees or employees changing job role, are also an impediment to business efficiencies. It takes time to provide staff with the right level of access. This can result in management requesting far greater access initially than may really required 'just in case' or because it is too difficult to identify exactly what access is required. Eventually the amount of access an individual employee accumulates, or employees share logon credentials. Below is a summary of the relevance awareness of access control plays for each of these stakeholders.

This section of the ISO/IEC 27002 standard is made up of a number of different aspects in relation to access control that have varying levels of reliance on the different stakeholder groups. As such the different aspects are shown within a table for each key stakeholder group and the key points in relation to the relevant awareness of access control are shown against each different aspect.

Table 2-8 Senior management awareness aspects for access control

Aspect	Senior management Awareness Importance for Access Control
Business requirement for access control	Need to provide the basis for who should have access. This should be based around business functions. Need to provide strong ownership of access removal requirements.
User access management	Need to set strong requirements in terms of password management. Need to set out who should have what levels of privilege. Need to ensure that access rights are reviewed on a regular basis.
User responsibilities	Need to show a good appetite to reinforce end user

Aspect	Senior management Awareness Importance for Access Control
	responsibilities for unattended equipment. Clear desk/screen compliance is largely an end user responsibility, reinforced/mandated by management and assisted (somewhat) by controls provided by IT.
Network access control	Need to mandate (based on guidance from IT staff) what devices should and should not be connected to the network. BYOD adds to this complexity.
Operating system access control	Normal management support required.
Application and information access control	Business unit senior management are often best placed to know what access controls should be applied to their applications and data.
Mobile computing and teleworking	Need awareness of the risks and take a strong stance to manage these risks. Teleworking requires good knowledge of technical aspects as well as environmental (location) ones. Good awareness across all stakeholders is needed.

Table 2-9 IT staff awareness aspects for access control

Aspect	IT staff Awareness Importance for Access Control
Business requirement for access control	IT staff would translate these business functional requirements into IT functionality and ensure security access matches these requirements. IT provides the mechanics for access review/removal.
User access management	IT staff need good understanding of their systems to implement technical password and access controls. IT staff need to translate managements access requirements into IT access techniques. IT needs to assist in the user access review process by providing suitable reporting for management to review.
User responsibilities	IT staff need good awareness of the technology (configuration settings) used. They need to provide complementary/compensating controls for when equipment is left unattended. Clear desk/screen compliance is largely an end user responsibility, reinforced/mandated by management and assisted (somewhat) by controls provided by IT staff.
Network access control	IT staff require significant knowledge in this area.
Operating system access control	IT staff need high levels of understanding in order to properly implement controls.
Application and information access control	IT staff need very good awareness of how the technical controls (to support the access policy) are to be implemented.
Mobile computing and teleworking	IT staff need to be knowledgeable in terms of mobile computing controls. Teleworking requires good knowledge of technical aspects, as well as environmental (location) ones.

Table 2-10 End user awareness aspects for access control

Aspect	End user Awareness Importance for Access Control
Business requirement for access control	End users need awareness in terms of how their access is based on the business function they are employed for.
User access management	End users require high levels of awareness to make password management effective. End users need to understand why access reviews are important.
User responsibilities	Strong awareness required from end users in terms of how to construct, protect and use their passwords. End users need good awareness in terms of the risks associated with leaving user equipment unattended. Clear desk/screen compliance is largely an end user responsibility, reinforced/mandated by management and assisted (somewhat) by controls provided by IT.

Aspect	End user Awareness Importance for Access Control
Network access control	End users need awareness of what should and should not be connected to the network and associated risks.
Operating system access control	End users need an understanding as to why these controls are in place.
Application and information access control	Business units and senior management are often best placed to know what access controls should be applied to their applications and data, however end users need to understand the purpose of these controls.
Mobile computing and teleworking	The very nature of mobile computing today has a high reliance on the end user doing the right thing. Teleworking requires good knowledge of technical aspects, as well as environmental (location) ones.

Consequence of poor awareness of Access Control

Some key consequences of poor awareness include:

- Employees and ex-employees may have more access than is required.
- Employees may not be granted access in a timely manner and may seek alternative (and undesirable) ways to gain access.
- Where employees are encouraged to 'take work home with them', the risk of losing that data increases if proper controls are not understood and used.

2.3.8 Information Systems Acquisition, Development and Maintenance

This section of ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 77) focused on ensuring information security is an integral part of how information systems are acquired, developed and maintained. It is important that security requirements are determined prior to any acquisition or development, and that these security requirements are incorporated and maintained during the life of the information system. Building information security early into the entire software lifecycle is less costly than introducing security later in that lifecycle (Khaiyum, Kumaraswamy & Karibasappa 2014; Yu et al. 2015). In their research focused on developing a methodology for security assurance-driven system development, Vivas et al. (2010, p. 62) presented their hierarchy of goals as part of their software development life cycle (SDLC). They propose that a 'security risk management process within the SDLC may include:

1. Security requirements specification and risk assessment;
2. Security architecture and design;
3. Secure implementation;
4. Security testing; and
5. Secure deployment and assurance'.

This importance of embedding security in the system development life cycle is reinforced by Mouratidis and Jurjens (2010, p. 814) who suggest that 'it is essential for security to be considered from the early stages and throughout the software development life cycle'. The aspects that need to be considered include ensuring that input validation occurs within these information systems, as well as developing sophisticated access control mechanisms. Not only does input validation play a role in enabling the safeguarding of the integrity of data being inputted, but the inputting of corrupt data for the purposes of hacking into systems is a widely-used technique aimed at infiltrating corporate systems, particularly through web based applications.

A 2009 article on client-side cross-site scripting protection (Kirda et al., p. 603) outlines ‘large variance among the technical sophistication and knowledge of web developers’ and a need for tools to protect against emerging attack mechanisms. Vulnerabilities such as SQL injection and cross-site scripting (XSS) are particularly troublesome. In their analysis of field data on web security vulnerabilities, Fonseca et al. (2014, p. 98) found ‘weak typed are the preferred targets for the development of exploits’, and also found ‘a single fault type (MFCE) was responsible for most (76 percent) of the security problems analyzed’. They believe that the fault types responsible for XSS and SQLi belong to a narrow list, and suggest improvement in the context of code inspections and the use of tools should be made.

There are commonly-known vulnerabilities such as buffer overflows, which occur when an application writes past the end of the allocated size of the buffer. These vulnerabilities can be used to gain full administrator rights. Web applications can be problematic because of poor software development security practices where security is an afterthought and the focus is on providing functionality. Padmanabhuni and Tan (2014, p. 394) found that buffer overflows are still ranked ‘third in the CWE/SANS list of Top 25 Most Dangerous Software errors’ and that ‘an web based application is particularly vulnerable when input validation is inadequate or absent’. Ensuring that developers have the right skills to develop software that builds security in throughout the system life cycle to protect against such attacks is vital. Integrity of messages and transactions must also be guaranteed; and designed based on the transmission route and the value of information being transmitted.

This portion of the ISO/IEC 27002 standard discusses output validation. This again is an area that developers must be concerned with and build in mechanisms to provide comfort that the output that is produced is suitably validated. Whilst the technology approach to integrity checking will be dependent on the application environment at an organisation (Oracle, SQL, CICS, etc.), the validation approach is similar. Whilst describing database consistency and integrity with transactions in the health sector, XU Zhong-wei (2009) describes the use of Delphi and the transaction controls such as start, commit or rollback. Sophisticated techniques are also generally available within most application development environments. Senior management and end users should be aware that this functionality is generally available and should be insisting upon this as a major requirement of their applications.

Data used to test systems must also be properly protected (Khurana & Bindal 2014; Rghioui et al. 2015). Although the data may be well protected when it resides in a production environment, this data often gets loaded into test or development systems, and often the level of security is not as tight as in the production systems. Suzanne Swanson (2008, p. 1) describes how non-production systems ‘are generally "open," and leave a large hole in the security practices at companies of all sizes’. She suggests that these systems contain ‘some of the most classified information in an organization, including employee records, customer records, and financial transaction documents’, yet these systems are ‘generally exposed with little or no logging and monitoring, and these systems are often made available for remote access’. But generation of obfuscated test data can be expensive; however, an appropriate security approach must be used.

Maintaining information systems over their lifecycles is important, not only to keep up with newly-discovered vulnerabilities, but also to ensure that the software being relied upon to support critical business functions is maintainable by the organisation and vendors. In their research into patch release behaviours of software vendors, Subramaniam et al. (2012, p. 329) concluded that 'a vendor's patch release decision is affected by the presence of other vendors' products with the same vulnerability, and the possibility that other vendors release a patch earlier'. So it is important that senior management establish agreements with the vendors to ensure that software maintenance by their vendors meets the organisation's business requirements.

Additionally, in their research into the management of lifecycle costs and benefits for information systems, Berghout et al. (2011, p. 763) found 'the use of cost/benefit management techniques has extended and more stakeholders now adopt this approach. Senior management involvement has significantly increased'. They also found that 'the absence of senior management in the evaluation of project proposals and IT in general remains a major concern'. Other aspects to consider include protection of software code, change control processes and license management.

Of particular concern for senior management is the outsourced development of systems and applications. Organisations should not just outsource without due care and diligence in terms of the outsourcers' credentials. Fanning (2014, p. 25) highlights the importance of 'assessing the validity of the service provider's internal control, privacy compliance, and other aspects of these outsourced activities from both the user's and deliverer's point of view'.

And, finally, the history of abandoned information system developments should be a warning to organisations to ensure appropriate development processes are in place (Gupta, Vinayak & Gupta 2012; Khaiyum, Kumaraswamy & Karibasappa 2014). Abdul-Rahman et al. (2012, p. 432) found 'risk management strategies relating to users' involvement, project management and planning and communication issues are considered very influential on reducing the effect of time and cost overrun'.

This section of the ISO/IEC 27002 standard is made up of a number of different aspects that, in relation to information systems acquisition development and maintenance information security controls, have varying levels of reliance on the different stakeholder groups. As such the different aspects are shown within a table and the awareness key points are shown against each different aspect.

Table 2-11 Senior management awareness aspects for information systems acquisition, development and maintenance

Aspect	Senior management Awareness Importance for information systems acquisition, development and maintenance
Security requirements of information systems	Supported by a strong commitment to information security from senior management.
Correct processing in applications	Supporting sufficient time and money to provide for suitable testing and data input validation techniques.
Cryptographic controls	Senior management need to show suitable support for the use of cryptography, given the cost implications of implementing encryption properly.
Security of system files	The protection of system test data requires all stakeholders to have a high level of awareness.
Security in development and	Senior management need to show support for good change

Aspect	Senior management Awareness Importance for information systems acquisition, development and maintenance
support processes	management practices. Information leakage is the responsibility of all stakeholders. Outsourcing requires good knowledge from IT, as well as good senior management understanding.
Technical Vulnerability Management	Vulnerability management requires good knowledge from IT staff and senior management support.

Table 2-12 IT staff awareness aspects for information systems acquisition, development and maintenance

Aspect	IT staff Awareness Importance for information systems acquisition, development and maintenance
Security requirements of information systems	Very strong involvement from IT staff driving the need for high levels of awareness.
Correct processing in applications	IT staff assist by building application controls focused on input data validation. IT staff developing validation steps would assist output validation.
Cryptographic controls	Cryptography is a specialist area to understand and implement. This is the domain of IT staff. Encryption Key Management is a very much specialist area to understand and implement properly.
Security of system files	Operation software control requires IT staff to understand how to implement appropriate controls. The protection of system test data requires all stakeholders to have a high level of awareness. Protecting program source code resides with IT staff.
Security in development and support processes	IT staff administers change control. They require a very good knowledge of, and commitment to, change management practices. Information leakage is the responsibility of all stakeholders. Outsourcing requires good knowledge from IT staff, as well as good senior management understanding.
Technical Vulnerability Management	Vulnerability management requires good knowledge from IT staff and senior management support for the resource commitment.

Table 2-13 End user awareness aspects for information systems acquisition, development and maintenance

Aspect	End user Awareness Importance for information systems acquisition, development and maintenance
Security requirements of information systems	Main involvement is in terms of using the systems, rather than a designer of information system security.
Correct processing in applications	End users are typically in the best position to provide validation around input data. End users play a key role in the validation of output.
Cryptographic controls	Ideally end users will not need to choose when to use cryptographic controls; the use of encryption should be automated based on information classifications.
Security of system files	The protection of system test data requires all stakeholders to have a high level of awareness.
Security in development and support processes	A level of understanding as to the importance of change management is required. Information leakage is the responsibility of all stakeholders.
Technical Vulnerability Management	Very little involvement required from end users.

Consequence of poor awareness of Information Systems Acquisition, Development & Maintenance

Some key consequences of poor awareness include:

- Information systems may be developed with security vulnerabilities embedded, putting at risk the correct functioning of the information system.
- Information systems may not be developed within time or budget.
- Information systems that are developed in an unstructured and undocumented manner may be very difficult to maintain after they have been developed.

2.3.9 Information Security Incident Management

This aspect of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 90) has a focus on communicating security events and weaknesses in a timely manner to allow for corrective actions to be taken. The management of information security incidents has evolved since the early days of viruses and amateur hacking attempts (Ab Rahman & Choo 2015; Hove et al. 2014). Early virus incidents saw organisations shutting down whole networks and information systems, and disconnecting from the Internet. Often the incidents were only detected once a mass infection had occurred; and prevention was less sophisticated than it is today. Today we see a greater balance between prevention and response.

Baskerville et al. (2014, p. 138) provide a framework aimed at balance between prevention and response and suggest current approaches ‘have proved appropriate in the past because they are particularly valuable for routine security tasks’. They suggest the ‘increasingly dynamic security environment requires more response-oriented security in addition to the existing preventative frameworks’. Because organisations are increasingly connected, they have to assume that software systems and networks may be eventually compromised, so response through detective and corrective controls has become increasingly important (European Network and information Security Agency (ENISA) et al. 2010; Friedberg et al. 2015).

This requires sophisticated approaches to handle information security incidents and, at times, this requires government or nationally and internationally focused approaches. Many organisations and countries have established Computer Emergency Response Teams (CERTs, also known as CSIRTs). In the *Report of the Inquiry into Cyber Crime* (2010, p. 71), the Australian Government relates to the ‘*Forum of Incident Response and Security Teams (FIRST)*’ which is used to ‘bring together a variety of computer security incident response teams from government, commercial, and educational organisations’ aimed at fostering ‘cooperation and coordination in incident prevention to stimulate rapid reaction to incidents’.

A greater focus on security incident handling in the cloud is also emerging as more organisations look towards the cloud for their applications. In a recent survey (Ab Rahman & Choo 2015, p. 55), the researchers found that ‘the adoption of cloud computing is significantly changing the landscape of incident handling, particularly between Cloud Service User (CSU) and Cloud Service Provider (CSP)’. What they found was that CSUs may be ‘limited in their ability to handle incidents efficiently on their sites because a CSP is solely (or partly) in control of the infrastructure’. Newer approaches will need to be developed. Senior management will need to be aware that as they either outsource or deploy applications into the cloud, that a new approach to security incident management will need to be developed.

In a recent study of incident management in three large organisations (Hove et al. 2014, p. 37), one of the organisations was found to have 'not implemented any specific standard or guideline for incident management, but has based their approach on components from the ISO/IEC 27001 and 27002 standards as well as the ITIL framework'. The ISO/IEC 27000 series of standards provides a significant basis for this current research. Incidents are not limited to deliberate or unauthorised events. It also includes system malfunctions. The recent Commonwealth Bank of Australia (Craw 2014) and National Australia Bank (Zappone 2012) disruptions in banking IT systems in Australia show how quickly external customers can be impacted, and how quickly others can be made aware of these incidents. Reporting exactly what has occurred when systems fail still remains a difficult aspect.

Organisations are often reluctant to report the exact causes, particularly if they remain exposed to a similar incident, although legislation that requires organisations to report security incidents such as data breaches are emerging (Burdon, Reid & Low 2010; Kierkegaard 2012). In a review of data breach notification laws in the EU and Australia (Burdon, Lane & von Nessen 2012, p. 306), the researchers concluded that it appears 'the overall approach adopted by the EU is more cognisant of the regulatory issues at stake'. They found that these 'involve the imposition of effective organisational information security measures and the relationship of adequate corporate information security to the societal interests'. Ultimately, senior management within organisations will need to understand what the impact of any such legislation will be on their organisation.

There are also incidents increasingly targeted at individuals. In their *Global State of Information Security Survey* (PricewaterhouseCoopers 2013), identity theft occurring in relation to financial services had increased from 15% to 25% on the previous survey. It is possible that some of these individuals are using the same password for their personal access to computer sites (eBay, Gmail, shopping sites) as they do in their work environment. These incidents targeted at individuals are often a result of social engineering activities which Applegate (2009, p. 40) describes as 'a methodology that allows an attacker to bypass technical controls by attacking the human element in an organization'. He suggests social engineering 'often exploit the natural tendency people have toward trusting others who seem likeable or credible'. Once a personal account has been hacked, it is not difficult to locate where that person works, what access they may have at their organisation, and the user account (often a derivative of their name) used by that organisation. Awareness of these risks, rather than just technical controls, seems an important level of defence.

The cause or extent of damage related to an information security incident is often difficult to determine. Computer forensics is seen as an emerging discipline within information security (Chakravarthy & Kumar 2012). Numerous tools have also been developed and universities are now offering courses in digital forensics. Forensics can assist when an incident may have gone undetected for a period of time. It can help determine exactly what has been done, which data may have been stolen or computer logon ids compromised. For example, should a system administrator's account be compromised, it may be difficult to track what damage has been caused.

CNN.com reported (Brown et al. 2014, p. 1) that the recent Sony hacking resulted from hackers who ‘stole the computer credentials of a system administrator to get access to Sony's computer system, allowing them broad access’. Some of the detection monitoring may have been switched off as part of this hack.

Interaction between law enforcement and government cyber authorities highlights an increased awareness of the importance of information security and the need for a more coordinated approach (Australian Government 2014; Davis 2012). The Sony hacking saw the US President passing comment that the incident was being ‘investigated by the FBI and Justice Department’ (Brown et al. 2014). Organisations need to establish mechanisms to interact with these authorities, and understand under what circumstances this interaction should occur. These mechanisms include documenting escalation procedures, contact details, who approves when to call, and what information will be provided. It should include additional escalation processes within the organisation. This needs to be established in advance of an incident because wasting precious time during an incident may result in further damage.

Evidence preservation and forensic techniques are also needed by organisations when they become aware that a system has been hacked; and the approach and processes should be predetermined. Sufficient literature exists (e.g. Garfinkel 2013; Kelly 2013) to provide senior management and law enforcement authorities with appropriate awareness of the importance of digital forensics. Senior management can provide suitable support in establishing and maintaining the relationships with the relevant authorities and support organisations. Below is a summary of the relevance *awareness* has for each of the three key stakeholders.

Senior management have an important role to play in terms of promoting a culture where the reporting of incidents is encouraged and becomes the responsibility of everyone (Hove et al. 2014; Narain Singh, Gupta & Ojha 2014). According to ENISA (European Network and information Security Agency (ENISA) et al. 2010, p. 19), ‘a CERT’s responsibility needs to be clearly described and then sanctioned by the highest management of the organisation for which the CERT works’. Senior management should ensure that the procedures for reporting of incidents is formalised and well communicated to all employees (Hove et al. 2014). Senior management also forms a key link in the escalation process for incidents and are often relied upon to form relationships with external organisations and government bodies that can play a role in managing serious incidents. The management of security incidents is not just about resolving the incident at hand.

Senior management need to understand and support procedures that enable the collection of forensic evidence that may require the prolonging of an incident in order to determine who the perpetrators are (Hou et al. 2013; Kelly 2013; Narayanan & Ashik 2012). Senior management also need to understand the potential cost of information security incidents. Research has shown security incidents ‘often cost organisations millions of dollars in losses’ (Herath & Rao 2009, p. 154).

IT staff are often the first point of contact for the detection or reporting of information security incidents because most employees would see this as an IT issue. The CERT may reside within the IT department and they would establish processes and procedures for reporting, recording and managing incidents. They need to have good awareness of senior management's requirements and risk tolerance in terms of incident management and escalation, when to involve external authorities, and what to communicate to both employees and external interested parties. ENISA (European Network and information Security Agency (ENISA) et al. 2010, p. 21) recommend that the CERT has 'a well-established and maintained mechanism for escalation'. IT staff need good awareness of the formality needed for managing an incident, and a growing need to understand how to preserve evidence of an incident in order to aid full detection of what was done, by whom, and how (Hou et al. 2013).

Narayanan and Ashik (2012, p. 156) suggest that 'after a computer system has been violated and an interruption has been detected, there is a need for a computer forensics investigation to follow'. This provides a greater insight into how long an organisation may have been subjected to an incident and the extent of the damage that has been caused. Importantly, it will help establish the root cause and assist with preventing a reoccurrence of the same type of incident and help to bring perpetrators to justice. New tools continue to be developed to assist with this work, and IT staff need to keep current with what tools and techniques can be applied.

The end users' main responsibilities relates to their need to be able to recognise an information security incident and to know how to report that incident and how to respond. They also need to understand what might reasonably lead to an incident.

Consequence of poor awareness of Information Security Incident Management

Some key consequences of poor awareness include:

- Security incidents may take too long to get resolved.
- Awareness of what security incidents are occurring may be incomplete and root cause may not be easily determined.
- External organisations that could provide assistance with security incidents may not be properly engaged.

2.3.10 Business Continuity Management

This aspect of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 95) discusses how to counteract interruptions to business activities and protect critical business processes. Organisations in recent times have received various reminders as to why suitable business continuity processes and capabilities are so important. These reminders include a fire in Gibraltar that disrupted online gambling (BBC News 2014), and floods in Thailand (Zolkos 2015) causing supply chain issues for companies such as Honda Motor Co and Western Digital. Business disruption is a significant issue.

Cyclones and hurricanes, terrorist attacks, and tsunamis have occurred with a sufficiently degree of regularly over the last 10 years to be no longer considered as something that is highly unlikely to occur, or something that only impacts other organisations. Stanciu, Pana et al. (2010, p. 155) suggest that disasters and adverse weather events can 'severely affect the integrity and functionality of the IT systems' with a resultant severe impact on organisations. In some cases organisations that suffer from one of these events fail to survive the event or are no longer in existence 12 months afterwards.

With high reliance on information technology by organisations, senior management must ensure that business continuity is not just ‘an IT thing’, but that it incorporates all aspects of business processes that rely upon technology (Costello 2012; Thejendra 2014). Forward planning by organisations on what they would do in terms of business continuity is critical to the survival of their business. Equally important, employees also need to play a key role in the process. This may entail having all information, systems, databases and spreadsheets on appropriate platforms that get backed up and made available during a business continuity event, or it may relate to staff being sufficiently trained in business continuity procedures.

Disasters such as fire and flood also impact on suppliers of goods and services to organisations. There is, therefore, the need for organisations to understand the business continuity capabilities of their third party providers and utilities. In a case study focused on data centre business continuity best practice (Brotherton & Dietz 2014), one of the cases studied was a power company that suffered a data centre outage. At the time (2003), it was the largest power blackout in US history and damage was estimated at $7-10 billion. Organisations reliant on power from that power company were significantly impacted. It is no use developing continuity plans that might rely upon mobile phones (as a contingency for fixed-line phone failure) when the provision of mobile phone services may also be impacted by the same event. Power supplies to mobile phone towers in recent Queensland floods (ABC News 2013) were affected, rendering the mobile phone network inoperable.

Key to having functional business continuity plans is ongoing testing, maintenance and reassessment of the capability of those plans, and the risk assessments they were built upon. It is important that as organisations upgrade or modify their information systems, that their business continuity plans relying upon those information systems are also updated and tested. Finally, security controls may become less robust during a business continuity event. This may be related to physical security, or it may relate to a ‘just get our systems up and running and do not worry too much about the information security controls’ attitude. Extra effort and focus could be required, particularly where key staff may no longer be available. Below is a summary of the relevance awareness plays for each of these stakeholders.

Senior management have a responsibility to ensure that a business continuity management process is implemented in order to minimize the impact on the organisation of a disaster and can enable recovery from loss of information assets (Sahebjamnia, Torabi & Mansouri 2015). In his article designed to explain a business continuity process to senior management, Lindstrom (2012, p. 269) developed a process to help explain the business continuity process because ‘senior management often lack awareness and understanding of their business contingency process and the terminology used’. He also found that this was ‘severely problematic in situations where normal business is interrupted by incidents or crisis’.

Senior management are best positioned to firstly identify and prioritise critical business processes, including identifying all the assets involved. They also need to understand the impact that interruptions caused by information security incidents are likely to have on the business. Additionally, they also need to ensure that the management of business continuity is incorporated into the organisation's processes and structure and not just seen as an add-on exercise.

Often IT staff, in conjunction with key end users, play a significant role in business continuity management. IT staff do this using their traditional role played in IT Disaster Recovery management, whilst end users whose business processes are disrupted play a key role. Jointly, they often drive the day-to-day business continuity planning framework. Research focused on developing integrated business continuity and disaster recovery planning (Sahebjamnia, Torabi & Mansouri 2015) highlights the roles played by IT staff and end users, in addition to the role previously mentioned for senior management. Key aspects for end users include developing fall-back procedures describing actions to be taken during a business disruption.

Consequence of poor awareness of Business Continuity Management

Some key consequences of poor awareness include:

- An organisation may cease to exist following on from an inability to recover from a disaster.
- Recovery activities may be more costly and take much longer if formal recovery plans have not been developed and tested prior to a disaster.
- Whilst an organisation may get by after a disaster, insufficient recovery planning may see the organisation fail in the medium term.

2.3.11 Compliance

This section of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, p. 100) has a focus on ensuring that information systems 'avoid breaches of any law, statutory, regulatory or contractual obligation, and of any security requirement'. Senior management in particular need to be aware (or have the appetite to be aware) of legislation that may be applicable to them - nationally as well as internationally. Data breach legislation (Burdon, Lane & von Nessen 2012) is evolving both in Australia and internationally. Singapore enacted personal data protection legislation in 2012 (Ter 2013). IT staff need to be able to interpret those legislations in terms of what it means from a technical controls perspective.

The Australian Payment Clearing Association (APCA) provide a standard for consumer electronic clearing system (CECS) that provides guidelines that members (major banks) must follow. The standard requires IT staff to interpret the requirements in terms of what technology should be used and how it should be configured. Additionally, the Australian Prudential Regulatory Authority (APRA) (2010, p. 3) published a prudential practice guide (PPG234) to 'assist regulated institutions in the management of security risk in information and information technology'. This could lead to enforceable standards being released in the future. It provides guidance that IT staff need to be aware of.

The *Payment Card Industry Data Security Standard (PCIDSS)* (2010) provides 'comprehensive standards and supporting materials to enhance payment card data security'. The US has the Gramm-Leach-Bliley Act (US Government 1999) focused on financial institutions and data privacy. Irrespective of which industry an organisation operates in, there is likely to be guidance, standards or compelling legislation regarding information, information systems and/or information security controls or techniques that need to be followed. In general, those that have an information security flavour are based on the standards outlined within the ISO/IEC 27000 series of standards and described extensively in this current research.

Adopting the ISO standards as best practice for information security practices can provide organisations with an appropriate framework in terms of information security. Intellectual property, protection of organisational records, and privacy of customer personal records is an important aspect of this section of the ISO/IEC 27002 standard as evidenced in the literature (Ghemri & Kannah 2015; Hou et al. 2013; Rghioui et al. 2015). The Australian Privacy Act (Australian Government 2015) and the emerging privacy principles sets guidance. As day-to-day incidents gain wider publicity within the media - board members, governments, shareholders and the general public will ask questions. These interested parties will be asking, 'could this also happen to my organisation'. Organisations need to be able to demonstrate good risk management practices, good data privacy practices (Ghemri & Kannah 2015), and a good process for demonstrating compliance.

Director responsibilities for APRA-regulated institutions saw prudential standard CPS 220 (Australian Prudential Regulatory Authority (APRA) 2013) come into force on January 1, 2015. This standard holds the board 'ultimately responsible for having a risk management framework in place that is appropriate to the size, business mix and complexity of the institution or group. The risk management framework must also be consistent with the institution's strategic objectives and business plan'. Board directors will need to assure themselves that this is in place.

Finally, auditing of information systems must be undertaken in order to assist with the overall audit of an organisation, particularly those that are publically listed (Byrne 2014; Kilgore et al. 2014). Often this is achieved by organisations having an IT audit function within their internal audit department. External auditors, as well as internal security functions undertaking technical compliance checking, would complement this. For functions that have been outsourced, there are specialist services that can provide this auditing of outsourced systems. Fanning (2014, p. 26) reports that 'SSAE 16 was issued by the Auditing Standards Board (ASB) of the AICPA in 2011'. Along with the SSAE 16, there are two different levels of service organisation controls reports, SOC 2 and SOC 3. SOC 2 focuses on the privacy issues, among others, and is restricted to certain users.

Demonstrating good compliance practices can be seen as a competitive advantage, particularly for information-centric organisations. The CEO of RIM Professionals Australasia suggests that 'information governance is policy-based management of information designed to lower costs, reduce risks and ensure compliance with legal, regulatory standards, and/or corporate governance' (Walker 2013).

Below is a summary of the relevance in relation to compliance that awareness has for each of these stakeholders. This section of the ISO/IEC 27002 standard is made up of a number of different aspects that have varying levels of reliance on the different stakeholder groups. As such, the different aspects are shown within a table and the awareness key points are shown against each different aspect.

Table 2-14 Senior management awareness of compliance aspects

Aspect	Senior management Awareness Importance for Compliance
Compliance with legal requirements	Senior management need a detailed understanding of their organisation's obligations and seek advice on legal requirements from the organisation's legal advisers, or suitably-

Aspect	Senior management Awareness Importance for Compliance
	qualified legal practitioners.
Compliance with security policies and standards, and technical compliance	Senior management need to ensure that the security of information systems is regularly reviewed.
Information systems audit consideration	Senior management need to provide an open and honest environment to maximise the effectiveness of, and to minimise interference to/from, the information systems audit process.

Table 2-15 IT staff awareness of compliance aspects

Aspect	IT staff Awareness Importance for Compliance
Compliance with legal requirements	IT staff would need to understand what compliance obligations there are for their organisation, how these would be assessed, how compliance would be demonstrated, and how this would be reported upon.
Compliance with security policies and standards, and technical compliance	IT staff would conduct reviews against appropriate security policies and the technical platforms, whilst information systems should be audited for compliance with applicable security implementation standards and documented security controls.
Information systems audit consideration	IT staff assist with protection controls that safeguard the integrity of, and prevent misuse of, audit tools.

End users generally need to understand their role in providing compliance with the obligations as outlined by senior management.

Consequence of poor awareness of Compliance

Some key consequences of poor awareness include:

- Organisations may be in breach of laws and regulations and penalised.
- Directors and senior officers of an organisation may be held personally responsible for breaches of the laws and regulations.
- Additional operational overhead may be incurred by an organisation if they do not have a structured approach to compliance management.

2.4 Research problem theory: analytical, theoretical frameworks and related research issues or propositions

The earlier part of this chapter discussed the main parent literature and theories covered in this thesis that underpin the theoretical framework within this research, including information security, situation awareness and capability measurements, and risk management. The next section provides a deeper examination of a number of particular aspects that form the basis of the Information Security Awareness Capability Model that has been developed in this research, including awareness importance, awareness capability, and awareness risk. Chapter 3 and Chapter 4 outline how these three aspects of ISACM, awareness importance, awareness capability, and awareness risk, were operationalised and measured in the methodological approach used in this research to develop and evaluate the ISACM in an organisational setting. The parent literatures presented earlier in this chapter highlighted the current gaps that exist in relation to the measurement of the effectiveness of information security awareness.

The introduction Chapter 1 of this current research presented a proposed theoretical framework in Figure 1-2 that linked some of the parent literature with a number of specific areas that will be examined further within this chapter. This includes: awareness importance that falls within information security (in particular ISO/IEC 27002) and information security awareness parent literatures. Awareness capability is examined in terms of situation awareness and general capability measurements parent literatures. Finally, awareness risk has its basis within general risk management literature. Each of these detailed areas is discussed below.

2.4.1 Awareness Importance and the ISO/IEC 27002 standard

The ISO/IEC 27002 standard was highlighted earlier as an important anchor point for the implementation and management of information security in organisations. The 11 security control clauses that make up the standard were discussed earlier in detail, and each of these security control clauses were analysed in terms of their specific relevance to awareness for each of the stakeholder groups: IT staff, senior management, and end users. The previous section also highlighted some of the key issues that could arise due to a lack of awareness by the stakeholder groups in relation to these 11 security control clauses. Figure 2-3 earlier clarified some of the key terms used within this research when referring to the ISO/IEC 27002 standard, including security control clauses (11 in total) and main security categories (39 in total). Each main security category has one control objective and one or more controls may be relevant in order to achieve that control objective.

Abawajy et al. (2008, p. 473) suggest that ‘human factors such as lack of awareness’ and the associated lack of understanding of potential risks to the organisation ‘could render any secure system into insecure system’. Clearly the presence of awareness is important. The richness of awareness guidelines contained within the ISO/IEC 27002 standard provides a wealth of information that, if properly captured, presented and categorised, could assist with the development of awareness importance ratings. By refining this information available in the ISO/IEC 27002 standard with the relevant literature, this current research has developed a mechanism for measuring awareness importance. This approach to measuring awareness importance is described in Chapter 3 Research Methodology I.

This ISO/IEC 27002 standard includes 39 main security categories. Each of these main security categories contains one control objective and one or more controls that could be considered. Complementing these clauses, categories, control objectives, and controls are implementation guidance for these controls and other supporting information. The ISO/IEC 27002 Standard provides a substantial body of knowledge to assist organisations with managing their information security. With so much material in the ISO/IEC 27002 standard, it is not practical or necessary for all stakeholders to be aware of all of the information in order for an organisation to have a high level of information security protection. For example, end users do not need to understand the technical aspects of how encryption works. Being able to determine the importance of awareness individually for each of the three key stakeholder groups (IT staff, senior management, end users) for the 39 main security categories and their associated control objectives of the ISO/IEC 27002 standard is likely to enable organisations to have a more focused approach to raising awareness. Effort (time and money) used to raise awareness can therefore be more targeted.

The standard setting by the International Standards Organisation leverages many experts in the field of information security. It is therefore likely that consideration would have been given to a wide variety of opinions as part of developing the standard. This hopefully leads to a broadly-accepted standard that meets (or at least considers) the opinions of the majority of information security practitioners.

2.4.2 Awareness Capability and Situation Awareness

An emerging application of Situation Awareness is Cyber Situation Awareness. Barford et al. (2009) suggests that situation awareness for Cyber Defense consists of:

- being aware of the current situation;
- being aware of the impact of the attack;
- being aware of how the situation evolves;
- being aware of the adversary behaviour;
- being aware of why and how the current situation is caused;
- being aware of the quality and trustworthiness of the collective situation awareness information; and
- plausible future of the current situation.

Tadda (2008) and Salerno (2008) support Endsley (1999) in the distinction between situation awareness and situation assessment, suggesting SA is a 'state of knowledge' and a cognitive human characteristic; whilst situation assessment is a set of processes that lends itself to automated techniques. Awareness capability bridges these two. Having the knowledge occurs at SA level 1, whilst assessing the situation occurs at SA level 2. Tadda & Salerno (2010, p. 33) also discuss *Measures of Effectiveness* (MoE), describing this as 'a decision maker's situation awareness'.

Although Cyber Situation Awareness has a high reliance on systems that process alerts and assess traffic patterns, it provides valuable insight (James et al. 2013; Webb et al. 2014). Tadda & Salerno (2010, p. 34) suggests 'minimal research has gone into measures of effectiveness but we expect to begin researching MoE in general and specifically for the cyber domain very soon'. Breton & Rousseau (2003, pp. 18-9) relate a model of SA developed by McGuiness and Foy, which supports the original SA model. This current research has adapted the model (see Table 2-16 below) to include linkages to the ISACM that will be developed in this research.

Table 2-16 Mapping SA levels to SA function

SA function	Contents	Processes	ISACM
PERCEPTION (What are the current facts?) Provides awareness of relevant information from external sources: readouts, displays, communications, environment, and so on.	Explicit objects, events, states, values	Sensing, detection, identification	Awareness Importance
COMPREHENSION (What is actually going on?) Provides awareness of what all this means, i.e. a more abstract understanding of the situation at hand, an appropriate schema for assimilating information.	Implicit meanings, situation types	Interpretation, synthesis	Awareness Capability
PROJECTION (What is most likely to happen?) Provides awareness of how this situation may develop over time by predicting or simulating possible scenarios, including one's own actions and their dynamic effects.	Future scenarios, possible outcomes	Prediction, simulation	Awareness Risk
RESOLUTION (What exactly shall I do?) Provides awareness of the best path to follow to achieve the required outcome to the situation, drawing a single course of action from a subset of available actions	Intension, courses of action	Decision-making, planning	Implementing Corrective Actions

Breton and Rousseau (2003, p. 19) suggest ‘one can readily recognise the three levels of Endsley’s model labelled here as functions’ in Table 2-16 above. Resolution is the decision-making process following level 3 of SA. Each higher level of SA leverages lower levels, although it is not necessarily a linear relationship (Endsley 2015). In terms of this research, and as shown below in Figure 2-4, perception is closely related to awareness importance, comprehension is related to awareness capability, and projection manifests itself as awareness risk. This mapping of the ISACM measurements onto the original SA model will lead to a key contribution in terms of providing an adapted model of SA that is applicable for information security awareness. An initial modification is presented below in Figure 2-4 and includes the awareness importance, awareness capability, and awareness risk measures mapped against the original model by Endsley (1995, p. 35). Aspects of SA functions shown in Table 2-16 are also shown in Figure 2-4.

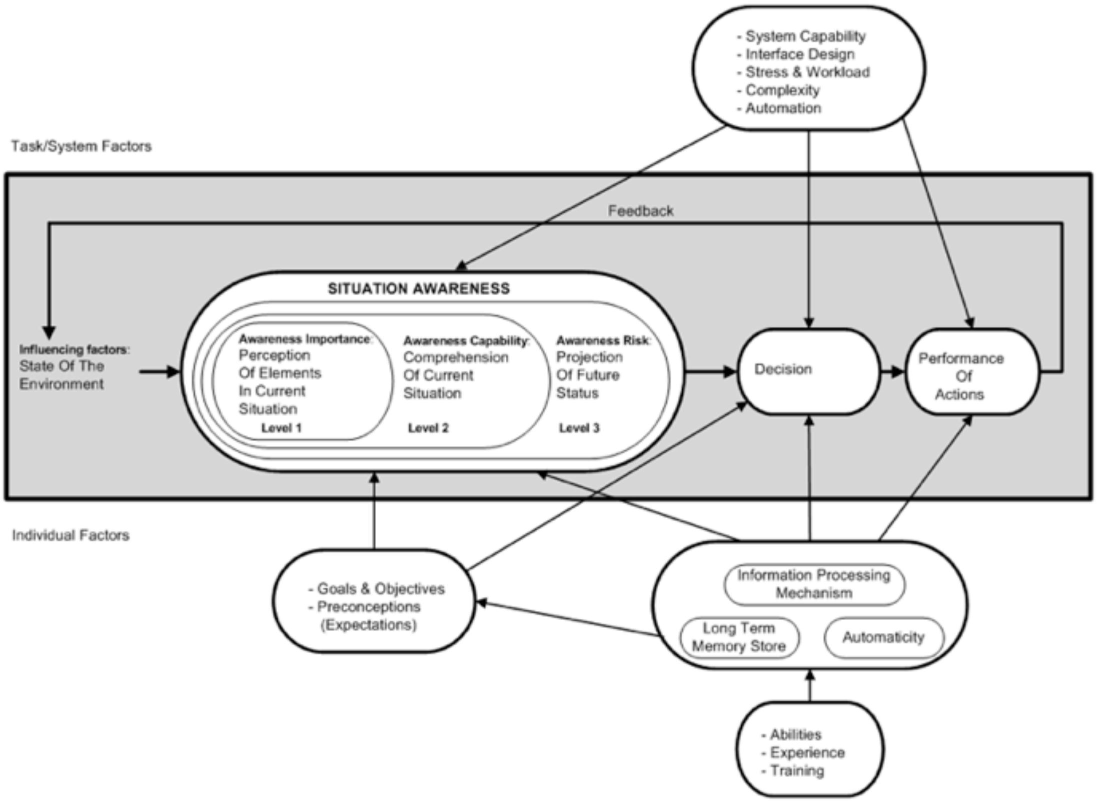


Figure 2-4 Adapted model of Situation Awareness in dynamic decision-making

Perception of Elements In a Current Situation in the original SA model links to awareness importance; *Comprehension of Current Situation* links to awareness capability; and *Projection of Future Status* links to awareness risk. The three-stage SA model appears an appropriate one to adapt for analysing the capability of information security awareness. Although applications of SA to information security do not deal with the life or death outcomes faced by pilots (where SA originated from), poor decisions on information security could have significant financial consequences for organisations and individuals as a result of threats such as online fraud and identity theft. Research by PricewaterhouseCoopers (PriceWaterhouseCoopers 2014), the Australian Bureau of Statistics (Australian Bureau of Statistics (ABS) 2011) and others (Nagunwa 2014; Seda 2014) provide evidence of a growing trend in computer-related fraud and theft.

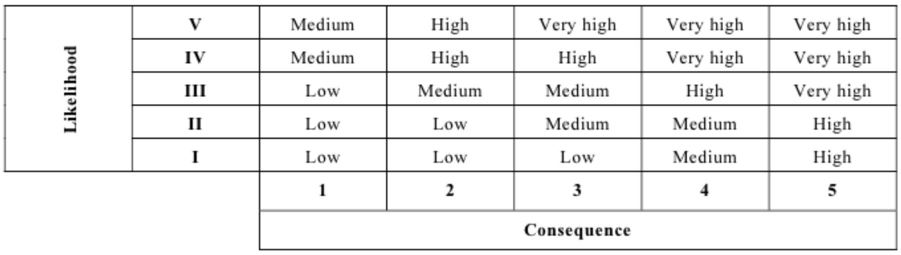
Support for the importance of SA finalises the discussion on SA (James et al. 2013; Webb et al. 2014; YinKarimi, et al. 2012). Breton and Rousseau (2003, p. 2) suggest ‘an improvement in SA could lead to a reduction in costly errors’ which could ‘enable the development of new abilities leading to high proficiencies in terms of planning, decision making and action’. Breton and Rousseau (2003, p. 3) provide support by relating how Klein (2000) presents the following importance of SA:

- SA appears to be linked to performance;
- Limitations in SA may result in errors;
- SA may be related to expertise; and
- SA is the basis of decision-making.

Improvements in SA of information security awareness at the individual level could lead to improvements in information security at an organisational level. The combination of awareness importance and awareness capability, and how they relate to a risk management measure of information security awareness is now examined.

2.4.3 Awareness Risk and the risk management standards

This current research will derive a measure for awareness risk as being the difference between desired awareness (awareness importance) and demonstrated awareness (awareness capability). The international standard on risk management ISO/IEC 31000 (Standards Australia/Standards New Zealand 2009a) provides guidance into how risks can be managed and measured. For example, Figure 2-5 from Standards Australia (Standards Australia/Standards New Zealand 2009b) guidelines on the risk management standard shows a way that the levels of risk can be calculated.

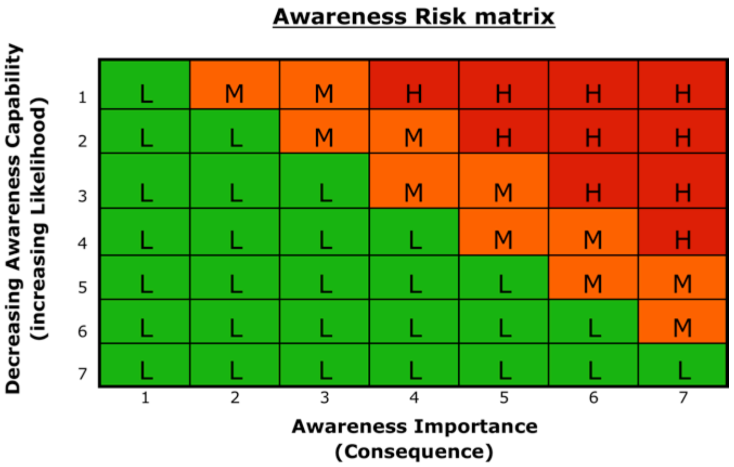


Likelihood	V	Medium	High	Very high	Very high	Very high
	IV	Medium	High	High	Very high	Very high
	III	Low	Medium	Medium	High	Very high
	II	Low	Low	Medium	Medium	High
	I	Low	Low	Low	Medium	High
		1	2	3	4	5
		Consequence				

Figure 2-5 Calculating level of risk

Awareness importance will be used as a proxy for consequence. The higher the awareness importance, the more important it is to have an understanding of the situation. This leads to a higher consequence resulting from that situation, particularly if the required level of awareness importance cannot be demonstrated. Higher consequences result from not knowing or not doing something that is required. The ISO/IEC 31000 standard (Standards Australia/Standards New Zealand 2009b) refers to consequences that ‘relate directly to objectives and arise when something does or does not happen’. In this research, it relates to awareness happening or not happening. The higher the need, then the higher the consequence.

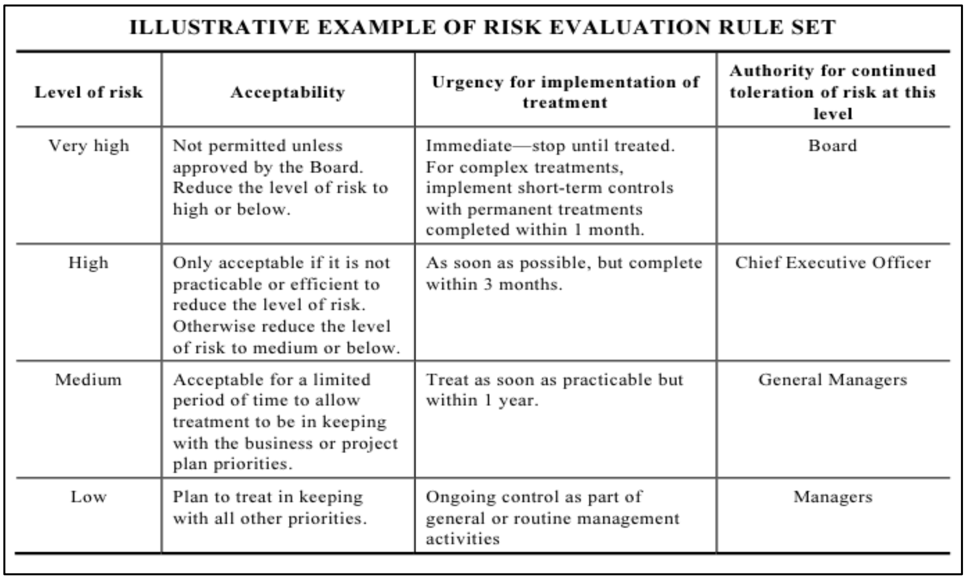
Awareness capability will be used as a proxy for likelihood. The lower the demonstrated awareness capability, the higher the likelihood that the appropriate information security control actions will not have been taken. The resultant square in the matrix then becomes the awareness risk measure. For example, in Figure 2-6 below where awareness importance is rated 6, but awareness capability is only rated 2, this presents a high awareness risk. Awareness capability is shown in descending order, reflecting increasing likelihood of controls not being demonstrated.



Decreasing Awareness Capability (increasing Likelihood)	1	2	3	4	5	6	7
1	L	M	M	H	H	H	H
2	L	L	M	M	H	H	H
3	L	L	L	M	M	H	H
4	L	L	L	L	M	M	H
5	L	L	L	L	L	M	M
6	L	L	L	L	L	L	M
7	L	L	L	L	L	L	L

Figure 2-6 Adapted Awareness Risk matrix related to information security awareness

Organisational risk management processes come into effect based on the awareness risk score. The treatment of risks will not be covered in detail in this research, however, the example shown in Figure 2-7 below is an approach an organisation may choose to take.



ILLUSTRATIVE EXAMPLE OF RISK EVALUATION RULE SET

Level of risk	Acceptability	Urgency for implementation of treatment	Authority for continued toleration of risk at this level
Very high	Not permitted unless approved by the Board. Reduce the level of risk to high or below.	Immediate—stop until treated. For complex treatments, implement short-term controls with permanent treatments completed within 1 month.	Board
High	Only acceptable if it is not practicable or efficient to reduce the level of risk. Otherwise reduce the level of risk to medium or below.	As soon as possible, but complete within 3 months.	Chief Executive Officer
Medium	Acceptable for a limited period of time to allow treatment to be in keeping with the business or project plan priorities.	Treat as soon as practicable but within 1 year.	General Managers
Low	Plan to treat in keeping with all other priorities.	Ongoing control as part of general or routine management activities	Managers

Figure 2-7 Example of risk evaluation rule set

Furthermore, employees demonstrating high levels of awareness capability are proactively managing the risks associated with a particular security category and security control objective. The level of risk column will be shown in the ISACM developed in this research as the awareness risk. Organisations could then determine how they will deal with that level of risk. The acceptability column for an organisation would describe whether a risk (particularly a low one) would be accepted. The urgency column would describe the timeframe, and authority column would determine the effective owner of the risk treatment or risk acceptance.

2.5 Theoretical and conceptual model – ISACM

In order to develop the information security awareness capability model that will be relevant and usable by industry participants, strong linkages to a well-established and well-known framework or series of standards was required. Hence, the international ISO/IEC 27000 information security series of standards were chosen to provide the foundation for the conceptual model in this study. The initial elements of the model were developed mainly from the secondary data obtained from these published standards (in particular AS/NZS ISO/IEC 27002:2006 Information technology-Security techniques-Code of practice for information security management), as well as other published security awareness guidance material, information security guides and assessment tools. This industry-based information security awareness literature was reviewed and discussed in the context of this research in Chapter 2.

Whilst the ISO/IEC 27002 standard provides a wealth of knowledge about information security management best practice, the volume and detailed nature of this standard can overwhelm individuals in an organisation. Should every stakeholder be aware of every aspect within the ISO/IEC 27002 standard to ensure good information security? Whilst that would be beneficial, it is clearly impractical and unachievable. Therefore, the first part of the model needed to cater for and rate what was more important to each of the key stakeholder groups in organisations. Earlier, awareness importance was defined as being ‘how important awareness is, or how influential awareness is in the success of a process or control’. *Awareness importance* therefore became the first component of the ISACM (model).

The ISACM also needed to capture how capable a person is of comprehending a situation they are faced with, and what actions (or controls) they should take. In other words, their situation awareness and their ability to perceive, comprehend and project the appropriate action when faced with a particular information security event. Hence, this research leveraged the cognitive theory of situation awareness, which is a three level information-processing model (perception, comprehension, projection) to determine an individual’s information security awareness in an organisation. For example, when faced with a situation such as receiving a phishing email, are they capable (through awareness) to understand what to do (delete without clicking any links or responding back) with that email. This *awareness capability* therefore became the second component of the ISACM (model).

The third and final component of the model was the application of the performance gap between how important awareness is (awareness importance) compared to how much awareness is being demonstrated (awareness capability), resulting in the *awareness risk* component of the ISACM (model). Its derivation is shown below.

$AR = AI - AC$ where AI = Awareness Importance; AC = Awareness Capability; AR = Awareness Risk

Where the required awareness importance is greater than the awareness capability being displayed, this results in a positive awareness risk score. A positive score for this third component results from less awareness being possessed (capability) than is required (importance) for that situation and presents risk for an organisation. Alternatively, if more awareness is possessed (capability) than the situation requires (importance), then a negative awareness risk score results and no such awareness risk exists. This does, however, have implications in terms of areas that require awareness to be increased (or not) within an organisation.

2.5.1 Elements of the ISO/IEC 27002 Standard that underpin ISACM

The ISO/IEC 27002 Standard is a recognised authoritative source for information security (Information Systems Audit and Control Association [ISACA] et al. 2011; Ramirez 2006). Section 2.3 above provided a detailed breakdown of the standard and its relevance to this research. The standard is the foundation of measurement points for the awareness importance component of the ISACM. The 39 main security categories and their associated control objectives were chosen as the awareness importance measurement points.

The control objectives, controls and implementation guidance provided in the standard for each of these 39 main security categories were analysed in terms of their awareness importance for each of the three key stakeholder groups. This provided the basis for developing the survey questions to capture information security awareness importance of each of these 39 main security categories for three key stakeholder groups. These 39 main security categories are summarised within their 11 high-level security control clauses as shown in Table 2-17 below.

Table 2-17: List of security control clauses and their main security categories

Security control clauses (11 in total)	Main security categories (39 in total)
1 Security Policy	1 Information security policy
2 Organization of Information Security	2 Internal organization
	3 External parties
3 Asset Management	4 Responsibility for assets
	5 Information classification
4 Human Resources Security	6 Prior to employment
	7 During employment
	8 Termination or change of employment
5 Physical and Environmental Security	9 Secure areas
	10 Equipment security
6 Communications and Operations Management	11 Operational procedures & responsibilities
	12 Third party service delivery management
	13 System planning and acceptance
	14 Protection against malicious and mobile code
	15 Back-up
	16 Network security management
	17 Media handling
	18 Exchange of information
	19 Electronic commerce services
	20 Monitoring
7 Access Control	21 Business requirement for access control
	22 User access management
	23 User responsibilities
	24 Network access control
	25 Operating system access control
	26 Application and information access control
	27 Mobile computing and teleworking
8 Information Systems Acquisition, Development and Maintenance	28 Security requirements of information systems
	29 Correct processing in applications
	30 Cryptographic controls
	31 Security of system files
	32 Security in development and support processes
	33 Technical Vulnerability Management

Security control clauses (11 in total)	**Main security categories (39 in total)**
9 Information Security Incident Management	34 Reporting information security events and weaknesses
	35 Management of information security incidents and improvements
10 Business Continuity Management	36 Information security aspects of business continuity management
11 Compliance	37 Compliance with legal requirements
	38 Compliance with security policies and standards, and technical compliance
	39 Information systems audit considerations

Source: Extracted from (Standards Australia/Standards New Zealand 2006b)

The ISACM reflects this structure and contains the 39 main security categories, grouped in the 11 security control clauses.

2.5.2 Elements of Situation Awareness that underpin ISACM

The starting point for developing the awareness capability instrument was to leverage insight gained from situation awareness (SA) theory (Endsley 2015; Webb et al. 2014). Situation awareness is the awareness an individual has of a situation - their dynamic understanding of 'what is going on' (Endsley 1995). Endsley defined situation awareness theory as a cognitive information-processing model based on three hierarchical levels. Situation awareness is a product of three hierarchical levels (1) perceptions of task-relevant elements in an environment; (2) the comprehension of their meaning; and (3) the projection of their status in the near future.

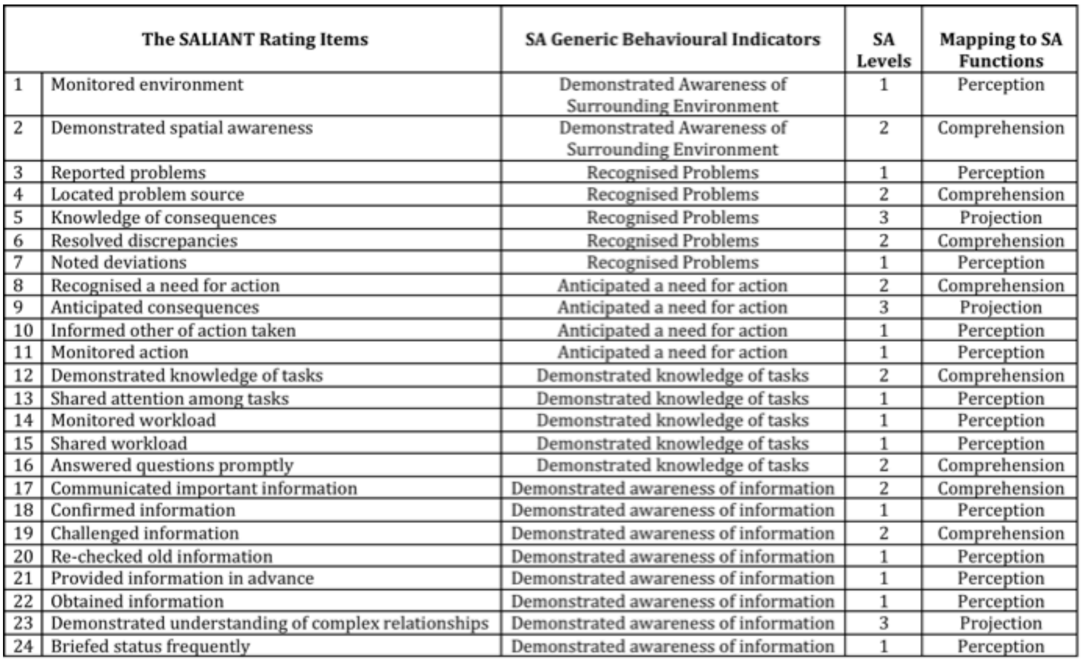
A low level of situation awareness would be associated with only a perception of something being present. For example, a low level of situation awareness regarding password management might result in someone changing their password regularly only because ‘that's what the IT security manager has told them to do’. A higher level of situation awareness would be associated with greater comprehension of a situation. For password management, this greater comprehension would result in someone not only changing their passwords regularly, but also making their password complex and of sufficient length in order to minimize the risk of the password being compromised.

And, finally, at the optimal level of situation awareness, the individual would be able to project what may result from a situation. For example, the use of the same password for personal and work-related user accounts may result in a broad compromise of that person’s identity at a personal and professional level should their password become known to a hacker.

Situation awareness is a cognitive information processing theory, which explains the information processing approach that will be taken by an individual in a situation depending on their level of perception, comprehension and projection of that situation (Endsley 2015; Howard & Cambria 2013; Webb et al. 2014). The ability of an individual to respond appropriately to a situation will be determined by their ability to perceive and comprehend a situation and then project the status of the situation in the future and act accordingly. Situation awareness is based on a three-level information-processing model that views situation awareness as a product of the levels of perception, comprehension and projection that one, two or all three may exist in varying degrees within an individual at a point in time. The three levels of situation awareness are hierarchical and are progressively dependent on each previous level. For instance, projection generally cannot exist without comprehension, which cannot exist without perception.

The cognitive theory of situation awareness informs the methodological approach to measuring the situation awareness of specific events. By measuring an individual's perception of the elements of a situation, comprehension of those elements and their ability to project the status of the situation in the near future and act appropriately, the situation awareness capability of an individual in an organisation can be captured in relation to a specific event. If an individual has poor perception of a situation then it is unlikely that they can comprehend what is the meaning of the elements of a situation; and even less likely that they would be able to project the status of a situation in the near future and act appropriately. This approach when applied to information security will allow the measurement of the awareness capability of individuals such as end users in organisations and then cross-reference this against the benchmark of information security awareness importance ratings provided by information security industry experts. Then it can be determined if there is an information security awareness gap and potential awareness risk to an organisation in relation to a specific information security category and control objective.

In order to develop this approach to measuring information security awareness capability, this research drew upon an existing measurement tool for situation awareness, the Saliant model shown below in Figure 2-8.



The SALIANT Rating Items		SA Generic Behavioural Indicators	SA Levels	Mapping to SA Functions
1	Monitored environment	Demonstrated Awareness of Surrounding Environment	1	Perception
2	Demonstrated spatial awareness	Demonstrated Awareness of Surrounding Environment	2	Comprehension
3	Reported problems	Recognised Problems	1	Perception
4	Located problem source	Recognised Problems	2	Comprehension
5	Knowledge of consequences	Recognised Problems	3	Projection
6	Resolved discrepancies	Recognised Problems	2	Comprehension
7	Noted deviations	Recognised Problems	1	Perception
8	Recognised a need for action	Anticipated a need for action	2	Comprehension
9	Anticipated consequences	Anticipated a need for action	3	Projection
10	Informed other of action taken	Anticipated a need for action	1	Perception
11	Monitored action	Anticipated a need for action	1	Perception
12	Demonstrated knowledge of tasks	Demonstrated knowledge of tasks	2	Comprehension
13	Shared attention among tasks	Demonstrated knowledge of tasks	1	Perception
14	Monitored workload	Demonstrated knowledge of tasks	1	Perception
15	Shared workload	Demonstrated knowledge of tasks	1	Perception
16	Answered questions promptly	Demonstrated knowledge of tasks	2	Comprehension
17	Communicated important information	Demonstrated awareness of information	2	Comprehension
18	Confirmed information	Demonstrated awareness of information	1	Perception
19	Challenged information	Demonstrated awareness of information	2	Comprehension
20	Re-checked old information	Demonstrated awareness of information	1	Perception
21	Provided information in advance	Demonstrated awareness of information	1	Perception
22	Obtained information	Demonstrated awareness of information	1	Perception
23	Demonstrated understanding of complex relationships	Demonstrated awareness of information	3	Projection
24	Briefed status frequently	Demonstrated awareness of information	1	Perception

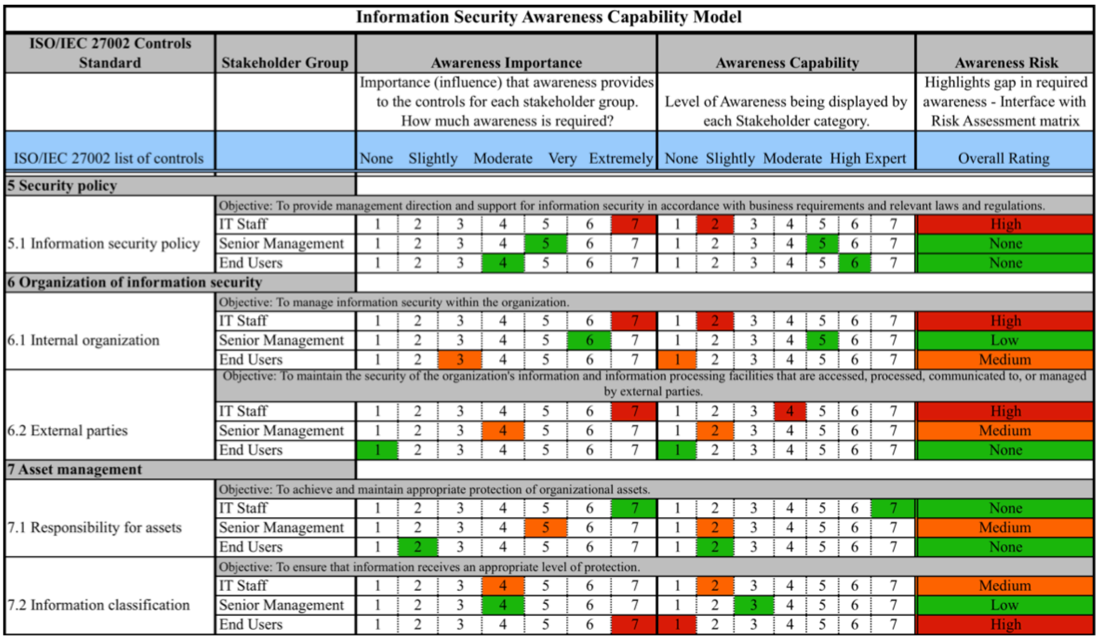
Figure 2-8 Combined SALIANT model influencing Awareness Capability

The Saliant model uses a range of actions (24 rating items) that people will take in relation to an event and associated tasks. These rating items could then be categorised into the SA generic behaviours such as Recognised Problem, Demonstrated knowledge of tasks, etc. In turn, these behaviours could be categorised into the SA functions or levels of perception, comprehension, or projection.

For this current research, a range of tests (via questions) could be developed to mimic the approach taken in Saliant so that the responses could demonstrate whether certain SA behaviours were being met, and these could then be mapped to the three SA functions (perception, comprehension, projection). Figure 2-8 above is an adaptation of this Saliant model. It shows observation categories (*Saliant Rating Items*) and *Generic Behaviour Indicators* that could be used for rating how stakeholders behave. The adaptation below (Adapted from Breton & Rousseau 2003, p. 46 drawn from Fink & Major) shows what likely links to the original SA levels could look like, as well as how they could be mapped to the SA functions.

This research investigated whether it was valid to have a single Saliant tool that could be applied to all of the ISO/IEC 27002 control objectives so that it could provide a consistent measure of information security awareness capability. The result of this investigation is detailed further in section 4.3.1. That section describes how the awareness capability instrument was developed and describes the challenges that would have been faced by using a single Saliant measurement tool, and why this research opted for developing a new awareness capability instrument.

An excerpt of the overall ISACM model is shown below in Figure 2-9. It demonstrates how the results of the assessment of information security awareness importance and awareness capability across an organisation can be interpreted in terms of performance gaps (awareness risk) for specific security categories. It shows the combination of the various components. For example, *Security policy* is one of the 11 security control clauses and contains one of the 39 main security categories, being *Information security policy*. Similarly, *Organization of information security* is another of the 11 security control clauses, however it contains two of the 39 main security categories: *Internal organization* and *External parties*. The final example shown is *Asset management* and it contains *Responsibility for assets,* as well as *Information classification*.



Information Security Awareness Capability Model

ISO/IEC 27002 Controls Standard	Stakeholder Group	Awareness Importance							Awareness Capability							Awareness Risk
		Importance (influence) that awareness provides to the controls for each stakeholder group. How much awareness is required?							Level of Awareness being displayed by each Stakeholder category.							Highlights gap in required awareness - Interface with Risk Assessment matrix
ISO/IEC 27002 list of controls		None Slightly Moderate Very Extremely							None Slightly Moderate High Expert							Overall Rating
5 Security policy																
5.1 Information security policy	Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.															
	IT Staff	1	2	3	4	5	6	**7**	1	**2**	3	4	5	6	7	**High**
	Senior Management	1	2	3	4	**5**	6	7	1	2	3	4	**5**	6	7	**None**
	End Users	1	2	3	**4**	5	6	7	1	2	3	4	5	**6**	7	**None**
6 Organization of information security																
6.1 Internal organization	Objective: To manage information security within the organization.															
	IT Staff	1	2	3	4	5	6	**7**	1	**2**	3	4	5	6	7	**High**
	Senior Management	1	2	3	4	5	**6**	7	1	2	3	4	**5**	6	7	**Low**
	End Users	1	2	**3**	4	5	6	7	**1**	2	3	4	5	6	7	**Medium**
6.2 External parties	Objective: To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.															
	IT Staff	1	2	3	4	5	6	**7**	1	2	3	**4**	5	6	7	**High**
	Senior Management	1	2	3	**4**	5	6	7	1	**2**	3	4	5	6	7	**Medium**
	End Users	**1**	2	3	4	5	6	7	**1**	2	3	4	5	6	7	**None**
7 Asset management																
7.1 Responsibility for assets	Objective: To achieve and maintain appropriate protection of organizational assets.															
	IT Staff	1	2	3	4	5	6	**7**	1	2	3	4	5	6	**7**	**None**
	Senior Management	1	2	3	4	**5**	6	7	1	**2**	3	4	5	6	7	**Medium**
	End Users	1	**2**	3	4	5	6	7	1	**2**	3	4	5	6	7	**None**
7.2 Information classification	Objective: To ensure that information receives an appropriate level of protection.															
	IT Staff	1	2	3	**4**	5	6	7	1	**2**	3	4	5	6	7	**Medium**
	Senior Management	1	2	3	**4**	5	6	7	1	2	**3**	4	5	6	7	**Low**
	End Users	1	2	3	4	5	6	**7**	**1**	2	3	4	5	6	7	**High**

Figure 2-9: Demonstration of the results from assessment of awareness importance, capability and risk

The model will allow organisations to identify and subsequently target areas requiring improvement in awareness by identifying performance gaps (potential awareness risks) in current levels of awareness in an organisation's workforce. The linkage to the ISO/IEC 27002 standard will allow organisations to reference the guidance material in the standard, helping them understand what controls are available to assist them, and how these controls can be implemented.

2.6 Conclusion

In summary, there is a substantial amount of literature that describes what to include in security awareness programs. The literature describes how to conduct education and training to improve information security awareness, and why awareness is important. The literature also provides some guidance on how to undertake the measurement of success of the awareness programs. There is, however, only minimal literature describing frameworks for measuring the importance and capability of information security awareness. Addressing this limitation and gap in the current literature is a prime motivator for conducting this current research, which will draw from the key literature streams discussed above to develop and evaluate an IS artefact - Information Security Awareness Capability Model (ISACM) - that will provide an informed understanding on how organisations can proactively address this problem of information security awareness capability and reduce the associated information security awareness risks to the organisation to an acceptable level.

This chapter has also provided an insight into the major parent theories including information security, situation awareness and capability measurements, and risk management. Information security was covered in great detail, firstly because it is the primary basis for this research and integral to information security awareness, and, secondly, there was extensive coverage of what makes up the major information security international standard, the ISO/IEC 27000 series. In particular, the ISO/IEC 27002 standard provides significant insight into what organisations should be doing in terms of information security. It therefore provides a substantial basis and guidance for examining information security awareness in greater detail.

There was extensive coverage of the existing literature in relation to information security awareness. The focus of coverage in this chapter was to highlight the extensive amount of material available to organisations in terms of what could be covered in an awareness program. Different aspects of awareness were highlighted and the benefits to organisations were discussed. The aspect of measuring the effectiveness of awareness education and training programs was also discussed. This forms a key part of this research in terms of how information security awareness can be measured. The coverage in this chapter highlighted there are gaps in the existing literature in how the effectiveness of security awareness programs is measured.

This leads onto the next major parent theory of situation awareness. This field of study presents theories on the different levels of situation awareness, and how perceptions of what is around us (including information) can help us to predict what might occur in the future. Although these theories were initially developed within the military air force, the science of SA is now being successfully applied to a number of other fields. This current research uses situation awareness as a theoretical lens to understand how awareness can be gained and applied to determine an outcome in the context of information security management in an organisation. Some measurement mechanisms were also discussed in this chapter.

The chapter was completed with a discussion on theories associated with capability measures, as well as risk management. These two areas play a role in this research in terms of approaches to use to measure awareness capability and being able to develop a measurement for awareness risk. These measures are covered in greater detail in the Research Methodology chapters (Chapters 3 and 4) and form part of the Information Security Awareness Capability Model (ISACM).

3.0 Methodology I

3.1 Introduction

The purpose of this chapter is to describe and justify the overall research methodology used in this PhD research, including the research paradigm adopted by the researcher which guided the methodological approach and specific research design employed in this thesis. This chapter provides an overview of the overall research design, and specifically covers the research design for phase 1. The next chapter (Chapter 4) covers the research design for phase 2. Figure 3-1 below outlines the structure of this chapter.

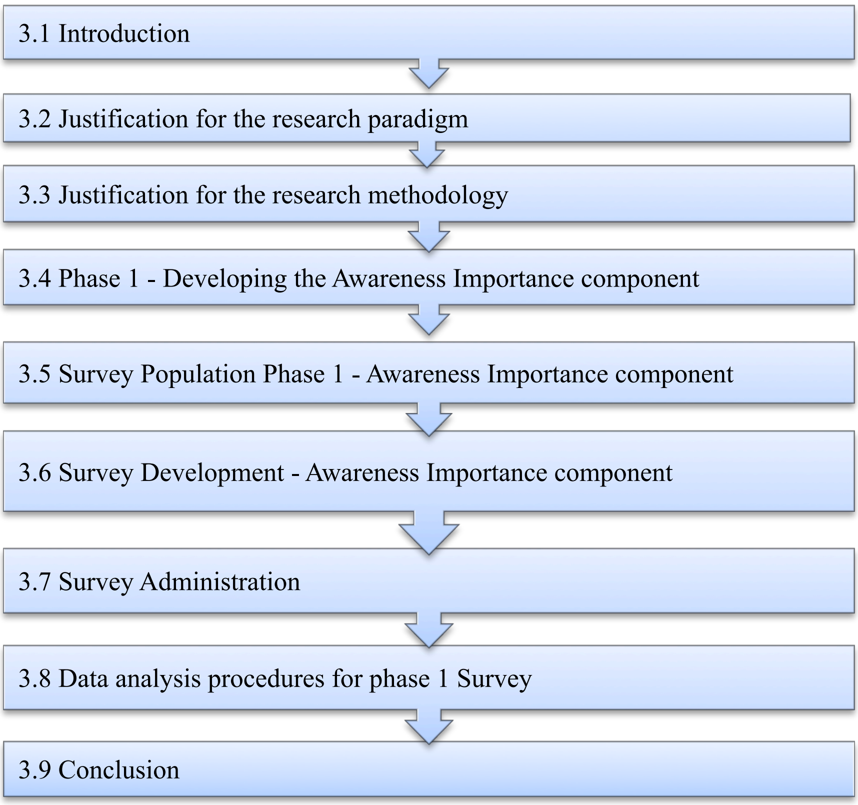

3.1 Introduction
3.2 Justification for the research paradigm
3.3 Justification for the research methodology
3.4 Phase 1 - Developing the Awareness Importance component
3.5 Survey Population Phase 1 - Awareness Importance component
3.6 Survey Development - Awareness Importance component
3.7 Survey Administration
3.8 Data analysis procedures for phase 1 Survey
3.9 Conclusion

Figure 3-1 Structure of Chapter 3

Firstly, an appropriate research paradigm for the thesis is determined and justified. Secondly, the thesis overall research methodology is described and justified. Thirdly, the research design and procedures for phase 1 are described, including the approach of using a survey in phase 1. The instrument used to collect data in phase 1 is also described and, finally, the chapter concludes with a brief summary.

3.2 Justification for the research paradigm

Although there are a variety of definitions for the word ‘paradigm’, one that captures the essence of the word is ‘*a philosophical and theoretical framework of a scientific school or discipline within which theories, laws, and generalizations and the experiments performed in support of them are formulated*’ (Merriam-Webster Dictionary 2015a). Thus, the research paradigm used reflects the philosophical and theoretical framework of the discipline in which this research has been undertaken.

A paradigm consists of a number of components: ontology, epistemology, methodology, and methods (Scotland 2012, p. 9). Scotland suggests ontology is concerned with reality (what is). Researchers 'need to take a position regarding their perceptions of how things really are and how things really work'. Epistemology is concerned with the nature and form of knowledge (what it means to know). Researchers must ask the question ' what is the nature of the relationship between the would-be knower and what can be known'(Guba & Lincoln 1994, p. 108). Methodology is 'concerned with why, what, from where, when and how data is collected and analysed' (Scotland 2012, p. 9). Researchers must ask 'how can I go about finding out whatever I believe can be known' (Guba & Lincoln 1994, p. 108). And finally methods are the techniques and procedures used to collect and analyse data.

Guba and Lincoln (1994, p. 109) summarise in Table 3-1 below how the aspects of ontology, epistemology and methodology can be compared across a number of research paradigms.

Table 3-1 Basic beliefs in inquiry paradigms

Item	Positivism	Postpositivism	Critical Theory	Constructivism
Ontology	naive realism- "real" reality but apprehendable	critical realism- "real" reality but only imperfectly and probabilistically apprehendable	historical realism- virtual reality shaped by social, political, cultural, economic, ethnic, and gender values; crystallized over time	relativism-local and specific constructed realities
Epistemology	dualist/objectivist; findings true	modified dualist/ objectivist; critical tradition/community; findings probably true	transactional/ subjectivist; value-mediated findings	transactional/ subjectivist; created findings
Methodology	Experimental/ manipulative; verification of hypotheses; chiefly quantitative methods	modified experimental/ manipulative; critical multiplism; falsification of hypotheses; may include qualitative methods	dialogic/dialectical	hermeneutical/dialectical

Additionally, Tronvoll et al. (2011) categorise research paradigms as belonging to one of three primary types. These are qualitative, quantitative, and mixed - as well as a number of variants of these three. Others, such as Burke (2007), attempt to look at research approaches that will help information managers in the current networked and digitised age. Burke (2007) describes the paradigms more in terms of social theory frameworks and includes paradigms such as radical humanist (critical social), radical structuralist (post-modernist), functionalist (positivist), and interpretive views. Below in Table 3-2 is a summary of how Burke (2007, pp. 480-81) describes the key attributes of these paradigms.

Table 3-2 Summary of research paradigms

Paradigm	Aim
Radical humanist (Critical social)	This aims to look beyond what is present, often looking to the past to discover the strong influences. This approach can assist with recognising reality in an objective way.
Radical structuralist (Post-modernist)	A post-modernist would take issue with the fact that results are presented in a detached way and would want the researcher's experience to be part of the final results.
Functionalist (Positivist)	The positivist approach to research can be defined as an approach where facts are clearly defined and results are measurable.
Interpretive	At its most basic level, the interpretive approach allows for discussion and questioning of assumptions.

Neuman (2006, pp. 86-87) suggests that a researcher adopting a positivist approach 'begins with a cause-effect relationship' and that this is logically derived 'from a possible causal law in general'. These abstract ideas are then linked to precise measurements. Another key aspect of the positivist approach is that the researcher 'remains detached, neutral, and objective' whilst measuring and examining evidence. Neuman (2006) recalls how objectivism (seen as a strong form of positivism) evolved in the 1920s and developed a rigor that 'created careful measures of external behaviour of individuals to produce quantitative data that could be subjected to statistical analysis'.

This rigor is similar to the approach that has been applied to this current research. Other attributes of positivism are also displayed in this current research, including attempts to discover 'laws' (the greater the awareness the more likely a control will be effective), as well as explanations of the results that will allow for this research to be replicated by other researchers. Overall based on the philosophical assumptions of this study in relation to ontology, epistemology and methodology, the functional positivism paradigm best fits the philosophical beliefs of this researcher. A quantitative approach using online surveys was an appropriate research method for this study.

3.3 Justification for the research methodology

This research investigated the following research questions which, in turn, determined the methodological approach adopted:

RQ1. What is the appropriate level of awareness importance of the main controls of the ISO/IEC 27002 Information Security Standard in terms of three stakeholder groups (IT staff, senior management, end users)?

RQ2. How can the awareness capability of these three stakeholder groups be measured, based on situation awareness theory?

RQ3. How can resultant awareness risk evidenced from insufficient awareness capability (in comparison to awareness importance) be combined into a risk management model that will assist organisations in measuring and managing information security awareness risk?

The methodology chosen used secondary data analysis as a mechanism for developing an initial model. Thirty-nine high level main security categories identified by well-established best practices in the ISO/IEC 27002 Information Security standards form the basis of the model. Each of these main security categories contains one control objective and one or more controls that can be applied to achieve the control objective. These security categories and control objectives provide the basis for measuring information security awareness in organisations and identifying performance gaps between the actual levels of information security awareness and the desirable levels of information security awareness. By identifying performance gaps in information security awareness, organisations can identify potential risks that exist where information security awareness capability of employees is less than what it should be.

The limitations of the methodology applied in this research have been included in Section 7.4 on page 190.

3.3.1 The use of surveys

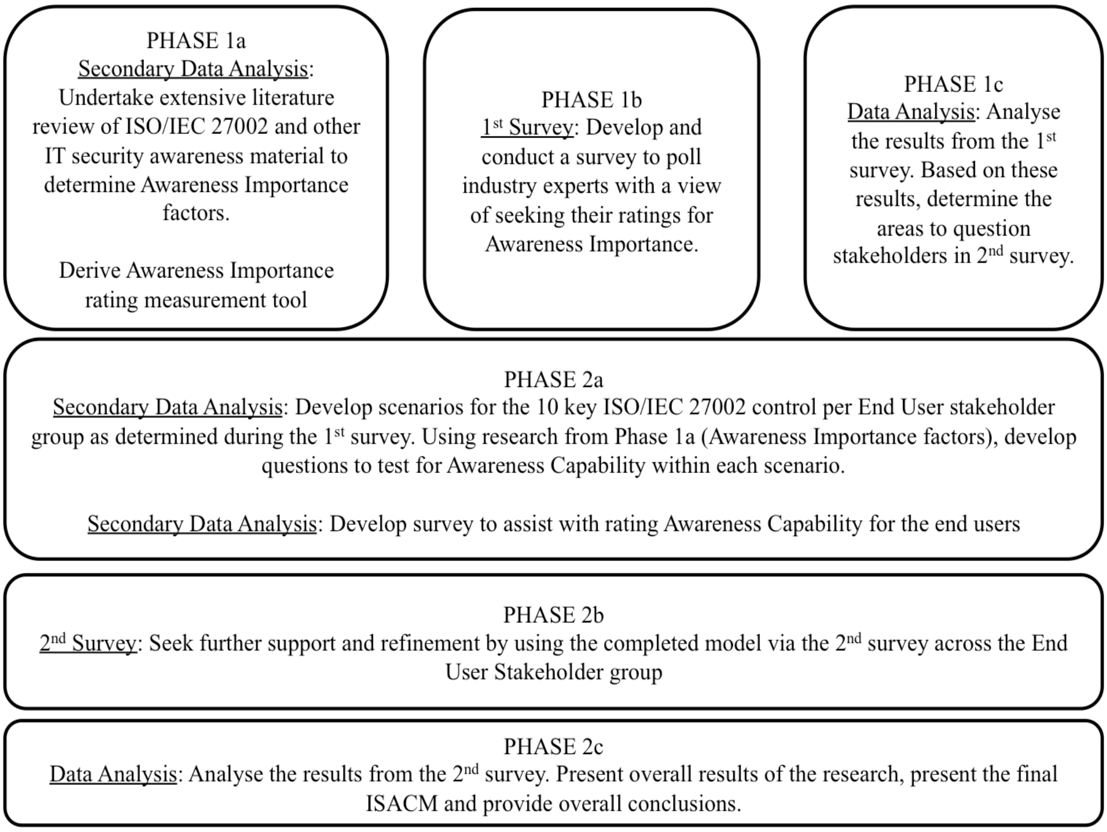
Surveys were the method used for data collection in this research and used to seek support for the first component of the Information Security Awareness Capability Model (ISACM), awareness importance, with industry experts. This involved rating awareness importance for each of the 39 main security categories and their associated control objectives. The second component of the model leveraged both the results from the first survey and secondary data analysis for the design of the second survey to measure the second component of the ISACM, information security awareness capability of employees.

Yin (2003, pp. 28-33) suggests surveys are beneficial when research is attempting to understand a ‘what’ question. Bhattacherjee (2012, p. 73) believes surveys can be used ‘for descriptive, exploratory or explanatory research’. This current research is a mixture of these types of research. Bhattacherjee (2012) suggests it is suited when the unit of analysis is an individual person. For this current research the unit of analysis for phase 1 is the three stakeholder groups (IT staff, senior management, and end users) in terms of desired awareness importance. The unit of analysis for phase 2 of this research is the end user stakeholder group.

Surveys are beneficial in comparison to other alternative methods, particularly when trying to measure the unobservable data (such as people’s preferences) (Bhattacherjee 2012, p. 73). It is also useful when capturing factual information (such as job role or years of experience). Because of the remote nature of collecting data from people that could not be economically directly observed, survey techniques are also very suitable (Pedersen & Nielsen 2014). The relative unobtrusive nature of the survey (people are not compelled to complete it, and the results are kept anonymous), and the electronic completion and capturing of survey responses also makes it an appropriate method for data collection and analysis (de Leeuw 2012).

3.3.2 Two-phased research approach

The development and evaluation of the ISACM was conducted in two phases. Figure 3-2 below provides a snapshot of the overall phases of this research.



PHASE 1a
Secondary Data Analysis: Undertake extensive literature review of ISO/IEC 27002 and other IT security awareness material to determine Awareness Importance factors.

Derive Awareness Importance rating measurement tool

PHASE 1b
1st Survey: Develop and conduct a survey to poll industry experts with a view of seeking their ratings for Awareness Importance.

PHASE 1c
Data Analysis: Analyse the results from the 1st survey. Based on these results, determine the areas to question stakeholders in 2nd survey.

PHASE 2a
Secondary Data Analysis: Develop scenarios for the 10 key ISO/IEC 27002 control per End User stakeholder group as determined during the 1st survey. Using research from Phase 1a (Awareness Importance factors), develop questions to test for Awareness Capability within each scenario.

Secondary Data Analysis: Develop survey to assist with rating Awareness Capability for the end users

PHASE 2b
2nd Survey: Seek further support and refinement by using the completed model via the 2nd survey across the End User Stakeholder group

PHASE 2c
Data Analysis: Analyse the results from the 2nd survey. Present overall results of the research, present the final ISACM and provide overall conclusions.

Figure 3-2: Summary of Research Design Phases 1 and 2

Phase 1 of the research was the development of the structure of the overall ISACM that provided the key measures for this research. These key measures are awareness importance, awareness capability and awareness risk. Phase 1 of this research was used to survey information security, IT risk and IT audit professionals to seek their ratings of awareness importance. The results from phase 1, and in particular the main security categories and control objectives that rated highest for awareness importance for the end user stakeholder group, informed the design of an instrument developed in phase 2 to measure information security awareness capability for a specific stakeholder group - end users. These two measures, awareness importance and awareness capability, which were captured in phase 1 and phase 2 surveys, then enabled the identification of performance gaps in information security awareness capability in organisations and the associated information security awareness risks that may exist.

Phase 2 utilised the results of phase 1 to identify main security categories and their associated control objectives for which questions were to be developed for the second survey. The ISACM (model) can cater for presenting every control in the ISO/IEC 27002 standard and testing for awareness capability; however, those being surveyed would not be receptive to being questioned on aspects that may have little relevance or importance for their particular stakeholder group. Such an approach would also lead to a very lengthy survey. In order to demonstrate the feasibility of the ISACM, this research focused on the measurement of awareness capability for a single stakeholder group, that of end users.

The second survey was developed to assess the end user stakeholder group on their awareness capability of the top 10 main security categories and their associated control objectives that have a higher level of awareness importance (as determined during the first phase of the data collection) than others. This allowed for the demonstration of the robustness of the ISACM for one stakeholder group – end users. This was then tested with two separate population groups. The first was the general population group who were derived from a survey panel, constructed for this research, of end users who were employed across a range of industry groups, and utilising computing technology as part of their employment. The second specific population were staff at an Australian university.

The model was tested for a selected stakeholder group, end users, and provides organisations with a robust approach that can be used across their whole organisation and for all stakeholder groups. In terms of the overall research questions (RQ1, RQ2, and RQ3), Table 3-3 and Table 3-4 below provide a high-level outline of the steps undertaken in addressing each research question. The full details of the steps undertaken for phase 1 and phase 2 are provided in this Chapter 3, as well as in Chapter 4.

Table 3-3: High-level steps for phase one – Develop Awareness Importance survey instrument and seek ratings for each ISO/IEC 27002 control objective based on expert knowledge and experience (RQ1)

What was done	How this was done
Extensive review of ISO/IEC 27002 standard and relevant information security and information security awareness literature.	Identifying aspects of the ISO/IEC 27002 control objectives that influence the importance factor in terms of awareness did this. This also fed into later steps (awareness capability), as these are the factors that need to be demonstrated.
Develop the survey instrument for phase 1 survey.	Researching each of the 39 main security categories and their associated control objectives, and constructing questions that could assess the importance that awareness has on the success of the control objectives. Conducted pre-testing of the survey with information security, IT risk and IT Audit professionals knowledgeable about information security.
Administer the survey for the first component of the ISACM to obtain industry expert opinions as to how they would rate awareness importance.	Provide survey to information security experts and practitioners via Australian Information Security Association (AISA), as well as to international information security, IT risk and IT audit professionals via LinkedIn to solicit their ratings for awareness importance.
Analyse the results of the phase 1 data collection and calculate **Awareness Importance. (RQ1)**	The data collected was analysed using SPSS. Results from the first survey were used to determine which areas would be examined in phase 2.

The following Table 3-4 is a high-level outline of the steps involved in phase 2.

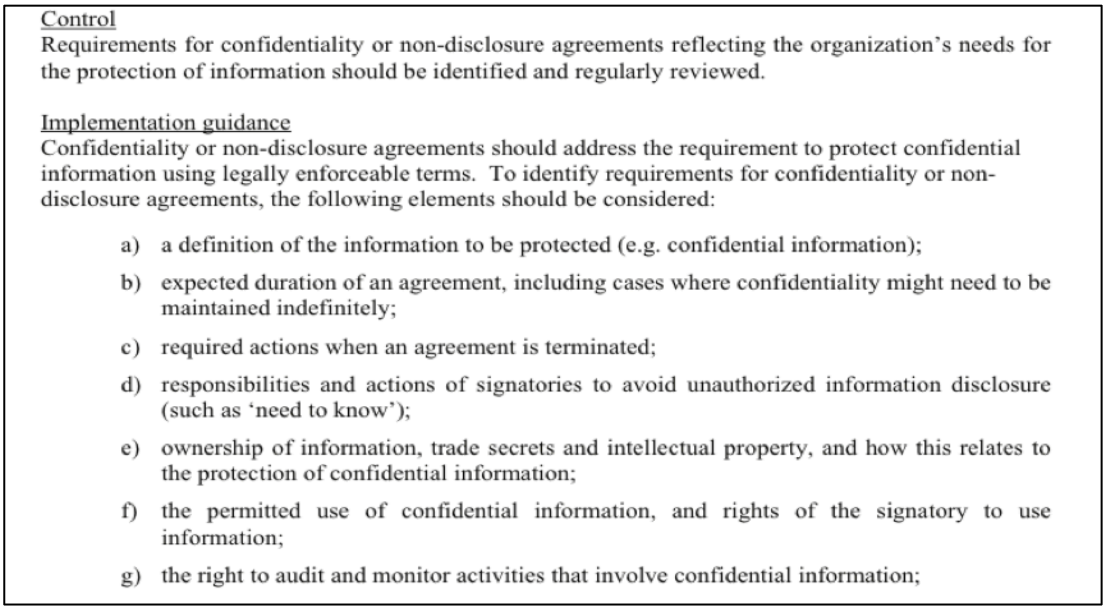
Table 3-4: High-level steps for phase two – Develop a measurement instrument for Awareness Capability (RQ2) and Awareness Risk (RQ3)

What was done	How this was done
Leverage the insights from SA theory and, in particular, the Saliant instrument in the context of information security awareness in order to measure the level of awareness being demonstrated.	The Saliant model (Muñiz et al. 1998) was examined to determine whether it could be adapted for this research. Whilst not fully applicable, the approach helped to inform this research.
Determine the appropriate areas for developing the initial scenarios.	Using the results of the phase 1 data collection, this research identified the top 10 rated awareness importance responses across the 11 security control clauses and 39 main security categories. This was undertaken for the end user stakeholder group.
Develop scenarios for the top ten rated ISO/IEC 27002 main security categories control objectives as captured in the awareness importance scores of phase 1 survey for end users.	Based on the top 10, scenario questions were developed (three parts for each of the 10 questions), with each part representing situation awareness style Level 1, 2 and 3 complexities.
Develop second Survey to measure Awareness Capability.	The survey structure presented three parts per question. Each part requires increasingly more awareness than the previous and is designed to simulate escalating levels of SA. The results provide an indication of whether the respondent displays Level 1, 2 or 3 Situation Awareness.
Administer the second survey	The survey was provided to two distinct population groups. The first was the baseline population via a panel of generic end users employed across a range of industries using information technology in their work. The second was the specific population of staff at an Australian university.
Analyse the results of the phase 2 data collection and calculate **Awareness Capability. (RQ2)**	The data collected was analysed using SPSS. Chapter 5 discusses the analysis of the results.
Develop a measurement for **Awareness Risk**. (**RQ3**)	
Develop an Awareness Risk matrix.	Use risk management approach to develop a suitable rating mechanism. Discussed further in Chapter 4.
Finalise the **ISACM model**	

3.4 Phase 1 - Developing the Awareness Importance component

The starting point for developing the awareness importance component was assessing the information provided in the *AS/NZS ISO/IEC 27002:2006 Information technology-Security techniques-Code of practice for information security management*. This structure was illustrated earlier in Figure 2-3 on page 35. This ISO/IEC 27002 standard includes a significant amount of guidance information in terms of how to implement and manage security controls in an organisation. It is this guidance information that provides detailed insight of what will assist with achieving the main security categories control objectives.

Figure 3-3 below shows an example from the ISO/IEC 27002 standard for: Organisation of Information Security, *security control clause:* 2, *security category:* Internal Organisation, and *control:* Confidentiality agreements.



Control
Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.

Implementation guidance
Confidentiality or non-disclosure agreements should address the requirement to protect confidential information using legally enforceable terms. To identify requirements for confidentiality or non-disclosure agreements, the following elements should be considered:

a) a definition of the information to be protected (e.g. confidential information);
b) expected duration of an agreement, including cases where confidentiality might need to be maintained indefinitely;
c) required actions when an agreement is terminated;
d) responsibilities and actions of signatories to avoid unauthorized information disclosure (such as 'need to know');
e) ownership of information, trade secrets and intellectual property, and how this relates to the protection of confidential information;
f) the permitted use of confidential information, and rights of the signatory to use information;
g) the right to audit and monitor activities that involve confidential information;

Figure 3-3 Example ISO/IEC 27002 guidance material

Much of this guidance is in the form of 'the following should be considered', or 'the following should take place', or 'should take account of'. The example above describes what should be considered for inclusion in a confidentiality agreement. Clauses that detail what happens when an agreement is terminated, responsibilities, and the right to audit are important aspects for an organisation to include within a confidentiality agreement. Awareness of what should be considered, or put in place, or taken account of helps organisations with achieving these control objectives. This approach became the foundation on which the awareness importance measure has been developed for the ISACM.

3.5 Survey Population Phase 1 – Awareness Importance component

The target population for this component of the research were people with significant industry experience (5–10 years +) in the closely related fields of information security, IT auditing, and IT risk management. The online survey was targeted at the membership of Australian Information Security Association (AISA) with more than 2,000 members, and a number of special interest groups from the social networking site LinkedIn, including Information Security Group ISO/IEC 27000, Certified Information Systems Auditors, Certified Information Security Managers, Information Security Community, Institute of Information Security Professionals, and Perth Security Professionals.

These specific industry and special interest groups were considered to be the most appropriate people to answer the online survey given that many of the membership of these groups have significant industry experience and knowledge of information security, IT auditing and IT risk management around which the ISO/IEC 27002 standard is framed.

The phase 1 awareness importance online survey was distributed via a URL link in the AISA newsletter, which is sent out to its membership. A posting on the LinkedIn Special Interest groups targeted by the phase 1 awareness importance online survey contained an invitation to participate in phase 1 of this research and a URL link to the online survey. Because of the anonymous nature of the survey, and the fact that the online survey was distributed to a number of industry and special interest groups as outlined previously, it was not possible to calculate a response rate.

The purpose of the online survey was to establish an initial baseline of awareness importance for each of the 39 main security categories and associated control objectives in the ISO/IEC 27002 based on the expert opinions of practitioners knowledgeable in the field of information security. The demographics of the survey respondents who completed the phase 1 online survey (see Chapter 5 Data Analysis, Section 5.2 Descriptive Statistics - Phase 1 Survey) would indicate that this was achieved.

3.6 Survey Development – Awareness Importance component

The survey questionnaire was developed in a number of stages, which are described in greater detail below. These steps included:

- ISO/IEC 27002 standard in relation to each of the 39 main security categories, associated control objective, controls and implementation guidance was analysed and used to construct a high level awareness importance rating question which captured the essence for each of the 39 main security categories;
- A pre-test to verify the appropriateness of each survey question;
- The survey questionnaire was designed;
- The survey questionnaire was pilot tested; and
- The survey questionnaire was given a final proof prior to link distribution.

3.6.1 Pre-test to verify the appropriateness of each survey question

Pre-testing of a survey allows for sense checking of the wording and structure of the questions being asked. Whilst a question may appear to be very clear to the author, obtaining opinions from others provides a valuable review mechanism and can improve the face validity of the awareness importance survey instrument. Once the development of the questions measuring awareness importance had progressed sufficiently, they were distributed to a number of information security professionals, as well as a number of academics who were collectively knowledgeable about information security and survey design. This process was used to solicit comments to improve the face validity and content validity of the proposed survey questions. Subsequent feedback received from these information security professionals and academics resulted in some changes to the wording of a number of the questions.

3.6.2 Survey Questionnaire design

The survey questionnaire design was informed by established guidelines regarding survey layout and structure (Dillman 2000; Lefever, Dal & Matthíasdóttir 2007; Van Selm & Jankowski 2006). The layout, presentation and format of the survey questionnaire for this research were designed by incorporating the following principles:

- Ensuring individual questions and statements would be easy to understand;
- Providing adequate information to the respondents in order to allow them to complete the survey; and
- Grouping questions and answers in a logical sequence to aid in the completion of the survey.

3.6.2.1 Survey Questionnaire layout

Cover page. In the opening frame of the survey, details were provided of the purpose of the survey, as well as clarification of the three stakeholder groups that survey participants were asked to provide ratings about. An option to see further details as to the development of the awareness importance measure was provided.

Demographic information. With the survey aimed at information security, IT audit and IT risk professionals, it was important to obtain the level of expertise the respondents possessed. It was also important to see which stakeholder group the survey participant associated with. Although the stakeholder definition of IT staff included information security staff, there was a need to verify this with the survey participant. Also, for those who identified themselves as IT staff, the specific IT job field they most associated with was obtained. This information would allow for further categorisation of the survey result data based on the profile of the survey respondents. Chapter 5 includes the results analysis.

The body of the questionnaire. Designing the 39 questions that measured awareness importance for each of the 39 main security categories in the ISO/IEC 27002 standard was the next task. Feedback received when pre-testing the survey was that the survey was too long. Initially, the research was looking at the feasibility of constructing questions for each of the controls that were supporting the 39 control objectives in the ISO/IEC 27002 standard, but this would have resulted in a questionnaire of many hundreds of questions. Presenting 39 questions (with three answers required per question for each of the stakeholder groups) was required in order to adequately cover key elements of the ISO/IEC 27002 standard whilst ensuring that the survey was not too long and onerous. Although there is a widespread view that long surveys should be avoided, de Vaus (2002, p 112) suggests there is ‘little research that supports this as a common sense assumption’.

The back cover. The back cover was kept simple and it invited respondents to make additional comments and feedback about the questionnaire.

3.6.2.2 Considerations to increase response rate of the survey

De Vaus (2002, p. 127) suggests that to maximise response rates in Internet surveys the researcher/s should ‘get the survey to the selected population in a way that makes people want to respond’. With the survey targeting AISA members, approval and support of the AISA executive was obtained. The members of AISA were presented with a link to the survey by an email sent out to them by the various AISA State chapters encouraging participation. It also meant that the members would be receiving the invitation through their normal communications with AISA, rather than through an anonymous email from someone they may not know or trust.

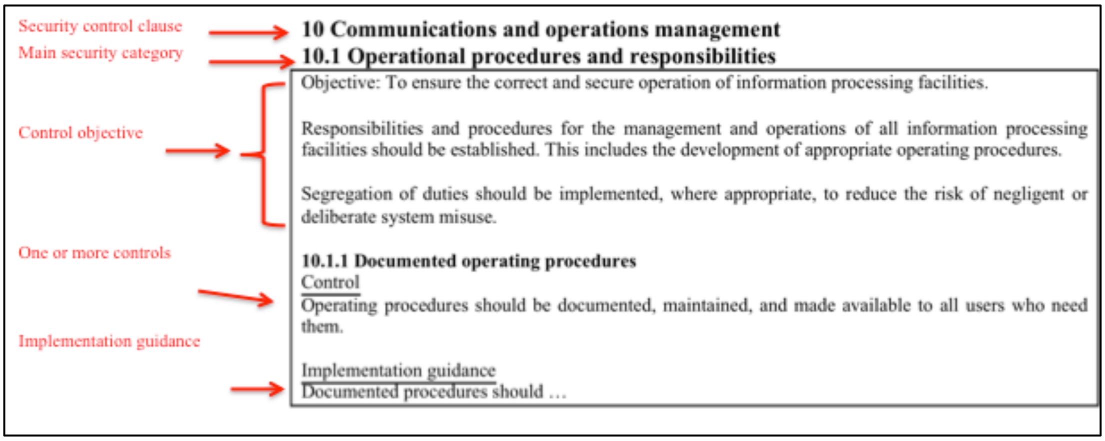
To achieve reasonable response rates, De Vaus (2002) suggests a follow-up of non-responders be conducted. Because the survey was anonymous it was not possible to just target the non-responders, however, the survey link was reposted numerous times through the AISA LinkedIn group. De Vaus (2002) advises that to ensure quality in Internet surveys one should 'know the characteristics of the population the sample is meant to represent'. By using AISA members, this was correctly aligned with the target population of information security professionals. Information security special interest groups on LinkedIn were also targeted for this survey. This provided access to those professionals who have joined these groups in order to collaborate on their topics of interest. The LinkedIn special interest groups targeted for this research were: Information Security Group ISO/IEC 27000, Institute of Information Security Professionals Certified Information Systems Auditors, Certified Information Security Managers, Information Security Community, and Perth Security Professionals.

Other advice from De Vaus (2002) suggests that responses are improved from 'anonymous and secure' surveys. This is particularly important when surveying information security professionals. In the survey it was emphasised that the survey is anonymous and no personally identifiable information was sought. Additionally, De Vaus (2002) suggests 'careful use of skips and piping', 'requiring an answer before proceeding' and the 'use of a specially designed internet survey package'. The use of the Qualtrics online survey tool enabled this capability and simplified the process of building the questionnaire, distributing it, and retrieving the survey response data.

3.6.2.3 Survey Questionnaire content

To illustrate how the questions developed for the phase 1 survey were derived from the ISO/IEC 27002 standard, and to further illustrate the terminology used within this standard and in this research, a breakdown of the structure of the standard is provided below in Figure 3-4. The ISO/IEC 27002 standard includes:

- 11 security control clauses
- 39 main security categories
    - each main security category contains:
        - a control objective
        - one or more controls
        - implementation guidance
        - additional information


Security control clause
Main security category
Control objective
One or more controls
Implementation guidance

10 Communications and operations management

10.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

Responsibilities and procedures for the management and operations of all information processing facilities should be established. This includes the development of appropriate operating procedures.

Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

10.1.1 Documented operating procedures

Control

Operating procedures should be documented, maintained, and made available to all users who need them.

Implementation guidance

Documented procedures should …

Figure 3-4 Example ISO/IEC 27002 Standard

To illustrate the linkage between material contained within the standard and the survey questions that were developed, an example showing the question developed for the control objective shown above in Figure 3-4 was:

> How aware of **formalising operational procedures and responsibilities**, do the stakeholder groups need to be, so that the correct and secure operation of information processing facilities is managed?

As shown above, the text in the survey question has been significantly reduced from the material provided within the standard without losing the key aspects of the control objective. This approach was applied to the construction of all 39 survey questions. These questions were used to capture the information security awareness importance rating for each of the 39 main security categories and their associated control objectives in the ISO/IEC 27002 standard. The full set of the 39 survey questions that were developed is included within Appendix A. To assist respondents with the completion of the survey, each of the 39 questions were constructed in a standard format in order to maintain a consistent approach. These questions began with the phrase, *'How aware….'*; and then included content that was specific to that particular control objective.

3.6.2.4 Scale used for the survey questions

Figure 3-5 below shows the sliding scale used for all 39 questions. A 7-point scale was chosen and descriptive text ranging from *Not at all aware* (scores of 1 or 2), through to *Moderately aware* (a score of 4), finally through to *Extremely aware* (scores of 6 or 7). Joshi et al. (2015, p. 398) argue that 'the 7 point scale is better than a 5 point scale and provides more varieties of options which in turn increase the probability of meeting the objective reality of people'. They also argue that this scale 'reveals more description about the motif and thus appeals practically to the 'faculty of reason' of the participants'.

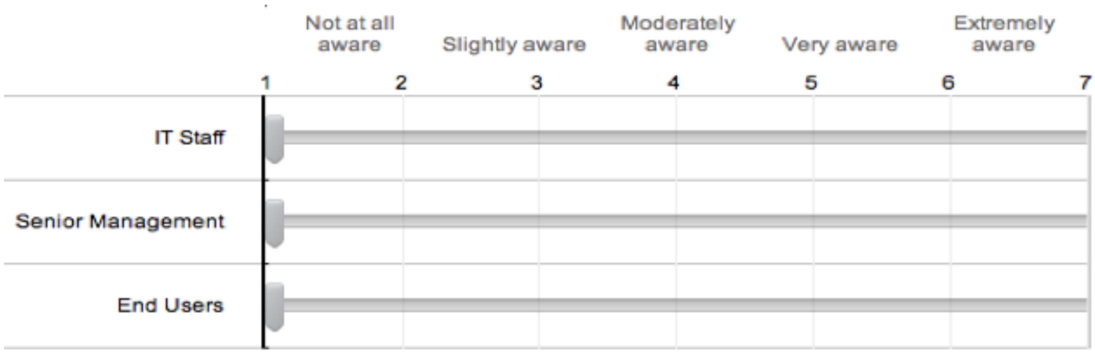


Figure 3-5 Scale used for phase 1 Survey

3.6.2.5 Coding questions in Qualtrics

Qualtrics (online survey tool) was used to develop and administer the online survey (Qualtrics Labs Inc). All questions were numbered within Qualtrics with instructional questions (i.e. do you want to see more information) and demographical questions (i.e. stakeholder experience) were coded using roman numerals. For each of the 39 primary questions, these were prefixed Qxx_yy where xx was the primary question number and yy is the stakeholder group response. IT staff was the first stakeholder for each question, senior management the second and end users the third. Table 3-5 below provides an example of how the results were extracted from the

Qualtrics tool. For example, for Question 1 and stakeholder senior management, the response is collected under Q1_2. This allowed the Qualtrics tool to automatically code the responses. The Qualtrics tool provided an extraction facility that allowed this data to be downloaded into a SPSS file format ready for data analysis in SPSS.

Table 3-5 Extract of survey responses

Question #	Extracted Text labels from Qualtrics
i	Information Security Awareness Survey / / Information Security Awareness Capability Mode...
ii	If you would like to see additional information about the ethics clearance for this survey, includin...
iii	Participants Information Sheet / / / / HREC Approval Number: H12REA163 / / Full Project Title: Developme...
iv	If you would like to see additional information about my research or how I have been developing the...
v	How have I developed a measure for Awareness Importance? / / / / A key component of my model is a m...
vi	Stakeholder Experience and Role Information: / / To assist with categorising responses, please select...
vii	Please select which Stakeholder group you most associate yourself with?
Q1_1	SECURITY POLICY: / / / / / / How aware of information security policies, do the stakeholder groups nee...-IT Staff
Q1_2	SECURITY POLICY: / / / / / / How aware of information security policies, do the stakeholder groups nee...-Senior Management
Q1_3	SECURITY POLICY: / / / / / / How aware of information security policies, do the stakeholder groups nee...-End Users

3.6.3 Pilot testing the survey questionnaire

The purpose of conducting the pilot test was to fine-tune the survey questionnaire with feedback from experienced information security professionals, as these were the targeted respondents for the survey. It also provided an opportunity to ensure that there were no grammatical errors, that the survey tool functioned correctly, and that data could be successfully retrieved from the survey tool. The participants in the pilot test indicated that there were no problems with the survey. Some minor amendments to the wording of the survey questionnaire were made to improve the understanding and readability of the survey questionnaire.

3.6.4 Final survey questionnaire steps prior to survey launch

The research and survey received ethical clearance from the University of Southern Queensland (USQ) Ethics Committee (H12REA163). Participants were informed this survey had ethical clearance from USQ and that the survey was anonymous. The researcher also outlined some of the benefits that participants may gain from participation in the survey and pointed out there was minimal risk to participants other than the time imposition in completing the survey.

3.7 Survey Administration

The use of an online survey tool was chosen as this enabled easy distribution of the survey via the Internet. This also allowed for distribution across all parts of Australia, as well as Internationally, and it allowed respondents to easily remain anonymous. The survey for this research was built using a tool called Qualtrics (Qualtrics Labs

Inc). Similar to many of the current online survey tools, this allowed for quick development of the survey; allowed for the use of various techniques to obtain a response (extensive use of slider bars to obtain ratings); it allowed for skip and piping logic to be used in the question so control over which questions would be presented could be based on a prior result; and it provided excellent tools for retrieving the survey results for analysis. The security over the survey data was also very good. The Qualtrics survey tool also provided for:

- version control of the survey being developed, tested and modified;
- sharing of the survey with the researcher's supervising lecturer; and
- ease of distribution by providing a unique URL link to the survey.

3.8 Data analysis procedures for phase 1 Survey

The approach to analysing the phase 1 awareness importance survey data was relatively straightforward. The awareness importance ratings provided by the respondents were the primary focus of the survey. Once the survey was closed, a number of validation checks on the data were conducted, included determining the levels of completion of the survey and which surveys would be included in the overall analysis. Some analysis of the incomplete surveys was also undertaken.

3.8.1 Descriptive data analysis

Table 3-6 below summarises the descriptive data analytics that would be applied to phase 1 survey, whilst the overall analysis is included in Chapter 5. The analysis falls into two main categories. The first category relates to assessing the quality of the survey data. Some analysis was done in relation to completion rates, where abandonment of the survey occurred (at which question), which stakeholder group the respondents associated with (phase 1 survey was not aimed at end users), and how experienced the respondents were in the field of information security, IT risk and IT audit.

The second category of analysis relates to the ratings provided for each of the 39 primary questions (and for each of the three stakeholder groups) and how those results would be used to determine the overall awareness importance rating. The detailed analysis is shown in Chapter 5.

Table 3-6 Analysis conducted on Phase 1 Survey data

Data Analytics used	Relevance for this research
Analysis of completion rates and profile of participants.	- which survey results were usable. - surveys that were abandoned, and at which point of the survey this occurred. - stakeholder group respondents associated with. - which respondents fully completed the survey. - level of experience of respondents. - country of location of respondents.
Scoring of Awareness Importance.	- the awareness importance rating is the primary measure for this survey - an average of the scoring, per question, per stakeholder group (for usable surveys) would provide an awareness importance rating for each of the 39 questions. - 39 questions directly linked to the ISO/IEC 27002 39 main security categories and their associated control objectives.

3.8.2 Relevance for research phase 2 survey

The results from the phase 1 survey were used to identify the top 10 (of 39) information security awareness importance questions for the end user stakeholder group that would be evaluated in phase 2. In order to demonstrate the suitability of the ISACM model, the top 10 awareness importance ratings for end users were used to measure awareness capability against controls of the ISO/IEC 27002 standard. The ratings derived in phase 1 survey identified which of the main security categories and their associated control objectives required demonstration of the highest levels of awareness by end users. These results form part of phase 2 of this research and are discussed in the following Chapter 4.

3.9 Conclusion

This chapter has described the overall philosophical beliefs of the researcher and the methodological approach used to design the Information Security Awareness Capability Model (ISACM). An overview was provided of the overall two-phased approach, and this chapter focused on phase 1 of this research. This chapter covered the development of the survey instrument used to capture the first element of the ISACM, that of the awareness importance rating, in the first phase of this research. This phase 1 survey was used to collect data to determine the awareness importance of each of the 39 main security categories and their associated control objectives of information security as outlined in the international standard ISO/IEC 27002.

The approach used for developing this awareness importance measure was described in significant detail, which will allow for future improvements to be made to the approach used for measuring awareness importance. The survey instrument was used to obtain awareness importance ratings from industry professional groups who were targeted because they were likely to have expertise and be knowledgeable about the management of information security in organisations. Special attention was given to demonstrate the linkages to the international security standard ISO/IEC 27002.

The statistical data analysis techniques used to analyse the data collected in the phase 1 awareness importance survey were described and justified. The results of the data analysis of data collected in the phase 1 awareness importance online survey are reported in Chapter 5. Some of the results of the data analysis of the phase 1 awareness importance survey were used to determine the areas of focus for the phase 2 awareness capability instrument. The next chapter describes and justifies the methodological approach used in the second phase of this research, the development and evaluation of the second and third elements of the ISACM, that of awareness capability and awareness risk.

4.0 Methodology II

4.1 Introduction

The purpose of this chapter is to describe the research design for phase 2 of this study: the development and evaluation of the awareness capability instrument and awareness risk measurement. This chapter describes the data preparation techniques used, and the computer programs adopted to analyse the survey data collected in phases 1 and 2 of this study. The limitations of the methodological approach used in this study are acknowledged. Finally, given this research involves humans and the primary data collected in this study were collected from online surveys, it is important to describe how the ethical considerations of this study were addressed. Figure 4-1 below outlines the structure of this chapter.

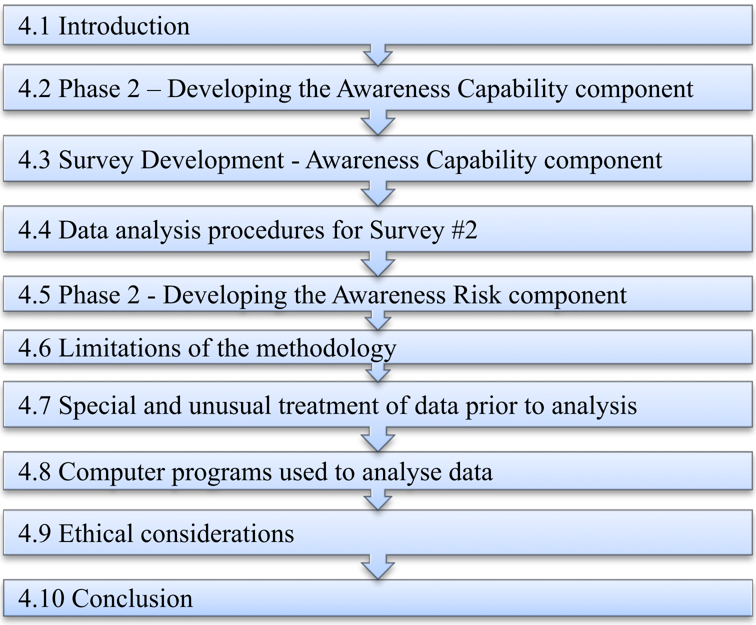

4.1 Introduction
4.2 Phase 2 – Developing the Awareness Capability component
4.3 Survey Development - Awareness Capability component
4.4 Data analysis procedures for Survey #2
4.5 Phase 2 - Developing the Awareness Risk component
4.6 Limitations of the methodology
4.7 Special and unusual treatment of data prior to analysis
4.8 Computer programs used to analyse data
4.9 Ethical considerations
4.10 Conclusion

Figure 4-1 Structure of Chapter 4

The research design and procedures for phase 2 are now described in this chapter, including the development of the instrument used to collect phase 2 data for the second component of the ISACM, awareness capability. Phase 2 also includes building the third component of the ISACM, awareness risk. This chapter describes limitations of the methodology used for phase 1 and 2, as well as how data was prepared prior to analysis. A brief discussion on the techniques used to analyse the data (Chapter 5 describes the analysis in detail) also includes details of what computer programs were used to analyse the data. This chapter concludes with details of the ethical considerations of this research, as well as a brief conclusion.

4.2 Phase 2 – Developing the Awareness Capability component

In the previous chapter, the overall methodology used for this research was described. The model for the ISACM contains three key measurements. The first of these, awareness importance was described in detail in Chapter 3. This chapter now describes the next two key measurements (awareness capability and awareness risk), commencing with a description of how the awareness capability instrument was developed.

4.3 Survey Development – Awareness Capability component

The survey questionnaire chosen was developed in a number of stages, which are described in detail below.

- Analysing existing measures relevant to the research, adopted and/or adapted from relevant literature;
- The survey questionnaire was designed;
- Pre-testing to verify the appropriateness of each survey question; and
- Survey questionnaire given a final proof prior to link distribution.

4.3.1 Existing measures relevant to the research constructs

Chapter 2 highlighted the linkages between situation awareness and this research's awareness capability measure. This linkage was also highlighted earlier in Chapter 2 in section 2.5.2. Many of the early measures for SA were derived from situation awareness of pilots and involved observing the level of situational awareness they displayed, often through the use of a simulation of an actual event (French & Hutchinson 2002; Salmon et al. 2008). These observers were generally skilled flying experts who could adjust the simulation based on their observations of what actions the pilots were taking. The observers were able to directly assess the level of SA being displayed based on these observed actions taken by the pilots.

In principle, the use of direct observation - that is, observing computer end users - could be adopted for this research on information security awareness. However, this would be difficult to develop and assess for large numbers of end users. For example scenarios could be presented to a group of end users and the actions taken could be observed. However, unlike pilots who were presented with a specific exercise (such as flying from point A to point B, avoid being shot down, etc.), in trying to capture a broad range of small activities for computer end users (such as setting up a password, preparing a file to be used at a remote location, disposing of obsolete computer equipment), the tasks are too varied to economically present in a direct observation scenario situation.

Whilst numerous mechanisms for measuring situation awareness are available, one that was applicable for this research (and was briefly described earlier) is where Breton and Rousseau (2003, p. 46) relate an adaptation of the Situation Awareness Linked Indicators Adapted to Novel Tasks (SALIANT) which was originally designed in 1998 (Muñiz et al. 1998).

Fink and Major (2000) adapted the model and concluded 'their Saliant version is the most promising measurement compared with the two other measures included in their analysis'. SA content is inferred from these behaviours, which are claimed to be indicative of good SA. The behaviours are general enough to be used in natural or technological environments'. Situation awareness and Saliant appeared to be suitable to be applied to information security awareness. Initially, this research investigated deriving awareness capability from the overall ratings that could be obtained from an adapted Saliant instrument for each of the key stakeholder groups.

In general terms, this research investigated whether the *Saliant Rating Items* could form categories of awareness capability. For example, 'Recognised a need for action' and ‘Knowledge of consequences’ are two of the rating items that exist in Saliant. When confronted with an information security event, these two aspects are important measures in determining how capable someone is in terms of their level and capability of awareness. It appeared that Saliant would be relevant for information security awareness and that an adaptation of the existing rating items could possibly be suitable as a measure for awareness capability for information security awareness.

However, the complexity of constructing questions that could specifically test for those categories would be a significant exercise, and one that would be difficult to present via a survey-like tool. Direct observation could be a suitable mechanism, but the ability to observe a large enough group across a wide range of information security related activities would also be difficult to achieve. Nonetheless, the use of technology to perform these observations does present a valid future option. This, however, is outside of the scope of this current research. Although this research did not proceed with the adapted Saliant model, it did influence the approach used for measuring awareness capability in this research. The approach adopted is described below in section 4.3.2.3.

4.3.2 Survey Questionnaire design

The questionnaire design was informed by established guidelines regarding layout and structure (Dillman 2000; Lefever, Dal & Matthíasdóttir 2007; Van Selm & Jankowski 2006). The layout, presentation and format of the survey questionnaire for this research were designed by incorporating the following aspects:

- Individual questions and statements that would be easy to understand;
- Adequate information was provided to the respondents in order to allow them to complete the survey; and
- Questions and answers were grouped in a logical sequence to aid in the completion of the survey.

4.3.2.1 Survey questionnaire layout

Cover page. In the opening frame of the survey, details were provided of the purpose of the survey and how the questions were presented as typical scenarios. Whilst highlighting that some respondents may not have been exposed to these scenarios in their working career, they were asked to select the best course of action based on the scenario presented to them for each question.

Demographic information. Obtaining some key demographic data was the first task the survey needed to achieve. This included obtaining the highest level of education achieved, age group of the respondent, whether they do work, or have ever worked in an IT role, and which industry sector they work in. Ideally for this survey, the views of pure end users (rather than those with significant IT skills) would be of greater value. Chapter 5 includes a full analysis of the results.

The body of the questionnaire. Following on from the demographic questions, the questionnaire was designed to include 10 primary questions – each with three parts, which measured information security awareness capability in terms of the three levels of situation awareness (L1 perception, L2 comprehension, L3 projection) - for each of the top 10 security control objectives for end users. In order to establish if an appropriate level of situation awareness exists for an information security control objective it was important to determine if adequate perception, comprehension and projection existed. Comprehension typically depends on adequate perception of an information security event or control, and projection is typically dependent on adequate comprehension of an information security event or control.

The back cover. The back cover was kept simple and it invited respondents to make additional comments about the questionnaire.

4.3.2.2 Considerations to increase response rate of the survey

Similar to what was described earlier in Chapter 3 with regards to phase 1 survey, De Vaus (2002) suggests that to maximise response rates in Internet surveys one should 'get the survey to the selected population in a way that makes people want to respond'. In the case of phase 2 survey, it targeted end users who were employed in organisations where they were exposed to using computers in their job role.

Two populations were used for this survey. The first was the baseline population constructed by a third party organisation (MyOpinions) so that potential survey respondent meet the requirements for a baseline population. MyOpinions were also able to guarantee a minimum number of responses. The required number of 220-plus responses were therefore obtained. The members of the survey panel constructed by MyOpinions for the first phase 2 awareness capability online survey were presented with a link to the survey via mechanisms used by MyOpinions. These mechanisms allowed MyOpinions to monitor the quota of surveys completed, and check for skimming or flat lining (both inappropriate ways of filling in the survey). They were also able to provide the survey to more respondents in order to meet the guaranteed responses in a way that is representative of the distribution of the Australian population.

The second population was a specific population of staff at an Australian university. To distribute the survey to the Australian university staff members, approval and support of the Deputy Vice-Chancellor at that university was obtained. The staff members of the university were presented with a link to the survey by way of an email invitation to participate in this study's survey. To be able to achieve reasonable response rates, De Vaus (2002) suggests that a follow up of non-responders be carried out. Because the survey was anonymous it was not possible to just target the non-responders. Because the two separate populations provided a suitable number of respondents for phase 2 of this study, no further follow-ups were carried out.

De Vaus (2002) advises that to ensure quality in Internet surveys one should 'know the characteristics of the population the sample is meant to represent'. By using a survey panel of participants constructed by MyOpinions, the required criteria to be met could be specified. People 18 years or older, employed and using information technology and networks in their workplace were targeted, thereby meeting this research's end user target group. Similarly, staff at the Australian university also met the end user requirements. Other advice from De Vaus (2002) suggests response rates will be improved if respondents are 'confident that their responses are anonymous and secure'. This is particularly important when surveying about a potentially sensitive subjective such as information security awareness. In the survey it was emphasised to the respondents that the survey was anonymous and no personally-identifiable information was asked for. Additionally, De Vaus suggests the 'use of a specially designed internet survey package'. The use of these packages simplifies the process of building the questionnaire, distributing it, and retrieving the response data. The Qualtrics tool used for the two phases of surveys in this research provided this capability.

4.3.2.3 Survey Questionnaire content

Situation awareness and the Saliant measurement tool influenced how this research developed and evaluated an instrument for measuring awareness capability. The awareness capability instrument was developed for the top ten rated ISO/IEC 27002 information security control objectives in terms of awareness importance (as identified in phase 1 and described in Chapter 3) for end users. This top ten were chosen in order to develop an awareness capability instrument that was targeted at a specific key stakeholder group and would not be overly onerous in terms of length and complexity. This allowed the researcher to fully test and evaluate the ISACM for one specific stakeholder group within the scope and time constraints of a PhD research.

Beginning with the top ten measures of awareness importance for end users from phase 1 survey (shown below in Table 4-1), three sub-questions were developed to test for capability of the control objectives. Each of the three parts of these questions was aimed at a higher level of awareness, reflecting the Level 1, Level 2 and Level 3 approach that is used within situation awareness.

Table 4-1 Top 10 end user Awareness Importance questions from phase 1 survey

1	How aware of user responsibilities for maintaining effective access controls, do the stakeholder groups need to be, to prevent unauthorised user access, and compromise or theft of information and information processing facilities?
2	How aware of the need for timely reporting of information security events and weaknesses, do the stakeholder groups need to be, to allow timely corrective action to be taken?
3	How aware of the risks associated with mobile computing and teleworking in an unprotected environment, do the stakeholder groups need to be?
4	How aware of policies and procedures for exchanging information, do the stakeholder groups need to be, to preserve the security of any information or software exchanged within an organisation or with any external entity?
5	How aware of the techniques required to protect removable media, do the stakeholder groups need to be, in order to minimise unauthorised disclosure, modification, removal or destruction of assets?
6	How aware of the need to classify information, do the stakeholder groups need to be, so that information receives an appropriate level of protection?
7	How aware of business requirement and policies for information dissemination and authorisation, do the stakeholder groups need to be, in order to control access to information?
8	How aware of compliance with legal requirements, do the stakeholder groups need to be, in order to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any related security requirements?
9	How aware of the need for ownership and accountability for assets, do the stakeholder groups need to be, in order to maintain appropriate protection of organisational assets?
10	How aware of physical and environmental threats, do the stakeholder groups need to be, to prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities?

Additionally, the answer choices presented within the survey questions developed had similar characteristics to the generic SA behaviour indications shown earlier. The extensive review of the relevant literature conducted in Chapter 2 provided background into what types of issues were important for each particular question. The literature provided insight into the types of behaviours and/or actions that should be displayed or enacted in order to demonstrate sufficient awareness. This allowed for a way of posing questions that could be used to test each progressive level of awareness capability.

This second survey asked participants to indicate what they should do after seeing all of the options presented to them. It tests their level of information security awareness at three progressive levels (perception, comprehension, projection). As mentioned earlier, SA is best measured through expert observation, however, that is difficult to replicate for the wide range of information security actions that this research would like to test. When using a survey instrument to conduct the measurement, and asking participant to choose from a set of selections (rather than asking them to describe their actions), many may identify the correct response. This, however, does not mean that is what they would do in a particular situation.

Similar to other surveys, when presented with a number of choices people may know what they would actually do in a particular situation, but they may also be able to identify what they perceive to be the 'correct answer'. For example, when asking how many drinks someone should have per night, presenting the correct answer amongst incorrect answers could lead the participant to select the correct answer. They may know what is right, but may not necessarily demonstrate that choice in real life. In such a situation, demonstrated awareness capability is lower than their knowledge. The questions in phase 2 survey ask what actions respondents would take, or have previously taken. There is no guarantee that they will answer with what they would actually do in a particular situation. The alternative would be to directly observe (maybe using monitoring technology or matching know actions taken) what choice is taken. Again, the participants' actions may be biased given they would know they are participating in a survey. Furthermore, by presenting the 'I don't know' answer option for each of the questions, this provided a mechanism for measuring self-identified lack of awareness capability.

Whilst developing the information security awareness capability instrument questions, comparisons of this research's question categories could be made with what others had focused on in terms of security awareness. A 2009 study on the *Impact of Security Awareness Training Components on Perceived Security Effectiveness* (Quagliata 2011, p. 4) reported (133 ISACA members participated in the survey) the following topics shown in Table 4-2 as the most widely-used within organisations. Many of these topics have also been included in the information security awareness capability questions developed for this current research.

Table 4-2 Security Awareness Training Topics

Security Awareness Training Topics	Count
E-mail	86
Passwords	83
Internet use	80
Locking workstations	74

Security Awareness Training Topics	Count
Privacy	72
Data handling/classification	68
Social engineering	66
All of the topics listed	53
Network security	47
Data encryption	35
No user awareness security training is conducted.	8
I do not know.	2

As described above, the development of the questions and 'answers to select from' for this second survey leveraged the extensive literature that was reviewed for Chapter 2. The full list of the information security awareness capability questions/answers developed for end users has been included in Appendix B. Below a detailed description is provided of how the questions were formulated, including references to the supporting literature used in the construction of these questions/answers. The format for each of the questions shown below begins by presenting (in a bordered box) the following reference information:

- The question number from phase 2 survey;
- The related section from the ISO/IEC 27002 standard (such as *User Responsibilities*); and
- The aspects covered within that section of the ISO/IEC 27002 standard (such as *Password use*, *Unattended user equipment*, etc.), using the standard's numbering convention for ease of referencing.

Each question is then presented with supporting literature that has provided additional context for the construction of the questions. Finally, the three sub-questions being posed are presented. The survey therefore presents a total of 30 questions. These questions are presented below without the answers that were provided to respondents (the full survey questions and answer choices are contained within Appendix B). There is also linkage shown for each of the 30 questions to the most appropriate situation awareness level. This follows a similar approach to how responses have been presented in SA Saliant measurement tools described earlier.

Question 1 – User Responsibilities
The ISO standard incorporates the three following aspects:
11.3.1 Password use
11.3.2 Unattended user equipment
11.3.3 Clear desk and clear screen policy

Much has been written about poor user behaviour. For this question, the focus is on the main aspects listed above, which have been extracted from the ISO/IEC 27002 standard. In their article on security culture, ISACA (2011) describe password sharing, disclosing sensitive information and bypassing access control as 'impermissible' and suggest these actions should be permanently recorded on employees' personal files. Furthermore, Herath and Rao (2009) in their article on security behaviours in organisations describe behaviours such as sharing passwords as being something that cannot be monitored. Awareness may be the only option.

Shaw et al. (2009, p. 93) believe a 'robust awareness program is paramount to ensuring people understand their IT security responsibilities' and 'layers of technological defence can be as strong as possible' but these can be undermined by activities such as disclosing passwords (e.g. by writing them down for others to discover) or leaving an unlocked PC. End users undertaking these activities display low security awareness and 'are one of the weakest security loopholes'.

Finally, in terms of clear desk, most acknowledge that confidential information in written form is vulnerable if left lying around unsecured. But translating that procedure so that it is embedded in the organisation culture where people follow a clear desk policy may be more difficult. Connelly (2011, p. 214) suggests that people avoid 'identity-threatening events' and tasks such as cleaning a desk may be seen as 'outside the range of one's profession'. When describing the interaction between information security, behaviour and culture, Da Veiga and Eloff (2010, p. 199) suggest a clear desk policy is seen as 'conducive to the protection of information assets'. The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
1.1	A work colleague has asked you for your computer access password because they are having troubles getting their computer access set up. What would you do?	**1 -** Perception that sharing access is wrong.
1.2	Do you use the same password for multiple systems, say for your personal email account and your work accounts?	**2 -** Comprehension that if one of your personal accounts is cracked, your work account may be at risk.
1.3	Is a passphrase better to use than just a set of characters and numbers in your password?	**3 -** Projection that being able to remember a phrase as a password makes it extremely difficult to be guessed or randomly cracked.

Question 2 Reporting information security events and weaknesses
The ISO standard incorporates the two following aspects:
13.1.1 Reporting information security events
13.1.2 Reporting security weaknesses

Security events may be observed, suffered, or caused directly by a person. When describing techniques for effective knowledge transfer practices to improve IS security awareness, Sannicolas-Rocca et al (2014, p. 3432) reported 40% of higher education institutes that reported data breaches were due to 'end user activity, including the unintended disclosure of and/or an insider explicit intent to share'.

What is concerning is that, according to the key findings from the *Global State of Information Security Survey 2013* (PricewaterhouseCoopers 2012, p. 7), the number of security incidents is on the rise and 'most organisations lack an incident-response process to report and handle breaches at third parties'. Data loss arguably represents a growing concern for organisations. Detection and reporting of security weaknesses (vulnerabilities) often has a technology focus. In their presentation on the impact of training and awareness on *Improving Organisational Information Security Management*, Waly et al (2012, p. 1270) found that 'studies which concentrate on finding technological solutions to prevent vulnerabilities and attacks tend to overlook human and organisational aspects'. Similarly, in their focus of aligning security awareness with system security management, and their discussion of the 'check' phase of security management, Tsohou et al (2010, p. 873) suggest that 'errors can happen if users do not report in time security incidents or vulnerabilities. Awareness is quite important in eliciting the sense of the importance of incident reporting to the users'. The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
2.1	Would you be able to recognise a potential computer incident (i.e. virus, spam, infected web site) and do you know what to do?	**1 -** Perception that something is wrong and the incident may need to be reported.
2.2	Assume that you or a colleague has taken some work related data home on an unencrypted USB device. It has some customer related data on it. However you can't find the USB device. What would you do or suggest to your colleague?	**2 -** Comprehension that data needs to be protected on portable devices by encryption.
2.3	Do you know what social engineering is and can it lead to security incidents?	**3 -** Projection that if you provide personal details to untrusted sources, then these could be used to launch a social engineering attack on you.

Question 3 –Mobile computing and teleworking
The ISO standard incorporates the two following aspects:
11.7.1 Mobile computing and communication
11.7.2 Teleworking

Mobile devices have evolved since the ISO/IEC 27002 standards were first published. NIST (National Institute of Standards and Technology [NIST], Souppaya & Scarfone 2013) suggest a baseline of functionality for these devices now include a small form factor, a wireless network interface (for Wi-Fi or cellular), built in (non-removable) storage, an operating system, and applications available through multiple methods. Each of these aspects presents potential information security risks. Flexible working arrangements and greater availability of high-capacity broadband in people's homes and non-workplaces means 'protecting data and information used by teleworkers from non-office-based locations is a situation faced by many businesses' (Godlove 2012, p. 216). Often, flexible working arrangements are achieved using a mobile device such as a smart phone or tablet laptop, or a traditional PC or laptop.

The use of bring your own device (BYOD) has emerged in recent years. This approach to computing (teleworking or mobile computing), when working for an organisation, presents additional risks that may not be present, or are different, to the normal risks of physically using technology within an organisation. In their 2013 *Global state of information security survey*, PricewaterhouseCoopers (2012, p. 21) found 'as mobile devices, social media, and the cloud become commonplace both inside the enterprise and out, technology adoption is moving faster than security'.

The differing threats (National Institute of Standards and Technology [NIST], Souppaya & Scarfone 2013) such as reduced physical security controls, untrusted networks, untrusted applications, interaction with other systems, untrusted content, and use of location services require different levels of awareness from end users. The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
3.1	Is it OK to connect your work computer to a public Internet service such as those offered by Starbucks or public Libraries?	**1 -** Perception that there are some risks associated with connecting to free or public Wi-Fi.
3.2	Why is it important to have an encrypted hard drive on any computer used away from the office?	**2 -** Comprehension that data needs to be protected on portable devices by encryption.
3.3	How does a VPN connection provide you with security when connecting with your work or other companies?	**3 -** Projection that if you connect over an unsecure connection, that traffic may be sniffed and stolen or compromised.

Question 4 – Exchange of information

The ISO standard incorporates the five following aspects:
10.8.1 Information exchange policies and procedures
10.8.2 Exchange Agreements
10.8.3 Physical media in transit
10.8.4 Electronic messaging
10.8.5 Business information systems

In their article focused on *Information Privacy Situation Awareness*, Sim et al. (2012, p. 61) found that 'even when managers realize that human errors constitute the biggest threat to protection of their customers private information, they rarely seek practical ways to prevent or mitigate such errors'. Awareness must therefore play a key role. User involvement in information security risk management, particularly when the exchange of information is involved, is crucial. A 2010 study on the effect of user participation (Spears & Barki, p. 520) suggested that rather than end users being a weak link, 'business users were found to add value to IS security risk management when they participated in the prioritization, analysis, design, implementation, testing, and monitoring of user-related security controls within business processes'. It also found that it 'raised organisational awareness'.

For example, Spears and Barki's study (2010, p. 514) reported that at 'one manufacturing firm, a security council of senior business and IS managers had formed during the previous two months to classify information and to develop global policies on protecting intellectual property'. Clearly understanding why a policy statement exists (or influencing the writing of that policy) related to information classification and information exchange could result in 'better alignment of security measures with business objectives'. The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
4.1	You are working on analysing some customer data that you have access to in order to determine	**1 -** Perception that customer data should be properly

	customer profitability. Is it OK to share this information with other people within your organisation?	protected and not readily shared.
4.2	Your organisation uses an external company to do its letter mail out (physical and email) to customers. Is this secure?	**2 -** Comprehension that an organisation can be securely using external organisations, providing suitable agreements and due diligence are in place.
4.3	When exchanging electronic information with another organisation, you should ensure that …	**3 -** Projection that unless certain things are put in place, the exchanged data may be at risk.

Question 5 – Media handling
The ISO standard incorporates the four following aspects:
10.7.1 Management of removable media
10.7.2 Disposal of media
10.7.3 Information handling procedures
10.7.4 Security of system documentation

ENISA Threat Landscape - Responding to the Evolving Threat Environment (European Network and Information Security Agency (ENISA), Marinos & Sfakianakis 2012, p. 47), referred to the *Trojan.AutorunINF* as 'one of the world's top three e-threats for about four years'. It can spread via removable media. Management of removable media involves more than just losing confidential information, and 'removable media such as USBs have become a very common means for insiders to sneak data out of organisations' (Sarkar 2010, p. 120). The *2012 Cyber Crime & Security Survey Report* (Australian Government, p. 12) found 'less than 50% of respondents have plans in place for the management of removable computer media, such as USB memory drives, and less than 25% have policies and procedures in place for using cryptographic controls'.

Lack of technological controls puts the onus on end users. Disposal of media that contains information incorporates numerous aspects (National Institute of Standards and Technology [NIST], Souppaya & Scarfone 2013) including preserving information to meet legal requirements, sanitising the media (e.g. scrubbing the data using techniques to make the information irretrievable), or physically destroying or demagnetizing the media. Protection of information and, therefore, handling procedures that need to be applied are intertwined with notions of data classification.

In the *Computer Fraud & Security* journal, Everett (2011b, p. 5) suggests that 'although data classification is considered by many professionals to be the foundation of any information security activity, few organisations outside of defence and the security services have done much about it'. This article also put forward the view that 'more than half of the data in most organisations does not need to be classified at all, as it falls into the default "public" category'. But unless end users are in tune with how to classify data at the creation or modification phase, and then how to handle data of certain classifications, mishandling is likely to occur. The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
5.1	What is the best way to dispose of unwanted data contained on media such as a dvd, usb stick, and magnetic tape?	**1 -** Perception that devices containing data need to be disposed of in a secure manner.
5.2	You are required to work on a sales presentation spreadsheet over the weekend. Because of the sensitive nature of the information you know not to send it home via email. Instead you load it onto a USB memory stick. Is that safe?	**2 -** Comprehension that sensitive data on memory sticks needs to be encrypted to protect the data.
5.3	You are responsible for the disposal of photocopying machines. Are there any security related things that you need to do before you dispose of them?	**3 -** Projection that devices such as photocopiers contain recording devices (hard disks) that upon disposal need to be correctly wiped to protect sensitive data that is stored on them.

Question 6 – Information classification
The ISO standard incorporates the two following aspects:
7.2.1 Classification guidelines
7.2.2 Information labelling and handling

Puhakainen and Siponen (2010, p. 769) posed a number of questions around information classification and found some users had a 'lack of skills to apply the information classification rule'. Some were unable to determine what level of protection (i.e. encryption) was required. Others suffered a 'lack of skill to use e-mail encryption software'. Although some users may have correctly determined the information classification, they were not able to apply the necessary technical controls.

Tsohou, Aggeliki et al. (2008, p. 222) suggest that 'security policies that do not include an information classification scheme are regarded as an obstacle to security awareness, since there is no criterion for the appropriate treatment and protection of information'. In applying data classification methodologies to utility data, Rajagopal et al. (2014) provided the following features as the purpose for data classification:

- to establish protection profiles and assign control settings for each category of data for which an organization is responsible; and
- after classifying data, baseline security controls are identified for all the information types handled by the organization. The security control for an IT system will be an aggregate of security controls defined for information types handled by the IT system'.

The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
6.1	Is it important for your organisation to have data/information classification rules and if so why?	**1 -** Perception that classifying data will assist with protection.
6.2	How does information classification influence access controls?	**2 -** Comprehension that access controls are influenced by the classification type applied to

		the information.
6.3	What are the key risks for your organisation if it has **correctly** classified information?	**3 -** Projection of risks that still exist even if information is correctly classified.

Question 7 – Business requirements for access control
The ISO standard incorporates the following aspect:
11.1.1 Access control policy

Access control is an acknowledged area where user (business) participation is required. In their article *User participation in information system security*, Spears and Barki (2010, p. 509) suggest access control to data is one of the security controls where most user participation is required. Their research found that 'users participated in SRM (security risk management) by performing an access control review and reaching consensus with IS professionals on user-defined access control rules'. Spears and Barki (2010, p. 515) also found that:

> *'Control development was assessed via three 7-point scales as perceived improvements that had occurred in the definition or implementation of access control, segregation of duties, and security policy. These three controls were most commonly associated with user participation in IS security within business processes. Security policy contains rules of acceptable and unacceptable behaviour, serving as organizational law and was associated with senior business management's participation in defining organizational policies, such as risk tolerance and data classification'.*

Separation of Duties (SoD) is commonly referred to when looking at access control (Habib et al. 2014; Yu & Brewster 2012). It is the approach for ensuring that the level of access for performing conflicting job roles (i.e. purchasing and receivables of goods or services) is not vested in the one individual. Relating to benefits of a culture of security, ISACA (2011, p. 39) suggest that security without culture 'cannot be sustained over time. All of the other organizational dynamics will distort security to the point that it is unrecognizable'. They further warn that 'competitive pressures will dissipate access controls and separation of duties'.

The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
7.1	Who should determine the level of access to data within your organisation?	**1 -** Perception of who owns the data and should therefore determine levels of access.
7.2	What is the greatest risk to your organisation if access is not based on business requirements?	**2 -** Comprehension that just applying access controls without linkage to business requirements leads to certain risks.
7.3	What do you understand about the term "separation of duties" and it's importance to your organisation?	**3 -** Projection of what could an individual do if they have been given conflicting levels of access.

Question 8 – Compliance with legal requirements
The ISO standard incorporates the six following aspects:
15.1.1 Identification of applicable legislation
15.1.2 Intellectual property rights (IPR)
15.1.3 Protection of organisational records
15.1.4 Data protection and privacy of personal information
15.1.5 Prevention of misuse of information processing facilities
15.1.6 Regulation of cryptographic controls

Compliance with organisational policies is a common way to influence employees to comply with external legal requirements. For example, organisations include within their policies the requirement for staff to comply with harassment and discrimination behaviours that would typically cover legal aspects. However, staff are often advised or required 'not to engage in illegal activities or behaviours' as a catchall condition of employment. By being sufficiently prescriptive in formulating organisational policies, there is a greater likelihood of at least capturing key legal requirements within these policies.

Policy setters within an organisation need awareness of compliance with legal requirements so these requirements can be captured and articulated in the organisation's policies. The ISO/IEC 27002 standard refers to aspects of compliance with legal requirements that have an information security related impact. It is reasonable to expect these requirements to be captured in organisational information security policies (ISPO). In their conference presentation, Lowry and Moody (2013, p. 2998) presented findings on how employees react to new ISPO delivered to staff via memos. They found that 'in practice, actual ISPO compliance is also highly mixed: many employees are apathetic about ISPOs and ignore them; other times employees try to circumvent ISPOs intentionally; and, even worse, some employees will often purposely do the opposite of the desired behaviour'.

When specifically looking at data privacy, and by incorporating a situation awareness perspective, Sim, Liginlal and Khansa (2012, p. 61) suggest 'organizations have found it challenging to recognize and manage human error in the context of privacy. Even when managers realize that human errors constitute the biggest threat to protection of their customers' private information, they rarely seek practical ways to prevent or mitigate such errors'.

The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
8.1	Who within your organisation should be responsible for understanding how to comply with legal requirements?	**1 -** Perception that complying with legal requirements does not just belong with the legal people in an organisation.
8.2	What do you know about data privacy?	**2 -** Comprehension of privacy requirements, including the principles that they contain.
8.3	Why are there laws regarding the use of encryption software?	**3 -** Projection of what encryption laws are trying to protect against.

Question 9 – Responsibility for assets
The ISO standard incorporates the three following aspects:
7.1.1 Inventory of assets
7.1.2 Ownership of assets
7.1.3 Acceptable use of assets

Responsibility for IT Asset Management (ITAM) can be a difficult thing to assign. Purchasers of assets often have a different role from those that will use those assets. Galusha (2001, p. 40) suggest that 'to benefit from an ITAM initiative, all the affected areas must learn to share data—a task sometimes harder than everyone would care to admit'. The management of an inventory of IT assets can be assigned in many ways. What is important is that an organisation agrees upon the division of responsibilities for this. It is likely that the IT department would have the responsibility for maintaining within the asset register the technical aspects of an IT asset. For example, this could include details of the version of operating system, the configuration of the hardware, etc. When IT departments/staff undertake changes to those IT assets it would be expected that they would be responsible for updating the relevant information in the asset register.

Other information associated with these assets, such as who are the users, where is the asset physically located, or who is the ultimate owner (say in the case of a business application) will require maintenance by people outside the IT department. In the case of assets such as laptops, these may often be distributed and redistributed within a business unit without the knowledge of IT staff. And, finally, the acceptable use of these assets needs to be clearly outlined (Laughton 2008). The owners of these assets, whether it is the IT department or a business unit, need to outline the terms under which these assets should and should not be used.

The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
9.1	Who should be responsible for owning technology related assets?	**1 -** Perception that technology asset ownership is not solely an IT thing, but shared with the business.
9.2	Who should be responsible for maintaining and updating an asset register of technology assets?	**2 -** Comprehension of what roles IT departments and the business undertake.
9.3	Who should be setting the policy of acceptable use for a computing asset?	**3 -** Projection of the need for an acceptable use policy and who should own this policy.

Question 10 – Equipment security
The ISO standard incorporates the seven following aspects:
9.2.1 Equipment siting and protection
9.2.2 Supporting utilities
9.2.3 Cabling security
9.2.4 Equipment maintenance
9.2.5 Security of equipment off-premises
9.2.6 Secure disposal or re-use of equipment
9.2.7 Removal of property

Protection for computer equipment takes on many forms. One related issue reported in a government department audit report (Western Australian Auditor General 2010, p. 31) warned that 'infrastructure and systems will fail in the event of a power disruption and information may be permanently lost'. The WA Auditor General found that 'several agencies had not tested their "uninterrupted power supplies" (UPS). Without regular testing and maintenance of the UPS, agencies cannot be confident that equipment will work in the event of a power disruption'. There is a substantial amount of literature available to guide organisations with recovery and testing procedures (Costello 2012; Sahebjamnia, Torabi & Mansouri 2015).

Disposal of computer equipment continues to be a growing problem. Photocopiers with hard disks containing confidential health records highlighted the problem of data storage in non-traditional computer equipment. Any device with storage capability (smart phone, cameras, video recorders, etc.) needs to have its recorded data suitably cleaned when being disposed of. The US Department of Defense (US Government 2009, p. 4) were recently issued with an audit report highlighting that 'DRMS processing centers processed excess unclassified IT equipment for disposal or redistribution without proof that equipment had been properly sanitized'. Awareness around this issue is becoming increasingly important.

Finally, the use of remote computing facilities calls for appropriate information security protection measures to be in place. Because this computing equipment may not reside in an organisation's primary data centre does not mean that it does not require a high level of protection. The following questions have been developed from the relevant literature.

#	Questions to be asked	SA Level to be tested
10.1	What controls provide the best protection for essential computer equipment against power disruptions?	**1 -** Perception that devices such as UPS and backup generators are important in guaranteeing continuity of power supply.
10.2	When disposing of computer equipment, what key information security step is required to be done?	**2 -** Comprehension of the need to securely wipe data when disposing of computer and data storage equipment.
10.3	From an information security perspective, what is the most important reason to protect remotely located computer equipment?	**3 -** Projection of what risks can occur if remotely located computer equipment is compromised.

4.3.2.4 Scale used for awareness capability questions

In order to derive an overall score for awareness capability for each of the 10 questions, scores were allocated to each of the selection of answers of their three sub-questions. By selecting the 'perfect answers' for each of these three parts, a total overall score of 7 could be achieved per overall question. The rating scale for awareness importance in phase 1 also used a scale of 7. This approach would then allow for the awareness importance and awareness capability to be directly compared, therefore arriving at an awareness risk score. An example of the scoring of questions is presented later in this chapter in section 4.4.

The survey questions were all multiple choice questions which consisted of five possible answers for each of the questions – making it more difficult for the survey participants to guess the correct answer. The respondents were asked to choose the most appropriate answer to the information security event/control scenario they were presented with for each question. Only one answer could be chosen, with the first part (sub-question) of each of the 10 main question targeting Level 1 SA (perception). The second part (sub-question) targeted Level 2 SA (comprehension). The final part (sub-question) targeted Level 3 SA (projection). The overall score is a summation of the answer scores for these three elements of SA. This then becomes the awareness capability score for that question, and for that particular respondent.

4.3.2.5 Coding questions in Qualtrics

Qualtrics (an online survey tool) was used to develop and administer the online survey. All questions were numbered within Qualtrics. The full phase 2 online survey details are available in Appendix B of this dissertation. The demographical questions (such as highest level of education, which industry sector respondents work in) were coded using roman numerals. For each of the 10 primary questions and their sub-questions, these were prefixed with Qx.y where x was the primary question number and y is the sub question number. Table 4-3 below shows an example of how the results were extracted from the Qualtrics tool.

Table 4-3 Extract of survey responses

Question number	Extracted Text labels from Qualtrics
iii_1	DEMOGRAPHIC / INFORMATION / / Â / / The following demographic information will assist us with / .-Level of digital literacy
iv	What is your highest level of education
v	Please select which Age group you belong to
vi	Have you ever worked in an IT role?
vii	Which industry sector do you work in
viii	Top 10 security controls for / End Users / Â / / The / following 10 sets of information security contro...
Q1.1	1) PASSWORDS / / Â / / / A work colleague has asked you for your computer access password / because th...
Q1.2	Do you use the same password for multiple systems, say for your / personal email account and your w...
Q1.3	Is a passphrase better to use than just a set of characters and / numbers in your password?Â Â Â

For example, for Question 1 and sub-question 2 (*Do you use the same password for multiple systems…*), the response would be collected under Q1.2. This allowed the Qualtrics tool to automatically code the responses. The Qualtrics tool provided an extraction facility that allowed this data to be downloaded into a SPSS file format for analysis in SPSS.

4.3.3 Pre-test to verify the appropriateness of each survey question

Once the development of the questions measuring awareness capability for end users had progressed sufficiently, it was distributed to a number of information security professionals, as well as a number of academics who were collectively knowledgeable about information security and survey design. This process was used to solicit comments to improve the face validity and content validity of the proposed survey questions and answers. Feedback that was received resulted in some changes to the wording of some questions, and a more standardised length being applied to the choice of possible answers that were provided.

4.3.4 Final survey questionnaire steps prior to survey launch

This research received ethical clearance from the University of Southern Queensland (USQ) Ethics Committee (H12REA163) before commencing data collection and conducting this survey. Participants were informed this survey had ethical clearance from USQ, that the survey was anonymous, and their participation in this survey was voluntary.

4.3.5 Survey population design – Awareness Capability component

In selecting a sample for this second phase of the research, a number of choices were made in terms of (1) target population; (2) population unit; (3) survey population frame; and (4) population size. Each of these is described below.

4.3.5.1 Target population

Unlike phase 1 survey which targeted IT security, IT risk and IT audit professionals, phase 2 survey was aimed at testing awareness capability for end users working in any organisation where they would be using computers as part of their working day.

4.3.5.2 Population unit

Two population units were identified. The first population unit for this research was people working in various industries and roles where they made use of information technology as part of their work. This spread of people from different industries and geographic locations would provide a broad range of opinions when surveyed. No requirement was placed on how experienced these people were in terms of their use of information technology, as this research sought to capture a realistic picture of information security awareness as it exists in organisations in general.

The second population unit for this research was staff working for an Australian university. This provided a user population from a specific industry sector that is a heavy user of computing and networks that would allow for comparisons with the first population unit. It could also provide an indicator at an organisational level of any areas that were significantly different than that shown in the first sample, which is a cross sectional population of people working in Australian organisations.

4.3.5.3 Survey Population frame

The first population for the phase 2 survey were end users using information technology within their work environment. They were surveyed via the use of a third party organisation (MyOpinions), which constructed a survey panel with the required end user characteristics and guaranteed a minimum number of responses. The criteria for the survey panel population provided by MyOpinions was that these people needed to be currently working for an organisation, over the age of 18, and they needed to be using information technology as part of their work. No requirements were placed on the size of organisation they worked for, or how many hours per week they worked. This approach provided this current research with a broad overview of end user information security awareness.

The second population for this phase 2 survey were staff members at an Australian university, who were end users using information technology as part of their work.

4.3.5.4 Population size

The population size for the first phase 2 survey was achieved through the use of a survey panel, which meant a guaranteed minimum of 220 responses was achieved. Because this was not targeted at one particular organisation, it also allowed the researcher to obtain a generalisable baseline of awareness capability measures that were not unnecessarily influenced by either a very proactive organisational information security culture, or by an organisation where an information security culture did not exist. The population size for the second phase 2 survey group was 900 staff at an Australian university.

4.3.6 Survey Administration

The use of an online survey tool was chosen to allow for easy survey distribution via the Internet, and it allowed the respondents to remain anonymous. This second survey was also built using the online survey tool Qualtrics. Like many of the online survey tools that are available today, this tool allowed for quick development of the survey, allowed for the use of various techniques aimed at eliciting a response, and it provided excellent tools for retrieving the survey results for analysis.

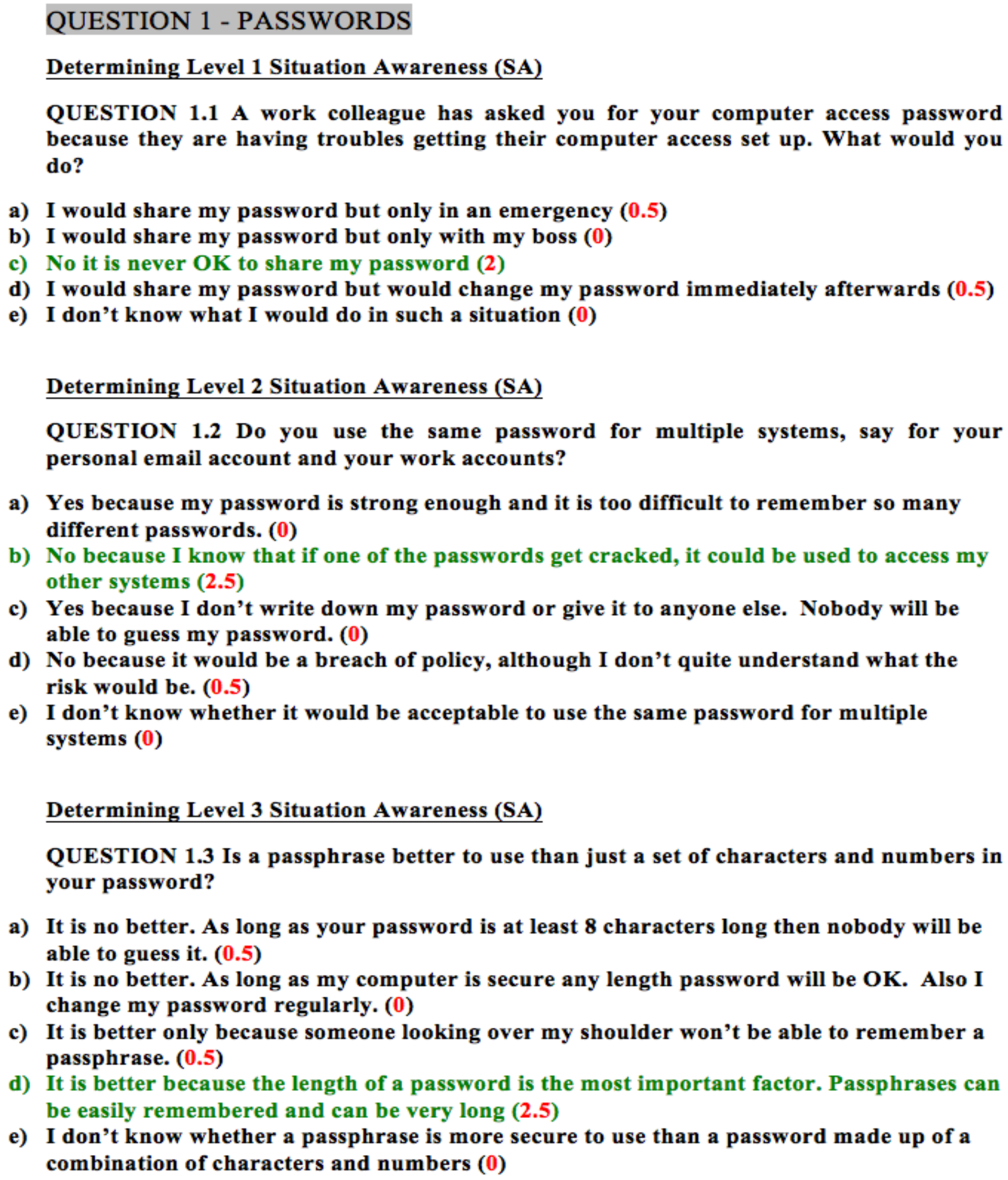
The security of the survey tool provided by Qualtrics, given it is an online survey was also very good. The Qualtrics survey tool:

- provided version control of the surveys being developed, tested and changed based on feedback;
- facilitated sharing of the survey with the researcher's supervisor; and
- facilitated ease of distribution by providing a unique URL link to the survey.

4.4 Data analysis procedures for phase 2 survey

The methodological perspective to the approach for analysing the data was relatively straightforward. Once the survey was closed, it was necessary to perform a number of checks on the survey responses data. These checks included determining the levels of completion of the survey; and which surveys would be included in the overall analysis. For those responses that were deemed suitable, an allocation of score values needed to be applied to the responses of each of the sub questions.

The scoring approach used is shown below in Figure 4-2 and demonstrates how the scoring has been assigned on a question/sub-question basis. In the example shown for phase 2 survey Question 1, there are five possible responses for each sub-question. The 'correct answer' is highlighted in green text, and the individual scores allocated are shown in red in brackets at the end of each of the sub-question answers. These scores reflect the approach described earlier where situation awareness theory informed this research on how to measure awareness capability. Every sub question within phase 2 survey contained five possible responses to choose from.



QUESTION 1 - PASSWORDS

Determining Level 1 Situation Awareness (SA)

QUESTION 1.1 A work colleague has asked you for your computer access password because they are having troubles getting their computer access set up. What would you do?

a) I would share my password but only in an emergency (0.5)
b) I would share my password but only with my boss (0)
c) No it is never OK to share my password (2)
d) I would share my password but would change my password immediately afterwards (0.5)
e) I don't know what I would do in such a situation (0)

Determining Level 2 Situation Awareness (SA)

QUESTION 1.2 Do you use the same password for multiple systems, say for your personal email account and your work accounts?

a) Yes because my password is strong enough and it is too difficult to remember so many different passwords. (0)
b) No because I know that if one of the passwords get cracked, it could be used to access my other systems (2.5)
c) Yes because I don't write down my password or give it to anyone else. Nobody will be able to guess my password. (0)
d) No because it would be a breach of policy, although I don't quite understand what the risk would be. (0.5)
e) I don't know whether it would be acceptable to use the same password for multiple systems (0)

Determining Level 3 Situation Awareness (SA)

QUESTION 1.3 Is a passphrase better to use than just a set of characters and numbers in your password?

a) It is no better. As long as your password is at least 8 characters long then nobody will be able to guess it. (0.5)
b) It is no better. As long as my computer is secure any length password will be OK. Also I change my password regularly. (0)
c) It is better only because someone looking over my shoulder won't be able to remember a passphrase. (0.5)
d) It is better because the length of a password is the most important factor. Passphrases can be easily remembered and can be very long (2.5)
e) I don't know whether a passphrase is more secure to use than a password made up of a combination of characters and numbers (0)

Figure 4-2 Example of scoring for survey question

In general terms, the first part (sub-question) of each of the 10 main questions targets Level 1 SA and assigns a maximum score of 2 for the most correct answer. The second part of the questions targets Level 2 SA with a maximum score of 2.5 for the most correct answer. Lastly, the final part equates to a Level 3 SA 'difficulty' and scores a maximum of 2.5 for the most correct answer. Thus, for question 1 shown above, answering the most correct answers for each of the sub-questions by selecting answers *c*, *b* and *d* respectively would result in an overall score of 7 for Question 1 - which indicates a high level of awareness capability for that security control objective. This overall score of 7 then becomes the *awareness capability* score for that question, and for that particular respondent.

4.4.1 Descriptive data analysis

Table 4-4 below provides a summary of the descriptive statistical data analysis that was conducted on the data collected from phase 2 survey. The results of the data analysis for the phase 2 surveys are presented in Chapter 5.

Table 4-4 Analysis to be conducted on phase 2 survey data

Data Analytics used	Relevance for this research
Analysis of completion rates and profile of participants	- which survey results were usable. - education level of those completing the survey. - digital literacy of respondents. - age of those completing the survey. - whether respondents had ever worked in an IT role. - industry sector of respondents.
Scoring of Awareness Capability	- primary measure for this survey. - individual respondents score per question is made up by tallying each of the scores for the 3 sub-questions (see Figure 4-2 above). - average of the scoring for each of the 10 question, would provide an organisational awareness capability score.
Analysis of L1, L2 and L3 scores	- percentage of respondents that at least scored (i.e. greater than 0) for each of the three sub-questions of the questions. - how does the overall score for each question rank in terms of overall situation awareness.

The statistical data analysis techniques conducted on the data collected from the Phase 2 survey shown above in Table 4-4 fall into three main categories. The first category is related to preparing and assessing the data for analysis and determining the demographics of survey respondents. Some analysis was done in relation to completion rates, whether the respondents do or had worked in an IT role (phase 2 survey was aimed at end users), and which industries they work in. The second category of analysis was related to the scores provided for each of the 10 main questions (via their sub-questions) and how that was used to determine the awareness capability scores overall for each of the 10 main questions.

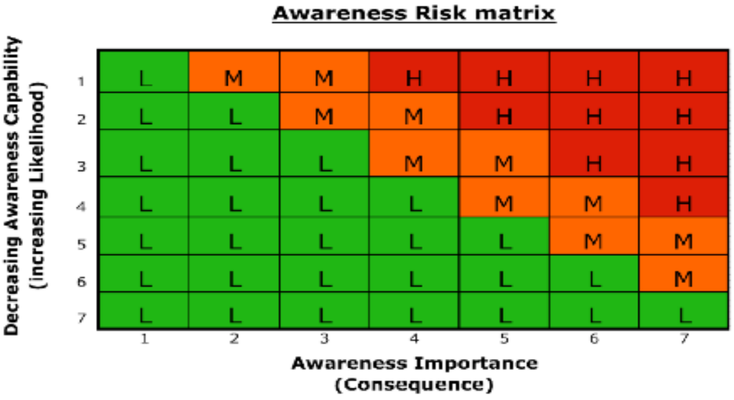
The final category provides a deeper analysis of each of the sub-questions to assess how these scores relate to the situation awareness approach used to construct these questions. SA theory suggests that people generally need to attain Level 1 SA before they can attain Level 2 SA, and Level 2 SA before than can attain Level 3 SA. The full analysis in regards to the awareness capability scores is shown in Chapter 5.

4.5 Phase 2 – Developing the Awareness Risk component

The final component of the ISACM is awareness risk. As discussed in Chapter 3, this third and final measurement point can be derived by comparing how important awareness (*awareness importance*) is with how much awareness is being demonstrated (*awareness capability*) to arrive at a risk measurement (*awareness risk*). Awareness risk is the gap between these two measures. The development of awareness importance was described in section 3.4 on page 87. The development of awareness capability was described earlier in this chapter in section 4.2. The awareness risk calculation is shown below.

$AR = AI - AC$	where AI = Awareness Importance; AC = Awareness Capability; AR = Awareness Risk

Awareness importance and awareness capability measures were combined to demonstrate awareness risk by focusing on the gap between desired (importance) behaviour compared to what is observed (capability). Further details are contained in section 2.4.3 on page 72. Figure 4-3 below is adapted from ISO/IEC 27005 (International Organization for Standardization (ISO) 2008) and illustrates how the awareness risk measurement is portrayed using the ISACM developed in this current research.



Awareness Risk matrix

Decreasing Awareness Capability (increasing Likelihood)	1	2	3	4	5	6	7
1	L	M	M	H	H	H	H
2	L	L	M	M	H	H	H
3	L	L	L	M	M	H	H
4	L	L	L	L	M	M	H
5	L	L	L	L	L	M	M
6	L	L	L	L	L	L	M
7	L	L	L	L	L	L	L

Awareness Importance
(Consequence)

Figure 4-3 Adapted Awareness Risk matrix related to information security awareness

This risk matrix follows a traditional approach used in likelihood versus consequence (impact) risk matrices (NSW Government 2012; Standards Australia/Standards New Zealand 2009b). In this study, where awareness capability exceeds or is equal to the awareness importance, then the awareness risk is low (reflected by the green area). Where the awareness capability falls short of the required awareness importance, the awareness risk enters the medium risk zone (orange area) and progressively into the high risk zone (red area). The larger the gap between the two measures, the higher the risk rating. A detailed discussion of the results of data analysis from the phase 2 surveys regarding awareness risk is presented in Chapter 5.

4.6 Limitations of the methodology

Although the ISACM has been built with three underlying measurement points, there are some limitations in the methods used to construct each of these measurement points. Whilst the ISACM relies upon the use of specific measures, traditionally such risk models can only provide an approximation as to the real risk that an organisation may face (Duijm 2015; NSW Government 2012). Furthermore, in reality an approximation is sufficient in that it can help direct attention to those areas perceived as being higher risk than those that are seen as lower risk. Risk measurements are not always an exact measure, as they rely upon aspects such as likelihood and impact - both of which can be subjective - and approximations are often used (Mejias 2012; Yu et al. 2015). In their guidance to the Australian NSW government agencies, (NSW Government 2012, p. 65), the NSW Government advise 'risk assessment is ultimately an activity that requires subjective judgment. Although there may be other causes for faulty risk assessments, cognitive biases can be particularly pervasive'.

4.7 Special and unusual treatment of data prior to analysis

The data obtained from both surveys did not require special preparation prior to analysis. Checking for completeness and addressing some of the missing values from the survey was the primary preparation undertaken before the data could be analysed. The tools used to conduct the analysis are described below.

4.8 Computer programs used to analyse data

The data from both surveys were analysed using a number of computer applications run on an Apple iMac personal computer. Initially, survey responses were captured by the survey provider, Qualtrics, and made available as downloadable data files. The data files were a csv format for importation into Microsoft Excel and a sav format for importation into IBM's SPSS software. The analysis was conducted using IBM's SPSS, Microsoft Excel, and Microsoft Access. Initial preparation of the data files downloaded from Qualtrics was carried out within SPSS, which also allowed the results to be saved into an Excel format for further analysis and graphing.

4.9 Ethical considerations

Ethical clearance was obtained from the University of Southern Queensland (USQ) Ethics Committee before any data collection was undertaken. This research involved surveying humans, information security professionals in phase 1; and in phase 2 surveying staff at an Australian university and members of the MyOpinions survey panel. Ethical clearance ensured the ethical considerations of this research were addressed in accordance with USQ policy on ethical research as set out in the National Statement on Ethical Conduct in Research Involving Humans.

Participants of both surveys were provided with details of the ethics clearance obtained for this research. They were offered the opportunity to contact the USQ Ethics Coordinator if they had any concerns or complaints about the conduct of this research. A '*Participants Information for USQ Research Project'* sheet was provided within each of the surveys. This highlighted that the privacy of survey participation was ensured, as well as highlighting that the research did not collect any personally-identifiable information about individual survey participants.

4.10 Conclusion

This chapter described the methodological approach used for phase 2 of the research. Chapter 4 covered the development of the second element of the ISACM, that of awareness capability, and described the development of this research's second survey. The awareness capability instrument in the phase 2 survey leveraged situation awareness theory and was used to collect data to determine the awareness capability for the top ten rated main security categories and their associated control objectives for end users from the first survey. The phase 2 awareness capability online survey was undertaken for the end user stakeholders of two separate populations groups.

The approach for developing this awareness capability measure was described in significant detail so as to firstly allow researchers to satisfy themselves of the rigor applied and, secondly, to also allow for future improvements to be made to the approach. This included the approach used to develop the awareness capability survey instrument that was used to obtain scores from the end users. Special attention was given to demonstrate the linkages of the questions and sub-questions to the three levels of situation awareness. This chapter also described how the third element of the ISACM, that of awareness risk, was calculated.

Finally, this chapter described how the data collected from the two surveys was prepared and analysed and what computer programs were used to analyse the data. Ethical clearance was obtained for this research which involved humans. The ethical considerations of this research in relation to the phase 1 survey and the phase 2 surveys were described.

The next chapter presents the key results of a detailed analysis of the data collected during phase 1 and phase 2 of this research, including presenting the overall ISACM and the awareness importance, awareness capability and awareness risk scores.

5.0 Data Analysis – Research phase 1 and 2

5.1 Introduction

The purpose of this chapter is to present the analyses of data collected from the questionnaire surveys from phase 1 and phase 2. The first section presents the results of descriptive statistics for phase 1 survey data. The second section presents the results of the statistical analysis of the phase 1 survey data used to determine the awareness importance measure for each of the 39 main security categories and their associated control objectives in the ISO/IEC 27002 standard. The third section presents the results of the descriptive statistics for the phase 2 survey data, and the fourth section presents the results of statistical analysis of phase 2 survey data. This was used to determine the awareness capability measures and subsequent awareness risk measures for one stakeholder group (end users) to demonstrate the Information Security Awareness Capability Model (ISACM) could be implemented in an organisation. Figure 5-1 below outlines the structure of this chapter.

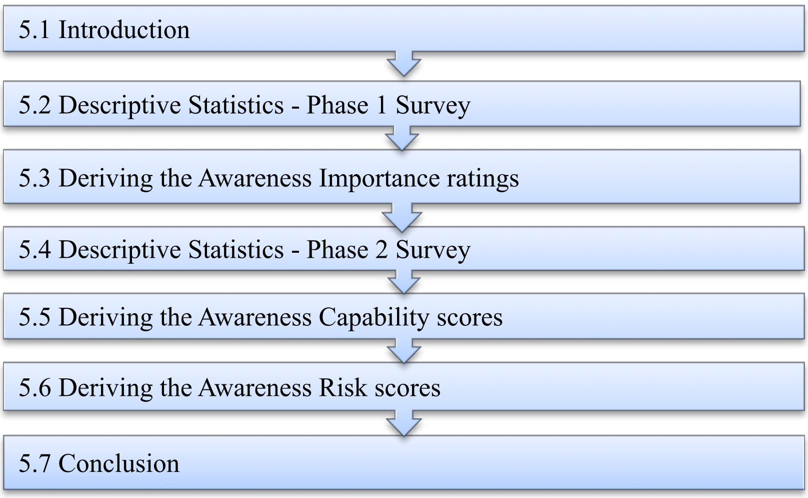

5.1 Introduction
5.2 Descriptive Statistics - Phase 1 Survey
5.3 Deriving the Awareness Importance ratings
5.4 Descriptive Statistics - Phase 2 Survey
5.5 Deriving the Awareness Capability scores
5.6 Deriving the Awareness Risk scores
5.7 Conclusion

Figure 5-1 Structure of Chapter 5

5.2 Descriptive Statistics - Phase 1 Survey

The primary aim of this phase 1 survey was to elicit responses from information security, IT Audit and IT Risk professionals in order to derive the awareness importance rating for each of the 39 main security categories and their associated control objectives. This survey targeted information security, IT risk and IT audit professionals who were considered to be knowledgeable in the management of information security. They were deemed capable of providing informed ratings of awareness importance for the 39 main security categories and their associated control objectives across three key stakeholder groups in organisations. Each question for the 39 main security categories and their associated control objectives provided a rating for each of the three stakeholder groups. Overall, 117 ratings were obtained, as shown in Table 5-1 below.

Table 5-1 Summary of Awareness Importance ratings

Security control clauses (11 in total)	Main security categories (39 in total)	IT Staff	SM	End Users
1 Security Policy	1 Information security policy	5.92	5.56	4.47
2 Organization of Information Security	2 Internal organization	5.36	5.54	3.79
	3 External parties	5.59	5.30	3.71
3 Asset Management	4 Responsibility for assets	5.56	5.59	4.65
	5 Information classification	5.53	5.56	4.89
4 Human Resources Security	6 Prior to employment	5.04	5.72	4.49
	7 During employment	5.28	5.74	4.45
	8 Termination or change of employment	5.53	5.72	4.22
5 Physical and Environmental Security	9 Secure areas	5.82	5.39	3.77
	10 Equipment security	5.74	5.50	4.62
6 Communications and Operations Management	11 Operational procedures & responsibilities	5.67	5.31	3.97
	12 Third party service delivery management	5.54	5.74	3.94
	13 System planning and acceptance	6.15	5.13	3.47
	14 Protection against malicious and mobile code	6.24	5.13	4.38
	15 Back-up	6.26	4.87	4.15
	16 Network security management	6.27	4.72	3.47
	17 Media handling	6.17	5.12	4.94
	18 Exchange of information	5.77	5.51	5.23
	19 Electronic commerce services	5.72	5.04	4.16
	20 Monitoring	6.15	4.61	3.40
7 Access Control	21 Business requirement for access control	5.68	5.58	4.75
	22 User access management	5.98	5.14	4.53
	23 User responsibilities	5.81	5.31	5.36
	24 Network access control	6.14	4.45	3.73
	25 Operating system access control	6.19	4.03	3.32
	26 Application and information access control	6.15	4.17	3.62
	27 Mobile computing and teleworking	6.12	5.77	5.27
8 Information Systems Acquisition, Development and Maintenance	28 Security requirements of information systems	6.01	5.08	3.82
	29 Correct processing in applications	5.84	4.32	3.67
	30 Cryptographic controls	6.08	4.00	3.02
	31 Security of system files	6.10	3.77	2.80
	32 Security in development and support processes	6.06	3.97	3.02
	33 Technical Vulnerability Management	6.24	4.30	3.00
9 Information Security Incident Management	34 Reporting information security events and weaknesses	6.13	5.62	5.28
	35 Management of information security incidents and improvements	6.05	5.61	4.49
10 Business Continuity Management	36 Information security aspects of business continuity management	5.94	5.82	4.21
11 Compliance	37 Compliance with legal requirements	5.60	6.10	4.69
	38 Compliance with security policies and standards, and technical compliance	5.75	5.68	3.87
	39 Information systems audit considerations	5.61	5.22	3.43

The survey ran from 8 March 2013 and closed on 17 May 2013. It was an online survey (administered using Qualtrics) and access was provided via an Internet URL. The distribution of the survey was administered through:

- Email message to members of the Australian Information Security Association (AISA) inviting them to participate. The AISA Management sent this out. Follow up LinkedIn messages were also sent out to AISA members.

- Direct email to around 60 industry contacts of the author of this research.
- The survey link and an invitation to participate in the survey was posted on the LinkedIn special interest groups Information Security Group, ISO/IEC 27000, Certified Information Systems Auditors, Certified Information Security Managers, Information Security Community, Institute of Information Security Professionals, and Perth Security Professionals.

5.2.1 Survey completion rate

Prior to performing detailed quantitative data analysis on the survey results, an initial assessment of the responses was conducted. There were 163 participants who took part in the survey, with a breakdown by country of participant shown in Table 5-2.

Table 5-2 Countries of survey participants

Country	No.	%	Country	No.	%	Country	No.	%
Australia	47	28.8	Saudi Arabia	2	1.2	Hungary	1	0.6
USA	23	14.1	Sweden	2	1.2	Italy	1	0.6
United Kingdom	18	11.0	Ukraine	2	1.2	Japan	1	0.6
India	8	4.9	Argentina	1	0.6	Jersey Saint Helier	1	0.6
Netherlands	7	4.3	Austria	1	0.6	Kenya	1	0.6
Can't tell	6	3.7	Barbados	1	0.6	Korea	1	0.6
France	4	2.5	Brazil	1	0.6	Luxembourg	1	0.6
Canada	3	1.8	Bulgaria	1	0.6	Malaysia	1	0.6
Germany	3	1.8	China	1	0.6	Morocco	1	0.6
Switzerland	3	1.8	Columbia	1	0.6	Norway	1	0.6
Belgium	2	1.2	Denmark	1	0.6	Portugal	1	0.6
New Zealand	2	1.2	Egypt	1	0.6	Spain	1	0.6
Philippines	2	1.2	Georgia	1	0.6	United Arab Emirates	1	0.6
Qatar	2	1.2	Greece	1	0.6	**Total**	**163**	**100**
Romania	2	1.2	Hong Kong	1	0.6			

Most participants were from the researcher's country of Australia, with participation from another 41 countries. Not all surveys were completed. Table 5-3 below shows that of the initial 163 surveys, 32 respondents (20%) stopped without filling out their *Experience* and *Role* information. This was one of the first questions asked (and was compulsory), but appeared in the survey after details of the ethics clearance and purpose of the research and its approach had been presented.

Table 5-3 Respondents' experience level

	Respondents' experience in Info Security	Frequency	Percentage
Valid	Significant level (10 years plus)	71	54.2
	Good level of experience (5 -10 years)	35	26.7
	A general level (less than 5 years)	18	13.8
	Little or no information security experience	7	5.3
	Total	131	**100**
Missing	Not completed	32	
Total		**163**	

Of those 131 that completed the experience level question, 81% indicated they had 5 years plus experience or formal qualification in information security, information technology auditing, or information risk management. This high percentage matches the target population for this survey. Overall, of the 163 people who started the survey, 80 people fully completed the survey. This is a completion rate of 49%.

5.2.2 Identifying usable responses

Analysis of the number of survey questions completed is shown in Table 5-4 below. Whilst 131 people completed the question regarding their experience level, only 124 completed question 1, falling further to 80 respondents who completed all 39 questions. Table 5-4 also shows the stakeholder groups that the respondents most closely associated with.

Table 5-4 Completion rate by Question number and Experience level

At least Completed **Question 1**	Significant level (10 years plus)	Good level of experience (5-10 years)	A general level (less than 5 years)	Little or no information security experience	Total
IT staff	24	12	10	2	48
Senior management	41	20	4	1	66
End users	1	2	3	4	10
Total	66	34	17	7	124

At least Completed **Question 11**	Significant level (10 years plus)	Good level of experience (5-10 years)	A general level (less than 5 years)	Little or no information security experience	Total
IT staff	16	10	5	0	31
Senior management	34	14	2	1	51
End users	1	1	2	2	6
Total	51	25	9	3	88

Completed **All 39 Questions**	Significant level (10 years plus)	Good level of experience (5-10 years)	A general level (less than 5 years)	Little or no information security experience	Total
IT staff	14	10	5	0	29
Senior management	31	14	1	1	47
End users	0	1	2	1	4
Total	45	25	8	2	80

The majority of respondents classified themselves as senior management - which may reflect where these people currently reside within the organisation, rather than where they may have previously worked and where they have gained their information security experience. These people could be working in IT Audit, IT Risk or other senior management roles.

Table 5-4 above highlights that 124 respondents completed question 1. This number falls to 88 respondents who at least completed question 11 and, finally, fell to 80 respondents who completed all 39 questions. Question 11 of the survey represents the start of the more technically-focused questions contained within the *Communications and Operations Management* section which consists of 10 questions. Being technically-focused questions, this may have presented a challenge to those not familiar with the ISO/IEC 27002 standard, or not experienced enough in information security. However, the target audience for the survey was those people expected to be familiar with the ISO/IEC 27002 standard.

To determine whether including partially completed surveys in the data analysis would impact on the overall results of this research, this research examined the experience level of those who at least completed question 1 (shown in Table 5-4 above). Nineteen percent of respondents who completed question 1 possess a relatively low level of experience (<5 years, or little or no experience). Comparing this to those who fully completed the survey (all 39 questions), only 13% of respondents had less than 5 years' experience.

Table 5-5 and Table 5-6 show what this impact would be to the resultant awareness importance ratings. The awareness importance ratings for each of the stakeholder groups increases when only looking at those who have fully completed the survey (Table 5-6), compared to those who have at least completed question 1 (Table 5-5). For example, awareness importance for IT staff increased from 5.82 to 5.92. This is not a significant increase, but an increase nonetheless.

Table 5-5 Anyone who answered Question 1

	Awareness Importance for IT staff	Awareness Importance for senior management	Awareness Importance for end users
Valid	124	124	124
Mean	5.82	5.52	4.36

Table 5-6 Only those who fully completed the survey

	Awareness Importance for IT staff	Awareness Importance for senior management	Awareness Importance for end users
Valid	80	80	80
Mean	5.92	5.56	4.47

The survey was purposely targeted at experienced information security, IT audit and IT risk professionals, so excluding those who may have realised after answering question 1 that they may not know enough about the material presented seems appropriate. However, it also eliminates some of those more experienced respondents who did not fully complete the survey. A more compelling reason for excluding the partially completed surveys is that, to obtain consistency across all questions, only completed surveys should be used so that the respondent population is the same for all questions. As a result, the decision was made to exclude incomplete survey responses from the main analysis of this research. The total pool of valid responses was, therefore, 80 fully completed surveys.

5.2.3 Demographics of Survey 1 Respondents

This section presents the results of descriptive statistics from the survey questionnaire. These include the experience level (in terms of information security) of the respondents, which stakeholder groups the respondents identify with, and the 39 questions (with 3 stakeholder sub-questions) related to awareness importance ratings. Having decided to only use fully-completed surveys for data analysis, the valid survey responses were grouped by the respondents' experience level. Table 5-7 below shows that only two out of the 80 respondents indicated little or no experience in information security or IT audit or IT risk. These two responses were merged within the group titled '*A general level (less than 5 years)*'. This allowed for comparison of three different levels of experience rather than four levels.

Table 5-7 Experience levels of those who completed the survey

Completed All 39 Questions	Significant level (10 years plus)	Good level of experience (5 - 10 years)	A general level (less than 5 years)	Little or no information security experience	Total	%
IT Staff	14	10	5	0	29	36%
Senior Management	31	14	1	1	47	59%
End User	0	1	2	1	4	5%
Total	45	25	8	2	80	
%	56%	31%	10%	3%		

The survey responses also identified which stakeholder groups the survey respondents most closely identified with. This provided mixed results. Firstly, with the main aim of the survey being that of targeting those people with good knowledge of the ISO/IEC 27002 standard, it was thought that a majority of respondents would categorise themselves as IT staff. However this did not fully cater for those people working as IT audit and IT risk professionals, many of whom seem to have selected senior management as their stakeholder group. In hindsight, it would have been better to include a specific category for IT audit and IT risk staff. However, distinguishing between IT and non-IT staff has been achieved.

Examining those who identified themselves as IT staff, Table 5-8 below shows a breakdown of which field of IT they work in. Of the 29 current IT staff who completed the survey, 24 (83%) work in an information security role. Information security was the primary area of IT staff that was targeted.

Table 5-8 What field of IT do they work in

Developers/ Programmers	Management	Networks and Systems Administration	Security	Team Leaders	**Total**
1	1	2	24	1	29

From those who categorised themselves as senior management stakeholders (refer to Table 5-7 above), these 47 respondents represent 59% of all respondents who completed the survey. Furthermore, 96% of those specifying themselves as senior management have more than 5 years information security experience. This also meets the primary aim of the survey to elicit responses from experienced information security professionals. These people are likely to be former information security staff, or staff currently working in senior IT roles or in fields such as IT audit, IT risk and IT governance and compliance.

To facilitate the analysis of responses, the respondent stakeholder categories were reduced from three to two, that of IT staff and Non-IT staff. Grouping the four end user respondents with the 47 senior management respondents and categorising this group as Non-IT staff achieved this. This left two groups of survey respondents - those currently working as IT staff and those not. The final profile of respondents who fully completed the survey is shown below in Table 5-9.

Table 5-9 Final breakdown of survey respondents

	Final View of the data to be fully analysed	Significant level (10 years plus)	Good level of experience (5 -10 years)	A general level (less than 5 years)	Total
IT Staff	Count	14	10	5	29
	% within Group you work in	48.3%	34.5%	17.2%	100%
	% within Experience	31.1%	40.0%	50.0%	36.2%
	% of Total	17.5%	12.5%	6.2%	36.2%
Non-IT Staff	Count	31	15	5	51
	% within group you work in	60.8%	29.4%	9.8%	100%
	% within Experience	68.9%	60.0%	50.0%	63.7%
	% of Total	38.8%	18.8%	6.2%	63.7%
Total	Count	**45**	**25**	**10**	**80**
	% within group you work in	56.2%	31.2%	12.5%	100%
	% within Experience	100.0%	100.0%	100.0%	100%
	% of Total	56.2%	31.2%	12.5%	100%

In summary, the respondent groups have been consolidated into two groups of who the respondents most closely associate themselves with, that of IT staff and Non-IT staff. The experience levels of the respondents have also been consolidated into three groups, that of 10 years plus experience, between 5 and 10 years' experience, and less than 5 years. These 80 valid responses form the basis of the following analysis used to determine the awareness importance ratings.

5.3 Deriving the Awareness Importance ratings

Phase 1 survey data collection was aimed at deriving the awareness importance rating (covering the 39 main security categories and their associated control objectives from the ISO/IEC 27002 Standard), for each of the three stakeholder groups. This measure was directly scored by each of the respondents on a scale of 1 to 7, and selectable to one decimal place of accuracy. No rescaling of the respondent results was required. The overall awareness importance rating was calculated as an average of all responses for that particular question and for that particular stakeholder group question. These results are shown earlier in Table 5-1.

Graphically, the awareness importance scores are shown in
Figure 5-2 below. By segmenting the questions into their respective 11 security control clause sections (from the ISO/IEC 27002 standard) of like-focused questions, this presents a view that highlights the responses as a group for each of the 11 security control clauses, rather than as 39 individual questions. In general, the awareness importance rating for IT staff is higher than that for senior management; which, in turn, is higher than that for end users. However, with some of the security control clauses, for example security control clause 4 (Human Resources Security), the ratings for senior management outrank those of IT staff and end users. Further analysis of this trending is discussed in section 5.3.2.

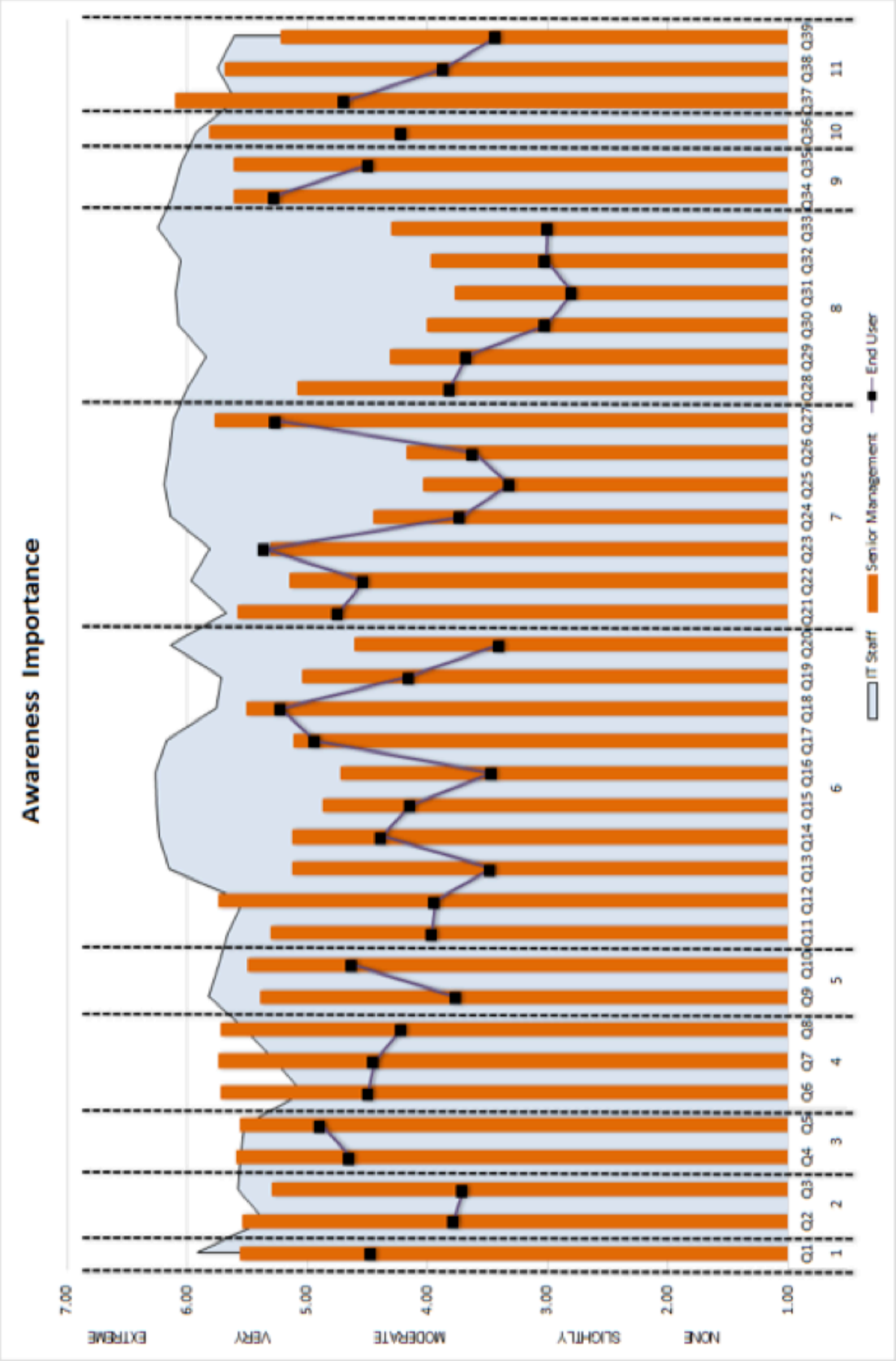


Figure 5-2 Summary of Awareness Importance rating by stakeholder group

Although the absolute ratings for awareness importance are the key output of this first phase of data collection, the survey results provide additional insight, trends and patterns that were not an initial focus of this study. There are important messages gleaned from this data that are discussed in Chapter 6. For example, a wide spread of rating scores could signal that, particularly across those respondents with the same level of information security experience, there exists conflicting opinions as to how important something is for a particular stakeholder group.

Additionally, the relative ratings of importance by stakeholder groups are also an important aspect to examine. These implications could aid those organisations developing information security awareness programs, or those trying to measure the effectiveness of those programs. The differences in importance based on the stakeholder group could indicate the need to have a much more targeted awareness program depending on which stakeholder group the awareness program is aimed at.

5.3.1 Rating Awareness Importance by stakeholder groups

The graphical representation below (

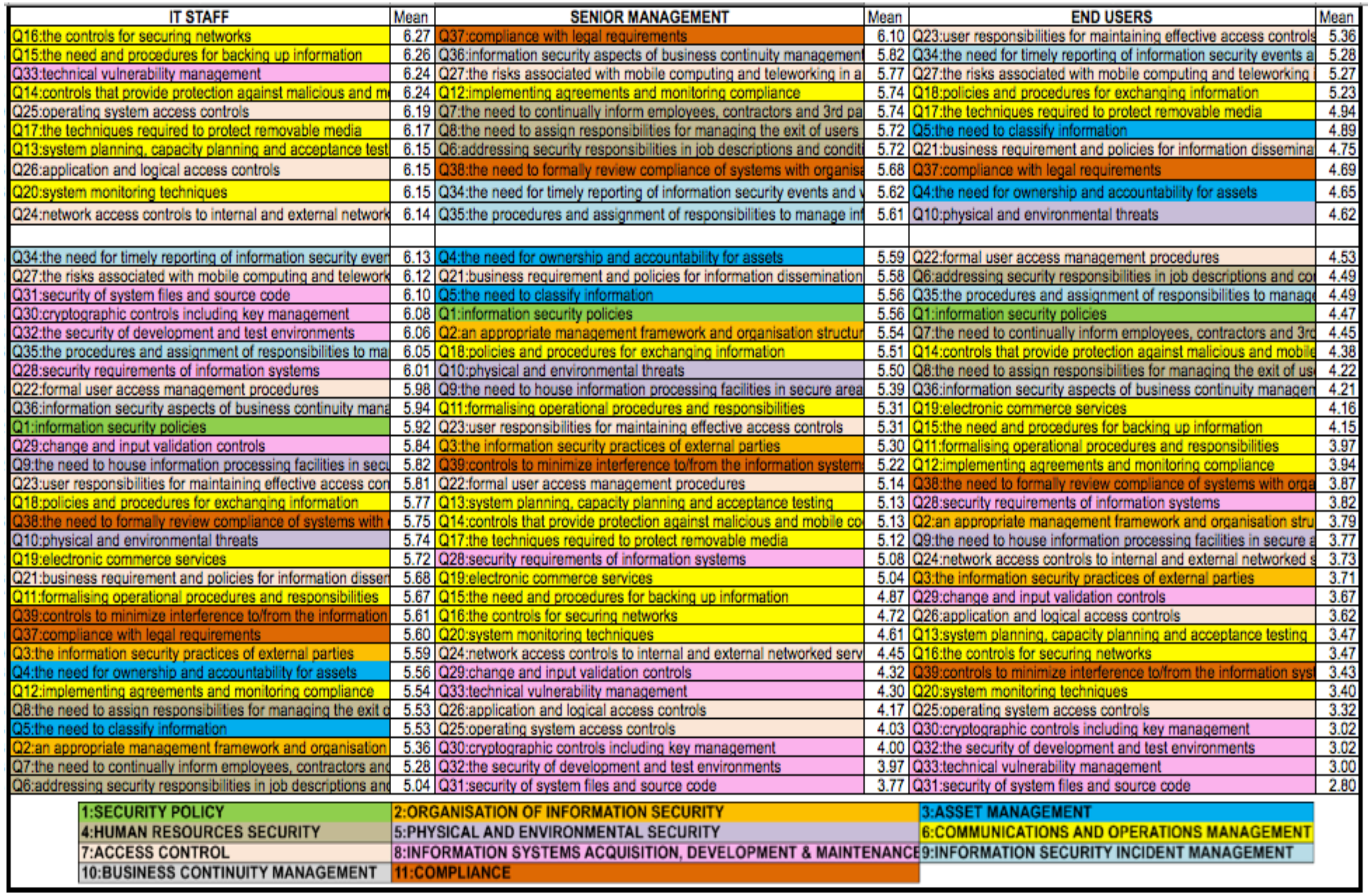
Figure 5-3) presents the 39 question responses for each of the three stakeholder groups. Within each of the stakeholder groups these awareness importance ratings are sorted in descending value. They are colour coded based on which of the 11 security control clause sections the questions belong to. The survey question number is included as well as some of the question text.

The benefit of this graphic is not for the reader to try and read the details of the individual questions in the graphic. Referring to the data within the various tables shown earlier best presents that information. The aim of the graphic is to view the aggregation and positioning of the colours to quickly see how the ratings group and vary based on the stakeholder group. The colour coding quickly highlights where groupings of like-focused questions are positioned from a priority perspective, and how that compares with the other stakeholder groups.

An example of this colour coding is the yellow highlighted questions dominating the top rating positions for IT staff. These belong to *security control clause 6, Communications and Operations Management* and, not surprisingly, have a largely technical focus. Conversely, the ratings of this security control clause are much lower in priority for both senior management and end users.

A similar situation exists for the pink highlighted questions. These rate at the bottom for end users and senior management. These questions belonging to *security control clause 8 Information System Acquisition, Development & Maintenance*. They rate much higher for IT staff. However, questions belonging to *security control clause 4 Human Resources Security* (tan coloured) rate in the top 10 for senior management, but fall in the bottom rating for IT staff and are middle rated for end users. Further discussion of this analysis is included in Chapter 6.

Figure 5-3 Heatmap ranking in descending order of survey responses by Security Control Clauses



IT STAFF	Mean	SENIOR MANAGEMENT	Mean	END USERS	Mean
Q16:the controls for securing networks	6.27	Q37:compliance with legal requirements	6.10	Q23:user responsibilities for maintaining effective access controls	5.36
Q15:the need and procedures for backing up information	6.26	Q36:information security aspects of business continuity management	5.82	Q34:the need for timely reporting of information security events a	5.28
Q33:technical vulnerability management	6.24	Q27:the risks associated with mobile computing and teleworking in a	5.77	Q27:the risks associated with mobile computing and teleworking i	5.27
Q14:controls that provide protection against malicious and m	6.24	Q12:implementing agreements and monitoring compliance	5.74	Q18:policies and procedures for exchanging information	5.23
Q25:operating system access controls	6.19	Q7:the need to continually inform employees, contractors and 3rd pa	5.74	Q17:the techniques required to protect removable media	4.94
Q17:the techniques required to protect removable media	6.17	Q8:the need to assign responsibilities for managing the exit of users	5.72	Q5:the need to classify information	4.89
Q13:system planning, capacity planning and acceptance test	6.15	Q6:addressing security responsibilities in job descriptions and conditi	5.72	Q21:business requirement and policies for information dissemina	4.75
Q26:application and logical access controls	6.15	Q38:the need to formally review compliance of systems with organisa	5.68	Q37:compliance with legal requirements	4.69
Q20:system monitoring techniques	6.15	Q34:the need for timely reporting of information security events and v	5.62	Q4:the need for ownership and accountability for assets	4.65
Q24:network access controls to internal and external network	6.14	Q35:the procedures and assignment of responsibilities to manage inf	5.61	Q10:physical and environmental threats	4.62
Q34:the need for timely reporting of information security even	6.13	Q4:the need for ownership and accountability for assets	5.59	Q22:formal user access management procedures	4.53
Q27:the risks associated with mobile computing and telework	6.12	Q21:business requirement and policies for information dissemination	5.58	Q6:addressing security responsibilities in job descriptions and co	4.49
Q31:security of system files and source code	6.10	Q5:the need to classify information	5.56	Q35:the procedures and assignment of responsibilities to manage	4.49
Q30:cryptographic controls including key management	6.08	Q1:information security policies	5.56	Q1:information security policies	4.47
Q32:the security of development and test environments	6.06	Q2:an appropriate management framework and organisation structur	5.54	Q7:the need to continually inform employees, contractors and 3rd	4.45
Q35:the procedures and assignment of responsibilities to ma	6.05	Q18:policies and procedures for exchanging information	5.51	Q14:controls that provide protection against malicious and mobile	4.38
Q28:security requirements of information systems	6.01	Q10:physical and environmental threats	5.50	Q8:the need to assign responsibilities for managing the exit of us	4.22
Q22:formal user access management procedures	5.98	Q9:the need to house information processing facilities in secure area	5.39	Q36:information security aspects of business continuity managem	4.21
Q36:information security aspects of business continuity mana	5.94	Q11:formalising operational procedures and responsibilities	5.31	Q19:electronic commerce services	4.16
Q1:information security policies	5.92	Q23:user responsibilities for maintaining effective access controls	5.31	Q15:the need and procedures for backing up information	4.15
Q29:change and input validation controls	5.84	Q3:the information security practices of external parties	5.30	Q11:formalising operational procedures and responsibilities	3.97
Q9:the need to house information processing facilities in secu	5.82	Q39:controls to minimize interference to/from the information system	5.22	Q12:implementing agreements and monitoring compliance	3.94
Q23:user responsibilities for maintaining effective access con	5.81	Q22:formal user access management procedures	5.14	Q38:the need to formally review compliance of systems with orga	3.87
Q18:policies and procedures for exchanging information	5.77	Q13:system planning, capacity planning and acceptance testing	5.13	Q28:security requirements of information systems	3.82
Q38:the need to formally review compliance of systems with	5.75	Q14:controls that provide protection against malicious and mobile co	5.13	Q2:an appropriate management framework and organisation stru	3.79
Q10:physical and environmental threats	5.74	Q17:the techniques required to protect removable media	5.12	Q9:the need to house information processing facilities in secure a	3.77
Q19:electronic commerce services	5.72	Q28:security requirements of information systems	5.08	Q24:network access controls to internal and external networked s	3.73
Q21:business requirement and policies for information disser	5.68	Q19:electronic commerce services	5.04	Q3:the information security practices of external parties	3.71
Q11:formalising operational procedures and responsibilities	5.67	Q15:the need and procedures for backing up information	4.87	Q29:change and input validation controls	3.67
Q39:controls to minimize interference to/from the information	5.61	Q16:the controls for securing networks	4.72	Q26:application and logical access controls	3.62
Q37:compliance with legal requirements	5.60	Q20:system monitoring techniques	4.61	Q13:system planning, capacity planning and acceptance testing	3.47
Q3:the information security practices of external parties	5.59	Q24:network access controls to internal and external networked serv	4.45	Q16:the controls for securing networks	3.47
Q4:the need for ownership and accountability for assets	5.56	Q29:change and input validation controls	4.32	Q39:controls to minimize interference to/from the information syst	3.43
Q12:implementing agreements and monitoring compliance	5.54	Q33:technical vulnerability management	4.30	Q20:system monitoring techniques	3.40
Q8:the need to assign responsibilities for managing the exit o	5.53	Q26:application and logical access controls	4.17	Q25:operating system access controls	3.32
Q5:the need to classify information	5.53	Q25:operating system access controls	4.03	Q30:cryptographic controls including key management	3.02
Q2:an appropriate management framework and organisation	5.36	Q30:cryptographic controls including key management	4.00	Q32:the security of development and test environments	3.02
Q7:the need to continually inform employees, contractors and	5.28	Q32:the security of development and test environments	3.97	Q33:technical vulnerability management	3.00
Q6:addressing security responsibilities in job descriptions and	5.04	Q31:security of system files and source code	3.77	Q31:security of system files and source code	2.80

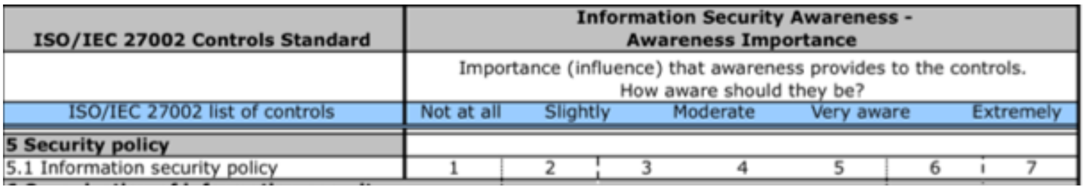
1:SECURITY POLICY	2:ORGANISATION OF INFORMATION SECURITY	3:ASSET MANAGEMENT
4:HUMAN RESOURCES SECURITY	5:PHYSICAL AND ENVIRONMENTAL SECURITY	6:COMMUNICATIONS AND OPERATIONS MANAGEMENT
7:ACCESS CONTROL	8:INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT & MAINTENANCE	9:INFORMATION SECURITY INCIDENT MANAGEMENT
10:BUSINESS CONTINUITY MANAGEMENT	11:COMPLIANCE	

5.3.2 *Patterns of data for Awareness Importance*

To further examine the results of the first phase of data collection, and to expand on some of the thoughts from the section above, a breakdown of each of the 11 security control clauses of the ISO/IEC 27002 standard is presented below. To aid the reader in interpreting the results, the specific questions that were asked in the survey have been shown, as well as the derived awareness importance rating for those individual questions. Within each section, a graph showing the distribution of the awareness importance ratings for each stakeholder group has also been included. These graphs represent the number of responses for each of the 11 security control clauses sections, broken down into each of the stakeholder groups. They are an aggregation of responses for that particular security control clause section.

For example, where a security control clause section has two questions within it, the number of respondent answers would be 160 aggregated responses (2 questions x 80 respondents). This presents a graphical insight into both the spread/congregation of responses, as well as the strength of opinion at any particular scoring point. The practical implications of these results are discussed in Chapter 6.

The 7-point likert scale that was used in the awareness importance survey is shown below in Figure 5-4.

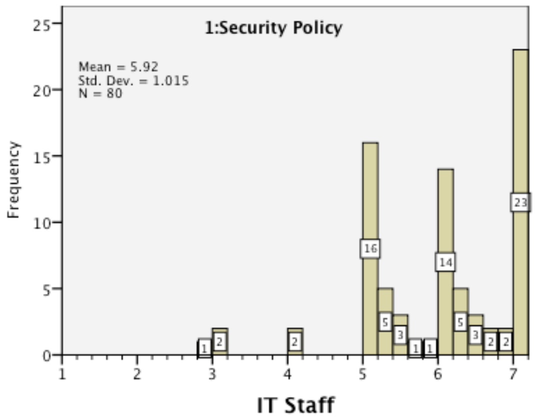


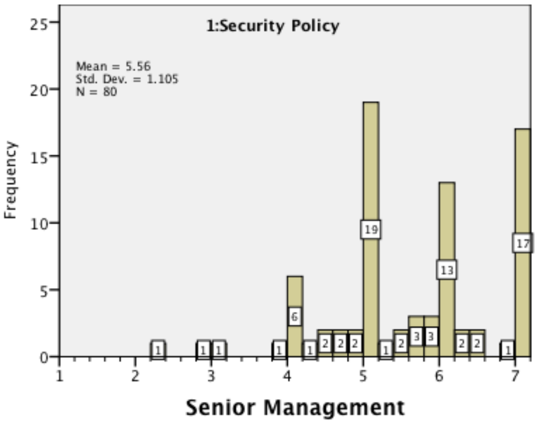
ISO/IEC 27002 Controls Standard	Information Security Awareness - Awareness Importance						
	Importance (influence) that awareness provides to the controls. How aware should they be?						
ISO/IEC 27002 list of controls	Not at all	Slightly		Moderate	Very aware		Extremely
5 Security policy							
5.1 Information security policy	1	2	3	4	5	6	7

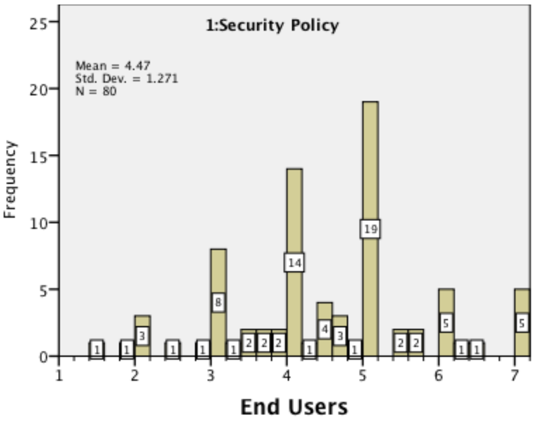
Figure 5-4 Awareness Importance survey question scale

5.3.2.1 Security control clause 1: Security Policy

Questions asked in the survey	Awareness Importance		
	IT	SM	EU
Q1: How aware of information security policies, do the stakeholder groups need to be, in order to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations?	5.92	5.56	4.47





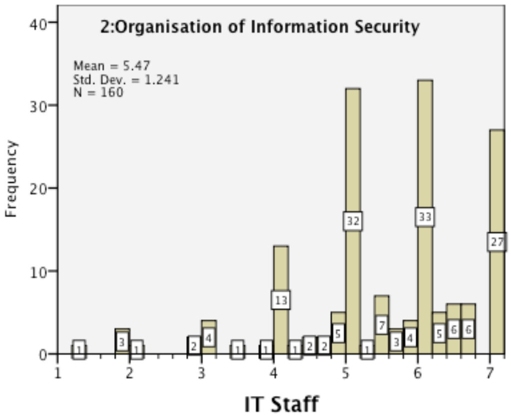


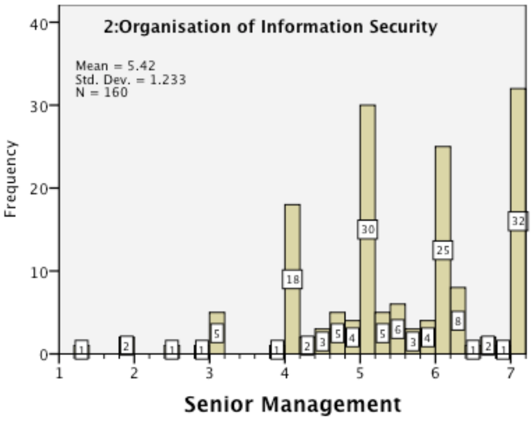
The results for IT staff show that 92% of scores are greater than or equal to 5 (very aware). Senior management results also show a reasonably high awareness importance rating with 78% of responses greater than or equal to 5 (very aware).

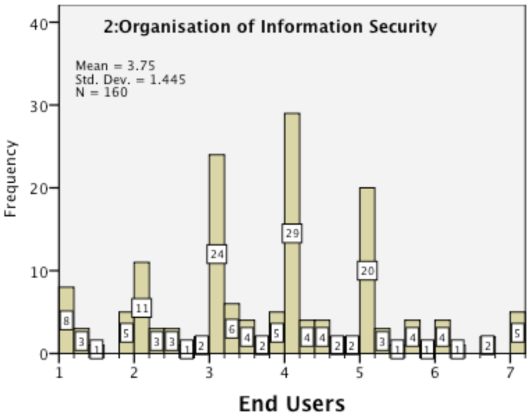
The results are quite varied on the opinion as to how important this is for end users. Although more than 43% of end user responses support awareness of 5 (very aware) or more, 19% suggest a rating of only 3 (slight to moderate) or less.

5.3.2.2 Security control clause 2: Organisation of Information Security

Questions asked in the survey	Awareness Importance		
	IT	SM	EU
Q2: How aware of an appropriate management framework and organisation structure to control information security, do the stakeholder groups need to be, in order to provide sound information security within the organisation?	5.36	5.54	3.79
Q3: How aware of the information security practices of external parties, do the stakeholder groups need to be when their information and information processing facilities are accessed, processed, communicated to, or managed by external parties?	5.59	5.30	3.71







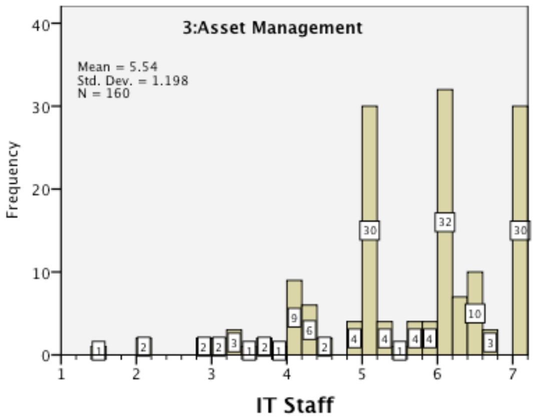
The results for IT staff show that the majority of scores rate 4 (moderate) or more, with high numbers of responses also rating at the 7 (extreme) level. IT staff are key players in this area.

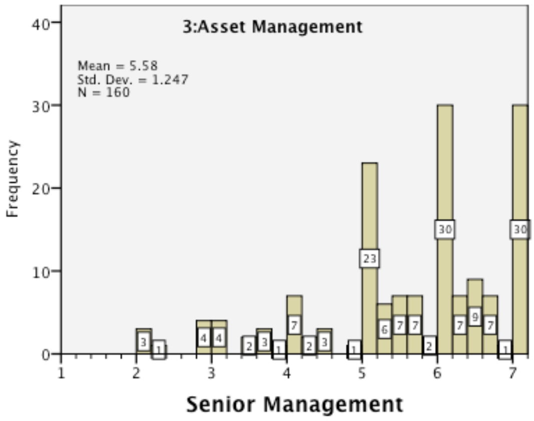
Senior management results show that 94% scored 4 (moderate) or more, with 73% greater than or equal to 5 (very aware). Senior management plays a key role in sponsoring and supporting information security. Equally, when it comes to dealing with third party organisations, senior management often own the relationship and drive any contract negotiations, so awareness in this area is quite important.

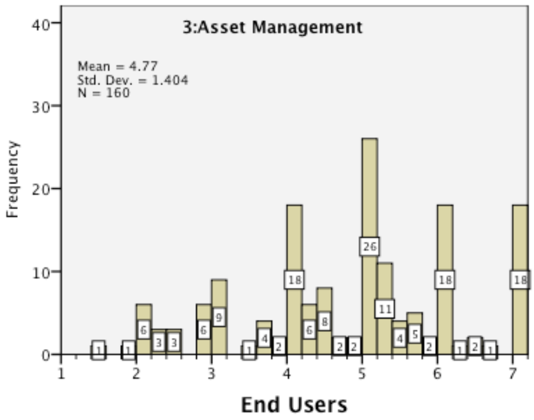
For end users, the results reflect relatively varied opinion as to the level of importance, with a higher weighting to scores below 4 (moderate).

5.3.2.3 Security control clause 3: Asset Management

Questions asked in the survey	Awareness Importance		
	IT	SM	EU
Q4: How aware of the need for ownership and accountability for assets, do the stakeholder groups need to be, in order to maintain appropriate protection of organisational assets?	5.56	5.59	4.65
Q5: How aware of the need to classify information, do the stakeholder groups need to be, so that information receives an appropriate level of protection?	5.53	5.56	4.89





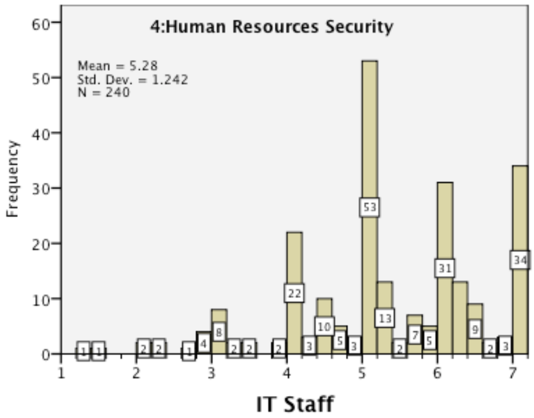


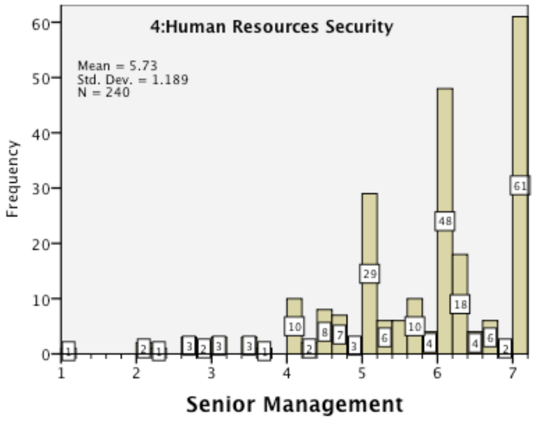
The results for IT staff show 78% of responses are greater than or equal to 5 (very aware). For senior management the results show that 80% of responses were greater than or equal to 5 (very aware).

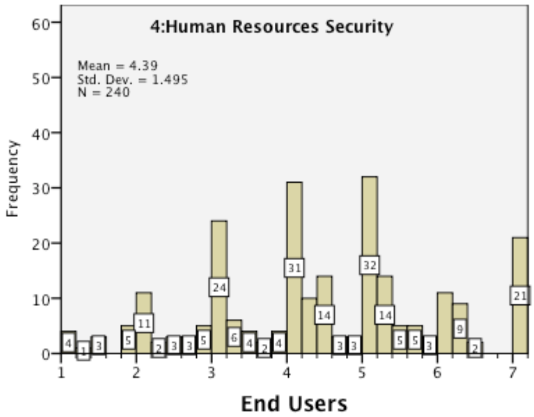
The end users continue to be quite varied, ranging from 18% of responses rating only 3 (slight to moderate) or less, whilst 55% of responses are greater than or equal to 5 (very aware).

5.3.2.4 Security control clause 4: Human Resources Security

Questions asked in the survey	Awareness Importance		
	IT	SM	EU
Q6: How aware of addressing security responsibilities in job descriptions and conditions of employment, do the stakeholder groups need to be?	5.04	5.72	4.49
Q7: How aware of the need to continually inform employees, contractors and 3rd party users of their ongoing information security responsibilities, do the stakeholder groups need to be, during the employment tenure of these staff?	5.28	5.74	4.45
Q8: How aware of the need to assign responsibilities for managing the exit of users, do the stakeholder groups need to be, so that employees, contractors and third party users exit an organisation or change their employment in an orderly and secure manner?	5.53	5.72	4.22





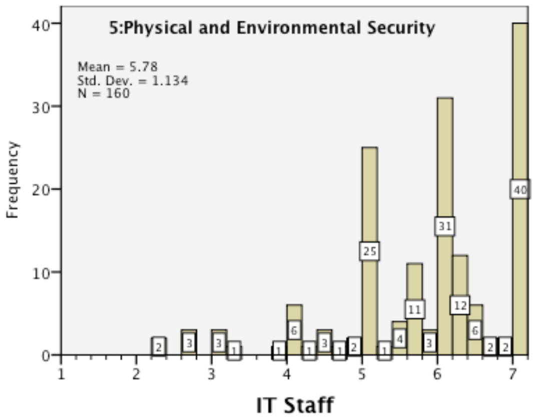


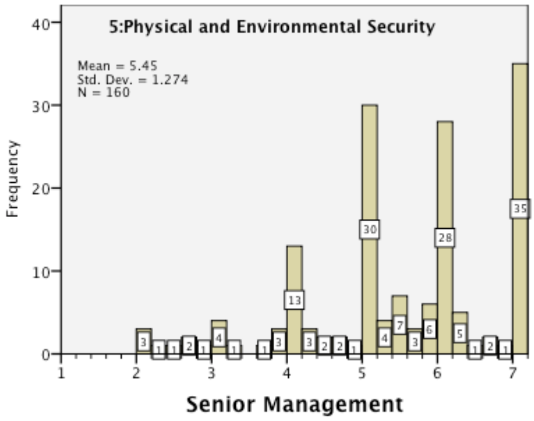
The results for IT staff show a broad spread of ratings, with 89% of responses rating 4 (moderate) or more, and 71% greater than or equal to 5 (very aware). For senior management, the results show strong weighting towards 7, with 81% greater than or equal to 5 (very aware).

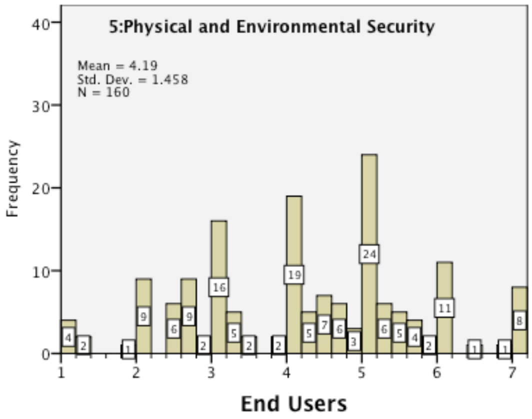
The overall average is higher than that for IT staff, reflecting the key role that senior management performs in this area. And, finally, for end users, the scores show a very broad range. The results show that 26% of responses suggest a rating of only 3 (slight to moderate) or less. Given that end users should sign and comply with these agreements, this level of awareness appears low. Despite this, 43% of respondents rated this question greater than or equal to 5 (very aware).

5.3.2.5 Security control clause 5: Physical and Environmental Security

Questions asked in the survey	Awareness Importance IT	 SM	 EU
Q9: How aware of the need to house information processing facilities in secure areas, do the stakeholder groups need to be?	5.82	5.39	3.77
Q10: How aware of physical and environmental threats, do the stakeholder groups need to be, to prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities?	5.74	5.50	4.62







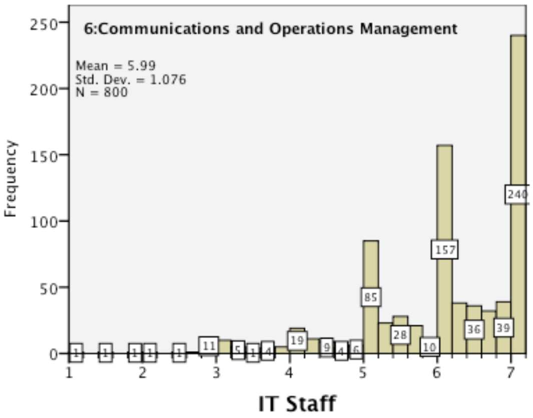
IT staff results show high levels of awareness importance, with 85% rated greater than or equal to 5 (very aware). The senior management results saw 76% rated greater than or equal to 5 (very aware).

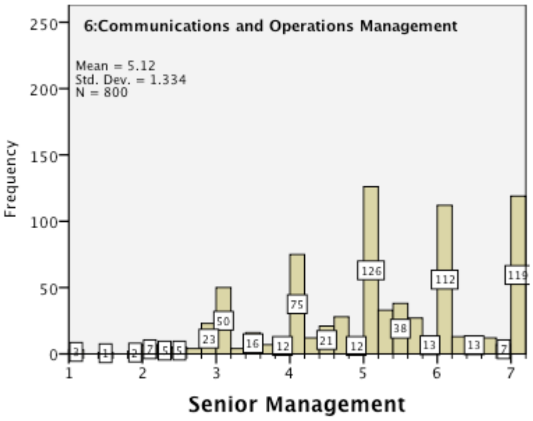
The results support an overall rating less than those for IT staff, although still quite high. For end users there is a broad spread of scores (some 1 and others 7), slightly biased to scores above 4. Some higher ratings could relate to the role end users play in disposal and re-use of equipment.

5.3.2.6 Security control clause 6: Communications and Operations

Questions asked in the survey	Awareness Importance		
	IT	SM	EU
Q11: How aware of formalising operational procedures and responsibilities, do the stakeholder groups need to be, so that the correct and secure operation of information processing facilities is managed?	5.67	5.31	3.97
Q12: How aware of implementing agreements and monitoring compliance, do the stakeholder groups need to be, so as to maintain the appropriate level of information security and service delivery in line with third party service delivery agreements?	5.54	5.74	3.94
Q13: How aware of system planning, capacity planning and acceptance testing, do the stakeholder groups need to be, in order to minimise the risk of systems failures?	6.15	5.13	3.47

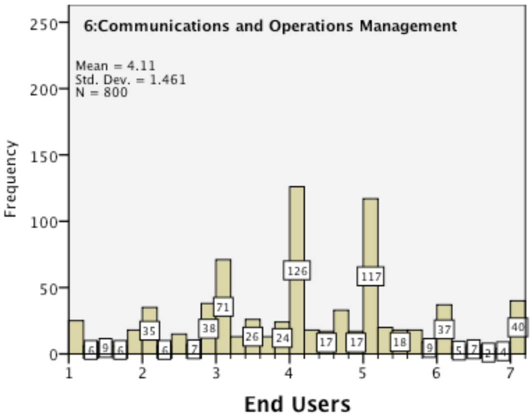
Q14: How aware of controls that provide protection against malicious and mobile code, do the stakeholder groups need to be, in order to protect the integrity of software and information?	6.24	5.13	4.38
Q15: How aware of the need and procedures for backing up information, do the stakeholder groups need to be, to ensure the integrity and availability of information and information processing facilities?	6.26	4.87	4.15
Q16: How aware of the controls for securing networks, do the stakeholder groups need to be, in order to protect information in networks and protect the supporting infrastructure?	6.27	4.72	3.47
Q17: How aware of the techniques required to protect removable media, do the stakeholder groups need to be, in order to minimise unauthorised disclosure, modification, removal or destruction of assets?	6.17	5.12	4.94
Q18: How aware of policies and procedures for exchanging information, do the stakeholder groups need to be, to preserve the security of any information or software exchanged within an organisation or with any external entity?	5.77	5.51	5.23
Q19: How aware of electronic commerce services, do the stakeholder groups need to be, to ensure the security of electronic commerce services, and their secure use?	5.72	5.04	4.16
Q20: How aware of system monitoring techniques, do the stakeholder groups need to be, to help detect and check the effectiveness of controls designed to prevent unauthorised information processing activities?	6.15	4.61	3.40





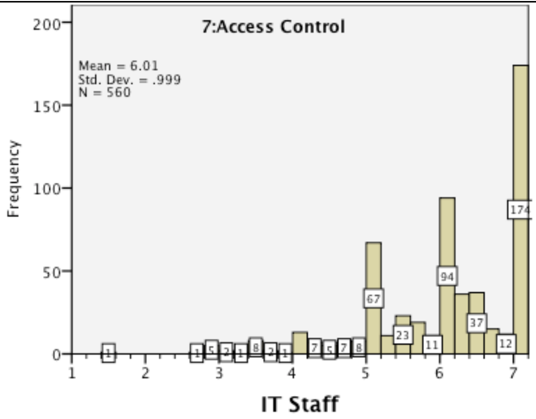
The results for IT staff show an average rating close to 6, with strong ratings also at the 7 level. This area is core to IT activities in an organisation and the results reinforce that level of ratings.

The senior management results show a broad spread of ratings. Higher ratings may be for particular questions within this section. For end users there is a broad spread of results, however, numerous ratings of both 7 and 1 were still obtained.



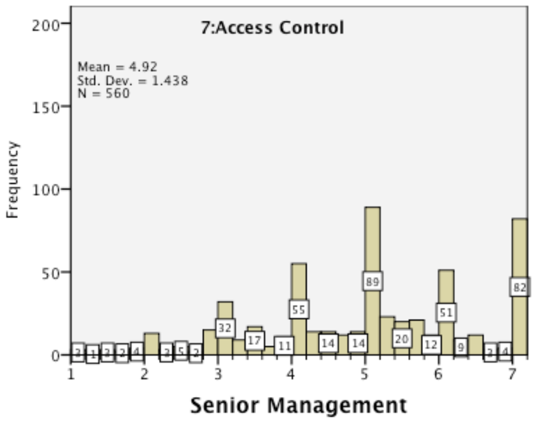
5.3.2.7 Security control clause 7: Access Control

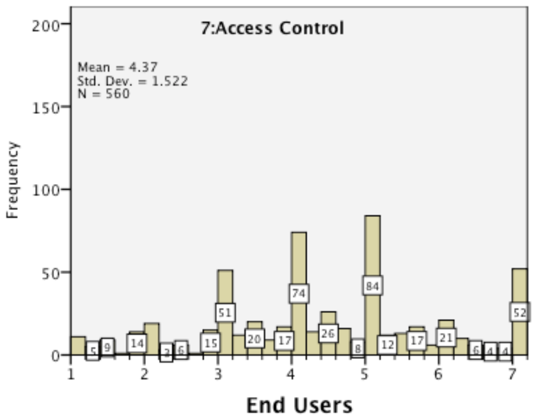
Questions asked in the survey	Awareness Importance		
	IT	SM	EU
Q21: How aware of business requirement and policies for information dissemination and authorisation, do the stakeholder groups need to be, in order to control access to information?	5.68	5.58	4.75
Q22: How aware of formal user access management procedures, do the stakeholder groups need to be, to ensure authorised user access and to prevent unauthorised access to information systems?	5.98	5.14	4.53
Q23: How aware of user responsibilities for maintaining effective access controls, do the stakeholder groups need to be, to prevent unauthorised user access, and compromise or theft of information and information processing facilities?	5.81	5.31	5.36
Q24: How aware of network access controls to internal and external networked services, do the stakeholder groups need to be?	6.14	4.45	3.73
Q25: How aware of operating system access controls, do the stakeholder groups need to be?	6.19	4.03	3.32
Q26: How aware of application and logical access controls, do the stakeholder groups need to be?	6.15	4.17	3.62
Q27: How aware of the risks associated with mobile computing and teleworking in an unprotected environment, do the stakeholder groups need to be?	6.12	5.77	5.27



The results for IT staff show an average of 6, with a strong number of responses also at the 7 level. The senior management results show a broad spread, many at the highest level of 7, but also many at a level of 3 and below.

Looking at the individual questions, those focused on business requirements are rated highly (average 5.6), whilst



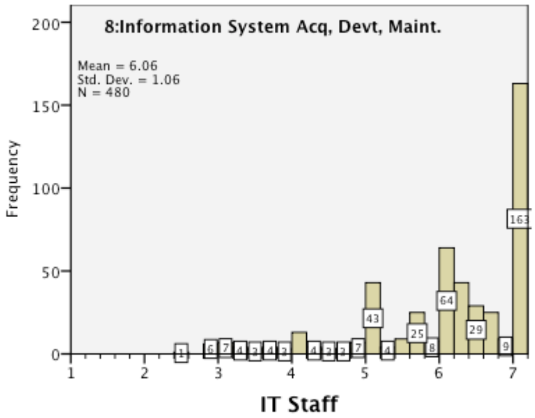


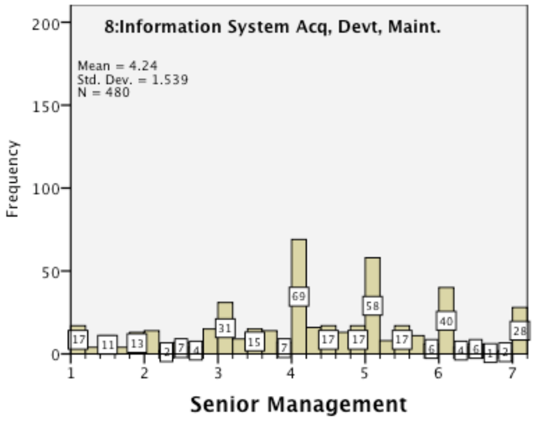
other more technically-focused questions are rated lower.

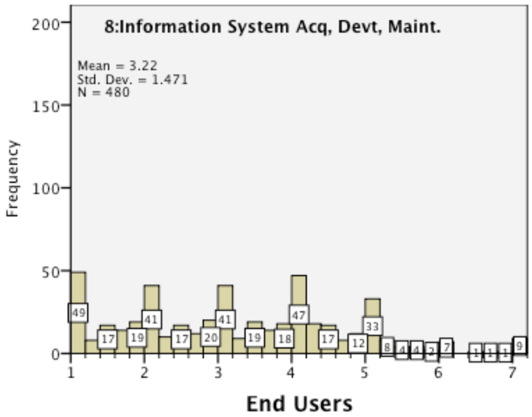
For end users there is also a broad spread of results; however, two of the questions averaged over 5 (5.35 and 5.28). These questions have a high level of relevance for end users, being *formal user access management* and *risks associated with mobile computing and teleworking*.

5.3.2.8 Security control clause 8: Information System Acquisition, Development & Maintenance

Questions asked in the survey	Awareness Importance IT	 SM	 EU
Q28: How aware of security requirements of information systems, do the stakeholder groups need to be, to ensure that security is an integral part of developing or acquiring information systems?	6.01	5.08	3.82
Q29: How aware of change and input validation controls, do the stakeholder groups need to be, to prevent errors, loss, unauthorised modification or misuse of information in applications?	5.84	4.32	3.67
Q30: How aware of cryptographic controls including key management, do the stakeholder groups need to be, to protect the confidentiality, authenticity or integrity of information?	6.08	4.00	3.02
Q31: How aware of security of system files and source code, do the stakeholder groups need to be?	6.10	3.77	2.80
Q32: How aware of the security of development and test environments, do the stakeholder groups need to be?	6.06	3.97	3.02
Q33: How aware of technical vulnerability management, do the stakeholder groups need to be, to prevent risks resulting from exploitation of published vulnerabilities?	6.24	4.30	3.00







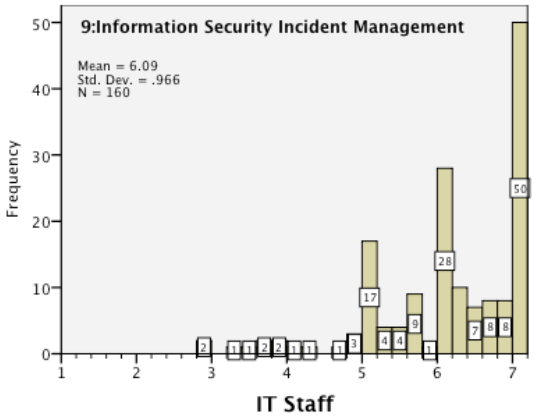
The results for IT staff show very strong ratings averaging over 6, with a high percentage rated at 7. Surprisingly, there are a number of scores rated below 4, but this rating appears in less than 5% of the responses.

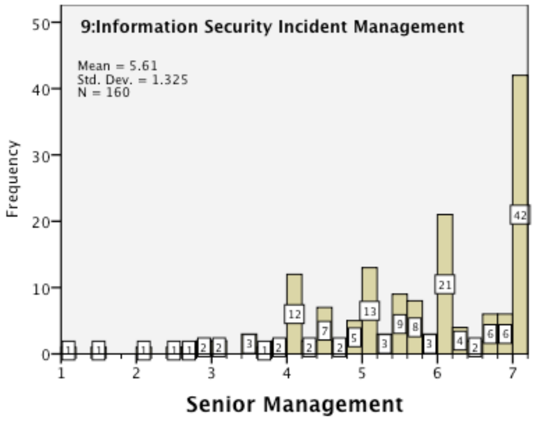
The results for senior management saw an average score rating just above 4 (moderate), with the highest individual question rating above 5 for *security requirements of information systems*.

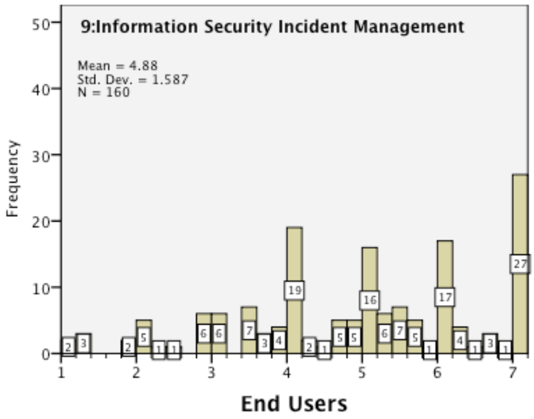
For end users there were generally low scores, however, some respondents still rated the importance above 5.

5.3.2.9 Security control clause 9: Information Security Incident Management

Questions asked in the survey	Awareness Importance IT	 SM	 EU
Q34: How aware of the need for timely reporting of information security events and weaknesses, do the stakeholder groups need to be, to allow timely corrective action to be taken?	6.13	5.62	5.28
Q35: How aware of the procedures and assignment of responsibilities to manage information security incidents and improvements, do the stakeholder groups need to be, to ensure a consistent and effective approach to the management of security incidents?	6.05	5.61	4.49







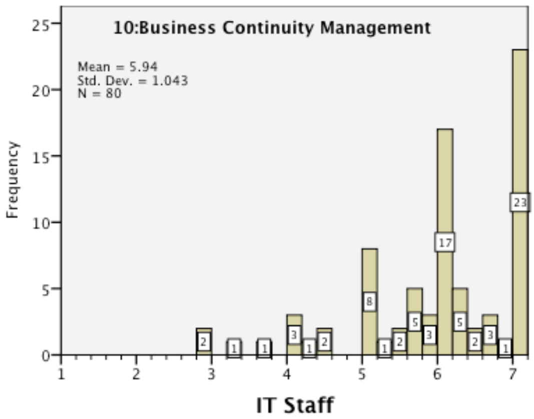
The results for IT staff show a very high percentage of ratings above 6.

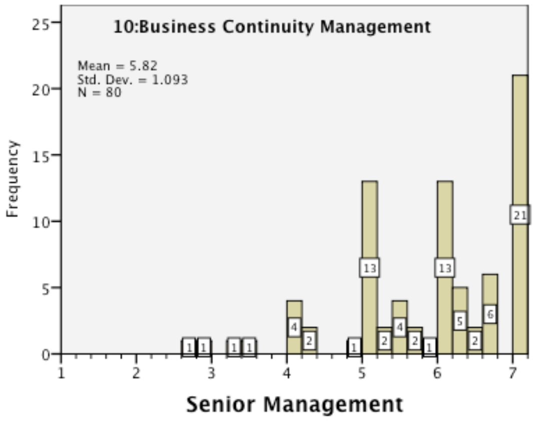
The senior management results are also quite high ratings; however, there are around 5% of respondents who rate this quite low (less than 3).

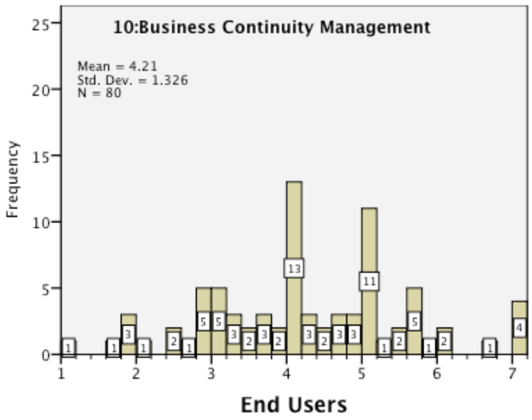
The ratings for end users also show reasonably high scores.

5.3.2.10 Security control clause 10: Business Continuity Management

Questions asked in the survey	Awareness Importance		
	IT	SM	EU
Q36: How aware of information security aspects of business continuity management, do the stakeholder groups need to be, to protect critical business processes from the effects of major failures of information systems?	5.94	5.82	4.21







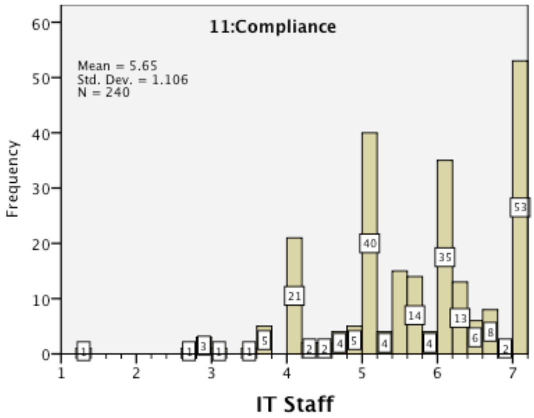
The results for IT staff saw a high level of awareness importance ratings reflected in the scores.

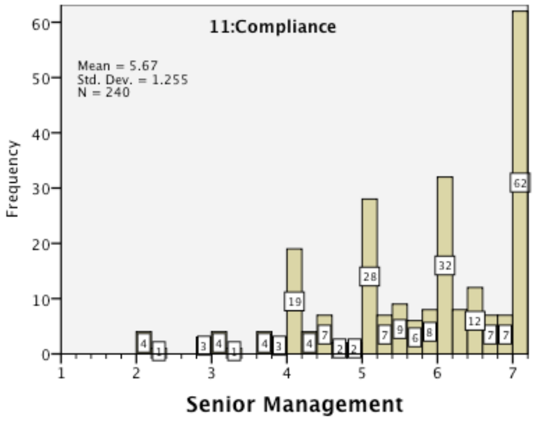
For senior management there are also strong ratings shown.

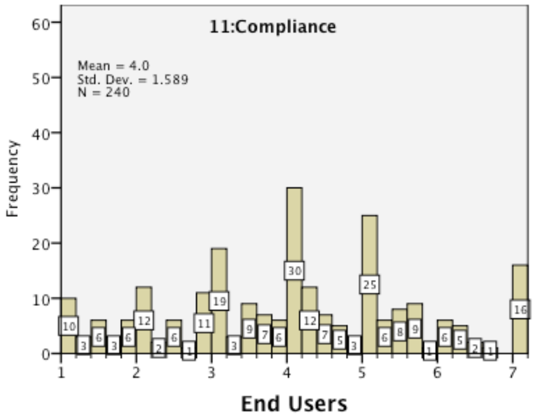
Finally, for end users, the ratings show a reasonable level of awareness is required.

5.3.2.11 Security control clause 11: Compliance

Questions asked in the survey	Awareness Importance		
	IT	SM	EU
Q37: How aware of compliance with legal requirements, do the stakeholder groups need to be, in order to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any related security requirements?	5.60	6.10	4.69
Q38: How aware of the need to formally review compliance of systems with organisational security policies and standards, do the stakeholder groups need to be?	5.75	5.68	3.87
Q39: How aware of controls to minimize interference to/from the information systems audit process, do the stakeholder groups need to be?	5.61	5.22	3.43







The results for IT staff show that IT is still best positioned to manage compliance with the assistance of senior management and IT risk and audit colleagues. The scores generally reflect this.

For senior management, compliance is a key responsibility for them and the scores generally reflect this.

The end user ratings saw varied responses.

5.4 Descriptive Statistics - Phase 2 Survey

The Methodology II Chapter 4 described this second survey's primary aim as deriving an awareness capability score. Each of the ten questions presented in this second survey were based on the awareness importance of specific aspects of the relevant security control clauses that were previously rated by information security experts as having the highest levels of awareness importance for end users (questions asked in phase 1 survey are shown in Table 4-1 on page 100). The subsequent ten survey questions developed for the second survey (to test for awareness capability) were broken down into three sub-questions, each aimed at examining a higher level of awareness, reflecting the cognitive information processing levels, Level 1 perception, Level 2 comprehension and Level 3 projection of situation awareness (SA) theory.

The second survey was distributed to two distinct populations. The first specific population was staff at an Australian university with a population of 900 staff members. This survey was conducted over a 5-week period, opening on 26th March 2015 and closing on 1st May 2015. The second population was the baseline population who were a survey panel of respondents provided by MyOpinions. This survey opened on 13th April 2015 and closed on 29th April 2015. This survey was targeted to end users who were using computing technology as part of their employment. The survey was delivered to the two population groups using the following approach:

- The Australian university staff received an email from their Senior Deputy Vice-Chancellor with details of the survey, including a link to the survey.
- The MyOpinions panel used their technology to deliver the survey to the respondents. It directed the respondents to the survey URL link.
- The survey presented to both populations contained the same elements, but separate surveys were used to keep responses of the two populations separate.

5.4.1 Survey completion rates and usable responses

Prior to performing detailed quantitative data analysis of the survey data, an initial assessment of the responses was conducted for both sample populations to ensure completeness of the survey responses. The total number of completed survey responses for both populations are shown below in Table 5-10.

Table 5-10 Survey completion rate

Survey population	Commenced Survey	Valid Surveys
Australian University	135	110
MyOpinions Panel	263	223

MyOpinions (an external organisation) provide a guaranteed 220 valid responses via a survey panel constructed for this research. MyOpinions matched the required profile of respondents aged over 18, employed, and using computing within their working environment. Quotas were set so that the level of responses was achieved and stratified proportionally for a national survey, whilst also restricting access to the survey once this quota had been achieved. However, there were 40 participants who did not complete the survey. To be consistent with the decision not to include incomplete survey responses in the data analysis of the phase 1 survey responses, the incomplete phase 2 survey responses were not included in the final data set for analysis, and 110 and 223 valid complete survey responses were used for the analysis.

5.4.2 Demographics of Survey 2 Respondents

This section presents the results of descriptive statistics from the valid responses for both survey populations. This includes the highest education level of the respondents, whether they have ever or currently work in an IT role, their level of digital literacy, the industry sector they work in, and the 10 questions (with 3 sub-questions) measuring awareness capability.

5.4.2.1 Australian university population

The breakdown of valid survey responses by highest educational level achieved, and whether respondents ever or currently work in an IT role, is shown in Table 5-11.

Table 5-11 Australian university survey – Demographics

	Currently in IT	Previously in IT	Never in IT	Grand Total
Secondary	1		3	4
Diploma	1	2	4	7
Undergraduate	5	2	20	27
Postgraduate	9	8	55	72
Grand Total	**16**	**12**	**82**	**110**

A high percentage of respondents (90%) were at least degree qualified, with 65% having post-graduate qualifications. There were 25% of respondents with current or previous experience working in an IT role. The survey also asked respondents to rate their level of digital literacy as a percentage out of 100 (see Table 5-12). This shows the average percentage of digital literacy increases in line with increasing highest education level. On average, the highest levels of digital literacy were for respondents currently working in an IT role.

Table 5-12 Australian university survey – Digital literacy

	Currently in IT	Previously in IT	Never in IT	Average
Secondary	68		44	56
Diploma	100	60	57	66
Undergraduate	85	60	68	69
Postgraduate	77	79	72	74
Average	**79**	**74**	**70**	**72**

5.4.2.2 MyOpinions panel population

The breakdown of valid survey responses by highest educational level achieved, and whether respondents had or currently work in an IT role, is shown in Table 5-13.

Table 5-13 MyOpinions panel respondents – Demographics

	Currently in IT	Previously in IT	Never in IT	Grand Total
Primary			4	4
Secondary	3	3	72	78
Diploma	3	4	51	58
Undergraduate	6	6	43	55
Postgraduate	7	4	17	28
Grand Total	**19**	**17**	**187**	**223**

Unlike the Australian university population, there is a much lower percentage (37%) of respondents who were at least degree qualified, and only 13% of respondents had postgraduate qualifications (compared to 65% at the Australian university). There were also only 16% of the respondents with current or previous experience of working in an IT role. The survey also asked respondents to rate their level of digital literacy as a percentage out of 100. These results are shown below in Table 5-14. The average percentage of digital literacy is highest with those with postgraduate qualifications, but no significant trend exists between respondents currently working or not working in an IT role.

Table 5-14 MyOpinions panel respondents – Digital literacy

	Currently in IT	Previously in IT	Never in IT	Average
Primary			86	86
Secondary	64	72	70	69
Diploma	66	84	73	73
Undergraduate	63	57	70	69
Postgraduate	84	63	77	76
Average	**71**	**69**	**72**	**71**

The MyOpinions panel survey captured the responses of end users across a range of industry sectors that they are employed in. The survey respondent count across each of these industry sectors is shown below in Table 5-15.

Table 5-15 MyOpinions panel – Sector count of responses

	Currently in IT	Previously in IT	Never in IT	Grand Total
Accommodation, restaurants			8	8
Agriculture			5	5
Communications services			4	4
Construction		3	5	8
Cultural and recreational			1	1
Education	2	2	23	27
Electricity gas water			3	3
Finance and insurance	1		11	12
Government and defence	1	2	11	14
Health & Community services		2	31	33
Manufacturing			10	10
Mining			5	5
Other	10	2	31	43
Personal and other services		1	2	3
Property & business services	1		6	7
Retail trade	3	3	23	29
Transport and storage	1	1	7	9
Wholesale trade		1	1	2
Grand Total	**19**	**17**	**187**	**223**

The average digital literacy across industry sectors is shown below in Table 5-16 and indicates some variance in the digital literacy of survey respondents across sectors.

Table 5-16 MyOpinions panel – Sector percentage of digital literacy

	Currently in IT	Previously in IT	Never in IT	Grand Total
Accommodation, restaurants			70	70
Agriculture			53	53
Communications services			83	83
Construction		82	74	77

	Currently in IT	Previously in IT	Never in IT	Grand Total
Cultural and recreational			81	81
Education	83	71	77	77
Electricity gas water			85	85
Finance and insurance	98		68	70
Government and defence	76	62	63	63
Health & Community services		71	61	62
Manufacturing			69	69
Mining			72	72
Other	70	63	70	70
Personal and other services		94	77	82
Property & business services	50		76	72
Retail trade	64	78	61	63
Transport and storage	95	64	56	61
Wholesale trade		71	73	72
Grand Total	**72**	**73**	**68**	**69**

5.5 Deriving the Awareness Capability scores

The aim of the phase 2 survey data collection was to derive the awareness capability scores based on questions constructed for the top 10 rated awareness importance main security categories as determined in phase 1 survey. This awareness capability score comprised of three sub-questions, with a total possible score across these sub-questions of 7. The scoring approach applied was shown in Figure 4-2 on page 115 and involves allocating certain scores to the various answers based on the level of situation awareness being captured. Deriving the awareness capability measure was carried out by adding the scores of the three sub-questions to arrive at a total awareness capability score for that overall question.

A total awareness capability score for the overall survey (10 survey questions each with three sub-questions) was calculated per respondent. An extract of this data (of eight individual respondents' scores) is shown below in Table 5-17. This scoring technique was applied to both survey populations; the Australian university and the MyOpinions panel populations.

Table 5-17 Awareness Capability extract

Response No.	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Survey Total
#1	2	0.5	0.5	4.5	2	2	4.5	2.5	1	3	22.5
#2	2	3	1	7	3	5	7	2	5	7	42.0
#3	4.5	7	7	7	7	7	4.5	5.5	4	7	60.5
#4	4.5	0.5	0.5	1	4.5	7	5.5	4	7	5.5	40.0
#5	3	7	7	5.5	7	5	7	7	7	7	62.5
#6	3.5	7	7	4	7	5	7	5	7	7	59.5
#7	7	7	7	7	7	7	4.5	7	7	7	67.5
#8	4.5	7	7	6	7	7	7	7	5	7	64.5

Once all the individual scores had been allocated to each of the responses, and the total per respondent calculated, this allowed for an organisational view to be achieved by averaging the question scores across all respondents for each of the 10 questions. The overall results of calculating this are shown below in Table 5-18.

Table 5-18 Overall Awareness Capability – Summary by survey population

Population	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total
Australian University	3.3	4.7	3.9	5.2	4.8	5.1	4.9	4.3	4.1	4.8	45.2
MyOpinions Panel	2.8	3.4	3.0	3.8	4.1	3.4	3.4	3.2	3.4	3.6	34.4

For each of the 10 questions, the average awareness capability scores for the Australian university population were higher than the average obtained from respondents to the MyOpinions panel population. This was not an unexpected result given the Australian university population had a higher digital literacy score overall. These results are graphically illustrated below in Figure 5-5.

5.5.1 Situation Awareness profile of responses

Whilst the total scores per question derived by adding the scores of the three sub-questions provides the overall score for awareness capability (shown above), analysis of the responses on a 'by sub-question' basis helps provide a perspective on whether the respondents are achieving the level 1, level 2 or level 3 stages of Situation Awareness (SA). As outlined in Chapter 4, the structure of the sub-questions reflected the three levels of SA. So sub-question 1 broadly targeted a situation awareness of level 1; sub-question 2 targeted level 2 situation awareness; and sub-question 3 equated to level 3 situation awareness.

Sub-question 1 had a maximum score of 2, whilst sub-question 2 and sub-question 3 each had maximum scores of 2.5. In general terms, an overall score of 2 signified full level 1 attainment (perception), 4.5 signified full level 2 attainment (comprehension), and 7 signified full level 3 attainment (projection). When looking at an average of all respondents, per questions, and per population samples, Figure 5-5 shows the results from both of the phase 2 surveys, highlighting the boundaries of the various levels of situation awareness.

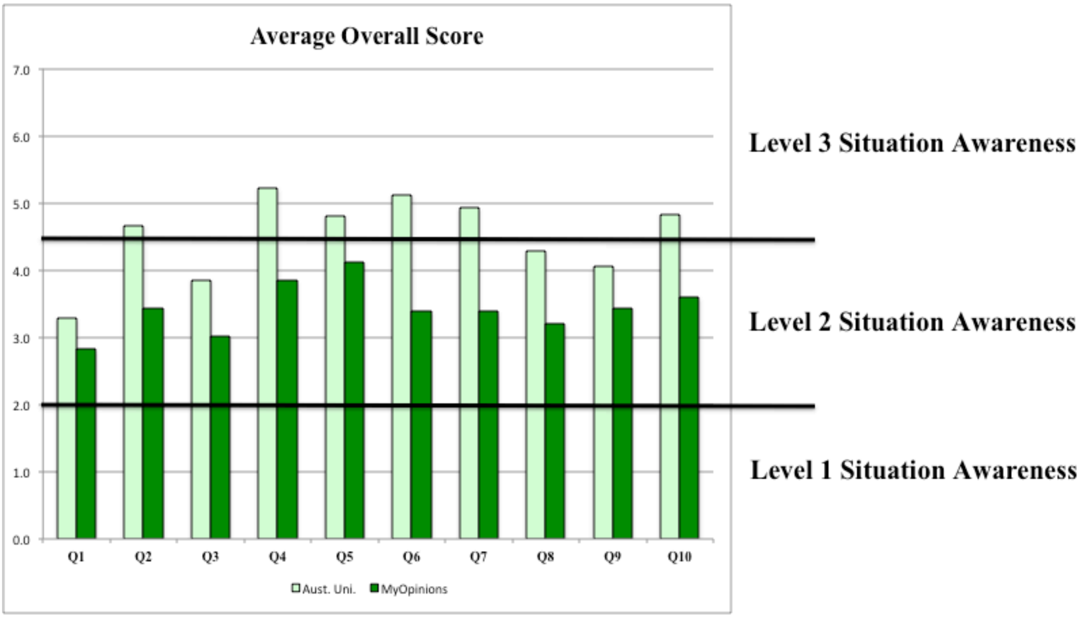


Figure 5-5 Attainment of SA levels

For the MyOpinions panel population, the results show that level 3 situation awareness was not achieved when looking at the population average for any of the 10 questions. This contrasts with the survey respondents of the Australian university population, which overall achieved average scores that fall into level 3 of SA for 60% of the questions. With the sub-questions developed to sequentially test the 3 levels of SA, the percentage of respondents who at least displayed some level of awareness in each of the three sub-questions were also examined. A survey respondent having a non-zero score for a sub-question reflects that they have some level of that SA. This analysis could help organisations determine where on the SA journey their employees are in terms of developing their SA.

Figure 5-6 below shows the percentage of L1, L2 and L3 for each question where some level of SA was shown. The y-axis reflects the percentage of the total score for that sub-question that was achieved. The x-axis shows all of the sub-questions, grouped by their main question number. The general trend is that there is a higher percentage for sub-question 1 (i.e. Q2.1) than for sub-question 2 (i.e. Q2.2) which, in turn, is higher than sub-question 3 (i.e. Q2.3).

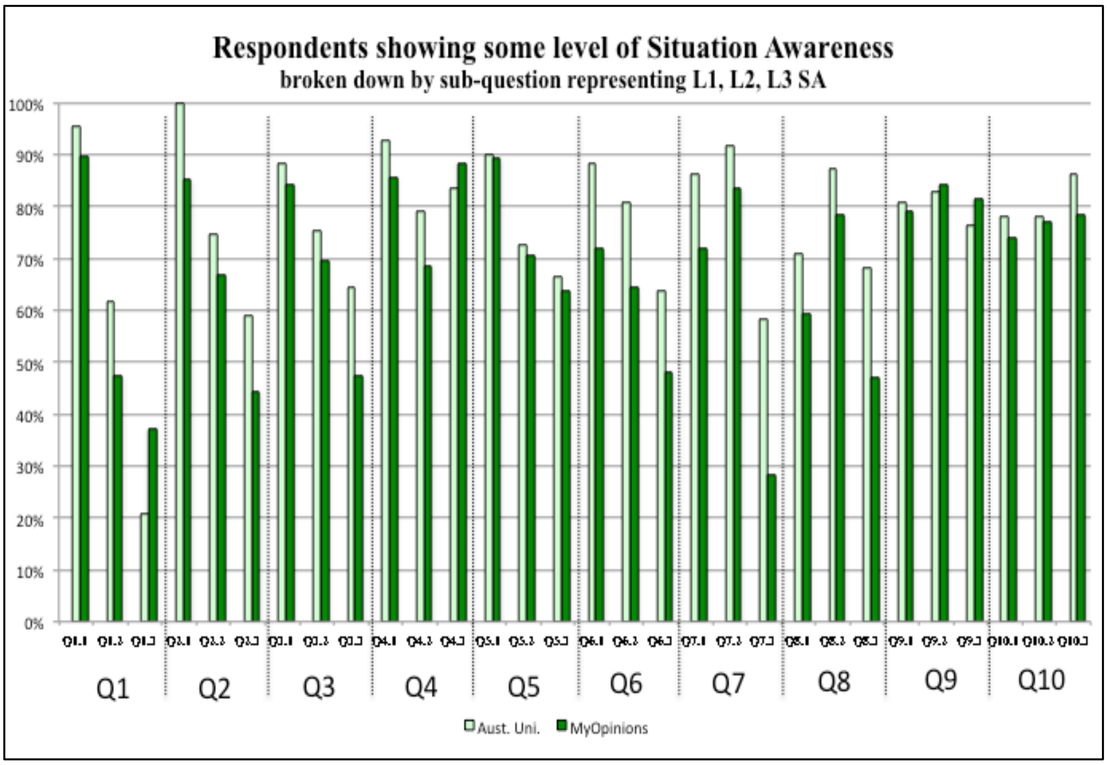


Figure 5-6 Respondents showing some level of SA

5.5.2 Patterns of data for Awareness Capability

Section 4.4 on page 114 described the scoring mechanism that was applied to the responses for phase 2 survey. The first sub-question (Level 1 SA) is assigned a maximum score of 2. The second sub-question (Level 2 SA) is assigned a maximum score of 2.5. And the third sub-question (Level 3 SA) is assigned a maximum of 2.5. The overall maximum score is 7.

The results of the second phase survey data collection, including the responses at a sub-question level, are examined below. The sub-questions that were asked are shown, as well as the derived awareness capability ratings for these sub-questions, and the overall awareness capability ratings. The table heading refers to the relevant security categories (i.e. *User Responsibilities*) from the ISO/IEC 27002 standard.

Table 5-19 User Responsibilities

Questions asked in the second survey	**Awareness Capability**	
	Aust. Uni.	**MyOpinions**
Q1.1: A work colleague has asked you for your computer access password because they are having troubles getting their computer access set up. What would you do?	1.42	1.26
Q1.2: Do you use the same password for multiple systems, say for your personal email account and your work accounts?	1.51	1.13
Q1.3: Is a passphrase better to use than just a set of characters and numbers in your password?	0.36	0.45
Average Total score for Question 1 (Max 7)	3.29	2.83

Whilst a majority of respondents indicated they would not share their passwords (L1 SA), a high percentage of respondents indicated that they would share their password under certain circumstances (i.e. in an emergency). There is greater recognition of the risks of using the same password for personal and work related accounts (L2 SA) by the Australian university respondents; however, this was not the case with the MyOpinions respondents. The use of a passphrase (L3 SA) and the benefits (password of significant length, easily remember) did not register greatly with either of the survey populations. The scores demonstrated poor level of awareness.

Table 5-20 Reporting Information security events and weaknesses

Questions asked in the second survey	**Awareness Capability**	
	Aust. Uni.	**MyOpinions**
Q2.1: Would you be able to recognise a potential computer incident (i.e. virus, spam, infected web site) and do you know what to do?	1.54	1.09
Q2.2: You have taken some work related data home on an unencrypted USB device. It has some customer related data on it. However you can't find the USB device. What would you do?	1.80	1.47
Q2.3: Do you know what social engineering is and can it lead to security incidents?	1.34	0.88
Average Total score for Question 2 (Max 7)	4.67	3.44

Australian university respondents showed good levels of awareness of security incidents (L1 SA), including escalation processes; however, the level was much lower for MyOpinions respondents. A very high level of awareness of risks related to data on portable unencrypted memory devices (L2 SA) and reporting data loss incidents was shown by the Australian university respondents, with a majority of the MyOpinions respondents also showing good levels of awareness.

Average levels of social engineering awareness (L3 SA) were displayed by Australian university respondents, while a much lower level of awareness was shown by MyOpinions respondents in relation to social engineering. This lower level of awareness puts at risk both populations to social engineering style cyber attacks.

Table 5-21 Mobile computing and teleworking

Questions asked in the second survey	**Awareness Capability** **Aust. Uni.**	 **MyOpinions**
Q3.1: Is it OK to connect your work computer to a public Internet service such as those offered by Starbucks or public Libraries?	1.09	0.88
Q3.2: Why is it important to have an encrypted hard drive on any computer used away from the office?	1.53	1.37
Q3.3: How does a VPN connection provide you with security when connecting with your work or other companies?	1.23	0.77
Average Total score for Question 3 (Max 7)	3.85	3.02

A slight majority of Australian university respondents believe it is safe to connect to their work environment from a public Internet connection using a VPN connection (L1 SA), whilst the majority of MyOpinions respondents believe it is unsafe to do so. This could limit the ability of these staff members to securely work remotely if they do not understand safe ways to do so. There is good awareness of the importance of encrypted hard drives (L2 SA) when using a portable computer for both populations of respondents. The level of understanding of the benefits of a VPN (L3 SA) was higher for the Australian university respondents than for the MyOpinions panel population. This awareness was undoubtedly also reflected in the responses to Q3.1.

Table 5-22 Exchange of information

Questions asked in the second survey	**Awareness Capability** **Aust. Uni.**	 **MyOpinions**
Q4.1: You are working on analysing some customer data that you have access to in order to determine customer profitability. Is it OK to share this information with other people within your organisation?	1.50	1.19
Q4.2: Your organisation uses an external company to do its letter mail out (physical and email) to customers. Is this secure?	1.92	1.28
Q4.3: When exchanging electronic information with another organisation, you should ensure that ...	1.80	1.37
Average Total score for Question 4 (Max 7)	5.22	3.85

A good level of awareness of the risks of sharing data (L1 SA) was displayed by both populations of respondents in terms of data owners providing approvals, although many of the scores were much higher for the Australian university respondents. The Australian university respondents also displayed a high level of awareness regarding the use of external organisations to provide external communications on behalf of their organisation (L2 SA). They recognised that this can be done securely if suitable formal agreements and third party assessments have been put in place. There was a slight majority of MyOpinions respondents who also recognised this could be done safely, although this was lower than the Australian university respondents.

The Australian university respondents displayed high levels of awareness on how to securely exchange information with another organisation (L3 SA). They recognised the importance of exchange agreements being put in place, as well as the appropriate security mechanisms. Slightly more than half of MyOpinions respondents also demonstrated some level of awareness.

Table 5-23 Media handling

Questions asked in the second survey	Awareness Capability Aust. Uni.	 MyOpinions
Q5.1: What is the best way to dispose of unwanted data contained on media such as a dvd, usb stick, magnetic tape?	1.70	1.50
Q5.2: You are required to work on a sales presentation spreadsheet over the weekend. Because of the sensitive nature of the information you know not to send it home via email. Instead you load it onto a USB memory stick. Is that safe?	1.59	1.36
Q5.3: You are responsible for the disposal of photocopying machines. Are there any security related things that you need to do before you dispose of them?	1.53	1.27
Average Total score for Question 5 (Max 7)	4.81	4.12

There are good levels of awareness demonstrated by both populations of survey respondents for the secure methods of disposing of portable magnetic media (L1 SA), such as secure erasure and physical destruction. This good level of awareness continues with the understanding of the risks of sending sensitive data via email compared with transporting it via an appropriately encrypted USB memory device. Whilst the levels of awareness decrease for risks associated with disposing of non-traditional data stores (L3 SA) such as photocopiers (using secure wiping techniques), awareness is still displayed by some respondents in both populations.

Table 5-24 Information classification

Questions asked in the second survey	Awareness Capability Aust. Uni.	 MyOpinions
Q6.1: Is it important for your organisation to have data/information classification rules and if so why?	1.76	1.33
Q6.2: How does information classification influence access controls?	1.88	1.10
Q6.3: What are the key risks for your organisation if it has correctly classified information?	1.48	0.96
Average Total score for Question 6 (Max 7)	5.12	3.39

There are good levels of awareness of information classification (L1 SA) from the Australian university respondents, but lower levels of awareness among the MyOpinions respondents. This may be reflective of organisational awareness being raised within the Australian university, whereas the MyOpinions respondents represent many different organisations. Australian university respondents demonstrated good awareness of how information classification impacts on access controls (L2 SA), whereas the level of awareness falls for the MyOpinions respondents. The awareness of key risks (L3 SA) such as authorised users making the data available (accidently or deliberately) to non-authorised users, drops to a lower level for both groups of respondents, although it is much lower for the MyOpinions respondents.

Table 5-25 Business requirements for access control

Questions asked in the second survey	Awareness Capability Aust. Uni.	 MyOpinions
Q7.1: Who should determine the level of access to data within your organisation?	1.47	1.04
Q7.2: What is the greatest risk to your organisation if access is not based on business requirements?	2.00	1.64
Q7.3: What do you understand about the term "separation of duties" and it's importance to your organisation?	1.45	0.71
Average Total score for Question 7 (Max 7)	4.93	3.39

Australian university respondents demonstrate good levels of awareness regarding who should be involved in determining the levels of access to data (L1 SA). However, the level of awareness for MyOpinions respondents is much lower. Both groups of respondents demonstrate good awareness of risks to the organisation if access controls are not based on business requirements (L2 SA), such as either too much or too little access. Finally, an understanding of a key business control (separation of duties) was poorly scored by MyOpinions respondents, with only an average level of understanding demonstrated by Australian university respondents.

Table 5-26 Compliance with legal requirements

Questions asked in the second survey	Awareness Capability Aust. Uni.	 MyOpinions
Q8.1: Who within your organisation should be responsible for understanding how to comply with legal requirements?	1.14	0.97
Q8.2: What do you know about data privacy?	1.50	1.15
Q8.3: Why are there laws regarding the use of encryption software?	1.64	1.08
Average Total score for Question 8 (Max 7)	4.28	3.20

There was only an average level of understanding as to who (i.e. business managers) within an organisation should be responsible for compliance with legal requirements (L1 SA). There was greater awareness of data privacy (L2 SA) such as the government published privacy principles, demonstrated by the Australian university respondents, whilst the level of awareness by MyOpinions respondents was low. The legal aspects associated with encryption software (L3 SA), such as the exporting of encryption technology and the transmission of data using encryption techniques, were understood much better by the Australian university respondents than by the MyOpinions respondents.

Table 5-27 Responsibility for assets

Questions asked in the second survey	Awareness Capability Aust. Uni.	 MyOpinions
Q9.1: Who should be responsible for owning technology related assets?	1.41	1.04
Q9.2: Who should be responsible for maintaining and updating an asset register of technology assets?	1.50	1.02
Q9.3: Who should be setting the policy of acceptable use for a computing asset?	1.15	1.38
Average Total score for Question 9 (Max 7)	4.06	3.44

Australian university respondents demonstrated a good level of awareness of the benefits of shared ownership for technology assets (L1 SA), however, the levels for the MyOpinions respondents were much lower. Similar results were obtained in terms of responsibilities for maintaining asset registers (L2 SA). Interestingly, the awareness for setting the acceptable use policies (L3 SA) by the business owner was higher with the MyOpinions respondents than with the Australian university respondents. This may reflect the practices implemented at the Australian university, such as having a dedicated team (rather than business managers) that is responsible for developing and owning university-wide policies.

Table 5-28 Equipment security

Questions asked in the second survey	**Awareness Capability**	
	Aust. Uni.	**MyOpinions**
Q10.1: What controls provide the best protection for essential computer equipment against power disruptions?	1.00	0.71
Q10.2: When disposing of computer equipment, what key information security step is required to be done?	1.90	1.59
Q10.3: From an information security perspective, what is the most important reason to protect remotely located computer equipment?	1.93	1.29
Average Total score for Question 10 (Max 7)	4.84	3.59

Controls aimed at protecting against power disruptions, such as the use of (uninterrupted power supplies) UPS with diesel generator backup (L1 SA) resulted in only an average level of understanding by the Australian university respondents; and lower levels of awareness by the MyOpinions respondents. Secure disposal techniques for unwanted computer equipment (L2 SA) was well-understood by a majority of both populations. The Australian university respondents also displayed a high level of awareness of why remote computer equipment should be well protected. The MyOpinions respondents demonstrated an average level of awareness regarding this particular aspect.

5.6 Deriving the Awareness Risk scores

In this section an explanation is provided of how the final element of the ISACM, Awareness Risk, is calculated. As described earlier in section 4.5 on page 116, the following formulae are used to calculate the awareness risk measurement.

$AR = AI - AC$ where AI = Awareness Importance; AC = Awareness Capability; AR = Awareness Risk

The measurement's focus is on the gap between desired (importance) behaviour/action compared to what is observed (capability). The desired importance is reflected in the awareness importance measure, which was determined from an analysis of phase 1 survey data collection. The capability that the respondents are demonstrating is reflected in the awareness capability measure, which was determined from analysis of phase 2 survey data.

A positive score for awareness risk occurs when the awareness importance score is greater than the awareness capability score. When this occurs it indicates an undesirable level of risk for an organisation. The awareness importance (AI) measures for the top 10 end user main security categories from survey 1 were presented earlier in Table 4-1 on page 100. The corresponding awareness capability (AC) measures for these questions (for both the Australian university population and the MyOpinions panel population) were shown earlier in this chapter in Table 5-18. These awareness capability scores determined from these two population surveys are summarised and compared against the relevant awareness importance ratings as shown below in Table 5-29.

Table 5-29 Awareness Risk measure for end users

Phase 1 Survey				Phase 2 Survey	Aust. Uni.		MyOpinions	
Security Control Clauses	**Main security categories**	**AI Question**	**AI**	**AC Question**	**AC**	**AR**	**AC**	**AR**
Access Control	User Responsibilities	Q23	5.36	Q1	3.29	2.07	2.83	2.53
Information Security Incident Management	Reporting Information security events and weaknesses	Q34	5.28	Q2	4.67	0.61	3.44	1.84
Access Control	Mobile computing and teleworking	Q27	5.27	Q3	3.85	1.42	3.02	2.25
Communications and Operation Management	Exchange of information	Q18	5.23	Q4	5.22	0.01	3.85	1.38
Communications and Operation Management	Media handling	Q17	4.94	Q5	4.81	0.13	4.12	0.82
Asset Management	Information classification	Q5	4.89	Q6	5.12	-0.23	3.39	1.50
Access Control	Business requirements for access control	Q21	4.75	Q7	4.93	-0.18	3.39	1.36
Compliance	Compliance with legal requirements	Q37	4.69	Q8	4.28	0.41	3.20	1.49
Asset Management	Responsibility for assets	Q4	4.65	Q9	4.06	0.59	3.44	1.21
Physical & Environmental Security	Equipment security	Q10	4.62	Q10	4.84	-0.22	3.59	1.03
a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*

Legend: Each row of Table 5-29 is explained by the following columns and accompanying legend below:

a) Relevant security control clause from ISO/IEC 27002 standard this question was related to.
b) Relevant main security category from ISO/IEC 27002 standard this question was related to.
c) Question number presented in phase 1 survey for assessing awareness importance (AI).
d) Awareness Importance score for the top 10 end user questions.
e) Question number (including its 3 sub-questions) posed in phase 2 survey to assess the top 10 end user questions from phase 1 survey.
f) Awareness Capability score derived in phase 2 survey for the Australian university population.
g) Awareness Risk score derived for the Australian university population.
h) Awareness Capability score derived in phase 2 survey for the MyOpinions panel population.
i) Awareness Risk score derived for the MyOpinions panel population.

The following results for awareness risk for both the population groups are apparent from Table 5-29. They are an average across the respective phase 2 survey respondents. It is important to highlight the difference and purpose of the two populations that were surveyed. The Australian university survey respondents are a specific organisation; while the MyOpinions survey respondents are a more general population and provide a baseline awareness capability score for working populations in general.

Negligible risk

For the Australian university respondents, four out of the 10 questions in Table 5-29 show awareness risk being non-existent (negative) or negligible (0.01). This shows that sufficient or more than sufficient awareness is being demonstrated (capability) when compared to what is required (importance). These results may confirm areas where awareness raising has been (successfully) conducted, or where staff recruited into the Australian university have this as pre-requisite knowledge. In contrast to the Australian university respondents, none of the 10 questions show awareness risk as being non-existent across the MyOpinions survey respondents.

This shows that insufficient awareness is being demonstrated (capability) across the MyOpinions survey respondents when compared to what is required (importance). These scores may represent the levels of awareness capability that exist in the absence of additional awareness that is provided at an organisational level.

Low risk

For the Australian university respondents, four out of 10 questions show low awareness risk of between 0.01 and 0.61. This highlights areas where additional awareness raising is required, however, the level of risk reduction will not be significant. In contrast, only one out of 10 questions for the MyOpinions panel show low levels of risk at 0.82 across the survey respondents.

Medium risk

For the Australian university respondents, the final two out of 10 questions show awareness risk greater than 1.42. These would be an area of priority for the Australian university to invest in further awareness raising. For the MyOpinions survey respondents, seven out of 10 questions show awareness risk being prominent across the survey respondents - between 1 and 2.

High risk

Australian university respondents on average did not demonstrate any high level of risk. In contrast, two out of 10 questions for the MyOpinions panel show high awareness risk being more prominent across the survey respondents and greater than 2.25. Whilst numerical results point organisations to areas of greater risk (higher positive values for awareness risk), analysing the detailed answers may provide insight for organisations as to where more awareness raising needs to be undertaken.

For both the MyOpinions survey respondents and Australian university survey respondents, phase 2 survey *questions 1 and 3* exhibited the highest levels of awareness risk. Interestingly, these two questions respectively are linked to the highest level of awareness importance (5.36) from phase 1 survey question 23 and the third highest level of awareness importance (5.27) from phase 1 survey question

27. Hence, these two questions not only present the highest gaps between importance and capability, but also occur in those areas requiring the highest levels of awareness capability for end users.

5.6.1 In-depth analysis of areas of highest Awareness Risk

Analysing these top two questions in further detail could provide organisations with insight as to why the required level of awareness capability is not being displayed. Because the sub-questions present varying options that could be chosen by the respondents, awareness raising could be tailored based on the respondents' choices. For example, Figure 5-7 below shows respondents would share their password 'but would change it immediately afterwards'. Awareness of what risks this still presents could be included in the awareness material. Additionally, risks associated with sharing a password 'only in an emergency' could be minimised by providing additional awareness of what to do in an emergency. The following provides a breakdown of the sub-questions and the responses selected.

5.6.1.1 Awareness Capability question 1

Figure 5-7 below shows that 63% of Australian university respondents (and 54% of MyOpinions respondents) would not share their password. This leaves 37% of Australian university respondents (and 46% of MyOpinions respondents) indicating they would share their password under a variety of circumstances. Interestingly, of those who would share their password, approximately 20% of both respondent groups believe it is acceptable to share it provided they changed their password immediately after sharing. Only a minimal number of respondents indicated that they would share their password with their boss.

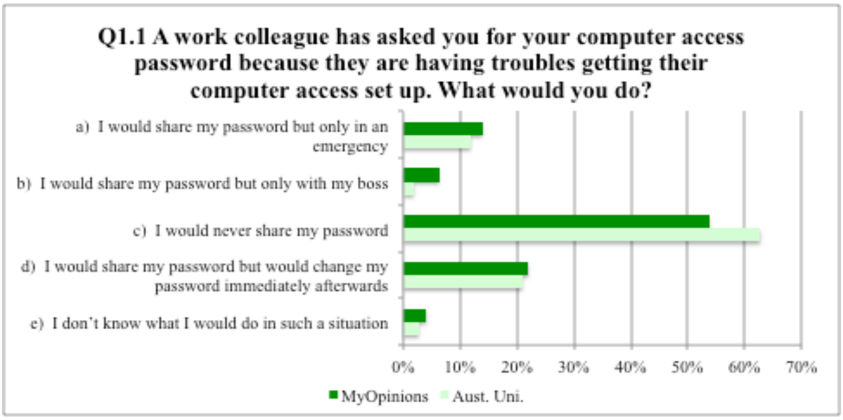


Figure 5-7 Awareness Capability Question 1.1

Figure 5-8 below shows that 36% of Australian university respondents (and 46% of MyOpinions respondents) use the same password for multiple systems, across personal and work accounts. Among the Australian university respondents, 21% (and 27% of MyOpinions respondents) do so because 'their password is strong enough and it is too difficult to remember so many passwords'. A further 15% of Australian university respondents (and 19% of MyOpinions respondents) do so because they believe that since they do not write down their password it cannot be guessed.

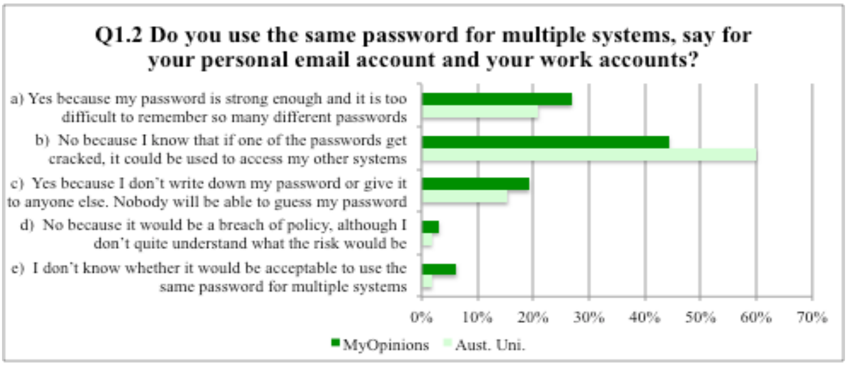


Figure 5-8 Awareness Capability Question 1.2

Figure 5-9 below shows that 65% of Australian university respondents (and 48% of MyOpinions respondents) do not understand what a passphrase is, or the benefits passphrases provide such as using very long passwords that are difficult to guess but are easy for the end user to remember. Within both populations, 15% of respondents believe that any length password, provided it is changed regularly, will be as secure as using a passphrase.

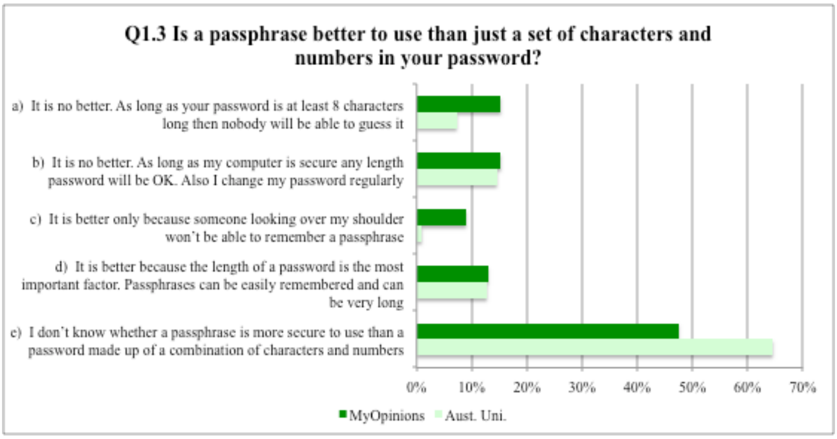


Figure 5-9 Awareness Capability Question 1.3

5.6.1.2 Awareness Capability question 3

Figure 5-10 below shows 63% of Australian university respondents (but a much lower 46% of MyOpinions respondents) believe it is safe to connect work computers to the corporate network via a public Internet service. However, only 35% of Australian university respondents (but a much lower 15% of MyOpinions respondents) identified the benefits that connecting via a VPN connection provided them. Many others (28% of Australian university and 23% of MyOpinions respondents) were only concerned that virus protection and software were up-to-date before connecting.

In contrast, a large percentage (25% for Australian university and a very large 46% for MyOpinions respondents) believed it was never acceptable to connect via public Internet services.

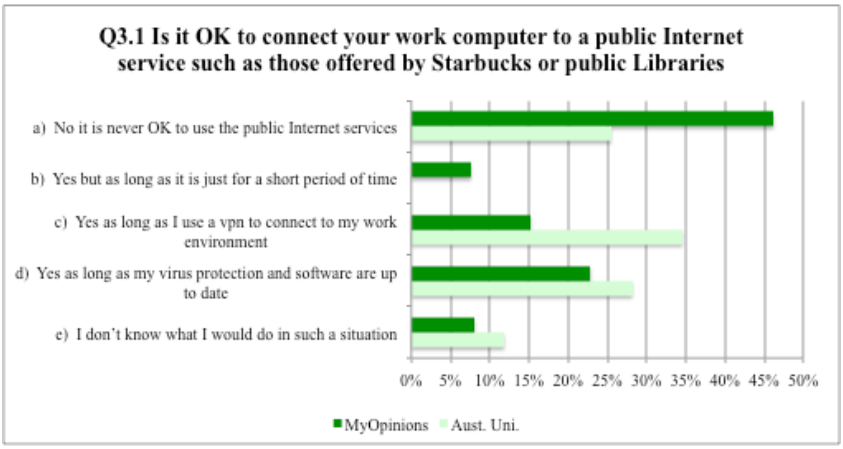


Figure 5-10 Awareness Capability Question 3.1

Figure 5-11 below shows that 52% of Australian university respondents (and 46% of MyOpinions respondents) correctly identified the benefits of hard disk encryption. However, 24% of respondents from both populations associated encryption with logical access control and authorised access. Approximately 20% of respondents from both populations were unaware of the benefits of hard disk encryption.

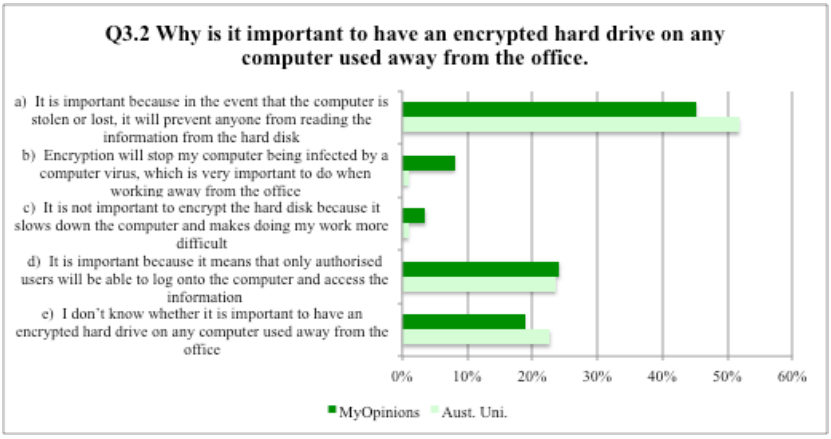


Figure 5-11 Awareness Capability Question 3.2

Figure 5-12 below shows that 45% of Australian university respondents (but a much lower 26% of MyOpinions respondents) recognised the full benefits of using a VPN connection; whilst another 17% of respondents from both populations associated this with authorised access control. A large percentage (35% of Australian university and 42% of MyOpinions respondents) were unaware of what benefits a VPN connection could provide. Interestingly, 10% of the MyOpinions respondents incorrectly believed that the use of a VPN would prevent their computer from being infected by a virus from the connecting computer system or network.

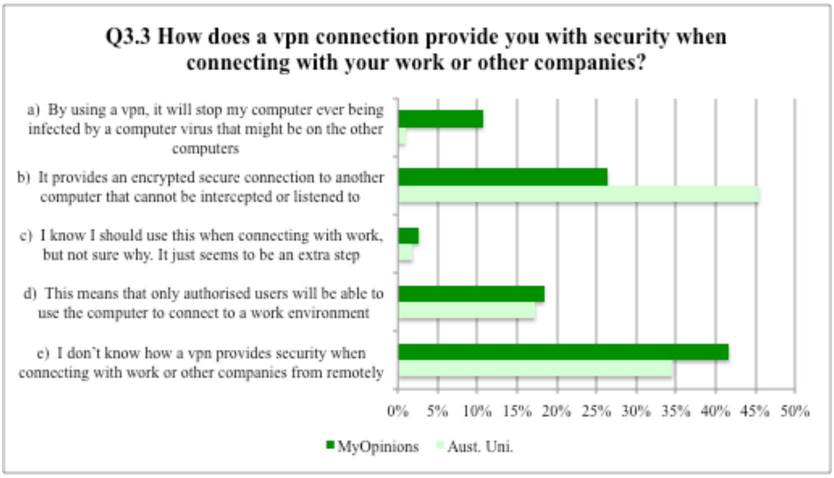


Figure 5-12 Awareness Capability Question 3.3

5.7 Conclusion

This chapter summarised the results of the data analysis of both phase 1 and phase 2 surveys in which quantitative data was collected in order to develop and test the ISACM. The results of the analysis of the phase 1 survey data was firstly used to develop the awareness importance ratings for the 39 main security categories and their associated control objectives of the ISO/IEC 27002 standard. This was performed for each of the three stakeholder groups: (IT staff, senior management, end users).

Secondly, the top ten rated main security categories for end users (based on the awareness importance ratings) were used to develop the awareness capability instrument. The awareness capability instrument consisted of ten survey questions, broken down into three sub-questions, each aimed at examining a higher level of awareness of the survey respondent, reflecting the cognitive information processing levels; Level 1 perception, Level 2 comprehension and Level 3 projection of situation awareness (SA) theory. This instrument was tested using two phase 2 survey populations, an Australian university and a MyOpinions survey panel.

Finally, the third element of the ISACM, awareness risk was calculated for the two survey populations. The results of the phase 2 survey data analysis highlighted areas of risk that were both acceptable and unacceptable within each of the survey populations, and helped to demonstrate that the ISACM could be used to link these risks back to main security categories and control objectives. The analysis also demonstrated that organisations could use more detailed analysis of the survey results to identify areas that require additional awareness.

The next chapter interprets and discusses the results of both data collection phases to provide answers to this study's research questions; and establishes and discusses the relationship between the key findings of this study and the relevant literature.

6.0 Discussion of data analysis and findings

6.1 Introduction

Based on the data analysis for research phase 1 and 2 (Chapter 5), the purpose of this chapter is to interpret the results of the data collection of both phases to answer this study's research questions (reflected below in Figure 6-1); and to establish and discuss the relationship between the key findings of this study and the relevant literature.

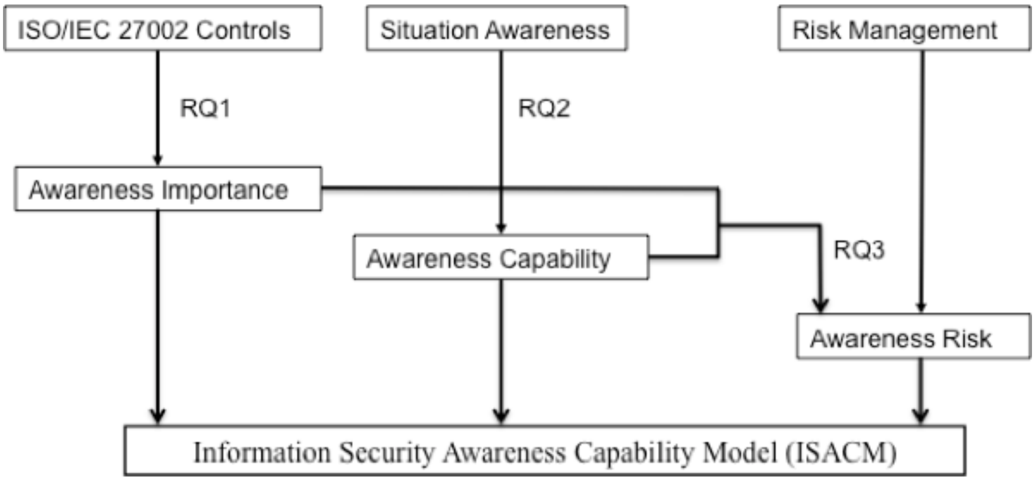


Figure 6-1: ISACM incorporating Awareness Importance, Awareness Capability, and Awareness Risk

This aim has been achieved through three main separate subsections, which discuss the relevant research questions for each research phase. Figure 6-2 below outlines the structure of this chapter.

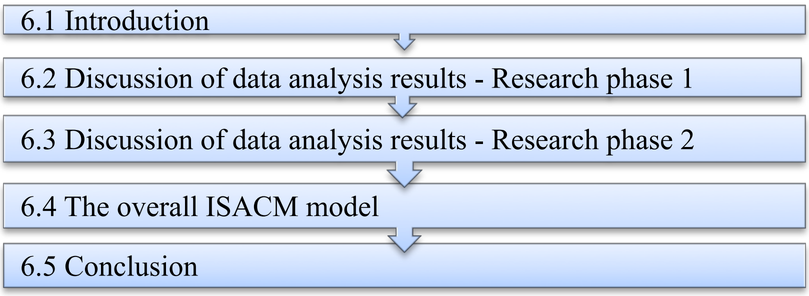

6.1 Introduction
6.2 Discussion of data analysis results - Research phase 1
6.3 Discussion of data analysis results - Research phase 2
6.4 The overall ISACM model
6.5 Conclusion

Figure 6-2 Structure of Chapter 6

6.2 Discussion of data analysis results – Research phase 1

The purpose of this subsection is to discuss the data analysis and key findings from the first research phase in relation to the general research question, the specific research question 1, and the relevant literature:

> **General Research Question: To what extent does the relationship between awareness importance and awareness capability predict the awareness risk associated with an organisation's current state of information security awareness of their information security controls?**

RQ1: What is the appropriate level of awareness importance of the main controls of the ISO/IEC 27002 Information Security Standard in terms of three stakeholder groups (IT staff, senior management, end users)?

6.2.1 Awareness Importance ratings

Chapter 5 section 5.3 presented the analysis of the results of the phase 1 survey used to determine the awareness importance ratings and provide answers to RQ1. The results shown in Table 5-1 on page 121 provide a numeric rating of awareness importance for each of the 39 main security categories and their associated control objectives for the three stakeholder groups. This was used to establish a baseline for awareness importance that would be used to compare against awareness capability scores in the phase 2 data collection. These baseline awareness importance ratings would also be utilised to determine the awareness risk scores in phase 2.

Figure 5-2 and

Figure 5-3 on pages 127 and 129 respectively provide a graphical depiction of these ratings grouped into the corresponding 11 ISO/IEC 27002 security control clauses. Section 5.3.2 on page 130 expands on the graphical representation of the key findings for RQ1 and established a baseline for awareness importance. Whilst this important baseline was established, there were interesting characteristics of the spread of ratings provided by the information security, information risk and IT audit professionals surveyed in relation to the extant literature.

Whilst the numeric rating derived for awareness importance provides a key component of the ISACM, the derivation of this component provides some valuable insights for organisations. The main implications of the key findings of this research in relation to RQ1 and a baseline of awareness importance is now discussed below in turn for each of the 11 ISO/IEC 27002 security control clauses.

6.2.1.1 Security control clause 1: Security Policy

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 7-8) for this security control clause have been outlined in section 2.3.1 on page 36, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.1 on page 130. The implications of the survey results for organisations when assessed against the key aspects and requirements of the *security control clause 1: Security Policy* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Survey results
Security policy provides a framework for setting control objectives.	IT staff	Main group for implementing controls and the awareness would need to be high. Results confirm this with majority of ratings (92%) being greater than or equal to 5 (very aware).
Security policy document should state management commitment and be approved by management.	Senior management	Senior management should provide approval for security policy. Expect awareness amongst senior management to be quite high. The results show a reasonably high awareness importance rating, 78% of responses greater than or equal to 5 (very aware).
Security policy should	End users	End users are not typically involved in developing an

Key aspects from the standard	Impacted Stakeholders	Survey results
be communicated to users in a form that is relevant and understandable to the intended reader.		information security policy, however, they are the key target audience. As a minimum there is an expectation of a moderate level of awareness. The survey results are quite varied. Although more than 43% of responses support awareness of 5 (very aware) or more, 19% suggest a rating of only 3 (slight to moderate) or less.

If awareness importance for security policy is set too low for senior management, there is a danger that there may not be full engagement and support from them. The information security policy 'represents the position of senior management toward information security, and sets the tone for the entire organization' (Kajava et al. 2006, p. 1520), so awareness must be high (Al-Omari, El-Gayar & Deokar 2012; Knapp et al. 2006). If not, this could impact on the effectiveness of the security policy, and its enforceability. Additionally, if awareness importance for security policy is set too low for end users, organisations may have a good security policy but the engagement from end users to understand and comply with the policy may be inhibited (Pahnila, Siponen & Mahmood 2007; Siponen & Vance 2010).

Therefore, 'security awareness can directly and indirectly alter employees belief sets about compliance with the information security policy' (Bulgurcu, Cavusoglu & Benbasat 2010), so awareness importance should be moderate to high for end users. Additionally, the level of 'information security awareness is likely to play a major role in shaping user compliance behaviour' (Al-Omari, El-Gayar & Deokar 2012, p. 3323) in relation to these security policies.

The variability (spread) of ratings for *security control clause 1: Security Policy* could present a challenge for an organisation. For example, if an organisation relies on their information security expert who believes that awareness importance is much lower that the ratings that this research have determined, then the risks mentioned above such as a lack of engagement by senior management or a lack of understanding from end users may arise. It could mean that awareness is not emphasised to certain stakeholder groups because the organisation's information security professionals did not perceive it to be of importance.

6.2.1.2 Security control clause 2: Organisation of Information Security

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 9-18) for this security control clause have been outlined in section 2.3.2 on page 39, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.2 on page 131. The implications for organisations of the survey results when assessed against the requirements of the key aspects and requirements of the *security control clause 2: Organisation of Information Security* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
A framework should be established to initiate and control the implementation of information security.	IT staff	IT staff are the primary group managing information security. A thorough understanding of the framework for implementing security is required. The majority of ratings are 4 (moderate) or more, with high numbers also seen at the 7 (extreme) awareness level.

Key aspects from the standard	Impacted Stakeholders	Findings
Management should assign security roles. Agreements with third parties should cover all relevant security requirements.	Senior management	Senior management plays a key role in sponsoring and supporting information security. Additionally, when it comes to dealing with third party organisations, senior management often own the relationships and drive contract negotiations, so awareness is important. The ratings support this required level of importance.
Not a significant area of focus for end users.	End users	The results show quite a varied opinion as to the level of importance, with a higher weighting of scores below 4 (moderate).

Whilst IT staff are the day-to-day group looking after information security, they are also increasingly being asked to provide 'governance, policy development, and consultancy-type functions' (Johnson & Goetz 2007, p. 18) related to information security. They also require high levels of awareness. IT staff need to understand what senior management's requirements are. This was reflected in the results obtained from the phase 1 survey.

The standard requires senior management to play an important role in ensuring the implementation of information security. Their commitment is 'important to achieving effective information system security (ISS) in organizations' (Tejay & Barton 2013, p. 3028). Chang and Ho (2006, p. 347) view information security as 'primarily a management issue', reinforcing the need for senior management to display good awareness of how their information security organisation should be structured and resourced. This is particularly important when IT services are provided by an external organisation - for instance, in the case of outsourcing. Nassimbeni, Sartor and Dus (2012) found that this area 'still presents a deep lack of knowledge on the combination of technical, managerial, and legal protection tools needed for managing data and knowledge security risks'. Senior management need a high level of awareness as to the risks associated with using these third party providers. This was reflected in the results obtained from the phase 1 survey.

End user involvement in managing information security structures within an organisation is low because of the ownership of this role by senior management. This is reflected in the survey results with many of the ratings below 4 (moderate), although there are still some high ratings for end users. This may lead to too much emphasis being placed on awareness of this area for the end user stakeholders.

6.2.1.3 Security control clause 3: Asset Management

The key aspects of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 19-22) for this security control clause have been outlined in section 2.3.3 on page 42, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.3 on page 132. The implications for organisations of these results when assessed against the key aspects and requirements of the *security control clause 3: Asset Management* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
An inventory of all important assets should be drawn up and	IT staff	The assets are technology related ones and include information, databases, IT equipment, software, etc. IT staff are often responsible for managing these, and often

Key aspects from the standard	Impacted Stakeholders	Findings
maintained. Levels of protection should be identified.		by default become the owners. A high level of awareness is required. The survey results support this.
Owners should be identified for all assets. Information classification should be agreed and documented.	Senior management	Often the responsible owners of these assets are (should be) senior management. They need to be able to articulate the importance of the information contained within Information Systems, and need to be able to 'value' these assets. Their awareness needs to be high. The survey ratings support this.
The owner may delegate implementation of specific controls.	End users	With delegation of end users identifying information assets, awareness needs to be sufficient. The survey results are varied, ranging from 18% of responses with a rating of only 3 (slight to moderate) or less, but 55% of responses are greater than or equal to 5 (very aware).

The awareness importance ratings for IT staff and senior management are almost identical and are approximately 5.5 (very aware). Organisations can experience significant damage 'through malicious and/or unintentional compromises of information assets' (Desouza 2009). Both stakeholder groups need to play a key role in ownership of assets, as well as implementing controls over those assets. Additionally, senior management must recognise that information is an 'increasingly important asset' (AlAboodi 2006). Senior management must champion the vital need of ensuring employees understand their 'responsibility in securing information assets' (Da Veiga & Eloff 2010). This reinforces the requirement for all stakeholders to have good levels of awareness in relation to Asset Management.

IT staff play a major role in managing technology configuration databases (Sharifi, Ayat & Sahibudin 2008) of IT assets. Increasing importance of information classification sees a shared responsibility between stakeholders. Operationally, end users are often called upon by senior management (through delegation) to 'own' and control information assets. This places a demand for higher levels of awareness on end users. Technology can protect the workforce against external security threats to IT assets, but educating end users will also protect them against themselves (Gartner et al. 2005). This is reflected in the survey results.

There is, however, a continuing trend in the survey results of a broad spread of ratings for end users, including some extreme (and low) scores from some of the survey responses for IT staff and senior management. If these low ratings of awareness importance are the norm in an organisation, this could leave some organisations lacking an appropriate level of awareness focus for particular stakeholder groups.

6.2.1.4 Security control clause 4: Human Resources Security

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 23-28) for this security control clause have been outlined in section 2.3.4 on page 45, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.4 on page 133. The implications for organisations of the survey results, when assessed against the key aspects and requirements of the *security control clause 4: Human Resources Security*, are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
Awareness training should commence with a formal induction process. Access rights should be removed on termination.	IT staff	Often awareness training is left to IT staff to deliver. Additionally, IT staff manage the process of user access provisioning. However, termination of employees is managed via human resources. IT staff may be requested to remove access, but not always in a timely manner. The survey results show high ratings for awareness.
Management should ensure employees are briefed on information security, and achieve a level of security relevant to their roles.	Senior management	The results show a strong weighting towards a rating of 7 (extreme), with 81% rating greater than or equal to 5 (very aware). The overall average is greater than that for IT staff, reflecting the key role that senior management performs in this area.
End users should sign employment terms and conditions, which should state theirs and their organisation's responsibilities for information security.	End users	The ratings for end users show a very broad range. 26% of responses suggest a rating of only 3 (slight to moderate) or less. Given that end users are required to sign and comply with these agreements, this level of awareness appears low. Additionally, only 43% rated greater than or equal to 5 (very aware).

When employees have been terminated there are actions (such as access removal) that need to be undertaken in a timely manner (Everett 2011a; Manders-Huits 2010; Young 2004). IT staff are often involved in the technical aspects of access removal, whilst human resources staff (and their senior management) are required to be aware of the risks if this termination process is not carried out in a timely manner (Baracaldo & Joshi 2013; Sarkar 2010). Risks in not doing so are frequently observed and reported by auditors, including for example, '11 active network users belonging to former employees, six of them had logged in to the network after their termination date' (Western Australian Auditor General 2013, p. 34).

Senior management perform an important role in human resources security. They need to ensure policies are in place so prior to employment; and human resource staff should conduct 'employee screening to establish past employments and other background details' (Sarkar 2010, p. 126). This screening now involves scanning social media postings by prospective employees for 'negative comments a candidate has made on social media, particularly comments about previous employers' (Jeffries 2014, p. 2). The level of awareness therefore needs to be high for senior management. This is confirmed by the results of the phase 1 survey presented in Chapter 5.

During their period of employment, employees should be provided with information security awareness training, as well as acknowledging compliance with information security policies. The Australian Prudential Regulatory Authority (APRA) suggest that end users would 'typically be required to periodically sign-off on information security policies as part of the terms and conditions of employment or contractual agreements' (Australian Prudential Regulatory Authority (APRA) 2010, p. 12). In order to comply with information security policies, and to be able to truthfully sign-off on this as part of their ongoing employment, this would require that end users demonstrate a good level of awareness. The results showed that 25% of respondents in the phase 1 survey believed that end users only require slight to moderate levels of awareness. This is in contrast with published literature that suggests that end user awareness needs to be high (Bulgurcu, Cavusoglu & Benbasat 2010; Siponen & Vance 2010; Talib, Clarke & Furnell 2010).

The broad spread of ratings for end users shows that some information security professionals believe awareness for end users is relatively unimportant, whilst others believe that it is vitally important. This lack of uniformity in terms of the amount of awareness required for end users could lead to a very different experience from organisation to organisation. Those information security professionals who believe that this awareness is important would typically ensure it was included within awareness programs; whereas those information security professionals who believed that this awareness is not important would not raise the awareness levels with their end users.

The results of the survey show high (very aware) ratings for both IT staff and senior management in relation to *security control clause 4: Human resources security*.

6.2.1.5 Security control clause 5: Physical and Environmental Security

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 29-36) for this security control clause have been outlined in section 2.3.5 on page 48, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.5 on page 134. The implications for organisations of the survey results when assessed against the key aspects and requirements of the *security control clause 5: Physical & Environmental Security* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
Information processing facilities should be well protected. Access properly managed. Equipment properly maintained.	IT staff	IT staff perform the primary role in designing and managing areas (i.e. data centres) where IT equipment is housed. They play a role in access allocation and control, and have a key role in managing environmental aspects (power, air, water) that support the IT equipment. The survey results support these very high levels of awareness.
Often play an ownership role in this area.	Senior management	76% rated greater than or equal to 5 (very aware). The spread of results supports an overall rating less than that for IT staff, although still quite a high overall rating.
Secure disposal or re-use of equipment.	End users	This continues the trend of a broad spread of ratings, slightly biased to ratings above 4. However, ratings of 1 appear, as do ratings of 7. Some of these higher ratings could relate to the role end users play in disposal and re-use of equipment.

With IT staff often performing a leading role in managing the physical and environmental aspects used to house their IT infrastructure, high levels of awareness are expected from them (Brotherton & Dietz 2014; Shuja et al. 2012; Simmons et al. 2006). The results of the phase 1 survey show a high level of awareness importance ratings in relation to physical and environmental security for IT staff. However, as IT equipment continues to decrease in size, it becomes increasingly more commoditised, and placement of this equipment requires less environmental support. This IT equipment may end up in normal office accommodation. End users may be required to play a greater role in physical protection. Consequently, their awareness importance may be required to increase as a result of this trend.

Australian government advice to senior management (CEO, Board of directors) gave notice that in terms of protecting enterprise information they were 'ultimately responsible for protecting...both physical and electronic...from unauthorised access or damage' (Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) 2007, p. 2). Overall. senior management must possess a high level of awareness. This was reflected in the awareness importance ratings obtained.

The awareness importance ratings obtained for end users in relation to physical and environmental security displayed a broad spread of results, with an average score indicating a moderate level of awareness. This appears to be suitable for most organisations.

6.2.1.6 Security control clause 6: Communications and Operations Management

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 37-59) for this security control clause have been outlined in section 2.3.6 on page 50, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.6 on page 135. The implications for organisations of the survey results when assessed against the key aspects and requirements of the *security control clause 6: Communications and Operations Management* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
This section has a broad range of responsibilities, many technical, and this forms the basis of what IT organisations do.	IT staff	The results show a high average rating of 6, with many ratings also at the 7 levels. This area is a core competency for IT staff and the results support that.
Required to support many of technology initiatives, significant in-depth knowledge not required.	Senior management	The results show a broad spread of ratings. Looking at the individual questions, those focused on business requirements are rated highly whilst other more technically focused questions are rated lower.
Some awareness, but no in-depth knowledge.	End users	A broad spread of results, however, numerous ratings of 7 and numerous ratings of 1were still obtained.

Communications and Operations Management form the key competency areas for IT staff, and the phase 1 survey results reflect this. When this competency (awareness) is not displayed, it could result in a significant impact on organisations and their customers. Recent events in the Australian Banking sector have highlighted the adverse impact on customers (Zappone 2012) when IT operational problems (in overnight processing of transactions) occur.

The awareness importance ratings from the phase 1 survey in relation to *Communications and Operations Management* highlights the fact that senior management need awareness of how their information processing facilities are managed. The Western Australian Auditor General (Western Australian Auditor General 2010, p. 32) reinforced the high levels of awareness required when he found documented policies and procedures often lacking 'for how changes are to be made' and, where transaction processes were involved, problems arose 'segregation of duties not in place to mitigate the risk of unauthorised or inappropriate transactions'.

End users require only general knowledge about Communications and Operations Management security because of the primary role that IT staff perform in this area. The phase 1 survey ratings reflect this, although there were some extreme ratings (1 and 7) obtained from both senior management and end users. This may have been as a result of a specific question in this clause, *security control clause 6: Communications and Operations Management*, because this section comprised 10 questions, some of which have more relevance to end users than other questions.

6.2.1.7 Security control clause 7: Access Control

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 60-76) for this security control clause have been outlined in section 2.3.7 on page 54, whilst the key results from phase 1 survey are presented in section 5.3.2.7 on page 137. The implications for organisations of the survey results when assessed against the key aspects and requirements of the *security control clause 7: Access Control* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
High level of knowledge of technical controls required.	IT staff	The results show an average rating of 6, with strong ratings also at the 7 levels. This area is a key competency for IT organisations and the results reinforce that.
Access to information should be controlled on the basis of business and information security requirements.	Senior management	A broad spread of ratings, many at the highest level of 7, but also many at levels of 3 and below. Looking at the individual questions, those focused on business requirements are rated highly (average 5.6), whilst other more technically focused ones are rated lower.
Users should be aware of their responsibilities for maintaining effective access controls, and good password management.	End users	A broad spread of results, however, two of the questions averaged over 5 (5.35 and 5.28). These questions have a high level of relevance for end users, being in the role of formal user access management (including passwords) and risks associated with mobile computing and teleworking.

The clause covers a broad range of topics. It includes many of the competencies required of IT staff, and the results support this high rating. However, as technologies evolve, access management is no longer just a technical issue (Everett 2011a; Kho 2009). Identity and Access Management (IAM) requires senior management awareness and support. Past approaches saw IAM as purely a technology issue and 'even if access rights were correct at the time that they were assigned, modifications to roles or organisational structure can mean that they go out of date quickly' (Everett 2011a). Equally, 'Human Resources (HR) can play a vital role in the enablement of effective employee IAM' (Young 2004). This was the case for the business-focused questions in the survey for this clause.

Responses for senior management and end users yielded a broad spread of results in relation to awareness importance for *security control clause 7: Access control*; however, looking at individual questions, those with higher levels of relevance for those stakeholders have been suitably rated. Awareness programs should target the various stakeholder groups with the relevant access control aspects that are relevant to those groups. For example, the proper use of passwords by end users requires a high level of awareness. In 2013 the independent regulator and competition authority for the UK communications industries (UK Office of Communications (Ofcom) 2013) conducted a survey of UK adults and found that 'more than half (55%) of adult internet users admit they use the same password for most, if not all, websites'. In terms of minimising the risks associated with poor password management, awareness seems to be a key defence (Qureshi, Younus & Khan 2009). The results confirm that high levels of awareness importance are required in this area.

6.2.1.8 Security control clause 8: Information System Acquisition, Development & Maintenance

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 77-89) for this security control clause have been outlined in section 2.3.8 on page 57, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.8 on page 138. The implications for organisations of the survey results when assessed against the key aspects and requirements of the *security control clause 8: Information System Acquisition, Development & Maintenance* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
Highly technical area.	IT staff	Very strong ratings averaging over 6, with a high percentage rated at 7. Surprisingly, there are a number of scores rated below 4, but this is less than 5% of the responses.
Incorporating security requirements within a business case.	Senior management	Average scores rated just above 4 (moderate), with the highest individual question rating above 5 for security requirements of information systems.
Low requirements needed for end users.	End users	Low scores, but still some rated above 5.

IT staff are primarily responsible for this security control clause. They are involved in developing or acquiring systems, and 'it is essential for security to be considered from the early stages and throughout the software development life cycle' (Mouratidis & Jurjens 2010). Awareness by IT staff is critical. As more applications become web based, awareness of security-related issues and subsequent required controls is becoming more important. There is 'large variance among the technical sophistication and knowledge of web developers' (Kirda et al. 2009, p. 603).

The results showed that the awareness importance ratings for IT staff has been rated appropriately for this clause, in line with previous research asserting that while 'senior management involvement has significantly increased, the absence of senior management in the evaluation of project proposals and IT in general remains a major concern' (Berghout, Nijland & Powell 2011, p. 763). However, for questions related to security requirements for information systems, senior management were rated appropriately. End user involvement is minimal for information system development and maintenance, except in terms of user testing (Hambling & Goethem 2013; Liu, Kuo & Chen 2010), and the low survey ratings support this viewpoint. However, there are some ratings that appear to be exceedingly high for end users.

6.2.1.9 Security control clause 9: Information Security Incident Management

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 90-94) for this security control clause have been outlined in section 2.3.9 on page 61, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.9 on page 139. The implications for organisations of the survey results when assessed against the key aspects and requirements of the *security control clause 9: Information Security Incident Management* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
Ensure an effective approach to manage information security incidents.	IT staff	A very high percentage of ratings above 6. IT staff play a pivotal role in this process.
Formal event reporting and escalation procedures should be in place.	Senior management	Quite high ratings here for senior management. Their support and being a point of escalation demands a suitably high level of awareness importance. Still, around 5% of respondents rate this quite low (less than 3).
All employees should be made aware of the procedures for reporting events and weaknesses that may impact on the security of the organisation.	End users	Reasonably high ratings for end users, reflecting their need to recognise a security incident and understand the importance of timely reporting.

IT staff are the key implementers of security controls (incident prevention), as well as playing a key role in responding when these controls fail (incident response). Awareness of newer techniques in responding to information security incidents is required. An ‘increasingly dynamic security environment requires more detective and response-oriented security in addition to the existing preventative frameworks’ (Baskerville, Spagnoletti & Kim 2014, p. 138). IT staff need high levels of awareness of emerging technology where ‘the adoption of cloud computing is significantly changing the landscape of incident handling, particularly between Cloud Service User (CSU) and Cloud Service Provider (CSP)’ (Ab Rahman & Choo 2015, p. 55).

A recent case study found three large organisations had ‘not implemented any specific standard or guideline for incident management, but have based their approach on components from the ISO/IEC 27001 and 27002 standards’ (Hove et al. 2014, p. 37). This reinforces the role that the ISO/IEC 27002 standard provides in terms of awareness in relation to information security incident management. Senior management require good levels of awareness so they can provide support to their IT organisation, as well as establish links to external organisations that can assist in incident management if required. The incident response team (often referred to as a CERT) responsibilities and mandate ‘needs to be clearly described and sanctioned by the highest management of the organisation for which the CERT works’ (European Network and information Security Agency (ENISA) et al. 2010, p. 19).

End users are often the trigger point for raising concerns regarding an information security incident. The ratings from the phase 1 survey appear to be appropriate.

6.2.1.10 Security control clause 10: Business Continuity Management

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 95-99) for this security control clause have been outlined in section 2.3.10 on page 64, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.10 on page 140. The implications for organisations of the survey results when assessed against the key aspects and requirements of the *security control clause 10: Business Continuity Management* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
Developing and implementing continuity plans including information security.	IT staff	Ensuring that information security is embedded in business continuity plans demands a high level of awareness from IT staff. This is reflected in the survey ratings. Also the strong links between business continuity and disaster recovery (which IT staff manage) reinforces this high level of awareness importance.
Business continuity planning framework.	Senior management	Strong ratings shown for senior management. They own (or should own) business continuity, so the awareness importance should be (and is) high.
Testing business continuity plans.	End users	End users play certain roles, so a reasonable level of awareness would be expected.

Business continuity is of critical importance to senior management (Speight 2011; Stanciu, Pana & Bran 2010). Significant disruptions often occur outside the control of an organisation. Recent reminders of this include a fire in Gibraltar that disrupted online gambling (BBC News 2014), and floods in Thailand (Zolkos 2015) causing supply chain issues for companies such as Honda Motor Co and Western Digital. Business disruption is a significant issue for organisations. And it is not just ‘an IT thing’ (Costello 2012; Thejendra 2014). Some believe that ‘senior management often lack awareness and understanding of their business contingency process and the terminology used’ (Lindström 2012, p. 269).

IT staff provide many of the technical aspects to assist with business continuity (Sahebjamnia, Torabi & Mansouri 2015), and end users perform tasks (during a disruption) designed by senior management for their overall business continuity plans. The awareness importance ratings obtained from the phase 1 survey appear to be appropriate for each of the three stakeholder groups (IT staff, senior management, end users).

6.2.1.11 Security control clause 11: Compliance

The key aspects and requirements of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2006b, pp. 100-106) for this security control clause have been outlined in section 2.3.11 on page 66, whilst the key results from phase 1 survey for this security control clause are presented in section 5.3.2.11 on page 141. The implications for organisations of the survey results when assessed against the key aspects and requirements of the *security control clause 11: Compliance* are summarised below.

Key aspects from the standard	Impacted Stakeholders	Findings
The design, operation, use and management of information systems may be subject to statutory, regulatory, and contractual security requirements.	IT staff	IT staff are still the best positioned personnel to manage this on a daily basis, with the assistance of senior management, line management and IT risk and audit colleagues. Therefore, their level of awareness needs to be high. The ratings generally reflect this.
Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements.	Senior management	This is a key responsibility of senior management. The ratings generally reflect this. Senior management would also be the key drivers behind ensuring the audit process is in place, and providing priority for any rectification work that may be needed.
Maintaining awareness of policies to protect intellectual property rights.	End users	Varied ratings were obtained for end users.

Globally, there are many compliance related regulations, standards and guidelines that are highly relevant to technology and information security. These include the Australian Payment Clearing Association (APCA), which provides a standard for the consumer electronic clearing system (CECS) (Australian Payments Clearing Association [APCA] 2014); Singapore enacted personal data protection legislation (Ter 2013); and the US has the Gramm-Leach-Bliley Act (US Government 1999) which is focused on financial institutions and data privacy. Additionally, there is the Payment Card Industry Data Security Standard (PCI Security Standards Council 2010) which provides ‘comprehensive standards and supporting materials to enhance payment card data security’. Australian Prudential Regulatory Authority’s prudential practice guide (PPG234) is used to ‘assist regulated institutions in the management of security risk in information and information technology’ (Australian Prudential Regulatory Authority (APRA) 2010).

There are many other areas of compliance related to the use of technology that organisations need to be aware of. Senior management in particular need to have high levels of awareness to be able to determine which areas are relevant to their organisation and what approach their organisation should take in terms of compliance. Equally important, IT staff have the best level of technical understanding to be able to implement compliance controls that senior management deem necessary, thus, IT staff awareness of compliance is also high. The awareness importance ratings obtained from the phase 1 survey appear to be appropriate overall for each of the three stakeholder groups (IT staff, senior management, end users).

6.2.1.12 Summary of security control clauses

In general terms, there was greater consensus amongst the survey respondents on the awareness importance ratings required for the IT staff stakeholders and the senior management stakeholders than for end user stakeholders. The information security professionals that were involved in the phase 1 survey used to determine the awareness importance ratings have typically worked amongst (often as part of) IT staff which probably assisted with them being very familiar (and relatively consistent in opinion) with the awareness requirements for IT staff. They also appear to be able to consistently rate what is required from senior management. Many years of “selling” the benefits of information security within their organisations would have assisted in this.

However, the level of consistency and agreement as to the levels of awareness required of end users was not observed in the results of the phase 1 survey. Given that the end users stakeholders represent the greater portion of employees targeted in information security awareness programs, this variation in opinions of awareness importance amongst information security professionals may result in inadequate levels of awareness being provided. This could lead to organisations being insufficiently prepared for information security threats.

6.3 Discussion of data analysis results – Research phase 2

This purpose of this subsection is to discuss the key findings from the data analysis of the second research phase in relation to the general research question, the interrelated specific research questions RQ2 and RQ3, and the relevant literature:

> **General Research Question: To what extent does the relationship between awareness importance and awareness capability predict the risk associated with an organisation’s current state of information security awareness of their information security controls?**
>
> **RQ2: How can the awareness capability of these three stakeholder groups be measured, based on situation awareness theory?**
>
> **RQ3: How can resultant awareness risk evidenced from insufficient awareness capability (in comparison to awareness importance) be combined into a risk management model that will assist organisations in measuring and managing information security awareness risk?**

Chapter 4 outlined the development of the awareness capability instrument and awareness risk calculation. To capture awareness capability data and evaluate awareness capability and awareness risk, end users were surveyed in order to establish their awareness capability and subsequent awareness risk for the top ten controls that were rated the highest in terms of awareness importance in phase 1 of this research. Chapter 5 presented the results of the analysis of the phase 2 survey data that determined the awareness capability scores which, in turn, were used to calculate awareness risk of two survey population groups. These key findings in relation to these two measures, awareness capability and awareness risk, are discussed below. These two measures are interlinked by capturing awareness capability so an organisation can determine the potential resultant awareness by comparing awareness capability with the baseline of awareness importance.

6.3.1 Awareness Capability scores

The summary of an average of the scores for awareness capability obtained from the second survey for the Australian university population and the MyOpinions panel population is represented below in Table 6-1.

Table 6-1 Awareness Capability – Summary by survey population

Population	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Total
Australian University	3.3	4.7	3.9	5.2	4.8	5.1	4.9	4.3	4.1	4.8	45.2
MyOpinions Panel	2.8	3.4	3.0	3.8	4.1	3.4	3.4	3.2	3.4	3.6	34.4

The scores for each sub-question have been totalled to arrive at an overall score for each of the ten questions. These results have also been displayed graphically in Figure 5-5 on page 147, and matched against the situation awareness (SA) levels to show where each of the phase 2 survey populations rated. The SA levels were determined based on the scoring mechanism used for the second survey. Level 1 SA scores ranged from 0 through to 2. Level 2 SA ranged from 2 through to 4.5, whilst Level 3 SA ranged from 4.5 through to 7.

The results shows that on a question-by-question basis (incorporating sub-questions scores), the MyOpinions population of respondents, on average, did not display Level 3 situation awareness capability for any of the top ten security categories and their associated control objectives. The average total scores for each of these ten questions were less than 4.5. The MyOpinions population results are in the middle of the Level 2 SA band. Whilst individual respondents may have displayed Level 3 SA, overall, MyOpinions population did not. Comparing the MyOpinions population results with the Australian university population, six of the ten overall questions fell within the level 3 SA band for the Australian university population.

Two questions for the Australian university population were in the higher range of level 2 SA. Overall, for all of the ten questions, the Australian university population displayed a higher level of awareness capability than did the MyOpinions panel population. Whilst the scoring of awareness capability is an important component of the ISACM, its main value from an organisational perspective is derived when comparing the awareness capability being demonstrated for a specific security category and their associated control objective with the matching required awareness importance ratings to arrive at an awareness risk rating.

6.3.2 Awareness Risk ratings

Section 2.4.3 on page 72 outlined the basis for assessing awareness risk, with section 5.6 on page 153 describing how awareness risk was calculated. Table 5-29 on page 154 summarises the desired awareness importance rating, demonstrated awareness capability scores and resultant awareness risk measures for both populations. The MyOpinions population displayed positive awareness risk for all of the ten overall questions. In comparison, the Australian university population displayed negative awareness risk (no risk) for three of the ten questions surveyed, with a further two questions displaying only negligible awareness risk scores (0.01 and 0.13). The presentation of awareness risk for information security in this research mirrors the approach used in classical organisational risk management. Likelihood and impact (consequence) were displayed in terms of awareness capability and awareness importance within an information security context.

Awareness capability and awareness risk was measured per question per population group. This provides organisations with an overall view of where awareness risk exists because of a lack of demonstrated awareness capability. There is also additional benefit to an organisation by looking at the individual scores of awareness risk calculated for those surveyed. These individual scores highlight which employees display awareness risk and for which questions. Targeted awareness can then be provided to these individuals for the control objectives associated with the questions asked, whilst those that demonstrate sufficient awareness are not burdened with awareness raising about control objectives that they already understand and demonstrate sufficient capability towards.

Dealing with unacceptable awareness risk

A substantive positive awareness risk score indicates that awareness risk is higher than desired (Duijm 2015; NSW Government 2012). It highlights the required level of awareness (awareness importance) is not being adequately demonstrated (awareness capability). Whilst awareness risk is presented as a numeric score, it can also be viewed in a tradition risk heat map (NSW Government 2012; Standards Australia/Standards New Zealand 2009b; Xiaosong et al. 2009). Figure 4-3 on page 117 showed how awareness importance and awareness capability could be plotted onto a heat map that shows whether the resultant awareness risk is low, medium or high. Organisations may have different scales for their risk ratings, so adjustments to the model can be made by those organisations.

The results of the ten awareness capability scores versus awareness importance ratings for both populations, shown in Table 5-29 on page 154, have been plotted on the risk heat map below in Figure 6-3.

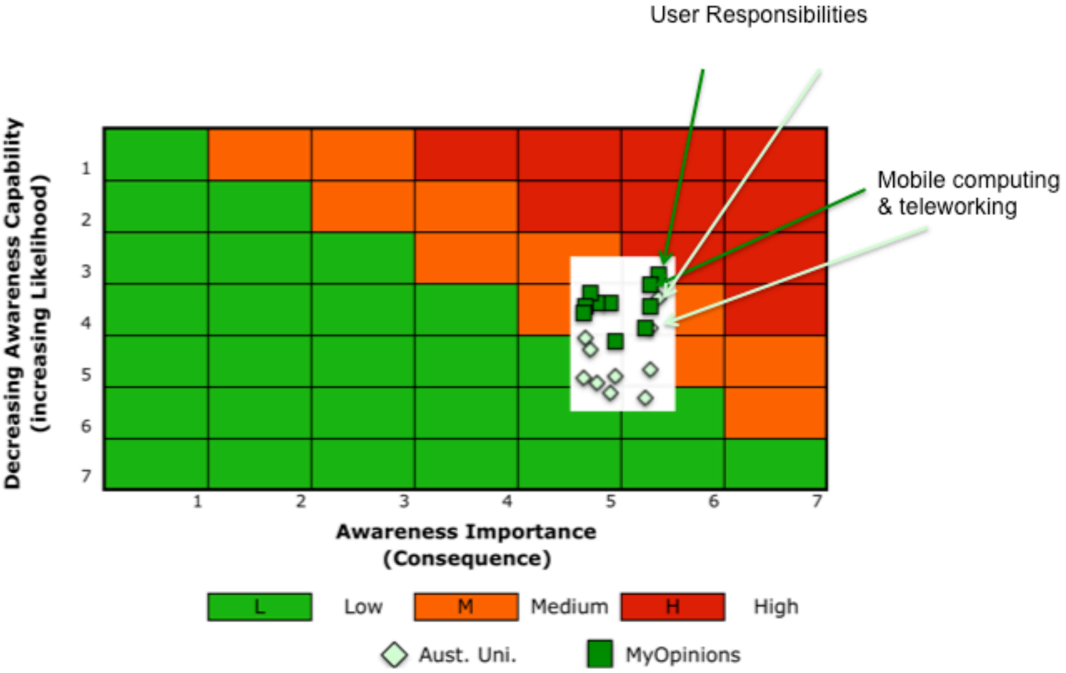


Figure 6-3 Awareness Risk heat map

Detailed analysis of the two highest awareness risk security categories is shown in section 5.6.1 on page 156. These risks relate to awareness capability question 1 (User Responsibilities) and awareness capability question 3 (Mobile computing and teleworking) and are shown in Figure 6-3 above.

For the MyOpinions population, awareness risk for both questions is in the high-risk section of the heat map, whilst for the Australian university population they are in the medium risk section. The other scores for the MyOpinions population are all in the medium risk section, whereas the majority of the Australian university scores are in the low risk section.

A benefit in presenting awareness risk in such a way is to portray information security risk in a similar manner as to other organisational risks (NSW Government 2012). This approach allows for easy identification of the priority of awareness risks to deal with. It also highlights those risk that appear on the boundaries, thereby identifying areas where proactive risk raising can help to avoid risks escalating in the future. The heat map approach allows organisations to visualise their information security risk profiles rather than just using a numerical approach. Table 6-2 below extends this heat map approach by showing the overall risk ratings (High, Medium, Low) that were assigned to the respective *Security Control Clause* and *Main Security Categories* from the ISO/IEC 27002 Standard.

Table 6-2 Awareness Risk ratings

			Aust. Uni.	**MyOpinions**
Security Control Clauses	**Main security categories**	**AC Question**	**AR**	**AR**
Access Control	User Responsibilities	Q1	M	H
Information Security Incident Management	Reporting Information security events and weaknesses	Q2	M	M
Access Control	Mobile computing and teleworking	Q3	M	H
Communications and Operation Management	Exchange of information	Q4	L	M
Communications and Operation Management	Media handling	Q5	L	L
Asset Management	Information classification	Q6	L	M
Access Control	Business requirements for access control	Q7	L	M
Compliance	Compliance with legal requirements	Q8	L	M
Asset Management	Responsibility for assets	Q9	L	M
Physical & Environmental Security	Equipment security	Q10	L	M

The two awareness risk ratings that rated the highest for both populations were examined in order to highlight what impact these ratings could have on their organisations. These are shown below and titled by their respective *Awareness capability question number*, *Security control clause*, and *Main security category*. This approach to analysing the results of the ISACM should be carried out by individual organisations. For example, with the Australian university, only the medium level awareness risks require more detailed analysis. This approach assists with providing a more focused view on where improvements are required in awareness.

6.3.2.1 Q1 Access Control - User Responsibilities

With *Access Control – User Responsibilities* showing a medium risk rating for the Australian university population, and a High risk rating for the MyOpinions panel population, this indicates a significant risk to both populations. Whilst consequences of poor awareness in the area of Access Control was highlighted earlier in section 2.3.7 on page 54, section 5.6.1.1 on page 156 presented an analysis of the detailed responses to the sub-questions related to this awareness capability question. The results of the phase 2 survey show that 37% of Australian university and 46% of MyOpinions panel populations would share their passwords. Much has been written about password management, the associated risks and possible solutions (Acar, Belenkiy & Küpçü 2013; Qureshi, Younus & Khan 2009; UK Office of Communications (Ofcom) 2013). Reducing risk through awareness of enhanced practices has been found to be a consistent theme in this research.

The phase 2 survey answers highlight that some of those who said they would share their password would do so 'only in an emergency' or 'would share but change password immediately after'. This level of detailed analysis allows an organisation to customise their awareness program to help specifically address the choices their employees are making. It may also allow organisations to include detailed information in their policies. For example, rather than specifying that 'employees must not share their password', they may tailor this to include 'not even with your manager'. Or include instruction as to what to do 'in an emergency'.

Further analysis of the sub-questions showed that 36% of Australian university and 46% of MyOpinions panel populations would use the same passwords across personal and work-related computer accounts. Researchers have reinforced the risks of such poor practices with consequences such as 'a breach on one system potentially renders the others vulnerable' (Furnell 2007, p. 445; Horcher & Tejay 2009). Awareness targeting this behaviour would help to minimise the risks.

6.3.2.2 Q3 Access Control - Mobile computing and teleworking

Section 5.6.1.2 on page 157 presented an analysis of the detailed responses to the sub-questions related to this awareness capability question. The results of the phase 2 survey showed that only 35% of Australian university and a much lower 15% of MyOpinions panel populations could identify the benefits of using a VPN connection for remotely connecting to their work environment. The necessity for using VPN technology for remote connections (National Institute of Standards and Technology [NIST], Souppaya & Scarfone 2013; TsohouKokolakis, et al. 2010), should be understood by organisations if they are going to allow their employees to remotely connect in a safe manner.

The risk that having a low percentage of end users not understanding the benefits of using a VPN is twofold. Firstly, they may avoid remotely connecting to their work environment. Whilst this in itself does not present a security risk, it will impact on productivity and work life balance that could be achieved by employees with secure remote working capabilities. The second scenario is that end users will connect remotely to their organisation without consideration as to whether the connection is secure, therefore putting themselves and their organisation at risk. And finally, this question saw around 50% of respondents of both populations understanding the benefits of hard disk encryption for portable devices. However, 20% of each population's respondents were not aware of the benefits. This lack of awareness of the importance of hard disk encryption as an effective security control could leave organisational data at risk.

6.4 The overall ISACM model

The final aspect of this chapter is to discuss the overall information security awareness capability model (ISACM) that has been the primary focus of this research, which incorporates the general research question:

> **General Research Question: To what extent does the relationship between awareness importance and awareness capability predict the risk associated with an organisation's current state of information security awareness of their information security controls?**

This research derived the awareness importance ratings for all 39 main security categories and their associated control objectives from the ISO/IEC 27002. This research then developed an instrument for capturing the awareness capability score, which tested 10 of the 39 main security categories and their associated control objectives. This instrument was tested with the end user stakeholders across two population groups, a general population to provide a baseline and a specific organisation population. Finally, the awareness risk scores were also calculated for these 10 main security categories for each of the two populations. Table 5-29 provided the key measures that make up the ISACM, namely, awareness importance, awareness capability and awareness risk.

The relationships posed in the general research question between awareness importance, awareness capability and awareness risk were empirically tested and this research demonstrated the level of awareness risk that both a general population and a specific organisation population would be exposed to. This level of risk was presented earlier in Figure 6-3 in the form of a traditional risk management heat map.

6.5 Conclusion

This chapter discussed the key findings from the analysis of phase 1 and phase 2 survey data in relation to the three research questions that were posed in Chapter 1. Firstly, this research discussed the awareness importance ratings that were derived and assessed in terms of the three stakeholder groups. Commentary on the derived awareness importance ratings was provided in terms of what are the desired awareness importance ratings expected for the three stakeholders groups, and any impacts that may result where there were deviations from these desired levels of awareness importance. This was intertwined with relevant literature to assist with clarifying the obtained results.

Secondly, awareness capability scores and resultant awareness risk ratings for both of the survey populations were examined. These awareness capability scores and awareness risk ratings were presented in a table, as well as in a commonly used risk heat map for ease of interpretation. Overall, the Australian university respondents demonstrated a higher awareness capability and, therefore, a lower awareness risk across all questions when compared with the MyOpinions panel respondents.

Finally, this research has provided an approach for analysing the awareness capability responses in greater detail that will allow organisations to determine exactly where awareness capability is lacking and where resultant awareness risk may exist in an organisation with a multiple key stakeholders. This approach will assist organisations in determining how they should target their information security awareness programs within an organisation for specific stakeholder groups.

7.0 Conclusions and Implications

7.1 Introduction

The last chapter of this thesis concludes this study. Figure 7-1 below outlines the structure of this chapter.

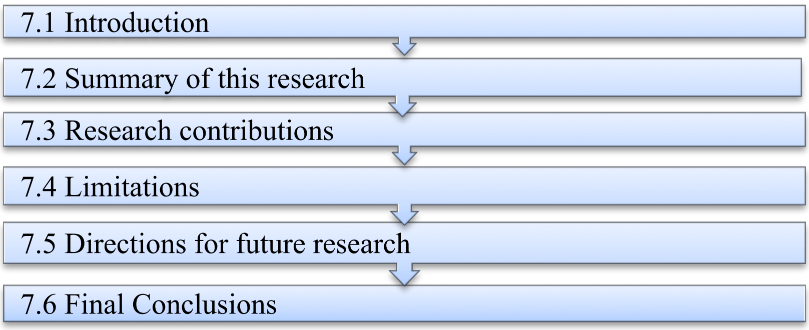

7.1 Introduction
7.2 Summary of this research
7.3 Research contributions
7.4 Limitations
7.5 Directions for future research
7.6 Final Conclusions

Figure 7-1 Structure of Chapter 7

This chapter provides a summary of the research study in terms of the research problem, the general research question, the three specific research questions investigated and tested, the methodological approach used, and the key findings of the study. This chapter discusses the key contributions that have been made for theory and practice; and the implications of this research for current and future research and practice. The limitations of this study are acknowledged. Lastly, suggestions for future research in this area of study are provided.

7.2 Summary of this research

The purpose of this section is to provide a summary of this research in terms of the research problem, general research question and specific research questions which were investigated, the methodological approach used to conduct this study, and major findings and conclusions that can be drawn from this study.

7.2.1 Research problem

This research developed and evaluated a model that examined what is the appropriate level of awareness importance in relation to the key information security control objectives as specified by the ISO/IEC 27002 Standard. This research then used that standard as the basis for evaluating the awareness capability of a general population of employees whose jobs involve the use of computing and then compared that against the evaluated awareness capability of a specific organisation. The resultant awareness risk can then be calculated to inform an organisation of the existence of any insufficient awareness capability in their employees.

Measuring the level of employee awareness of information security controls across an organisation continues to be a challenge (Sannicolas-Rocca, Schooley & Spears 2014; Shahri, Ismail & Rahim 2013; Tsohou et al. 2012). Without understanding the required awareness and without being able to measure the demonstrated awareness capability of these information security controls, an organisation may be unable to determine whether a lack of awareness and knowledge in their employees poses information security related risks.

This study aimed to address the identified gaps in the literature by investigating the following general research question:

> *To what extent does the relationship between awareness importance and awareness capability predict the awareness risk associated with an organisation's current state of information security awareness of their information security controls?*

To address and answer this general research question, the following three specific research questions were formulated for this research.

RQ1. What is the appropriate level of awareness importance of the main controls of the ISO/IEC 27002 Information Security Standard in terms of three stakeholder groups (IT staff, senior management, end users)?

RQ2. How can the awareness capability of these three stakeholder groups be measured, based on situation awareness theory?

RQ3. How can resultant awareness risk evidenced from insufficient awareness capability (in comparison to awareness importance) be combined into a risk management model that will assist organisations in measuring and managing information security awareness risk?

To achieve the research objectives, a two-phase research design was selected. This involved developing two survey instruments to collect data that were used to determine awareness importance as part of phase 1; and assess awareness capability as part of phase 2. These two measures, as well as the third measure of awareness risk (calculated from awareness importance and awareness capability), form the basis of the researcher's information security awareness capability model (ISACM). The relationship of the three main research questions that underpin and contributed to the development and evaluation of ISACM is shown below in Figure 7-2

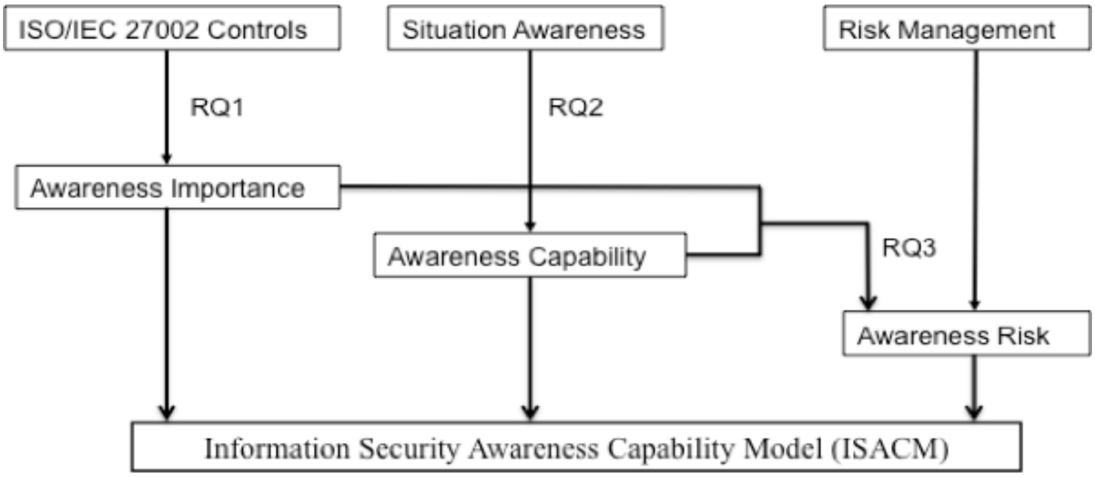


Figure 7-2 Summary of research questions supported in this study

7.2.2 Research methodology

Drawing upon the information security controls presented by the International Organization for Standardization (ISO/IEC 27002) and theories of situation awareness (Endsley 2015; Howard & Cambria 2013; Webb et al. 2014) and risk management (Mejias 2012; NSW Government 2012; Webb et al. 2014), this study adopted a functionalist-positivist research paradigm with quantitative factors (Burke 2007; Neuman 2006) to develop and test the Information Security Awareness Capability Model (ISACM). The first research phase developed a survey assessment instrument to measure awareness importance of the 39 main security categories and their associated control objectives in the ISO/IEC 27002 Standard.

The targeted respondents for this survey were information security, IT audit and IT risk professionals as they were considered the most appropriate persons to answer the survey and provide reliable awareness importance ratings for this set of information security controls. This provided the basis for the awareness importance ratings for the three stakeholder groups (IT staff, senior management, end users). Results from the first phase informed the second phase by providing a rating of the awareness importance of the 39 main security categories and their associated control objectives for the stakeholder groups. The second phase of the research developed an assessment instrument for measuring awareness capability that was based on the top 10 rated (of 39) information security categories and their associated control objectives in terms of awareness importance for the end user stakeholder group.

In the second phase of this research, a survey instrument was used to evaluate awareness capability for the end user stakeholders. This survey instrument for measuring awareness capability was tested on a baseline population (223 respondents provided by a MyOpinions survey panel), as well as a specific population of 110 Australian university staff. The second phase of this research then combined the measures of awareness importance from phase 1 with the awareness capability measures determined from the phase 2 survey to calculate the awareness risk for the two populations of end users.

7.2.3 Summary of results of Research Question Testing

The three specific research questions stated earlier in this chapter provided focus and the basis for the evidence that was collected in this research. The main contribution of this research was the development and evaluation measurement of awareness importance and awareness capability; and determining the resultant awareness risk that may exist if demonstrated awareness capability is less than the desired awareness capability (awareness importance).

This relationship between the desired awareness capability and the measured awareness capability was used to derive awareness risk scores that, in turn, are used to inform an organisation as to the awareness risk associated with an organisation’s information security controls. Figure 7-2 above provides an overview of the research model and how the research questions contributed to the ISACM.

Conclusions on how the three research questions addressed the general research question in this research are described below.

RQ1: What is the appropriate level of awareness importance of the main controls of the ISO/IEC 27002 Information Security Standard in terms of three stakeholder groups (IT staff, senior management, end users)?

This research reported the appropriate level of awareness importance in Table 5-1 on page 121. This research concluded that there are differing levels of awareness importance between the 39 main security categories and their associated control objectives and differing levels across the three key stakeholders considered in this research. Some security controls are more important than others from an organisational perspective, and this current research was able to rate these importance levels. This study also concluded that when looking at the individual main security categories and their associated control objectives, there are different levels of awareness importance required depending on which stakeholder group is being assessed. For example, the highest rated security control objective in terms of awareness importance for end users was *Access Control: User Responsibilities*. However for senior management their highest rated security control objective in terms awareness importance was *Compliance: Compliance with legal requirements*. Additionally, for IT staff the highest rated security control objective in terms awareness importance was *Communications and Operations Management: Network security management*.

The data collected from the phase 1 survey using the awareness importance measurement instrument demonstrated how awareness importance differed between the three stakeholder groups of interest in this research. This rating of the 39 main security categories and their associated control objectives from the ISO/IEC 27002 standard in terms of awareness importance for three key stakeholder groups provides an invaluable reference point for organisations wishing to identify the priority areas which should be covered in an information security awareness program. Distinguishing the appropriate level of awareness importance between the three key stakeholder groups allows organisations to identify which areas of information security awareness should be a focus in targeting specific groups in an organisation.

RQ2: How can the awareness capability of these three stakeholder groups be measured, based on situation awareness theory?

Situation awareness theory and the relevant supporting literature were used to develop a measurement instrument for the second component of the ISACM, awareness capability. The survey instrument for measuring the awareness capability of end users was tested with a baseline population group, as well as a second population of end users working in a specific sector (an Australian university). The scores obtained from surveying these two populations using the awareness capability instrument for end users provided the researcher with a measure of end user awareness capability for a general population and a specific organisation. This also demonstrated the suitability of the survey instrument for measuring awareness capability, and that it could be applied to all stakeholder groups within an organisation.

The awareness capability results for end users obtained from the phase 2 survey also demonstrated where the perceived awareness capabilities ranked within the three levels of situation awareness. The Level 1 SA scores that demonstrated perception went from 0 to 2, the Level 2 SA scores demonstrating comprehension went from 2 to 4.5, and the Level 3 SA scores demonstrating projection went from 4.5 to 7. Where awareness importance of end users was deemed to be of high importance, organisations should strive to achieve Level 3 situation awareness through awareness capability scores between 4.5 and 7.

In terms of information security, aiming for Level 3 situation awareness would allow employees to 'project' what the likely consequences of an information security event would be. For example, receiving an email from an unknown source, employees demonstrating Level 3 awareness capability (SA) would be able to proactively project what could happen in the event of them clicking on an unknown web link. Initially they would have a *perception* that because it is a link from an unknown source, it could be a problem. They would also *comprehend* that the website being presented via that link may not be the legitimate web site it purports to be. Finally, with Level 3 SA they would be able to *project* that if they provided personal details and banking information via that web link site they would likely experience identity theft and suffer financial theft.

The study surveyed two distinct populations: a general population of end users, which provided a baseline of awareness capability; and end users in a specific organisation. Figure 7-3 below shows how these two populations ranked comparatively in terms of the awareness capability across the three levels of situation awareness (L1, L2, L3). This study concluded that there were marked differences between the awareness capability demonstrated by the end users of a specific organisation (Australian university) when compared with the end users of a baseline population (MyOpinions).

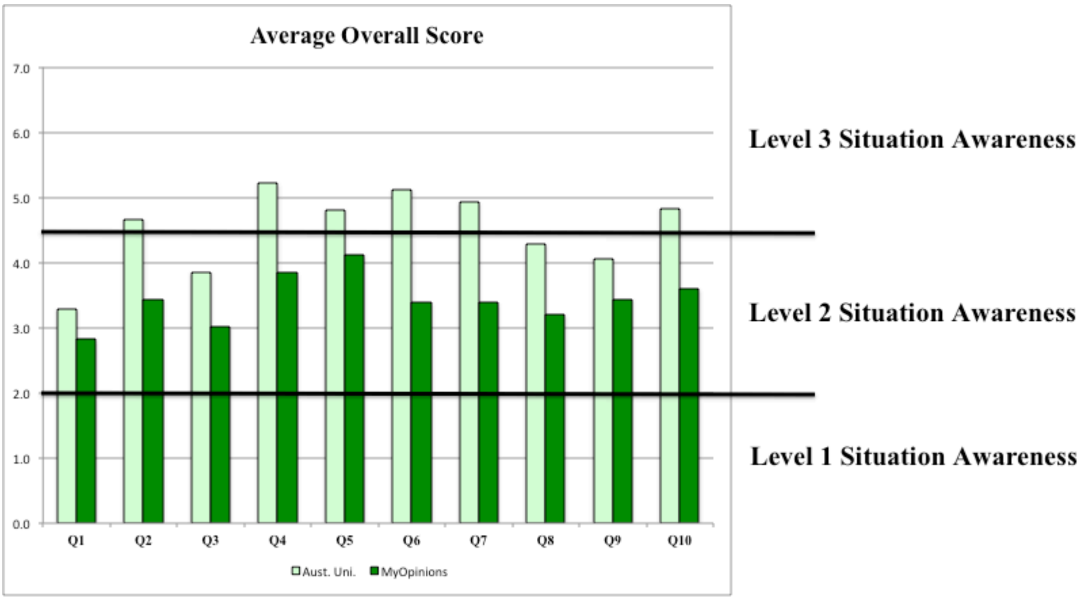


Figure 7-3 Awareness Capability versus Situation Awareness levels

The results from the phase 2 survey, using the awareness capability instrument developed in this research, demonstrated that awareness capability varied across the 10 main security categories and their associated control objectives that were assessed. The results also varied between the specific organisation population and the baseline population that were surveyed. The researcher believes that the awareness capability instrument provides an invaluable reference point for organisations wishing to identify the level of awareness being demonstrated by their employees. Whilst the results presented are representative overall for the two populations surveyed, the results of the survey at an individual level also provide invaluable information for organisations. This would allow an organisation to selectively provide additional awareness training to those individuals who have not demonstrated the required level of awareness capability overall.

RQ3: How can resultant awareness risk evidenced from insufficient awareness capability (in comparison to awareness importance) be combined into a risk management model that will assist organisations in measuring and managing information security awareness risk?

This study concluded the key benefit of the risk analysis derived from the ISACM is it identifies where sufficient awareness is being demonstrated in an organisation. This can be done at an overall organisational level, or for specific groups, or for individuals in an organisation. At an organisational level, this can provide a high level view in terms of whether overall awareness for a particular area is sufficient, particularly if measured following a targeted awareness program. At a group level, there may be specific requirements for that group to have a certain level of awareness for a particular area, for example, data privacy in a records management or human resources group. Moreover, at an individual level, organisations may wish to hold their individuals accountable for specific areas, such as password compliance or security policy compliance. This then allows the organisation to avoid investment in awareness programs where it is not required. There is no point in over-investing in efforts to raise awareness where it is already demonstrated as being sufficient.

The researcher concluded that low levels of awareness risk identifies for the organisations the specific security categories and associated control objectives that require only minor additional degrees of awareness. However, given that these controls only display low levels of risk, the priority of providing this awareness raising can be adjusted based on this lower level of risk. Furthermore, where medium levels of awareness risk are identified, these medium level risks for those security categories and control objectives require a greater level of urgency in addressing the issue than those risks identified as low, but not of a high priority.

When a high level of risk is identified, these control areas present a high level of risk and require urgent attention. In this research the responses of two out of 10 questions for the MyOpinions panel show *high* awareness risk for *Access control: User responsibilities* and *Access control: Mobile computing and teleworking*.

General Research Question: To what extent does the relationship between awareness importance and awareness capability predict the awareness risk associated with an organisation's current state of information security awareness of their information security controls?

This study concludes that the three components - awareness importance, awareness capability and awareness risk - can be measured using the 39 main security control categories and their associated control objectives in the ISO/IEC 27002 Standard as a focus point for awareness importance, using the three levels of situation awareness theory (perception, comprehension, projection) to determine awareness capability, which then allows organisations to identify the resultant awareness risk that may exist in an organisation. This research study has brought these three components together into a model termed the Information Security Awareness Capability Model (ISACM). Figure 7-2 shown earlier in this chapter shows a high level view of these components as part of the ISACM. Table 5-1 on page 121 shows the 39 awareness importance ratings derived for the three stakeholder groups (IT staff, senior management, end users) that were linked to the 39 main security categories and their associated control objectives as contained in the ISO/IEC 27002 standard.

The awareness capability instrument was developed and evaluated for the top ten awareness importance ratings previously determined in the phase 1 survey for end users. This awareness capability instrument was tested in a baseline general population of employees that use computers in their work and a specific population of end users of an Australian university. These results were shown in Table 5-18 on page 147. The developed ISACM brings these measures of awareness importance and awareness capability together into a single consolidated view that enables the calculation of the resultant awareness risk that may exist in an organisation.

Table 7-1 below shows the linkage and hierarchy of these measures of awareness importance, awareness capability and awareness risk.

Table 7-1 ISACM – Awareness importance, capability and risk comparison matrix

ISO/IEC 27002			Aust. Uni.		MyOpinions	
Security Control Clauses	Main security categories	AI	AC	AR	AC	AR
Access Control	User Responsibilities	5.36	3.29	2.07	2.83	2.53
Information Security Incident Management	Reporting Information security events and weaknesses	5.28	4.67	0.61	3.44	1.84
Access Control	Mobile computing and teleworking	5.27	3.85	1.42	3.02	2.25
Communications and Operation Management	Exchange of information	5.23	5.22	0.01	3.85	1.38
Communications and Operation Management	Media handling	4.94	4.81	0.13	4.12	0.82
Asset Management	Information classification	4.89	5.12	-0.23	3.39	1.50
Access Control	Business requirements for access control	4.75	4.93	-0.18	3.39	1.36
Compliance	Compliance with legal requirements	4.69	4.28	0.41	3.20	1.49
Asset Management	Responsibility for assets	4.65	4.06	0.59	3.44	1.21
Physical & Environmental Security	Equipment security	4.62	4.84	-0.22	3.59	1.03

The first column shows the security control clauses from the ISO/IEC 27002 standard (there are 11 within the standard) that are linked to the second column of top ten main security categories (there are 39 within the standard) that were evaluated for end users in the phase 2 survey based on the top ten awareness importance ratings previously determined in the phase 1 survey. The third column shows the awareness importance (AI) derived during the phase 1 survey. The fourth and fifth columns show the awareness capability (AC) and awareness risk (AR) measures for the specific population (an Australian university) and the sixth and seventh columns show the awareness capability (AC) and awareness risk (AR) measures for the baseline population (MyOpinions).

With the primary goal of the ISACM aimed at predicting '*the awareness risk associated with an organisation's current state of information security awareness of their information security controls'*, the resultant awareness risks were rated as high, medium and low (refer to Figure 6-3 on page 175). These rating levels used in the ISACM can be customised to the risk management approaches used within an organisation. The colour coding of the awareness risk ratings of green for low, amber for medium, or red for high visually depict awareness risk results that were derived from the completion of the analysis of the phase 2 survey responses. This awareness importance, capability and risk matrix provides an organisation with a simple method for focusing on those risk awareness areas of the ISO/IEC 27002 security control categories and their associated objectives that need to be addressed, and the priority determined in terms of low, medium or high risk.

7.3 Research contributions

The following subsections discuss this study's main contributions to theory and practice.

7.3.1 Contribution to Knowledge and Theory

This study's major theoretical contribution has been the development and evaluation of the Information Security Awareness Capability Model (ISACM), drawing on situation awareness theory and ISO/IEC 27002 information security standards and risk management theory. This important contribution includes the development and evaluation of an awareness importance instrument and awareness capability instrument. These two instruments allowed the calculation of the awareness risk that may exist if the existing awareness capability is less than the desired awareness importance for each ISO/IEC 27002 main security categories and their associated control objectives. This study further contributes to knowledge and theory by:

- Extending existing literature by breaking down the relevance of information security awareness for three key stakeholder groups within an organisation. These stakeholders are IT staff (including information security professionals), senior management (such as C class officers and key decision makers) and end users as the main consumers of information systems.
- Relating the cognitive information processing theory of situation awareness which draws on three progressive levels of information processing, level 1 - perception; level 2 - comprehension; and level 3 - projection, which were contextualised within best practice through the 39 main security categories and their associated control objectives of the ISO/IEC 27002 Standard;
- Introducing the concepts and measures of awareness importance, awareness capability, and awareness risk into the field of information security.
- Providing a model, the Information Security Awareness Capability Model (ISACM), that organisations can use to measure and monitor the effectiveness of information security awareness programs;

- Examining the 11 security control clauses and 39 main security categories and their associated control objectives that make up the ISO/IEC 27002 standard for information security, and identifying the relevant aspects of these clauses and control objectives that are important from an awareness perspective. This was carried out for three key stakeholder in an organisational context: IT staff, senior management, end users;
- Identifying information security awareness in terms of importance, capability and risk for three stakeholders, namely, IT staff, senior management, end users;
- Linking theories of situation awareness (Endsley 2015; Howard & Cambria 2013) with the awareness aspects of information security (SANS Institute 2015), and risk management theory (Sannicolas-Rocca, Schooley & Spears 2014), and providing an adapted model of situation awareness to incorporate information security awareness importance, awareness capability, and awareness risk into the ISACM; and
- Linking shortcomings in information security awareness capability with mainstream risk management theories and presenting information security awareness risks in a widely-accepted risk management framework (Duijm 2015; Standards Australia/Standards New Zealand 2009b).

To achieve these contributions, this study was grounded in the existing and relevant literature of information security and information security awareness, ISO/IEC 27002 standard, situation awareness theory and risk management theory. A generalisable framework and model, ISACM, was developed to investigate the extent that the relationship between awareness importance and awareness capability can predict the risk associated with an organisation’s current state of information security awareness of their information security controls.

The research results presented in Chapter 5 and discussed in Chapter 6 indicate that it is possible to determine the level of awareness capability displayed by an employee for particular security control objectives. In combination with the pre-determined awareness importance ratings for an information security control objective, the perceived level of risk that may exist for the organisation in terms of a particular information security control objective can be calculated. Based on the empirical data collected in this research from the phase 1 survey (awareness importance) and phase 2 survey (awareness capability), this level of risk could be determined at the employee level, at a stakeholder group level, and at an organisational level.

7.3.2 Contribution to Practice

Whilst many of the benefits of this research have been described above as contributions to knowledge and theory, there are also many practical benefits that flow from this research. This research contributes to practice in several ways.

Firstly, this study has focused on three separate key stakeholder groups within an organisation; these are the IT staff, senior management, and end users. Rather that treating all employees as a single homogenous group in terms of information security, this research has demonstrated that these three groups have differing requirements, priorities, and ‘need to know’ aspects in relation to information security. The results and approach to applying the ISACM developed and evaluated in this research can be utilised within a specific organisation and applied to their different stakeholder groups within their organisation. This will enable an organisation to customise their approach to managing the risks associated with information security awareness. In turn, this will result in a stronger information security posture for those organisations.

Secondly, the study identified specific aspects of the internationally-accepted information security standard (ISO/IEC 27002) that were important from an awareness perspective. This study identified these areas on a stakeholder-by-stakeholder basis. Therefore, IT staff, senior management, and end users can each be provided with guidance on what is important to them in terms of an appropriate level of awareness capability in relation to specific information security categories and their control objectives. The linkage to the international ISO/IEC 27002 standard is important for many organisations, as this is a widely-accepted best practice standard that informs the security practices of many organisations around the world. These standards are the basis for industry-accepted certification standards, often relied upon by governments, regulators and third parties that wish to satisfy themselves that an organisation is using best practice and has sound controls implemented for their information security. This current research directly links to those standards.

Thirdly, the 39 main security categories and their associated control objectives have been rated in terms of awareness importance for the three stakeholder groups. This rating provides organisations with guidance in terms of prioritising which areas of information security are more important for which stakeholder group. Many current awareness programs provide the same awareness material to all employees, irrespective of which stakeholder group they belong to. Additionally, expecting all employees to be aware of all aspects of information security is unrealistic and prone to failure. This current research, through the development and evaluation of the ISACM, provides a more targeted and holistic view for managing information security in organisations.

Fourthly, this research has developed a number of assessment instruments (in the form of survey questionnaires for awareness importance and awareness capability). The results from these assessment instruments were then combined to form an overall model, ISACM, and provide a rigorous means for determining the potential awareness risk that may exist in an organisation. The ISACM is a practical model that is grounded in well-established theory and industry standards. ISACM has strong practical application for organisations wishing to improve information security through improved awareness by identifying the performance gaps in current levels of information security awareness. ISACM allows organisations to measure the current state of information security awareness within their organisations across a number of stakeholder groups. This will highlight where awareness risk exists and allow organisations to target those areas that show the highest level of risk. By rectifying any such gaps that exist, an organisation should be able to improve their overall information security posture.

7.4 Limitations

As with most studies, this research does have some limitations. These limitations have been discussed in relation to the three major components of the ISACM.

7.4.1 Awareness Importance limitations

The methodology used to construct the awareness importance measurement relied upon the ratings provided from expert opinions of 80 information security, IT risk and IT audit professionals which provided an average score for each of the 39 main security categories and their associated control objectives. Validating the awareness importance ratings with the opinions from a much larger group of information security professionals could improve the measure of awareness importance.

Another limitation was that the version of the standard used for the basis of the awareness importance rating (ISO/IEC 27002) was the 2006 version which was subsequently updated after the researcher had conducted the phase 1 survey and data collection for determining awareness importance in the research. It was decided to use the 2006 version of the ISO/IEC 27002 standard because it is a widely-adopted standard and the new version of the standard may not be widely implemented at this point in time. Praxiom Research Group Limited (2014) provide a comparison between the old and new standard and highlight the following as the key changes:

> *'Perhaps the biggest difference between the old standard and the new one is the structure. ISO/IEC 27002:2005 had 11 main sections (5 to 14) while ISO/IEC 27002:2013 now has 14 (5 to 18). These new sections discuss cryptography, communications security, and supplier relationships (sections 10, 13, and 15 respectively)'.*

Given the updated standard was released well into the progress of this research, it was prudent to continue to use the 2006 Australian version of the standard. This minor limitation has a flow-on effect for the awareness capability and awareness risk measures. Furthermore, there are no readily available figures on the uptake rate of the updated ISO/IEC 27002 standard. It is likely that many organisations that had implemented aspects of the 2006 version of the standard would need time to assess the changes and decide when (or whether) to update their adoption of the changes to the standard. This is particularly relevant for organisations that have been certified as being compliant with the 2006 Australian version of the ISO/IEC 27002 Standard.

7.4.2 Awareness Capability limitations

An awareness importance measure was developed for each of the 39 main security categories and their associated control objectives across the three stakeholder groups (IT staff, senior management, end users). However, the awareness capability measurement developed for this research only focused on the top 10 main security categories and their control objectives (as determined by their awareness importance ratings) for end users. This was done in order to demonstrate the overall ISACM with a finite group of questions and responses within the scope, financial and time constraints of a PhD research. This research has demonstrated how the ISACM - developed from cognitive information processing theory, situation awareness and from a best practice international standard, ISO/IEC 27002 - can be implemented and has demonstrated the validity of this model in a specific organisation.

In order to deploy this ISACM more comprehensively within an organisation, the awareness capability measures could be extended to cover all 39 main security categories and their associated control objectives and extended to the other two key stakeholder groups, senior management and IT staff. The top 10 security categories and their associated control objectives in terms of awareness importance that can be determined from the phase 1 approach in ISACM represent the greatest risk points for an organisation and provide an efficient and effective way to approach raising information security awareness in organisations.

The use of a survey to capture the awareness capability score also introduces a limitation. The ideal situation would be to also incorporate direct observations of the actions someone would take when presented with an information security event. This would allow an expert observer to determine what level of awareness capability is being demonstrated in a real world situation. However, the undertaking of direct observations of employee awareness capability in an organisation is impractical due to privacy and ethical constraints. Hence, the survey approach provided a more practical way of measuring awareness capability in organisations; although it could be argued that presenting 'the right' answer amongst other answers to employees could lead to answers being selected that do not truly reflect the actions that would be taken by an employee in a real world situation.

However, this approach has the practical organisational benefit that if presented with a selection of answers, the respondent is able to identify what the correct action they should take - and this could also result in raising awareness of employees whilst trying to measure awareness capability of employees.

7.4.3 Awareness Risk limitations

There are no additional limitations to the awareness risk measurement that have not already been described above. The awareness risk measure is derived from the other two measures. Likening awareness importance to consequence (or impact) of an awareness risk for an information security control and likening awareness capability to likelihood of an awareness risk for a security control being realised has allowed this research to use classical risk management theory to portray the resultant awareness risk measure. The risk awareness measurement approach used in this research is aimed at allowing resultant risks to be determined as a qualitative measure of low, medium or high to complement the numerically-calculated score derived in the application of ISACM to a specific organisation.

7.5 Directions for future research

In this study, an awareness importance measurement was developed by relying upon the ratings provided from the expert opinions of 80 information security, IT risk and IT audit professionals. Obtaining the opinions from a much larger group could help to determine the measure in a more rigorous manner. This could be done via the International Standards Organisation standard setting group for information security (International Organization for Standardization (ISO) 2015). This organisation engages with many information security professionals as part of their standards development and updating processes. There could also be an opportunity to have these information security professionals provide a rating for awareness importance (as part of the guidance material) whilst they are developing or reviewing that specific area within the standard. Subsequently, consensus could be reached on what is an appropriate level of awareness importance for each of the 39 main security categories and their associated control objectives.

This research focused on the 39 main security categories and their associated control objectives to arrive at a rating for each of the categories. The study identified around 780 possible measurement points that could be derived from the ISO/IEC 27002 standard when it is broken down to specific supporting controls and guidance actions. Whilst this was an unrealistic number of measurement points to include in this current research, greater coverage and completeness of the ISO/IEC 27002 standard's main security categories, control objectives, and controls could be achieved by including more of these measurement points.

This presents another opportunity for the International Standards Organisation standard setting group and their wealth of reviewers who could provide this granularity of measurement points. As they work through every aspect of the standard, they would be able to obtain a consensus as to awareness importance for more of these 780 measurement points. It would also enhance the value of their standard by providing guidance as to which aspects are more important to focus on for which stakeholder group.

The awareness capability measurement instrument included in the ISACM should be expanded to include all of the 39 main security categories and their associated control objectives (rather than the 10 tested in this study). This would allow organisations to fully test the ISACM. This would also allow for the development of a full implementation guide for the ISACM. A high-level implementation guide is shown below in Figure 7-4.

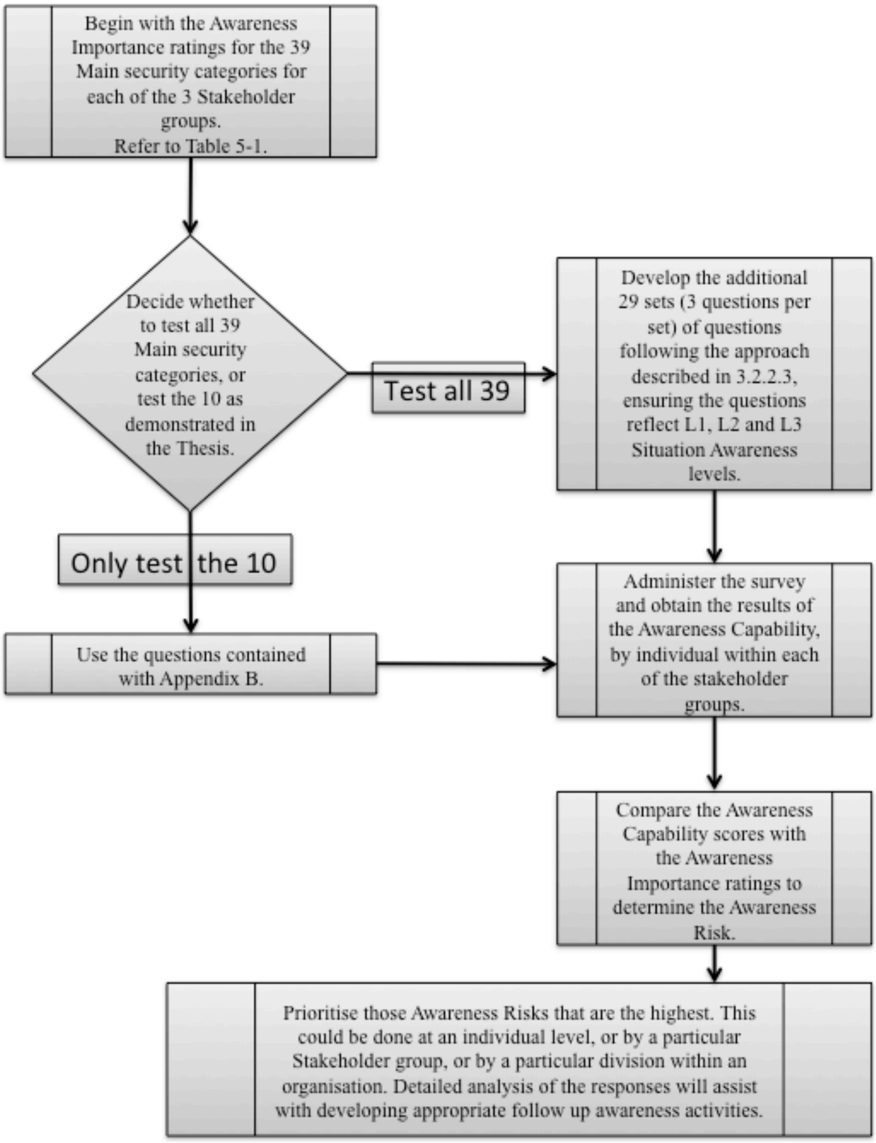

Begin with the Awareness Importance ratings for the 39 Main security categories for each of the 3 Stakeholder groups.
Refer to Table 5-1.
Decide whether to test all 39 Main security categories, or test the 10 as demonstrated in the Thesis.
Test all 39
Only test the 10
Develop the additional 29 sets (3 questions per set) of questions following the approach described in 3.2.2.3, ensuring the questions reflect L1, L2 and L3 Situation Awareness levels.
Use the questions contained with Appendix B.
Administer the survey and obtain the results of the Awareness Capability, by individual within each of the stakeholder groups.
Compare the Awareness Capability scores with the Awareness Importance ratings to determine the Awareness Risk.
Prioritise those Awareness Risks that are the highest. This could be done at an individual level, or by a particular Stakeholder group, or by a particular division within an organisation. Detailed analysis of the responses will assist with developing appropriate follow up awareness activities.

Figure 7-4 High level implementation guide for the ISACM

Finally, this research utilised the 2006 Australian version of the ISO/IEC 27002 standard to develop the ISACM (Standards Australia/Standards New Zealand 2006b). Future research on the ISACM should be updated to reflect the updated structure and content of the 2015 Australian version of the ISO/IEC 27002 standard (Standards Australia/Standards New Zealand 2015).

7.6 Final Conclusions

This chapter provided a summary of the theoretical and conceptual model developed and evaluated in this research. The methodological approach that guided the data collection and data analysis leading to key findings of this study was summarised, followed by the main contributions of this study to theory and practice. The limitations of this study were acknowledged, and directions provided for future research. This study developed an information security awareness capability model (ISACM), which is underpinned by an internationally-recognised standard for information security, ISO/IEC 27002, situation awareness theory, and risk management theory.

The following major contributions of this study in relation to the three research questions investigated are:

- An approach and instrument for measuring awareness importance of the main controls of the ISO/IEC 27002 standard for information security in terms of three stakeholder groups;
- An approach and instrument for measuring awareness capability within an organisation for these three stakeholder groups;
- An approach for calculating awareness risk of information security controls for these three stakeholder groups; and
- An overall information security awareness, capability and risk model, the ISACM, that captures the extent that the relationship between awareness importance and awareness capability predicts the awareness risks associated with an organisation's current state of information security awareness of their information security controls.

This study contributes to theory by (1) incorporating the theories of situation awareness to guide the measurement of awareness capability within an information security environment contextualised with the 39 main security categories and their associated control objectives; (2) extending existing literature by providing a breakdown of the relevance of information security awareness for three key stakeholder groups within an organisation; and (3) providing a model, the Information Security Awareness Capability Model (ISACM), that organisations can use to measuring the effectiveness of information security awareness programs.

This study further contributes to practice by providing practitioners and policy makers with a theoretical and practical information security awareness capability model. ISACM will assist and enhance organisations' approach to developing information security awareness programs, their approach to measuring awareness capability and awareness risk, and their approach to targeting the correct awareness to the appropriate stakeholder groups. The resultant benefits of improving information security awareness within an organisation, and therefore the information security posture of that organisation, are many and include:

- Enabling workplace mobility and flexibility,
- Increased confidence from customers and external partners,
- Preventing data loss, ensuring privacy and protecting intellectual property,
- Reduced likelihood of identity theft and financial fraud,
- Maintaining compliance with industry and government regulators,
- Improved business resilience (continuity),
- Minimising the impacts of any information security breaches,

8.0 List of References

Ab Rahman, NH & Choo, K-KR 2015, 'A survey of information security incident handling in the cloud', *Computers & Security*, vol. 49, pp. 45-69.

Abawajy, J, Thatcher, K & Kim, T-h 2008, 'Investigation of Stakeholders Commitment to Information Security Awareness Programs', in 2008 International Conference on Information Security and Assurance: *proceedings of the2008 International Conference on Information Security and Assurance* pp. 472-6.

ABC News 2013, 'Telstra sorry for north Qld outage', *ABC News*, viewed 11/01/2015, <http://www.abc.net.au/news/2013-01-29/telstra-sorry-for-north-qld-outage/4488544>

Abdul-Rahman, H, Mohd-Rahim, FA & Chen, W 2012, 'Reducing failures in software development projects: effectiveness of risk mitigation strategies', *Journal of Risk Research*, vol. 15, no. 4, pp. 417-33.

Acar, T, Belenkiy, M & Küpçü, A 2013, 'Single password authentication', *Computer Networks*, vol. 57, no. 13, pp. 2597-614.

Ahmad, A, Bosua, R & Scheepers, R 2014, 'Protecting organizational competitive advantage: A knowledge leakage perspective', *Computers & Security*, vol. 42, pp. 27-39.

Al-Hakim, L 2007, 'Information quality factors affecting innovation process', *International Journal Information Quality*, vol. 1, no. 2, pp. 162 - 88.

Al-Omari, A, El-Gayar, O & Deokar, A 2012, 'Security Policy Compliance: User Acceptance Perspective', in 45th Hawaii International Conference on System Sciences: *proceedings of the45th Hawaii International Conference on System Sciences* Hawaii, pp. 3317-26.

AlAboodi, SS 2006, 'A New Approach for Assessing the Maturity of Information Security', *ISACA Journal Online*, no. Journal Online, p. 7.

Albrechtsen, E & Hovden, J 2010, 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study', *Computers & Security*, vol. 29, no. 4, pp. 432-45.

Anttila, J, Kajava, J & RaunoVaronen 2004, 'Balanced integration of information security into business management', in 30th EUROMICRO Conference (EUROMICRO' '04): *proceedings of the30th EUROMICRO Conference (EUROMICRO' '04)*.

Applegate, SD 2009, 'Social Engineering: Hacking the Wetware!', *Information Security Journal: A Global Perspective*, vol. 18, no. 1, pp. 40-6.

Arabo, A & Pranggono, B 2013, 'Mobile Malware and Smart Device Security: Trends, Challenges and Solutions', pp. 526-31.

Aslam, BBM & Aziz, JSA 2015, 'E-mail Security Threats', *Indian Streams Research Journal*, vol. 5, no. 3, pp. 1-6.

Australian Bureau of Statistics (ABS) 2011, '4528.0 - Personal Fraud, 2010-2011', <http://www.abs.gov.au/ausstats/abs@.nsf/PrintAllPreparePage?>

Australian Government, *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime - The Report of the Inquiry into Cyber Crime,* 2010, HoRSCo Communications, House of Representatives: Standing Committee on Communications,, Canberra.

Australian Government, *Cyber Crime and Security Survey Report 2012,* 2012, CfI Safety, CERT Australia, <http://www.canberra.edu.au/cis/storage/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf>.

Australian Government, *Cyber Crime & Security Survey Report 2013,* 2013a, CERT Australia.

Australian Government 2013b, *Stay Smart Online*, Office of the Australian Information Commisioner, viewed 29/05/2013, <http://www.staysmartonline.gov.au>.

Australian Government, *Identity Crime And Misuse In Australia - Key findings from the National Identity Crime and Misuse Measurement Framework Pilot,* 2014, Attorney-General's Department, <http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/IdentityCrimeAndMisuseInAustralia.pdf>.

Australian Government, *The Privacy Act 1988,* 2015, Office of the Australian Information Commissioner, <http://www.oaic.gov.au/privacy/privacy-act/the-privacy-act>.

Australian Payments Clearing Association [APCA] 2014, *CECS manual for Consumer Electroni Clearing System*, <http://www.apca.com.au>.

Australian Prudential Regulatory Authority (APRA), *Prudential Practice Guide PPG234 - Management of security risk in information and information technology,* 2010, Australian Prudential Regulation Authority, Commonwealth of Australia, Barton.

Australian Prudential Regulatory Authority (APRA) 2013, *Draft APRA Prudential Standard CPS 220 - Risk Management.*

Australian Research Council [ARC] 2007, *Safeguarding Australia*, Australian Research Council, <http://www.dest.gov.au/sectors/research_sector/policies_issues_reviews/key_issues/national_research_priorities/priority_goals/safeguarding_australia.htm>.

Australian Securities and Investment Commission (ASIC) 2008, *Nigerian scams*, Australian Securities and Investment Commission (ASIC),, viewed 10/09/2008, <http://www.fido.asic.gov.au/fido/fido.nsf/byheadline/Nigerian+scams?openDocument>.

Australian Seniors Computer Clubs Association [ASCCA] 2013, *Australian Seniors Computer Clubs Association [ASCCA],*, viewed 29/05/2013, <http://www.ascca.org.au>.

Baracaldo, N & Joshi, J 2013, 'An adaptive risk management and access control framework to mitigate insider threats', *Computers & Security*, vol. 39, pp. 237-54.

Barford, P, Dacier, M, Dietterich, TG, Fredrikson, M, Giffin, J, Jajodia, S, Jha, S, Li, J, Liu, P, Ning, P, Ou, X, Song, D, Strater, L, Swarup, V, Tadda, G, Wang, C & Yen, J 2009, 'Cyber SA: Situational Awareness for Cyber Defense', in S Jajodia (ed.), *Cyber Situation Awareness: Issues and Research*, Springer, New York, ch 1.

Baskerville, R, Spagnoletti, P & Kim, J 2014, 'Incident-centered information security: Managing a strategic balance between prevention and response', *Information & Management*, vol. 51, no. 1, pp. 138-51.

Bayuk, J 2009, 'How to Write an Information Security Policy', *CSO Security and Risk*, viewed 27/03/2011, <http://www.csoonline.com/article/495017/how-to-write-an-information-security-policy>

BBC News 2014, 'Gibraltar fire disrupts online gambling industry', *BBC News*, viewed 11/01/2015, <http://www.bbc.com/news/uk-27098178>

Berghout, E, Nijland, M & Powell, P 2011, 'Management of lifecycle costs and benefits: Lessons from information systems practice', *Computers in Industry*, vol. 62, no. 7, pp. 755-64.

Bhattacherjee, A 2012, *Social Science Research: Principles, Methods, and Practices*, Second edn, Creative Commons Attribution 3.0 License:.

Boersma, K 2012, 'Leadership and Awareness as Key Issues in Information Security Management', *Organization Management Journal*, vol. 9, no. 1, pp. 63-.

Breton, R & Rousseau, R 2003, 'Situation Awareness: A review of the concept and its measurement', <http://pubs.rddc.gc.ca/BASIS/pcandid/www/engpub/DDW?W%3DAUTHOR+%3D+%27Breton%2C+R.%27%26M%3D8%26K%3D518754%26U%3D1>

Breton, R, Tremblay, S & Banbury, S, *Measurement of individual and Team situation awareness: A critical evaluation of the available metrics and tools and their applicability to command and control environments,* 2007, Defence R&D Canada.

Bronk, C 2015, 'Two securities: How contemporary cyber geopolitics impacts critical infrastructure protection', *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 24-6.

Brotherton, H & Dietz, JE 2014, 'Data Center Business Continuity Best Practice', in 2014 11th International Conference on Information Technology: New Generations: *proceedings of the2014 11th International Conference on Information Technology: New Generations* Las Vegas, Nevada, USA, pp. 496-501.

Brown, P, Sciutto, J, Perez, E, Acosta, J & Bradner, E 2014, 'Investigators think hackers stole Sony passwords', viewed 11/01/2015, <http://edition.cnn.com/2014/12/18/politics/u-s-will-respond-to-north-korea-hack/>

Bulgurcu, B, Cavusoglu, H & Benbasat, I 2010, 'Information Security policy compliance: An empirical study of rationality-based beliefs and information security awareness', *MIS Quarterly*, vol. 34, no. 3, pp. 523-48.

Burdon, M, Reid, J & Low, R 2010, 'Encryption safe harbours and data breach notification laws', *Computer Law & Security Review*, vol. 26, no. 5, pp. 520-34.

Burdon, M, Lane, B & von Nessen, P 2012, 'Data breach notification law in the EU and Australia – Where to now?', *Computer Law & Security Review*, vol. 28, no. 3, pp. 296-307.

Burke, ME 2007, 'Making choices: research paradigms and information management: Practical applications of philosophy in IM research', *Library Review*, vol. 56, no. 6, pp. 476-84.

Burkett, JS 2012, 'Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®', *Information Security Journal: A Global Perspective*, vol. 21, no. 1, pp. 47-54.

Byrne, A 2014, 'Governance, Strategic Risk, Internal Audit: What Auditors Need to Know', *Edpacs*, vol. 49, no. 2, pp. 6-14.

Cady, RP 2005, 'Expertise Required to Reap Rewards From Overseas Outsourcing of IT', *Pulp & Paper*, vol. 79, no. 9, p. 4.

Calder, A & Watkins, S 2007, *Information Security Risk Management for ISO27001/ISO17799*, IT Governance Publishing.

Cambridge Dictionaries Online 2011, *Awareness*, viewed 6 April 2011, <http://dictionary.cambridge.org/dictionary/british/awareness>.

Cameron, M, Robinson, B, Power, R & Yin, J 2012, 'Emergency Situation Awareness from Twitter for Crisis Management', in WWW 2012 – SWDM'12 Workshop: *proceedings of theWWW 2012 – SWDM'12 Workshop* Lyon, France.

Campello, M, Graham, JR & Harvey, CR 2010, 'The real effects of financial constraints: Evidence from a financial crisis', *Journal of Financial Economics*, vol. 97, no. 3, pp. 470-87.

Chai, S, Bagchi-Sen, S, Morrell, C, Rao, HR & S.Upadhyaya 2006, 'Role of Perceived Importance of Information Security- An Exploratory Study of Middle School Children's Information Security Behavior', *Issues in Informing Science and Information Technology*, vol. 3.

Chakravarthy, ASN & Kumar, TVS 2012, 'Survey on Computer Crime Scene Investigation Forensic Tools', *International Journal of Computer Trends and Technology*, vol. 3, no. 2.

Chang, SE & Ho, CB 2006, 'Organizational factors to the effectiveness of implementing information security management', *Industrial Management & Data Systems*, vol. 106, no. 3, pp. 345-61.

Chege, S 2007, 'Security Maturity Models', *ISACA South Africa,*, viewed 29/03/2013, <http://www.isaca.org.za/download.aspx>

Chen, CC, Medlin, BD & Shaw, RS 2008, 'A cross-cultural investigation of situational information security awareness programs', *Information Management & Computer Security*, vol. 16, no. 4, pp. 360-76.

Choi, N, Kim, D, Goo, J & Whitmore, A 2008, 'Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action', *Information Management & Computer Security*, vol. 16, no. 5, pp. 484-501.

Chou, T-S 2013, 'Security Threats on Cloud Computing Vulnerabilities', *International Journal of Computer Science and Information Technology*, vol. 5, no. 3, pp. 79-88.

Commonwealth Bank of Australia 2015, *Security & Privacy - Commonwealth Bank Group*, Commonwealth Bank of Australia,, viewed 29/05/2015, <http://www.commbank.com.au/security-privacy.html>.

Connelly, CE, Archer, NP, Yuan, Y & Guo, KH 2011, 'Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model', *Journal of Management Information Systems*, vol. 28, no. 2, pp. 203-36.

Costello, T 2012, 'Business Continuity- Beyond Disaster Recovery', *IT Professional*, vol. 14, no. 5.

Craw, V 2014, 'Commonwealth Bank experiencing 'system problems', *News.com.au*, viewed 10/01/2015, <http://www.news.com.au/finance/business/commonwealth-bank-experiencing-system-problems/story-fnkjidjt-1226884936206>

Curts, RJ, Campbell, D & MacArthur, JE 2002, *Building A Global Information Assurance Program*, CRC Press.

D'Arcy, J & Greene, G 2014, 'Security culture and the employment relationship as drivers of employees' security compliance', *Information Management & Computer Security*, vol. 22, no. 5, pp. 474-89.

D'Arcy, J, Hovav, A & Galletta, D 2009, 'User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach', *Information Systems Research*, vol. 20, no. 1, pp. 79-98.

Da Veiga, A & Eloff, JHP 2010, 'A framework and assessment instrument for information security culture', *Computers & Security*, vol. 29, no. 2, pp. 196-207.

Danish Jamil & Khan, MNA 2011, 'Is Ethical Hacking Ethical?', *International journal of engineering science and technology*, vol. 3, pp. 3758-63.

Davis, JT 2012, 'Examining perceptions of local law enforcement in the fight against crimes with a cyber component', *Policing: An International Journal of Police Strategies & Management*, vol. 35, no. 2, pp. 272-84.

de Leeuw, ED 2012, 'Counting and Measuring Online: The Quality of Internet Surveys', *Bulletin of Sociological Methodology/Bulletin de M&#x00E9;thodologie Sociologique*, vol. 114, no. 1, pp. 68-78.

de Vaus, DA 2002, *Surveys in Social Research*, Fifth Edition edn, Allen & Unwin, Crows Nest, NSW.

Dearne, K 2008a, 'IT Security needs makeover: experts', viewed 20 May 2008, <http://www.australianit.news.com.au/story/0,24897,23730194-5013040,00.html>

Dearne, K 2008b, 'Online users lack security skills: AusCERT', viewed 20 May 2008, <http://www.australianit.news.com.au/story/0,24897,23730194-5013040,00.html>

Deloitte LLP 2012, 'IT Outsourcing Risks and How to Mitigate Them', *CIO Journal*.

Desman, MB 2002, *Building an Information Security Awareness Program*, CRC Press, Boca Raton, Florida.

Desouza, KC 2009, 'Securing information assets: The great information game', *Business Information Review*, vol. 26, no. 1, pp. 35-41.

Dillman, D 2000, *Mail and Internet surveys: the tailored design method*, John Wiley, New York.

Drevin, L, Kruger, H & Steyn, T 2007, 'Value-focused assessment of ICT security awareness in an academic environment', *Computers & Security*, vol. 26, no. 1, pp. 36 - 43.

Duijm, NJ 2015, 'Recommendations on the use and design of risk matrices', *Safety Science*, vol. 76, pp. 21-31.

Edwards, C 2014, 'Ending identity theft and cyber crime', *Biometric Technology Today*, vol. 2014, no. 2, pp. 9-11.

Endsley, MR 1995, 'Toward a Theory of Situation Awareness in Dynamic Systems', *Human Factors*, pp. 32-64.

Endsley, MR 1999, 'Situation Awareness and Human Error: Designing to Support Human Performance', in High Consequence Systems Surety Conference: *proceedings of theHigh Consequence Systems Surety Conference* Albuquerque, NM.

Endsley, MR 2015, 'Situation Awareness Misconceptions and Misunderstandings', *Journal of Cognitive Engineering and Decision Making*, vol. 9, no. 1, pp. 4-32.

Endsley, MR & Garland, DJ 2000, *Situation Awareness Analysis and Measurement*, Lawrence Erlbaum Associates, Mahwah, New Jersey.

Endsley, MR & Robertson, MM 2001, 'Training For Situation Awareness', viewed 25/04/2011, <www.satechnologies.com/Papers/pdf/SATrainingchapter.pd>

Endsley, MR, Sollenberger, R & Stein, E 2000, 'Situation Awareness: A comparison of measures', in Human Performance, Situation Awareness and Automation: User Centred Design for the New Millennium: *proceedings of theHuman Performance, Situation Awareness and Automation: User Centred Design for the New Millennium*.

European Network and Information Security Agency (ENISA) 2007, 'Information security awareness: Local government and Internet service providers', p. 120, <http://www.enisa.europa.eu/pages/05_01.htm>

European Network and Information Security Agency (ENISA) 2010, 'The new users guide: How to raise information security awareness', viewed 11/05/2014,

European Network and Information Security Agency (ENISA) & PricewaterhouseCoopers, *Information security awareness initiatives: Current practice and the measurement of success,* 2007, ENISA.

European Network and Information Security Agency (ENISA), Marinos, L & Sfakianakis, A, *ENISA Threat Landscape - Reponding to the Evolving Threat Environment,* 2012.

European Network and information Security Agency (ENISA), Maj, M, Reijers, R & Stikvoort, D 2010, 'Good Practice Guide for Incident Management', <https://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management>

European Network and Information Security Agency (ENISA), Rywczyńska, A, Refalo, P-L, Telmon, C & Wiele, J 2008, 'Awareness Raising Quizzes Templates - Targeting Parents, End-users and SMEs', viewed 11/05/2014, European Network and Information Security Agency (ENISA), Haeberlen, T, Dupré, L, Catteddu, D & Hogben, G 2012, 'Cloud Computing: Benefits, risks and recommendations for information security', <http://www.enisa.europa.eu>

European Organisation for the Safety of Air Navigation 2003, *The Development of Situation Awareness Measures in ATM Systems*.

Everett, C 2010, 'Embedding security: when technology is no longer enough', *Computer Fraud & Security*, vol. 2010, no. 11, pp. 5-7.

Everett, C 2011a, 'Identity and Access Management: the second wave', *Computer Fraud & Security*, vol. 2011, no. 5, pp. 11 - 3.

Everett, C 2011b, 'Building solid foundations: the case for data classification', *Computer Fraud & Security*, vol. 2011, no. 6, pp. 5-8.

Facebook 2015, *Facebook Security*, viewed 21/01/2015, <http://www.facebook.com/security>.

Fanning, K 2014, 'Cloud Software: How to Validate Third-Party Vendors', *Journal of Corporate Accounting & Finance*, vol. 25, no. 5, pp. 25-30.

Fink, AA & Major, DA 2000, 'Measuring situation awareness: A comparison of three techniques', in Human performance, situation awareness & automation: User-centered design for the new millennium *proceedings of theHuman performance, situation awareness & automation: User-centered design for the new millennium* D.B. Kaber, & M.R. Endsley, Savannah, Georgia.

Folorunso, O, Taofiki, A & Ikuomola, AJ 2010, 'Using Visual Analytics to Develop Situation Awareness in Network Intrusion Detection System', *Computer and Information Science*, vol. 3, no. 4, p. 13.

Fonseca, J, Seixas, N, Vieira, M & Madeira, H 2014, 'Analysis of Field Data on Web Security Vulnerabilities', *IEEE transactions on dependable and secure computing*, vol. 11, no. 2.

French, HT & Hutchinson, A 2002, 'Measurement of Situation Awareness in a C4ISR experiment', in 7th International Command and Control Research and Technology Symposium,: *proceedings of the7th International Command and Control Research and Technology Symposium,* Quebec City, Canada.

Friedberg, I, Skopik, F, Settanni, G & Fiedler, R 2015, 'Combating advanced persistent threats: From network event correlation to incident detection', *Computers & Security*, vol. 48, pp. 35-57.

Furnell, S 2007, 'An assessment of website password practices', *Computers & Security*, vol. 26, no. 7-8, pp. 445-51.

Galusha, C 2001, 'Getting Started with IT Asset Management', *IT Professional*, vol. 3, no. 3.

Garfinkel, SL 2013, 'Digital Forensics', *American Scientist*, vol. 101, no. 5.

Gartner & Wagner, R 2006, 'Information Security Solved - Economics of IT', in Economics of IT Conference 2006: *proceedings of theEconomics of IT Conference 2006* Gartner, Sao Paulo, Brazil, <http://www.gartner.com/2_events/conferences/2006/brl27l/brl27l.jsp>.

Gartner, Witty, RJ & Wagner, R 2005, 'Awareness training is necessary to support your information security program ', no. G00125896, <http://www.gartner.com/DisplayDocument?id=470426&ref=g_sitelink>

Gartner, Pettey, C & Tudor, B 2010, *Gartner Says SAS 70 Is Not Proof of Security, Continuity or Privacy Compliance*, Gartner, viewed 15 May 2011, <http://www.gartner.com/it/page.jsp?id=1400813>.

Gartner, Witty, RJ, Mogull, R, Wagner, R, Williams, AT, Noakes-Fry, K & Allan, A 2005, 'Information Security Awareness Training Is Essential to Protect IT Assets', viewed 01/02/2015, <https://www.gartner.com/doc/468019?ref=ddisp>

Ghemri, L & Kannah, R 2015, 'Privacy in Medical Data Publishing', *International Journal of Cyber-Security and Digital Forensics*, vol. 1, no. 1, pp. 41-9.

Glen, P 2012, 'In the tech world, management is not a promotion', *Computerworld*, *Computerworld*, viewed 03/06/2013, <http://www.computerworld.com/s/article/9224565/Paul_Glen_In_Tech_Management_Is_Not_a_Promotion>

Godlove, T 2012, 'Examination of the Factors that Influence Teleworkers' Willingness to Comply with Information Security Guidelines', *Information Security Journal: A Global Perspective*, vol. 21, no. 4, pp. 216-29.

Gray, DM & Christiansen, L 2010, 'A Call to Action- The Privacy Dangers Adolescents Face through Use of Facebook.com', *Journal of Information Privacy & Security*, vol. 6, no. 2, p. 17.

Guba, EG & Lincoln, YS 1994, 'Competing Paradigms in Qualitative Research', in NK Denzin & YS Lincoln (eds), *Handbook of qualitative research*, Sage Publications, London, pp. 105-17.

Gundu, T & Flowerday, SV 2012, 'The enemy within: A behavioural intention model and an information security awareness process', in Information Security for South Africa (ISSA): *proceedings of theInformation Security for South Africa (ISSA)* Johannesburg.

Gupta, S, Vinayak, GV & Gupta, A 2012, 'Software failure analysis in requirement phase', in 5th India Software Engineering Conference: *proceedings of the5th India Software Engineering Conference* Kanpur, India, pp. 101-4.

Habib, MA, Mahmood, N, Shahid, M, Aftab, MU, Ahmad, U & Faisal, CMN 2014, 'Permission based implementation of Dynamic Separation of Duty (DSD) in Role based Access Control (RBAC)', in
8th International Conference on Signal Processing and Communication Systems (ICSPCS): *proceedings of the*
8th International Conference on Signal Processing and Communication Systems (ICSPCS) Gold Coast, Queensland, Australia, pp. 1-10.

Hagen, JM, Albrechtsen, E & Hovden, J 2008, 'Implementation and effectiveness of organisational information security measures', *Information Management & Computer Security*, vol. 16, no. 4, pp. pp. 377-97.

Hambling, B & Goethem, Pv 2013, *User acceptance testing: a step=by-step guide*, BCS Learning and Development Ltd, Swindon, U.K.

He, B-Z, Chen, C-M, Su, Y-P & Sun, H-M 2014, 'A defence scheme against Identity Theft Attack based on multiple social networks', *Expert Systems with Applications*, vol. 41, no. 5, pp. 2345-52.

He, W 2013, 'A survey of security risks of mobile social media through blog mining and an extensive literature search', *Information Management & Computer Security*, vol. 21, no. 5, pp. 381-400.

Herath, T & Rao, HR 2009, 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness', *Decision Support Systems*, vol. 47, no. 2, pp. 154-65.

Hesse, M & Pohlmann, N 2008, 'Internet Situation Awareness', viewed 12/06/2010,

Hetling, A, Watson, S & Horgan, M 2014, 'We Live in a Technological Era, Whether you like it or Not - Client Perspectives and Online Welfare Applications', *Administration & Society*, vol. 46, no. 5, pp. 519-47.

Höglund, F, Berggren, P & Nählinder, S 2009, *Using Shared Priorities to Measure Shared Situation Awareness*, Swedish Defence Research Agency.

Holmberg, R & Sundström, M 2012, 'Leadership and the Psychology of Awareness: Three Theoretical Approaches to Information Security Management', *Organization Management Journal*, vol. 9, no. 1, pp. 64-77.

Horcher, A-M & Tejay, GP 2009, 'Building A Better Password: The Role of Cognitive Load in Information Security Training', in International Conference onIntelligence and Security Informatics: *proceedings of theInternational Conference onIntelligence and Security Informatics* Dallas, Texas.

Horn, S, *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies,* 2000, United States General Accounting Office, United States General Accounting Office,, Washington, D.C.

Hou, S, Yiuy, S-M, Ueharaz, T & Sasakix, R 2013, 'A Privacy-Preserving Approach for Collecting Evidence in Forensic Investigation', *International Journal of Cyber-Security and Digital Forensics*, vol. 2, no. 1, pp. 70 - 8.

Hove, C, Tarnes, M, Line, MB & Bernsmed, K 2014, 'Information Security Incident Management: Identified Practice in Large Organizations', pp. 27-46.

Howard, N & Cambria, E 2013, 'Intention awareness- improving upon situation awareness in human-centric environments', *Human-centric Computing and Information Sciences*, vol. 3, no. 1.

HSBC Holdings 2015, *Online security - HSBC Holdings*, viewed 14 January 2015, <http://www.hsbc.com/1/2/online-security>.

Hu, Q, Dinev, T, Hart, P & Cooke, D 2012, 'Managing Employee Compliance with Information Security Policies- The Critical Role of Top Management and Organizational Culture', *Decision Sciences - A Journal of the Decision Science Institute*, vol. 43, no. 4.

Huang, S-M, Lee, C-L & Kao, A-C 2006, 'Balancing performance measures for information security management: A balanced scorecard framework', *Industrial Management & Data Systems*, vol. 106, no. 2, pp. 242-55.

Hutchinson, J 2011, 'Three months to rebuild Queensland comms: Telstra', *www.computerworld.com.au*, viewed 06/04/2011, <http://www.computerworld.com.au/article/373318/three_months_rebuild_queensland_comms_telstra/>

Imgraben, J, Engelbrecht, A & Choo, K-KR 2014, 'Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users', *Behaviour & Information Technology*, vol. 33, no. 12, pp. 1347-60.

Information Systems Audit and Control Association [ISACA] 2015, *Elevate your Professional Stature - Earn an ISACA Certification*, ISACA, viewed 12/02/2015, <http://www.isaca.org>.

Information Systems Audit and Control Association [ISACA], Ross, SJ, Stewart-Rattray, J, Dimitriadis, C, Goucher, W, Kromberg, N, Sveen, FO, Poole, V & Sethi, R 2011, *Creating a Culture of Security*, ISACA, viewed 21/10/2012, <http://www.isaca.org>.

International Information System Security Certification Consortium [ISC]2 2015, *Certification Programs*, International Information Systems Security Certification Consortium, United States, viewed 10/04/2015, <https://www.isc2.org>.

International Organization for Standardization (ISO) 2008, *ISO/IEC 27005:2008(E) Information technology - Security techniques - Information security risk management*, International Organization for Standardization (ISO),, viewed 01/11/2008, <http://www.iso.org/iso/home.htm>.

International Organization for Standardization (ISO) 2013, 'The ISO Survey of Management System Standard Certifications – 2013 Executive summary', viewed 17 April 2015, <http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2013>

International Organization for Standardization (ISO) 2015, *How does ISO develop standards?*, viewed 17 June 2015, <http://www.iso.org/iso/home/standards_development.htm>.

Ipsos Public Affairs 2010, '2010 MAAWG Email Security Awareness and Usage Report', p. 87, viewed March 2010, <www.maawg.org>

IT Governance Institute (ITGI) 2008, *Aligning COBIT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit*, http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT-ITIL-V3-ISO27002-for-Business-Benefit_res_Eng_1108.pdf>.

Ittersum, Kv, Pennings, JME, Wansink, B & Trijp, HCMv 2004, 'A Multidimensional approach to measuring attribute importance', *Advances in Consumer Research*, vol. 31.

IWS - The Information Warfare Site 2008, *Security Awareness Toolbox*, IWS, viewed 20/08/2008, <http://www.iwar.org.uk/comsec/resources/sa-tools/>.

Jajodia, S, Liu, P, Swarup, V & Wang, C 2010, *Cyber Situational Awarness: Issues and Research*, Springer, New York.

James, J, Mabry, F, Leger, AS, Cook, T & Huggins, K 2013, 'Cyber-Physical Situation Awareness and Decision Support', in Network Science Workshop (NSW), 2013 IEEE 2nd: *proceedings of theNetwork Science Workshop (NSW), 2013 IEEE 2nd* West Point, NY, <http://ieeexplore.ieee.org.ezproxy.usq.edu.au/xpls/abs_all.jsp?arnumber=6609205>.

Jeffries, K, 2014, 'Is Your Social Media Usage a Red Flag for Employers & Recruiters?', *People People blog*, <http://people2people.com.au/blog/social-media-usage-red-flag-employers-recruiters/>.

Johannsdottir, KR & Herdman, CM 2010, 'The Role of Working Memory in Supporting Drivers' Situation Awareness for Surrounding Traffic', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 52, no. 6, pp. 663-73.

Johnson, ME & Goetz, E 2007, 'Embedding Information Security into the Organization', *IEEE Computer Society*, no. May/June 2007, pp. 16-24.

Joshi, A, Kale, S, Chandel, S & Pal, D 2015, 'Likert Scale: Explored and Explained', *British Journal of Applied Science & Technology*, vol. 7, no. 4, pp. 396-403.

Kajava, J, Varonen, R, Anttila, j & Savola, R 2006, 'Senior Executives Commitment to Information Security - from Motivation to Responsibility', *IEEE Xplore*.

Kaner, M & Karni, R 2004, 'A Capability Maturity Model for Knowledge-Based Decisionmaking', *Information Knowledge Systems Management*, vol. 4, p. 29.

Kardos, M, *Behavioural Situation Awareness Measures and the Use of Decision Support Tools in Exercise Prowling Pegasus,* 2003, Do Defence, Australian Government, Edinburgh, South Australia.

Karokola, G, Kowalski, S & Yngström, L 2011, 'Towards An Information Security Maturity Model for Secure e-Government Services - A Stakeholders View', in 5th International Symposium on Human Aspects of Information Security & Assurance: *proceedings of the5th International Symposium on Human Aspects of Information Security & Assurance* London, <http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-67206>.

Kayworth, T & Whitten, D 2010, 'Effective information security requires a balance of social and technology factors', *MIS Quarterly Executive*, vol. 9, no. 3, pp. 163 - 75.

Kelly, K 2013, 'Computer forensics from a law enforcement perspective', in *Advances in Cyber Security: Technology, Operations, and Experiences*, Fordham Universal Press, pp. 188 - 99.

Khaiyum, S, Kumaraswamy, YS & Karibasappa, K 2014, 'Significance of Failure Avoidance in Software Development Process', pp. 340-4.

Khanmohammadi, K & Houmb, SH 2010, 'Business Process-Based Information Security Risk Assessment', in 2010 Fourth International Conference on Network and System Security: *proceedings of the2010 Fourth International Conference on Network and System Security* IEEE, Melbourne, Australia, pp. 199-206.

Kho, ND 2009, 'The Changing Face of Identity Management', *EContent*, no. April 2009, <http://www.econtentmag.com>

Khurana, P & Bindal, P 2014, 'Test Data Management', *International Journal of Computer Trends and Technology (IJCTT)*, vol. 15, no. 4, pp. 162-7.

Kierkegaard, P 2012, 'Medical data breaches: Notification delayed is notification denied', *Computer Law & Security Review*, vol. 28, no. 2, pp. 163-83.

Kilgore, A, Mazza, T, Azzali, S & Fornaciari, L 2014, 'Audit quality of outsourced information technology controls', *Managerial Auditing Journal*, vol. 29, no. 9, pp. 837-62.

Kim, EB 2013, 'Information Security Awareness Status of Business College: Undergraduate Students', *Information Security Journal: A Global Perspective*, vol. 22, no. 4, pp. 171-9.

Kirda, E, Jovanovic, N, Kruegel, C & Vigna, G 2009, 'Client-side cross-site scripting protection', *Computers & Security*, vol. 28, no. 7, pp. 592-604.

Kirk, D 2014, 'Identifying Identity Theft', *The Journal of Criminal Law*, vol. 78, no. 6.

Klein, G 2000, 'Analysis of situation awareness from critical incident reports', in *Situation Awareness Analysis and Measurement*, Lawrence Eribaum Associates Inc., ch In M.R. Endsley, & D.J.Garland (Eds), pp. 51-71.

Knapp, KJ, Marshall, TE, Rainer, RK & Ford, FN 2006, 'Information security: management's effect on culture and policy', *Information Management & Computer Security*, vol. 14, no. 1, pp. 24-36.

Kokar, MM & Endsley, MR 2012, 'Situation Awareness and Cognitive Modeling', *IEEE Computer Society*, vol. May/June 2012.

KPMG Australia 2015, 'Cyber Security Risk Management', viewed 7 January, 2015, <www.kpmg.com.au>

Kruger, H, Drevin, L & Steyn, T 2010, 'A vocabulary test to assess information security awareness', *Information Management & Computer Security*, vol. 18, no. 5, pp. 316-27.

Kruger, HA & Kearney, WD 2006, 'A prototype for assessing information security awareness', *Computers & Security*, no. 25, pp. 289-96.

Lai, F, Li, D & Hsieh, C-T 2012, 'Fighting identity theft: The coping perspective', *Decision Support Systems*, vol. 52, no. 2, pp. 353-63.

Lam, S & Chung, W 2010, 'Uses of Internet and Mobile Technology in Health Systems for the Elderly: A Case Study of Hong Kong', *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 4, no. 2.

Laughton, PA 2008, 'Hierarchical analysis of acceptable use policies', *South African Journal of Information Management*, vol. 10, no. 4.

Lebek, B, Uffen, J, Breitner, MH, Neumann, M & Hohler, B 2013, 'Employees' Information Security Awareness and Behavior: A Literature Review', pp. 2978-87.

Lefever, S, Dal, M & Matthíasdóttir, Á 2007, 'Online data collection in academic research: advantages and limitations', *British Journal of Educational Technology*, vol. 38, no. 4, pp. 574-82.

Lindström, J 2012, 'A model to explain a business contingency process', *Disaster Prevention and Management*, vol. 21, no. 2, pp. 269-81.

Liu, B, Shi, L, Cai, Z & Li, M 2012, 'Software Vulnerability Discovery Techniques: A Survey', pp. 152-6.

Liu, H, Kuo, F-C & Chen, TY 2010, 'Teaching an End-User Testing Methodology', pp. 81-8.

Lowry, PB & Moody, GD 2013, 'Explaining Opposing Compliance Motivations towards Organizational Information Security Policies', in 46th Hawaii International Conference on System Sciences: *proceedings of the46th Hawaii International Conference on System Sciences* IEEE, Hawaii, pp. 2998-3007.

Manders-Huits, N 2010, 'Practical versus moral identities in identity management', *Ethics and Information Technology*, vol. 12, no. 1, pp. 43-55.

Maqousi, A, Balikhina, T & Mackay, M 2013, 'An Effective Method for Information Security Awareness Raising Initiatives', *International Journal of Computer Science and Information Technology*, vol. 5, no. 2, pp. 63-72.

Martilla, JA & James, JC 1977, 'Importance-performance analysis', *Journal of Marketing*, vol. 41, pp. 77-9.

Masys, AJ 2005, 'A systemic perspective of situation awareness: An analysis of the 2002 mid-air collision over Überlingen, Germany', *Disaster Prevention and Management*, vol. 14, no. 4, pp. 548-57.

Matthews, MD & Beal, SA 2002, *Assessing Situation Awareness in Field Training Exercises*, 1795, U.S. Army Research Institute.

McCarthy, L, Watson, K & Weldon-Siviy, D 2012, 'Own Your Space: A Guide to Facebook Security For Young Adults, Parents, and Educators', <http://www.facebook.com/security/app_268616169836752>

McFadzean, E, Ezingeard, J-N & Birchall, D 2007, 'Perception of risk and the strategic impact of existing IT on information security strategy at board level', *Online Information Review*, vol. 31, no. 5, pp. 622 - 60, Emerald Group Publishing Limited.

Mejias, RJ 2012, 'An Integrative Model of Information Security Awareness for Assessing Information Systems Security Risk', pp. 3258-67.

Merriam-Webster Dictionary 2015a, *Paradigm - Definition by Merriam-Webster Dictionary*, <http://www.merriam-webster.com/dictionary/paradigm>.

Merriam-Webster Dictionary 2015b, *Projection - Definition by Merriam-Webster Dictionary*, <http://www.merriam-webster.com/dictionary/projection>.

Merriam-Webster Dictionary 2015c, *Comprehension - Definition by Merriam-Webster Dictionary*, <http://www.merriam-webster.com/dictionary/comprehension>.

Merriam-Webster Dictionary 2015d, *Perception - Definition by Merriam-Webster Dictionary*, <http://www.merriam-webster.com/dictionary/perception>.

Microsoft 2008, *Safety & Security Centre*, viewed 23/08/2008, <http://www.microsoft.com/security/default.mspx>.

Moghe, R, Cheung, JMY, Saini, B, Marshall, NS & Williams, KA 2014, 'Consumers using the Internet for insomnia information: The who, what, and why', *Sleep and Biological Rhythms*, vol. 12, no. 4, pp. 297-304.

Montesdioca, GPZ & Maçada, ACG 2015, 'Measuring user satisfaction with information security practices', *Computers & Security*, vol. 48, pp. 267-80.

Moore, T 2010, 'The economics of cybersecurity: Principles and policy options', *International Journal of Critical Infrastructure Protection*, vol. 3, no. 3-4, pp. 103-17.

Mouratidis, H & Jurjens, J 2010, 'From goal-driven security requirements engineering to secure design', *International Journal of Intelligent Systems*, vol. 25, no. 8, pp. 813-40.

Muñiz, EJ, Stout, RJ, Bowers, CA & Salas, E 1998, 'A Methodology for measuring team situation awareness: Situation Awareness Linked Indicators Adapted To Novel Tasks (SALIANT)', in RTO HFM Symposium on "Collaborative Crew Performance in Complex Operational Systems": *proceedings of theRTO HFM Symposium on "Collaborative Crew Performance in Complex Operational Systems"* Edinburgh, United Kingdom, 20-22 April 1998, and published in RTO MP-4.

Murray, WH 1995, 'Security should pay: it should not cost', in IFIP TC-11 Eleventh International Conference on Information Security (Sec'95), Information Security Management - The Next Decade: *proceedings of theIFIP TC-11 Eleventh International Conference on Information Security (Sec'95), Information Security Management - The Next Decade* Cape Town, South Africa.

Nagunwa, T 2014, 'Behind Identity Theft and Fraud in Cyberspace: The Current Landscape of Phishing Vectors', *International Journal of Cyber-Security and Digital Forensics*, vol. 3, no. 1, pp. 72-83.

Narain Singh, A, Gupta, MP & Ojha, A 2014, 'Identifying factors of "organizational information security management"', *Journal of Enterprise Information Management*, vol. 27, no. 5, pp. 644-67.

Narayanan, AS & Ashik, MM 2012, 'Computer Forensic First Responder Tools', in International Conference on Advances in Mobile Network, Communication and Its Applications: *proceedings of theInternational Conference on Advances in Mobile Network, Communication and Its Applications* IEEE, Bangalore, India, pp. 156-9.

Nassimbeni, G, Sartor, M & Dus, D 2012, 'Security risks in service offshoring and outsourcing', *Industrial Management & Data Systems*, vol. 112, no. 3, pp. 405-40.

National Institute of Standards and Technology [NIST] 2015, *NIST web site*, NIST, viewed 21/04/2015, <http://www.nist.gov/>.

National Institute of Standards and Technology [NIST], Souppaya, M & Scarfone, K, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* 2013, NIST - U.S. Department of Commerce.

Neuman, WL 2006, *Social Research Methods: Qualitative and Quantitative approaches*, Sixth edn, Pearson International.

News.Com.au 2012, *Police call for calm on hoax text and email that threatens recipents with death*, viewed 23/07/2012, <http://www.news.com.au/money/money-matters/police-warn-on-hoax-text-and-email-that-threatens-recipient-with-death/story-e6frfmd9-1226432660084>.

NSW Government, *Risk Management Toolkit for NSW Public Sector Agencies,* 2012, Treasury, <http://www.treasury.nsw.gov.au/Publications/treasury_policy_papers/2012-TPP/tpp_12-03/tpp_12-03_risk_management_toolkit>.

Nunn, C 1995, *Awareness: what it is, what it does*, Routledge, London ; New York

Oehri, C & Teufel, S 2012, 'Social Media Security Culture: The Human Dimension in Social Media Management', in Information Security for South Africa (ISSA): *proceedings of theInformation Security for South Africa (ISSA)* Johannesburg, Gauteng.

Oxford Dictionaries 2015a, *Dictionary - projection Oxford dictionary*, <http://www.oxforddictionaries.com/definition/english/projection>.

Oxford Dictionaries 2015b, *Dictionary - comprehension Oxford dictionary*, <http://www.oxforddictionaries.com/definition/english/comprehension>.

Oxford Dictionaries 2015c, *Definition - perception Oxford dictionary*, <http://www.oxforddictionaries.com/definition/english/perception>.

Padmanabhuni, BM & Tan, HBK 2014, 'Auditing Buffer Overflow Vulnerabilities Using Hybrid Static-Dynamic Analysis', in IEEE 38th Annual International Computers, Software and Applications Conference: *proceedings of theIEEE 38th Annual International Computers, Software and Applications Conference* IEEE, Vasteras, Sweden, pp. 394-9.

Pahnila, S, Siponen, M & Mahmood, A 2007, 'Employees’ behavior towards IS security policy compliance', in Proceedings of the 40th Hawaii International Conference on System Sciences: *proceedings of theProceedings of the 40th Hawaii International Conference on System Sciences* IEEE, Hawaii.

Parkinson, D 2011, 'Life after WikiLeaks', *SC Magazines: For IT Security Professionals*, vol. March-April 2011, p. 6.

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*, vol. 42, pp. 165-76.

Patil, BS & Prasanthi, ML 2013, 'Modern Approaches for Detecting Data leakage Problems', *International Journal Of Engineering And Computer Science*, vol. 2, no. 2, pp. 395-9.

Patil, R & Patil, A 2014, 'Use of information technology in healthcare sector for improving outcomes', *International Journal of Basic & Clinical Pharmacology*, vol. 3, no. 2, p. 269.

PCI Security Standards Council 2010, *PCI DSS Requirements and Security Assessment Procedures*, Data Security Standard, PCI Security Standards Council, viewed 10/04/2011, <https://www.pcisecuritystandards.org>.

Pedersen, MJ & Nielsen, CV 2014, 'Improving Survey Response Rates in Online Panels: Effects of Low-Cost Incentives and Cost-Free Text Appeal Interventions', *Social Science Computer Review*.

Peltier, TR 2005, 'Implementing an Information Security Awareness Program', *Information Systems Security*, vol. 14, no. 2, pp. 37-49.

Pike, RE 2013, 'The "Ethics" of teaching ethical hacking', *Journal of international technology and information management*, vol. 22, no. 4.

Ponemon Institute 2010, 'Ponemon Institute 2010 Access Governance Trends Survey'.

Popa, V 2013, 'Critical Infrastructure Protection within the European Union', *Journal of Defense Resources Management*, vol. 4, no. 1, p. 6.

Praxiom Research Group Limited 2014, *ISO IEC 27002 2013 vs ISO IEC 27002 2005*, <http://www.praxiom.com/iso-27002-old-new.htm>.

PricewaterhouseCoopers 2010, 'Respected but still restrained - Findings from the 2011 Global State of Information Security Survey', viewed 06/03/2011, <https://www.pwc.com/en_GX/gx/information-security-survey/pdf/giss-2011-presentation.pdf>

PricewaterhouseCoopers 2012, 'Changing the game: Key findings from The Global State of Information Security Survey 2013', viewed 29/05/2013,

PricewaterhouseCoopers 2013, 'Defending yesterday: Key findings from The Global State of Information Security Survey 2014', viewed 11/05/2014,

PriceWaterhouseCoopers 2014, 'Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015', <www.pwc.com/gsiss2015>

Puhakainen, P 2006, 'A design theory for Information Security Awareness', Academic Dissertation thesis, University of Oulu, Oulu.

Puhakainen, P & Siponen, M 2010, 'Improving Employees' Compliance Through Information System Security Training and Action Research Study', *MIS Quarterly*, vol. 34, no. 4, pp. pp. 757-78.

Quagliata, K 2011, 'Impact of Information Security Awareness Training Components on Perceived Security Effectiveness', *ISACA Journal*, vol. 4, p. 6.

Qualtrics Labs Inc *Qualtrics Web Site*.

Qureshi, MA, Younus, A & Khan, AA 2009, 'Philosophical Survey of Passwords', *International Journal of Computer Science Issues*, vol. 2, p. 5.

Rajagopal, N, Prasad, KV, Shah, M & Rukstales, C 2014, 'A New Data Classification Methodology to Enhance Utility Data Security', *IEEE Xplore*, <http://ieeexplore.ieee.org.ezproxy.usq.edu.au/stamp/stamp.jsp?tp=&arnumber=6816451>

Ramirez, D 2006, 'Streamline ISO 27001 Implementation: Reducing the Time and Effort Required for Compliance', *ISACA Journal Online*.

Ramon-Jeronimo, MA, Peral-Peral, B & Arenas-Gaitan, J 2013, 'Elderly Persons and Internet Use', *Social Science Computer Review*, vol. 31, no. 4, pp. 389-403.

Rand, E 2010, *CBS News Investigation into Photocopiers Raises Questions in Buffalo*, viewed 20/4/2010, <http://www.cbsnews.com/2102-31727_162-20002992.html?tag=contentMain;contentBody>.

Rantos, K, Fysarakis, K & Manifavas, C 2012, 'How Effective Is Your Security Awareness Program? An Evaluation Methodology', *Information Security Journal: A Global Perspective*, vol. 21, no. 6, pp. 328-45.

Ravitz, GUY, Shyu, M-L & Powell, MD 2010, 'Integrating Multimedia Semantic Content Analysis of Youtube Videos with Hurricane Wind Analysis for Public Situation Awareness and Outreach', *International Journal of Software Engineering and Knowledge Engineering*, vol. 20, no. 02, p. 155.

Rghioui, A, L'aarje, A, Elouaai, F & Bouhorma, M 2015, 'Protecting E-healthcare Data Privacy for Internet of Things Based Wireless Body Area Network', *Research Journal of Applied Sciences, Engineering and Technology*, vol. 9, no. 10, pp. 876-85.

Richardson, R 2007, 'CSI Survey 2007: The 12th Annual Computer Crime and Security Survey', viewed 27 July 2008, <http://www.gocsi.com/>

Sá-Soares, Fd, Soares, D & Arnaud, J 2014, 'A catalog of information systems outsourcing risks', *International Journal Information Systems and Project Management*, vol. 2, no. 3, pp. 23-43.

Safeena, R, Kammani, A & Date, H 2014, 'Assessment of Internet Banking Adoption- An Empirical Analysis', *Arabian Journal for Science and Engineering*, vol. 39, no. 2, pp. pp. 837 - 49.

Sahebjamnia, N, Torabi, SA & Mansouri, SA 2015, 'Integrated business continuity and disaster recovery planning: Towards organizational resilience', *European Journal of Operational Research*, vol. 242, no. 1, pp. 261-73.

Sai Global 2004, *AS/NZS 4360:2004 Risk Management*, <http://www.saiglobal.com.ezproxy.usq.edu.au/online/autologin.asp>.

Salerno, J 2008, 'Measuring Situation Assessment Performance through the Activities of Interest Score', in Information Fusion, 2008 11th International *proceedings of theInformation Fusion, 2008 11th International*

Salmon, P, Stanton, N, Walker, G & Green, D 2005, 'Situation awareness measurement - A review of applicability for C4i environment',

Salmon, PM, Stanton, NA, Walker, GH, Jenkins, D, Darshna Ladva, Rafferty, L & Young, M 2008, 'Measuring Situation Awareness in Complex Systems - Comparison of measure study'.

Samaras, V, Daskapan, S, Ahmad, R & Ray, SK 2014, 'An enterprise security architecture for accessing SaaS cloud services with BYOD', in 2014 Australasian Telecommunication Networks and Applications Conference (ATNAC): *proceedings of the2014 Australasian Telecommunication Networks and Applications Conference (ATNAC)* Melbourne, Australia, pp. 129-34.

Saner, LD, Bolstad, CA, Gonzalez, C & Cuevas, HM 2009, 'Measuring and Predicting Shared Situation Awareness in Teams', *Journal of Cognitive Engineering and Decision Making*, vol. 3, no. 3, pp. 280-308.

Sannicolas-Rocca, T, Schooley, B & Spears, JL 2014, 'Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance', pp. 3432-41.

SANS Institute 2013, *SANS Institute - CyberTalent Assessments*, viewed 03 June, <http://www.sans.org/cybertalent>.

SANS Institute 2015, *IT Information Security Awareness Training*, viewed 11 January, 2015, <http://www.securingthehuman.org>.

Sarkar, KR 2010, 'Assessing insider threats to information security using technical, behavioural and organisational measures', *Information Security Technical Report*, vol. 15, no. 3, pp. 112-33.

Savirimuthu, A & Savirimuthu, J 2007, 'Identity Theft and System Theory: The Fraud Act 2006 in Perspective', *Scripted*, vol. 4, no. 4, pp. 438-61.

Sawer, P 2013, 'Password alert as 250,000 Twitter accounts hacked', *Sunday Telegraph (London)*, Feb 03, 2013.

Schneiderman, R 2013, 'Defense budgets Shrink Technology Spending', *IEEE SIGNAL PROCESSING MAGAZINE*, 12 February 2013.

Scotland, J 2012, 'Exploring the Philosophical Underpinnings of Research: Relating Ontology and Epistemology to the Methodology and Methods of the Scientific, Interpretive, and Critical Research Paradigms', *English Language Teaching*, vol. 5, no. 9.

Seda, L 2014, 'Identity theft and university students: do they know, do they care?', *Journal of Financial Crime*, vol. 21, no. 4, pp. 461-83.

Shahri, AB, Ismail, Z & Rahim, NZA 2013, 'Security Culture and Security Awareness as the Basic Factors for Security Effectiveness in Health Information Systems', *Jurnal Teknologi*, vol. 64, no. 2.

Sharifi, M, Ayat, M & Sahibudin, S 2008, 'Implementing ITIL-Based CMDB in the Organizations to Minimize or Remove Service Quality Gaps', pp. 734-7.

Shaw, R, Chen, C, Harris, A & Huang, H 2009, 'The impact of information richness on information security awareness training effectiveness', *Computers & Education*, vol. 52, no. 1, pp. 92-100.

Sherwood Applied Business Security Architecture [SABSA] 2015, viewed 20/05/2015, <http://www.sabsa.org>.

Shi, M 2013, 'Capturing strategic competences: cloud security as a case study', *Journal of Business Strategy*, vol. 34, no. 3, pp. 41-8.

Shuja, J, Madani, SA, Bilal, K, Hayat, K, Khan, SU & Sarwar, S 2012, 'Energy-efficient data centers', *Computing*, vol. 94, no. 12, pp. 973-94.

Sim, I, Liginlal, D & Khansa, L 2012, 'Information Privacy Situation Awareness: Construct and Validation', *Journal of Computer Information Systems*, vol. 53, no. 1.

Simmons, B, Lutfiyya, H, Avram, M & Chen, P 2006, 'A Policy-Based Framework for Managing Data Centers', in Network Operations and Management Symposium: *proceedings of theNetwork Operations and Management Symposium* IEEE, Vancouver, BC.

Siponen, M & Willison, R 2009, 'Information security management standards: Problems and solutions', *Information & Management*, vol. 46, no. 5, pp. 267-70.

Siponen, M & Vance, A 2010, 'Neutralization: New Insight into the problem of Employee information security policy violation', *MIS Quarterly*, vol. 34, no. 3, pp. pp. 487 - 502.

Siponen, M, Mahmood, MA & Pahnila, S 2009, 'Are employees putting your company at risk by not following information security policies?', *Communications of the ACM*, vol. 52, no. 12, p. 145.

Siponen, MT 2000, 'A conceptual foundation for organizational information security awareness', *Information Management & Computer Security*, vol. 8, no. 1, pp. 31 - 41.

Siponen, MT 2002, 'Towards maturity of information security maturity criteria: six lessons learned from software maturity criteria', *Information Management & Computer Security*, vol. 10, no. 5, pp. 210-24.

Siponen, MT & Kajava, J 1998, *On the Information Security Management Industry - IT Security Awareness Perspective*, Department of Computer Science, Aalborg University, Sæby Søbad, Denmark.

Slack, N 1994, 'The Importance-Performance Matrix as a Determinant of Improved Priority', *International Journal of Operations & Production Management*, vol. 14, no. 5, pp. 59-75.

SMH 2014, 'Stolen nude photos of Rihanna, Kim Kardashian and more female celebrities leaked online', *SMH*.

Smolaks, M 2015, '44.4 ºC heat shuts down Australian data center', *SMH*, 6 January 2015.

Spears, JL & Barki, H 2010, 'User participation in Information Systems Security Risk Management', *MIS Quarterly*, vol. 34, no. 3, pp. 503-22.

Speight, P 2011, 'Business Continuity', *Journal of Applied Security Research*, vol. 6, no. 4, pp. 529-54.

Spoorthi V & Sekaran, KC 2014, 'Mobile single sign-on solution for enterprise cloud applications', in First International Conference on Networks & Soft Computing (ICNSC2014): *proceedings of theFirst International Conference on Networks & Soft Computing (ICNSC2014)*.

Srinivasan, M 2012, 'Building a secure enterprise model for cloud computing environment', *Academy of Information & Management Sciences Journal*, vol. 15, no. 1, pp. p127-33.

Stanciu, V, Pana, A & Bran, F 2010, 'Business Continuity and Disaster Recovery Plans - Organisations Response to the Natural Disasters', *Metalurgia International*, vol. XV, no. Special issue no. 1, p. 4.

Standards Australia/Standards New Zealand 2006a, *ISO/IEC 27001:2006 Information technology - Security techniques - Information security management systems - Requirements,*, Standards Australia/Standards New Zealand,, <http://www.standards.org.au>.

Standards Australia/Standards New Zealand 2006b, *ISO/IEC 27002:2006 Information Technology - Security techniques - Code of practice for information security management*, Standards Australia/Standards New Zealand <http://www.standards.org.au>.

Standards Australia/Standards New Zealand 2009a, *ISO 31000:2009 Risk management - Principles and guidelines*, Standards Australia/Standards New Zealand,, <http://www.standards.org.au>.

Standards Australia/Standards New Zealand 2009b, *SA/SNZ HB 436:2013 Risk management guidelines - Companion to AS/NZS ISO 31000:2009*, Standards Australia/Standards New Zealand,, <http://www.standards.org.au>.

Standards Australia/Standards New Zealand 2015, *Information technology - Security techniques - Code of practice for information security controls*, Standards Australia/Standards New Zealand <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*, vol. 20, no. 1, pp. 29-38.

Strater, LD, Endsley, MR, Pleban, RJ & Matthews, MD, *Measures of Platoon leader situation awareness in virtual decision making exercises,* 2001, UARIftBaS Sciences.

Subramaniam, C, Park, S, Kumar, RL & Temizkan, O 2012, 'Patch Release Behaviors of Software Vendors in Response to Vulnerabilities: An Empirical Analysis', *Journal of Management Information Systems*, vol. 28, no. 4, pp. 305-38.

Swanson, S 2008, 'How to Ensure Data Security for Non-Production Computer Systems', *eWeek (New York, N.Y.).*

Tadda, GP 2008, 'Measuring Performance of Cyber Situation Awareness Systems', in Information Fusion, 2008 11th International *proceedings of theInformation Fusion, 2008 11th International*

Tadda, GP & Salerno, JS 2010, 'Overview of Cyber Situation Awareness', in *Cyber Situational Awareness,*, vol. 46, ch 2.

Talib, S, Clarke, NL & Furnell, SM 2010, 'An Analysis of Information Security Awareness within Home and Work Environments', in 2010 International Conference on Availability, Reliability and Security: *proceedings of the2010 International Conference on Availability, Reliability and Security* IEEE Xplore.

Tejay, GPS & Barton, KA 2013, 'Information System Security Commitment: A Pilot Study of External Influences on Senior Management', pp. 3028-37.

Ter, KL 2013, 'Singapore's Personal Data Protection legislation: Business perspectives', *Computer Law & Security Review*, vol. 29, no. 3, pp. 264-73.

Tetmeyer, A & Saiedian, H 2010, 'Security Threats and Mitigating Risk for USB Devices', *IEEE Technology and Society Magazine*, vol. Winter 2010.

Thejendra, BS 2014, *Disaster Recovery and Business Continuity: A Quick Guide for Organisations and Business Managers*, Third edn, Ely, Cambridgeshire, U.K. .

Tomaszewski, B 2011, 'Situation awareness and virtual globes: Applications for disaster management', *Computers & Geosciences*, vol. 37, no. 1, pp. 86-92.

Tompkins, W 2008, 'Information security awareness - Beyond New Employee Orientation', in TASSCC Annual Conference 2008: *proceedings of theTASSCC Annual Conference 2008* Texas Association of State Systems for Computing and Communications, Texas, <http://www.tasscc.org/events/annl2008/default.htm>.

Tronvoll, B, Brown, SW, Gremler, DD & Edvardsson, B 2011, 'Paradigms in service research', *Journal of Service Management*, vol. 22, no. 5, pp. 560-85.

Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) 2007, *Secure Your Information: Secure Your Business - Advice for CEOs and Boards of Directors*, <www.tisn.gov.au>.

Tsohou, A, Kokolakis, S, Karyda, M & Kiountouzis, E 2008, 'Investigating Information Security Awareness: Research and Practice Gaps', *Information Security Journal: A Global Perspective*, vol. 17, no. 5, pp. 207-27.

Tsohou, A, Kokolakis, S, Karyda, M & Kiountouzis, E 2008, 'Process-variance models in information security awareness research', *Information Management & Computer Security*, vol. 16, no. 3, pp. 271-87.

Tsohou, A, Karyda, M, Kokolakis, S & Kiountouzis, E 2010, 'Aligning Security Awareness With Information Systems Security Management', *Journal of Information Sydtem Security*, vol. 6, no. 1, pp. 35-54.

Tsohou, A, Kokolakis, S, Lambrinoudakis, C & Gritzalis, S 2010, 'A security standards' framework to facilitate best practices' awareness and conformity', *Information Management & Computer Security*, vol. 18, no. 5, pp. 350-65.

Tsohou, A, Karyda, M, Kokolakis, S & Kiountouzis, E 2012, 'Analyzing trajectories of information security awareness', *Information Technology & People*, vol. 25, no. 3, pp. 327-52.

Tsukayama, H 2013, '2 million sets of log-in credentials stolen; Google, Facebook affected.pdf', *The Washington Post*.

Uhlarik, J & Comerford, DA, *A review of Situation Awareness Literature Relevant to Pilot Surveillance Functions,* 2002, OoA Medicine, U.S. Department of Transportation, Washington, DC.

UK Office of Communications (Ofcom) 2013, *UK adults taking online password security risks*, viewed 8 January 2015, <http://media.ofcom.org.uk/news/2013/uk-adults-taking-online-password-security-risks/>.

US Department of Homeland Security, *Information Technology (IT) Security Essential Body of Knowledge (EBK)- A Competency and Functional Framework for IT Security Workforce Development,* 2007, HSNCS Division, Washington, D.C.

US Government, *Gramm-Leach-Bliley Financial Modernization Act,* 1999, Federal Trade Commission, Federal Trade Commission,, <http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act>.

US Government, *Sanitization and Disposal of Excess Information Technology Equipment,* 2009, Inspector General United States Department of Defense.

US Government, *The Department of Health and Human Services Information Systems Security Awareness Training,,* 2014, Department of Health and Human Services.

US Government & Lew, JJ, *WikiLeaks - Mishandling of Classified Information,* 2010, Executive Office of the President, Washington, D.C.

Van Niekerk, JF & Von Solms, R 2010, 'Information security culture: A management perspective', *Computers & Security*, vol. 29, no. 4, pp. 476-86.

Van Selm, M & Jankowski, NW 2006, 'Conducting Online Surveys', *Quality and Quantity*, vol. 40, no. 3, pp. 435-56.

Vaneechoutte, M 2000, 'Experience, Awareness and consciousness - Suggestions for definitions as offered by an evolutionary approach', *Foundations of Science*, vol. 5, no. 4, pp. pp 429 - 56.

VansonBourne 2012, 'The Disaster Recovery Survey 2012: Middle East, Turkey and Morocco - commisioned by EMC', <http://middle-east.emc.com/collateral/microsites/2012/emc-brs-survey/mid-market-commentary-presentation.pdf>

Veiga, Ad, Martins, N & Eloff, JHP 2007, 'Information security culture - validation of an assessment instrument', *Southern African Business Review*, vol. 11, no. 1.

Venkatesh, V, Thong, JYL & Xu, X 2012, 'Consumer Acceptance and Use of Information Technology - Extending the Unified Theory of Acceptance and Use of Technology', *MIS Quarterly*, vol. 36, no. 1, pp. 157-78.

Verizon Business RISK Team 2009, *2009 Data Breach Investigations Report*.

Vivas, JL, Agudo, I & López, J 2010, 'A methodology for security assurance-driven system development', *Requirements Engineering*, vol. 16, no. 1, pp. 55-73.

Walker, K 2013, 'Information governance - creating a competitive advantage', *The RIM Quarterly*, vol. 29, no. 3, p. 2.

Waly, N, Tassabehji, R & Kamala, M 2012, 'Improving Organisational Information Security Management: The Impact of Training and Awareness', pp. 1270-5.

Webb, J, Ahmad, A, Maynard, SB & Shanks, G 2014, 'A situation awareness model for information security risk management', *Computers & Security*, vol. 44, pp. 1-15.

Western Australian Auditor General, *Western Australian Auditor General's Report - Information Systems Audit Report,* 2010, Western Australian Auditor General, Perth.

Western Australian Auditor General, *Western Australian Auditor General Report - Information Systems,* 2013, A General, <https://audit.wa.gov.au/wp-content/uploads/2013/06/report2013_11.pdf>.

Wickens, CD 2008, 'Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 50, no. 3, pp. 397-403.

Wikipedia 2011, *Awareness*, viewed 6 May 2011, <http://en.wikipedia.org/wiki/Awareness>.

Williams, PAH 2008a, 'In a 'trusting' environment, everyone is responsible for information security', *Information Security Technical Report*, vol. 13, no. 4, pp. 207-15.

Williams, PAH 2008b, 'A practical application of CMM to medical security capability', *Information Management & Computer Security*, vol. 16, no. 1, pp. 58-73.

Williams, PAH 2013, 'Information security governance: A risk assessment approach to health information systems protection', *Studies in Health Technology and Informatics*, vol. Volume 193: Health Information Governance in a Digital Environment, pp. 186-206.

Wilson, M & Hash, J 2003, 'Building an Information Technology Security Awareness and Training Program', vol. 2008, no. 19 August, <http://csrc.nist.gov/groups/SMA/ate/index.html>

Wright, M 1994, 'Protecting information: Effective security controls', *Review of Busioness*, vol. 16, no. 2.

Wright, S 2006, 'Measuring the Effectiveness of Security using ISO 27001 ', p. 15, <http://www.iwar.org.uk/comsec/>

Xiaosong, L, Shushi, L, Wenjun, C & Songjiang, F 2009, 'The Application of Risk Matrix to Software Project Risk Management', pp. 480-3.

Yaxley, L 2003, 'PM - Sydney Airport Customs under fire over computer theft', *ABC Online*.

Yin, J, Karimi, S, Robinson, B & Cameron, M 2012, *ESA: Emergency Situation Awareness via Microbloggers*, CSIRO.

Yin, J, Lampert, A, Cameron, M, Robinson, B & Power, R 2012, 'Using Social Media to Enhance Emergency Situation Awareness', *Intelligent Systems, IEEE*, vol. 27, no. 6, pp. 52 - 9.

Yin, RK 2003, *Case Study Research: Design and Methods*, 3rd edn, Sage Publications.

Yngström, L & Björck, F 1999, *The Value and Assessment of Information Security Education and Training*, Department of Computer and Systems Sciences, Stockholm University & Royal Institute of Technology, viewed 15 August 2008, <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.28.5206>.

Young, D 2004, 'Human Resources have a vital role to play within employee identity and access management', *Network Security*, vol. 2004, no. 11, pp. 5-7.

Yu, S & Brewster, J 2012, 'Formal Specification and Impementation of RBAC Model with SOD', *Journal of Software*, vol. 7, no. 4.

Yu, Y, Franqueira, VNL, Than Tun, T, Wieringa, RJ & Nuseibeh, B 2015, 'Automated analysis of security requirements through risk-based argumentation', *Journal of Systems and Software*, vol. 106, pp. 102-16.

Zappone, C 2011, 'Faulty ATMs in 'free cash' blunder after technical glitch', *The Age*.

Zappone, C 2012, 'NAB struggles with tech glitch', *Sydney Morning Herald*.

Zeadally, S, Yu, B, Jeong, DH & Liang, L 2012, 'Detecting Insider Threats: Solutions and Trends', *Information Security Journal: A Global Perspective*, vol. 21, no. 4, pp. 183-92.

Zhong-wei, X 2009, 'Maintaining Database Consistency and Integrity in HIS with Transactions', in IEEE International Symposium on IT in Medicine & Education: *proceedings of theIEEE International Symposium on IT in Medicine & Education*.

Zolkos, R 2015, *Thailand floods disrupt supply chains | Business Insurance*, Business Insurance, viewed 11 January 2015, <http://www.businessinsurance.com/article/99999999/NEWS060101/399999816>.

Appendix A. Phase 1 Survey – Awareness Importance

The following is a list of questions that were presented in the Phase 1 Survey and used to determine the Awareness Importance rating. Each question called for a rating of between 1 and 7 to be provided for each of the 3 stakeholder groups; IT staff, senior management and end users.

1. SECURITY POLICY

Q1 How aware of information security policies, do the stakeholder groups need to be, in order to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations?

2. ORGANISATION OF INFORMATION SECURITY

Q2 How aware of an appropriate management framework and organisation structure to control information security, do the stakeholder groups need to be, in order to provide sound information security within the organisation?

Q3 How aware of the information security practices of external parties, do the stakeholder groups need to be when their information and information processing facilities are accessed, processed, communicated to, or managed by external parties?

3. ASSET MANAGEMENT

Q4 How aware of the need for ownership and accountability for assets, do the stakeholder groups need to be, in order to maintain appropriate protection of organisational assets?

Q5 How aware of the need to classify information, do the stakeholder groups need to be, so that information receives an appropriate level of protection?

4. HUMAN RESOURCES SECURITY

Q6 How aware of addressing security responsibilities in job descriptions and conditions of employment, do the stakeholder groups need to be?

Q7 How aware of the need to continually inform employees, contractors and 3rd party users of their ongoing information security responsibilities, do the stakeholder groups need to be, during the employment tenure of these staff?

Q8 How aware of the need to assign responsibilities for managing the exit of users, do the stakeholder groups need to be, so that employees, contractors and third party users exit an organisation or change their employment in an orderly and secure manner?

5. PHYSICAL AND ENVIRONMENTAL SECURITY

Q9 How aware of the need to house information processing facilities in secure areas, do the stakeholder groups need to be?

Q10 How aware of physical and environmental threats, do the stakeholder groups need to be, to prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities?

6. COMMUNICATIONS AND OPERATIONS MANAGEMENT

Q11 How aware of formalising operational procedures and responsibilities, do the stakeholder groups need to be, so that the correct and secure operation of information processing facilities is managed?

Q12 How aware of implementing agreements and monitoring compliance, do the stakeholder groups need to be, so as to maintain the appropriate level of information security and service delivery in line with third party service delivery agreements?

Q13 How aware of system planning, capacity planning and acceptance testing, do the stakeholder groups need to be, in order to minimise the risk of systems failures?

Q14 How aware of controls that provide protection against malicious and mobile code, do the stakeholder groups need to be, in order to protect the integrity of software and information?

Q15 How aware of the need and procedures for backing up information, do the stakeholder groups need to be, to ensure the integrity and availability of information and information processing facilities?

Q16 How aware of the controls for securing networks, do the stakeholder groups need to be, in order to protect information in networks and protect the supporting infrastructure?

Q17 How aware of the techniques required to protect removable media, do the stakeholder groups need to be, in order to minimise unauthorised disclosure, modification, removal or destruction of assets?

Q18 How aware of policies and procedures for exchanging information, do the stakeholder groups need to be, to preserve the security of any information or software exchanged within an organisation or with any external entity?

Q19 How aware of electronic commerce services, do the stakeholder groups need to be, to ensure the security of electronic commerce services, and their secure use?

Q20 How aware of system monitoring techniques, do the stakeholder groups need to be, to help detect and check the effectiveness of controls designed to prevent unauthorised information processing activities?

7. ACCESS CONTROL

Q21 How aware of business requirement and policies for information dissemination and authorisation, do the stakeholder groups need to be, in order to control access to information?

Q22 How aware of formal user access management procedures, do the stakeholder groups need to be, to ensure authorised user access and to prevent unauthorised access to information systems?

Q23 How aware of user responsibilities for maintaining effective access controls, do the stakeholder groups need to be, to prevent unauthorised user access, and compromise or theft of information and information processing facilities?

Q24 How aware of network access controls to internal and external networked services, do the stakeholder groups need to be?

Q25 How aware of operating system access controls, do the stakeholder groups need to be?

Q26 How aware of application and logical access controls, do the stakeholder groups need to be?

Q27 How aware of the risks associated with mobile computing and teleworking in an unprotected environment, do the stakeholder groups need to be?

8. INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT & MAINTENANCE

Q28 How aware of security requirements of information systems, do the stakeholder groups need to be, to ensure that security is an integral part of developing or acquiring information systems?

Q29 How aware of change and input validation controls, do the stakeholder groups need to be, to prevent errors, loss, unauthorised modification or misuse of information in applications?

Q30 How aware of cryptographic controls including key management, do the stakeholder groups need to be, to protect the confidentiality, authenticity or integrity of information?

Q31 How aware of security of system files and source code, do the stakeholder groups need to be?

Q32 How aware of the security of development and test environments, do the stakeholder groups need to be?

Q33 How aware of technical vulnerability management, do the stakeholder groups need to be, to prevent risks resulting from exploitation of published vulnerabilities?

9. INFORMATION SECURITY INCIDENT MANAGEMENT

Q34 How aware of the need for timely reporting of information security events and weaknesses, do the stakeholder groups need to be, to allow timely corrective action to be taken?

Q35 How aware of the procedures and assignment of responsibilities to manage information security incidents and improvements, do the stakeholder groups need to be, to ensure a consistent and effective approach to the management of security incidents?

10. BUSINESS CONTINUITY MANAGEMENT

Q36 How aware of information security aspects of business continuity management, do the stakeholder groups need to be, to protect critical business processes from the effects of major failures of information systems?

11. COMPLIANCE

Q37 How aware of compliance with legal requirements, do the stakeholder groups need to be, in order to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any related security requirements?

Q38 How aware of the need to formally review compliance of systems with organisational security policies and standards, do the stakeholder groups need to be?

Q39 How aware of controls to minimize interference to/from the information systems audit process, do the stakeholder groups need to be?

Appendix B. Phase 2 Survey – Awareness Capability

The following is a list of questions that were presented in Phase 2 Survey and used to determine the Awareness Capability scores. The scores for each sub-question are shown in the brackets, whilst the most correct answer is coloured green.

QUESTION 1 – PASSWORDS

QUESTION 1.1 A work colleague has asked you for your computer access password because they are having troubles getting their computer access set up. What would you do?
a) I would share my password but only in an emergency (0.5)
b) I would share my password but only with my boss (0)
c) I would never share my password (2.0)
d) I would share my password but would change my password immediately afterwards (0.5)
e) I don't know what I would do in such a situation (0)

QUESTION 1.2 Do you use the same password for multiple systems, say for your personal email account and your work accounts?
a) Yes because my password is strong enough and it is too difficult to remember so many different passwords. (0)
b) No because I know that if one of the passwords get cracked, it could be used to access my other systems (2.5)
c) Yes because I don't write down my password or give it to anyone else. Nobody will be able to guess my password. (0)
d) No because it would be a breach of policy, although I don't quite understand what the risk would be. (0.5)
e) I don't know whether it would be acceptable to use the same password for multiple systems (0)

QUESTION 1.3 Is a passphrase better to use than just a set of characters and numbers in your password?
a) It is no better. As long as your password is at least 8 characters long then nobody will be able to guess it. (0.5)
b) It is no better. As long as my computer is secure any length password will be OK. Also I change my password regularly. (0)
c) It is better only because someone looking over my shoulder won't be able to remember a passphrase. (0.5)
d) It is better because the length of a password is the most important factor. Passphrases can be easily remembered and can be very long (2.5)
e) I don't know whether a passphrase is more secure to use than a password made up of a combination of characters and numbers (0)

QUESTION 2 – Reporting Information security events

QUESTION 2.1 Would you be able to recognise a potential computer incident (i.e. virus, spam, infected web site) and do you know what to do?
a) If there is unusual behaviour on my computer, I would escalate according to the incident management process. (2.0)
b) I would report it to the IT department only if my computer started doing strange things, but I wouldn't know what might have caused that. (0.5)
c) If my computer became infected with a virus, I probably wouldn't own up to having clicked on an unknown email attachment or visited a web site I wasn't sure of. (0)
d) If something goes wrong with my computer I would ask one of my work colleagues what to do. They can usually help me. (0.5)
e) I don't know what a security incident would look like. (0)

QUESTION 2.2 You have taken some work related data home on an unencrypted USB device. It has some customer related data on it. However you can't find the USB device. What would you do?

a) I will check what I had copied, and if it doesn't include credit card details or passwords then I won't do anything further. (1.0)
b) Because I am quite sure it is somewhere at my house I will wait and see if it turns up. No point in raising any false concerns. (0)
c) I would do nothing. No one will know that I copied the data, so if it is found then they won't know who copied it and I will not own up to it. (0)
d) Because the data contains personally identifiable information, I would report it to our Privacy officer as a precaution. (2.5)
e) I don't know what I would do in such a situation (0)

QUESTION 2.3 Do you know what social engineering is and can it lead to security incidents?
a) I think it somehow involves getting information from me, but I don't know how that would result in a security incident. I am careful in what I hand over (0.5)
b) It could involve tricking me to go to a web site, but no harm should come from that because I can recognise a fake web site. (0)
c) It is where people are manipulated or deceived into providing information or to act in an unsecure manner. This could result in aiding a hacker to gain benefit, which could result in a security incident. (2.5)
d) I wouldn't count social engineering as a security incident, but it could result in me handing over information I didn't intend to. (1.0)
e) I don't know what social engineering is and whether it can lead to security incidents (0)

QUESTION 3 – Mobile computing and communications

QUESTION 3.1 Is it OK to connect your work computer to a public Internet service such as those offered by Starbucks or public Libraries
a) No it is never OK to use the public Internet services. (1.0)
b) Yes but as long as it is just for a short period of time (0)
c) Yes as long as I use a VPN to connect to my work environment (2.0)
d) Yes as long as my virus protection and software are up to date (0.5)
e) I don't know what I would do in such a situation (0)

QUESTION 3.2 Why is it important to have an encrypted hard drive on any computer used away from the office.
a) It is important because in the event that the computer is stolen or lost, it will prevent anyone from reading the information from the hard disk. (2.5)
b) Encryption will stop my computer being infected by a computer virus, which is very important to do when working away from the office. (0)
c) It is not important to encrypt the hard disk because it slows down the computer and makes doing my work more difficult. (0)
d) It is important because it means that only authorised users will be able to log onto the computer and access the information. (1.0)
e) I don't know whether it is important to have an encrypted hard drive on any computer used away from the office (0)

QUESTION 3.3 How does a VPN connection provide you with security when connecting with your work or other companies?
a) By using a VPN, it will stop my computer ever being infected by a computer virus that might be on the other computers. (0)
b) It provides an encrypted secure connection to another computer that cannot be intercepted or listened to. (2.5)
c) I know I should use this when connecting with work, but not sure why. It just seems to be an extra step. (0.5)
d) This means that only authorised users will be able to use the computer to connect to a work environment. (0.5)
e) I don't know how a VPN provides security when connecting with work or other companies from remotely (0)

QUESTION 4 – Information exchange policies and procedures

QUESTION 4.1 You are working on analysing some customer data that you have access to in order to determine customer profitability. Is it OK to share this information with other people within your organisation?
a) Yes but only with those people that I trust. I know that they will look after the data properly. (0)
b) Yes as long as I remove the customers name then there is no risk of breaching any security or privacy. (0.5)
c) No as the data doesn't belong to me I am not going to give it to anyone else. (1.0)
d) Only if the data owner has given approval and the data is shared in a secure manner. (2.0)
e) I don't know what I would do in such a situation (0)

QUESTION 4.2 Your organisation uses an external company to do its letter mail out (physical and email) to customers. Is this secure?
a) No it is never secure. You read every day about how this can go wrong. This should only be done in-house within my organisation. (0)
b) Yes it can be secure. We have used an external company for a long time and we trust them with the data we give them. (1.0)
c) Yes because it is just correspondence and after all they are our customers so we can decide how they will receive mail from us. (0.5)
d) It is OK only if formal agreements and information exchange policies are in place and their security measures have been assessed as being adequate. (2.5)
e) I don't know what I would do in such a situation (0)

QUESTION 4.3 When exchanging electronic information with another organisation, you should ensure that ...
a) We can trust the other organisation's virus protection. That's all we need to worry about. (0.5)
b) We ask the other organisation to properly protect the data that we are exchanging with them. (0.5)
c) We have exchange agreements in place, and that we use secure mechanisms (i.e. VPN or secure connections) to exchange the data. (2.5)
d) We comply with any privacy requirements regarding the data. That way we will be in the clear if anything goes wrong. (1.0)
e) I don't know what I would do in such a situation (0)

QUESTION 5 – Management of removable media

QUESTION 5.1 What is the best way to dispose of unwanted data contained on media such as a dvd, usb stick, magnetic tape.
a) Disposal through normal waste management processes will be sufficient. Our rubbish ends up at the local rubbish dump, so that should be OK. (0.5)
b) Simply deleting the data from the media will be sufficient. That way nobody will see there is any information on the media. (0.5)
c) The disposal technique should be based on the information classification. The higher the classification, the more disposal techniques (secure erasure, demagnetisation, physical destruction) should be used. (2.0)
d) As long as the media is broken into pieces or torn, that should be secure enough. Nobody will go to the effort of trying to piece the stuff together. (1.0)
e) I don't know what I would do in such a situation (0)

QUESTION 5.2 You are required to work on a sales presentation spreadsheet over the weekend. Because of the sensitive nature of the information you know not to send it home via email. Instead you load it onto a USB memory stick. Is that safe?
a) I have encrypted the USB memory stick, so even if I lost it the information will be safe and not able to be read by others. (2.5)
b) Yes it is safe because I am very careful with the USB stick and will put it on my key ring. I never lose my keys. (0.5)
c) As long as I still have a copy at work then things will be fine. If I lose the USB memory stick I will still have the original information at work. (0)
d) I have password protected the spreadsheet so it will be OK. Nobody will be able to crack the password that I have used. (1.0)

e) I don't know what I do would do in such a situation (0)

QUESTION 5.3 You are responsible for the disposal of photocopying machines. Are there any security related things that you need to do before you dispose of them?
a) I need to make sure that I remove any physical identifiers that can link the photocopier back to my organisation. (0.5)
b) Because the photocopier has a hard disk that contains photocopied information, I need to make sure the hard disk is suitably and securely wiped (2.5)
c) Nothing from a security related perspective. This is just a standard piece of office equipment that most organisations have and readily dispose of. (0)
d) As long as I remove the photocopier from our asset register, and cancel the maintenance controls, that is all that is required. (0)
e) I don't know what I would do in such a situation (0)

QUESTION 6 – Information Classification

QUESTION 6.1 Is it important for your organisation to have data/information classification rules and if so why?
a) It is important because it is primarily used to determine how much space is allocated to each classification. (0)
b) The classification is important so that appropriate protection (such as access control, encryption) can be provided to that information. (2.0)
c) It is only important for organisations that have top-secret information such as the military. Other organisations don't need to go to the effort. (0.5)
d) It is only important to classify data that will be provided to external organisations. (1.0)
e) I don't know why it is important for an organisation to have data/information classification rules (0)

QUESTION 6.2 How does information classification influence access controls?
a) This is an IT issue that business users don't need to know about. The IT group should do the classifying and determine who should have the access. (0)
b) It is only used to determine whether someone should have read or write access to data, and for how long they should have that access. (0.5)
c) It only influences what access external organisations should have to the information. (0.5)
d) The classification is used to determine who should have access to that data, and what type of access they should have. (2.5)
e) I don't know how information classification rules influence access controls (0)

QUESTION 6.3 What are the key risks for your organisation if it has correctly classified information?
a) The risk to my organisation is that only a restricted number of people can get access to certain information. (0)
b) The risk is that people are prevented from doing their job because of the classification rules. They always get in the way. (0.5)
c) Someone with the access may accidently or deliberately make data available to someone with a lesser classification (i.e. public). (2.5)
d) It takes too long for someone to get access to data that is classified. People will be prevented from doing their job properly. (0.5)
e) I don't know what the key risks for my organisation are. (0)

QUESTION 7 – Business requirements for access control

QUESTION 7.1 Who should determine the level of access to data within your organisation?
a) Individual staff members know what data they need access to. They should get approval from their line manager and request this access from IT. (0.5)
b) The IT department maintain the rules, so they should determine who should and shouldn't have access to data. (0)
c) New employees should be granted access based around a similar work colleagues access. Makes it easier to set up their access. (0.5)
d) Business units own the data. The business owner should determine who (often by job function) should be able to access that data. (2.0)
e) I don't know who should determine the level of access to data within my organisation (0)

QUESTION 7.2 What is the greatest risk to your organisation if access is not based on business requirements?
a) People could end up with too much or too little access to the data and systems they need to perform their job. (2.5)
b) The IT department won't know who should have access to what and won't be able to correctly set up the access controls. (1.5)
c) Too much work will be created for the IT department, trying to keep up with who should have access to what. (1.0)
d) It will take longer to get access to the things staff needs to do their job. Time is money and waiting to be granted access wastes time. (0.5)
e) I don't know what is the greatest risk to my organisation if access is not based on business requirements (0)

QUESTION 7.3 What do you understand about the term "separation of duties" and it's importance to your organisation?
a) It is the division of labour where one person may perform one duty and another person performs another duty. It is important so that each individual is accountable for those duties (1.0)
b) It occurs when trying to measure how individuals perform different tasks. So by identifying or "separating" these duties, you will be able to measure them separately. (0)
c) It assists with not overloading an individual with too many complicated tasks. By separating these is makes it easier to balance the work loads.(0)
d) It is the separation of job tasks (such as purchasing and receivables) so a single individual does not perform both of them. This helps to minimise fraudulent or accidental errors. (2.5)
e) I don't know what is meant by the term "separation of duties" and its importance to my organisation (0)

QUESTION 8 – Compliance with legal requirements

QUESTION 8.1 Who within your organisation should be responsible for understanding how to comply with legal requirements?
a) Audit and risk management are responsible for compliance. They are the people that need to understand all of the legal requirements and how to comply. (0)
b) It is only the legal department. That is their primary role in my organisation and
it should be their responsibility. (1.5)
c) Business unit managers should understand how to comply with the legal requirements that impact on their business unit. (2.0)
d) As long as I comply with my organisation's policy, that should cover off compliance with any legal requirements. (0.5)
e) I don't know who within my organisation should be responsible for understanding how to comply with legal requirements (0)

QUESTION 8.2 What do you know about data privacy?
a) It is something that is the responsibility of IT departments. So they are the ones that need to understand it. (0.5)
b) It involves keeping the data that I am working on in my organisation away from any of my other work colleagues. (0.5)
c) I know that data privacy has a set of principles that my organisation need to follow. But that is about all I know. (1.0)
d) In Australia, there are 13 privacy principles, applying to handling of personal information by most Government agencies and some private organisation. (2.5)
e) I don't know much about data privacy (0)

QUESTION 8.3 Why are there laws regarding the use of encryption software
a) The laws are there to make sure that appropriate license fees are paid to the companies that provide the encryption technology. (0)
b) They are there solely to make sure that governments can still access data of citizens without being prevented by encryption techniques (1.5)
c) They are there to ensure that certain data transmissions and exchanges make use of appropriate encryption techniques, and to prevent the exporting of encryption technology to certain countries. (2.5)

d) Just another level of government bureaucracy. This provides the "authorities" with the ability to spy on its citizens. (0.5)
e) I don't know why there are laws regarding the use of encryption software (0)

QUESTION 9 – Responsibility for assets

QUESTION 9.1 Who should be responsible for owning technology related assets?
a) The IT department should own all of the technology assets. That is one of their primary responsibilities within my organisation. It doesn't make sense spreading the responsibility to others. (1.0)
b) Individual staff members should be solely responsible because they will demonstrate greater accountability. You can then penalise them if they abuse this responsibility. (0.5)
c) As the asset has a monetary value, the finance department should own all assets. They can then manage all aspects of the asset. (0.5)
d) Ownership should be broken down into a number of aspects. Physical ownership of technology assets would normally reside with the IT department. Business ownership would then reside with the primary user of the asset. (2.0)
e) I don't know who should be responsible for owning technology related assets (0)

QUESTION 9.2 Who should be responsible for maintaining and updating an asset register of technology assets?
a) The IT department should maintain and update anything to do with the technology assets, including any asset register. No one else need get involved in this. (0.5)
b) Ownership should be shared. Physical registering of the technology assets would normally reside with the IT department. Business ownership would then be responsible for other aspects of the asset. (2.5)
c) Individual staff members should maintain the asset register for the technology assets they use because they will demonstrate greater accountability and will ensure that the register is always up to date. (0.5)
d) As the asset has a monetary value, the finance department should own all assets and therefore should be responsible for maintaining the technology asset register. (0.5)
e) I don't know who should be responsible for maintaining and updating an asset register of technology assets (0)

QUESTION 9.3 Who should be setting the policy of acceptable use for a computing asset?
a) The business owner of the asset should set the policy. (2.5)
b) No specific acceptable use policy is required. General employment policies should be sufficient. (0.5)
c) The IT department should set the policy. (0.5)
d) As the asset has a monetary value, the finance department should own and set the acceptable use for all assets. (0.5)
e) I don't know who should be setting the policy for acceptable use for a computing asset (0)

QUESTION 10 – Equipment security

QUESTION 10.1 What controls provide the best protection for essential computer equipment against power disruptions?
a) Computer equipment plugged into different power points. (0.5)
b) Spike protection power points. (0.5)
c) The use of UPS with a diesel generator backup. (2.0)
d) Equipment with their own battery backup. (0.5)
e) I don't know what controls provide the best protection for essential computer equipment against power disruptions (0)

QUESTION 10.2 When disposing of computer equipment, what key information security step is required to be done.
a) Remove any physical labels from the computer equipment that could identify your company. (0.5)
b) Remove all of the licensed software from the computer equipment. (0.5)
c) Remove the computer equipment from the asset register. (0.5)
d) Wipe the data from the hard disk using DSD approved deletion software. (2.5)

e) I don’t know what key security step is required to be done when disposing of computer equipment (0)

QUESTION 10.3 From an information security perspective, what is the most important reason to protect remotely located computer equipment?
a) It is only important from a monetary asset point of view, not from an information security point of view. If the equipment is stolen it will cost my organisation money to replace. (0.5)
b) Data may be stolen if someone can access the computer equipment in the remote location. (0.5)
c) Not only could the data from the remote location be stolen or modified, access to my organisation’s network could be gained from that remotely located computer equipment. (2.5)
d) A computer virus could be introduced from that remotely located computer equipment. This could then spread across my organisation via its internal networks and/or storage. (1.5)
e) I don’t know from an information security perspective what is the most important reason to protect remotely located computer equipment (0)