A MODEL TO MEASURE THE MATURITY OF SMARTPHONE SECURITY AT SOFTWARE CONSULTANCIES

By

Mr. Sean Allam

Dissertation

submitted in fulfilment of the requirements for the degree

Master of Commerce

in

Information Systems

in the

Faculty of Management and Commerce

of the

University of Fort Hare

December 2009

Supervisor: Prof. Stephen Flowerday

Abstract

Smartphones are proliferating into the workplace at an ever-increasing rate, similarly the threats that they pose is increasing. In an era of constant connectivity and availability, information is freed up of constraints of time and place. This research project delves into the risks introduced by smartphones, and through multiple cases studies, a maturity measurement model is formulated. The model is based on recommendations from two leading information security frameworks, the COBIT 4.1 framework and ISO27002 code of practice. Ultimately, a combination of smartphone specific risks are integrated with key control recommendations, in providing a set of key measurable security maturity components.

The subjective opinions of case study respondents are considered a key component in achieving a solution. The solution addresses the concerns of not only policy makers, but also the employees subjected to the security policies. Nurturing security awareness into organisational culture through reinforcement and employee acceptance is highlighted in this research project.

Software consultancies can use this model to mitigate risks, while harnessing the potential strategic advantages of mobile computing through smartphone devices. In addition, this research project identifies the critical components of a smartphone security solution. As a result, a model is provided for software consultancies due to the intense reliance on information within these types of organisations. The model can be effectively applied to any information intensive organisation.

Declaration

I, Mr. Sean Andrew Allam, hereby declare that:

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

_____

Mr. Sean Andrew Allam

Acknowledgements

I would like to acknowledge various individuals and organisations for all the support shown throughout this project. Without their support, this research project would never have materialised.

I would like to thank my supervisor, Professor Stephen Flowerday, for the advice, encouragement, guidance and words of wisdom whenever I required them.

I would like to extend my gratitude to the University of Fort Hare, Department of Information Systems for the support it has provided me with through the duration of my academic career. I would like to extend special mention to my fellow students for their advice and support.

I would like to acknowledge the University of Fort Hare and its associated research body, The Govan Mbeki Research and Development Centre, for the financial support that they provided to me throughout this research project. I would also wish to thank the university library and its staff for their support.

I would like to thank each of the respondents who took the time out of their busy schedules to participate in this research project.

Finally, I would like to thank my family, my girlfriend and my friends for the understanding and support shown to me through this time consuming endeavour.

Sean Allam

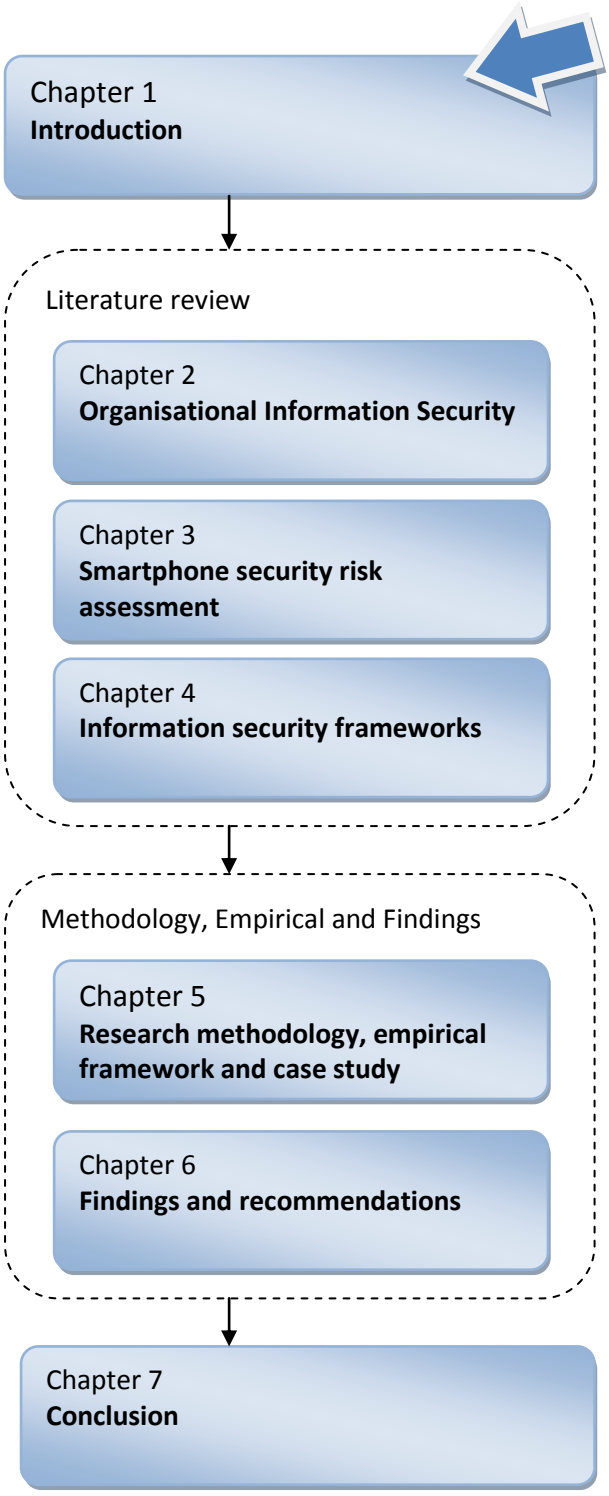
Table of contents

Table of images

List of tables

1 Introduction

Chapter 1



1.1 Background

"A chain is no stronger than its weakest link; but if you show how admirably the last few are united; half the world will forget to test the security of the parts which are kept out of sight" (Stephen, 1868, p. 295). Stephen suggests that a chain's strongest links often overshadow its greatest vulnerabilities. These vulnerabilities are the hidden weaker links in the chain. They are the issues in the chain that one prefers not to have to deal with, instead focusing on the more visible ones. The result, as concluded by Stephen, is that one is often under a false pretence that the strength of a chain is as strong as the strongest linkages, as these are the ones most visible.

Pironti (2005) places this into the mobile information security perspective, by highlighting how vitally important it is to remember that mobile security solutions are not stand-alone phenomena. Pironti indicates that when introduced, they need to become an integral part of the enterprise information infrastructure. An organisation's mobile security solution effectively becomes a link in its information security chain. This follows, that a weak mobile security solution will compromise the strength of the entire chain.

Identifying the weaknesses in this chain and replacing them with strengthened links, increases the strength of that entire chain. Many chief information officers (CIOs) are aware of the possibility of increased risk through the introduction of mobile computing, and that this risk could potentially weaken the existing chain of security currently operating in an organisation. Sacco (2008) highlights a study conducted by the Computing Technology Industry Association (CompTIA) which found that although nearly 80% of respondent organisations allowed mobile workers access to data on their corporate networks, less than a third had actually implemented security awareness training for those workers.

Software consultancy firms deal with the design and development of custom software solutions. These solutions are conceived from the knowledge within the software consultancy firm. Isaksen (2004) describes software consultancy as a knowledge intensive

industry. He points out that software consultancies contain large numbers of workers with tertiary education. Workers dealing with knowledge need access to information. That information is the main asset of the organisation. It is vitally important for software consultancy organisations to protect their information assets while maintaining its accessibility. This is confirmed by Isaksen (2004, p. 1160) who states that "knowledge entrepreneurs are seen to be among the most widely connected or mobile people, always on the move". This places the smartphone in an excellent position to serve the requirements of software consultancy organisations. This however requires a level of security control for smartphone adoption.

In some cases, it might be that mobile computing would seem to pose too big a risk for organisational consideration. However, due to the vast assortment of mobile computing devices available, organisations would be foolish in thinking that they could avoid the issue completely. Others simply ignore or do not understand the risks. The associated risks become even larger, as mobile computing moves from the realm of the enthusiast, to the ordinary office worker. Sharma (2007) confirms this trend by pointing out that it is no longer just executives who carry these devices. Specifically smartphone usage is growing within the ranks of both middle management and staff workers.

This trend is being driven by an evolution of the mobile phone into the smartphone, and this evolution is in turn being driven by a rapidly dropping unit cost. Best (2006, p. 1) provides the following Gartner definition of a smartphone: "A large-screen, data-centric, handheld device designed to offer complete phone functions whilst simultaneously functioning as a personal digital assistant (PDA)". According to a study by In-Stat, global Smartphone sales are predicted to increase by 30% year on year, for the next five years (Reardon, 2007). Smartphone usage is filling a gap that PDA devices failed to achieve. Unfortunately as pointed out by Pironti (2005, p. 31), smartphones are emerging as "primary points of

vulnerability in the new wireless enterprise", with their ability to not only send and receive information, but to store it as well.

Smartphone usage introduces a unique set of risks into a software consultancy organisation's information security. Pironti (2005) emphasises that these new risks emanate from a completely different direction to traditional security, which has primarily focused on protecting just the network. Existing traditional security mechanisms would need to be both extended and refined. This would allow one to accommodate for the added security risks introduced by the use of smartphones. In order to extend and refine existing security mechanisms, organisations need to be able to measure the existing security against the accepted minimum requirements needed to satisfy corporate governance requirements. Pironti (2005, p. 31) provides the following steps, which one should consider when measuring mobile security risks and defining a solution for these risks:

- Perform a thorough threat and vulnerability assessment of the devices that the enterprise will support, along with the business processes to which those devices align. This would help to analyse and quantify the risk that these mobile devices pose.
- Implement appropriate policies and security controls so that employees can use their mobile devices without harming the enterprise.
- Classify data (according to business importance) in order to mitigate some mobile computing threats and ensure security and integrity of that data.
- Establish a policy laying out the rules, communicate this to the user community and establish the logical and physical controls required to enforce the policy.

However, measuring these risks and defining appropriate solutions can be a difficult task without some guidelines. Sweren (2006) explains that the base or the foundation of an information security program needs acceptance in the information security industry, while remaining applicable to an organisation's environment. For this reason, recognised frameworks, standards and toolsets, such as the COBIT 4.1 framework and the ISO27002

(formally known as the ISO17799) code of practice for information security management, exist to assist with the implementation of enterprise security solutions. These frameworks have been developed by industry experts and have proven capability in improving enterprise security where applied.

COBIT 4.1 is self-defined as, “a framework and supporting toolset that allows managers to bridge the gap with respect to control requirements, technical issues and business risks, and communicate that level of control to stakeholders” (IT Governance Institute, 2007b, p. 8). Using COBIT 4.1, clear policies and good practices can be implemented throughout the enterprise. The governance-focused approach of COBIT 4.1 centres on the management and control of information. Complementing this, the ISO27002 provides a comprehensive and clear set of standards based controls to reduce and mitigate security risks. Garbani, Koetzle, and Powell (2006) indicate that the critical success factors, and key performance indicators of COBIT 4.1, together with the security processes and controls of ISO27002 are highly complementary. They continue by adding that COBIT 4.1 and ISO27002 also provide guidance, key indicators, and controls for the definition of service-level agreements, capacity planning, availability management, and business continuity (Garbani, Koetzle, & Powell, 2006).

Sweren (2006, p. 1) points out the benefits of aligning enterprise solutions to frameworks such as these:

- The organisation does not have to maintain the specific content of that framework, as this is the responsibility of the control group responsible for each framework.
- These frameworks have been reviewed and vetted by more people of knowledge than are available in the organisation.
- Finally, it is something the organisation’s management and board of directors can trust and recognise without the requisite knowledge of information security jargon.

In summary, software consultancy organisations require a holistic end-to-end security chain. This chain requires continuous monitoring for weaknesses of any links in the chain. Any weaknesses compromise the entire chain of security. Formulating a security strategy to encapsulate the entire chain would prove overwhelming for a single organisation or department. Instead, basing and aligning one's security strategy to trusted frameworks would result in a more effective security chain, end-to-end. Finally, establishing controls to monitor and measure each portion or link in the chain would ensure prolonged integrity of the entire chain.

Furlong, vice president of security and mobile connectivity at Nokia, states that, "as your employees become more mobile, the security policies that you implement need to adapt to the mobile market" (Lim, 2007, p. 12). Furlong is suggesting that existing security is not suitable for mobile security use. Sharma (2007) concurs, that while it is straightforward for IT departments to manage business applications that reside on laptops or PCs, conducting the same on mobile handsets provides far greater challenges. He explains that mobile devices and applications run on many different operating systems and through a wide range of access technologies. Pironti (2005) agrees that the security risks of smartphone devices are complex, requiring the establishment of controls that enable enforcement of a risk mitigating policy.

As noted previously, these new controls cannot be stand-alone phenomena, but must form part of the greater security chain. In order to establish the security required, existing risks need to be measured and mitigated. Measuring risk is the process of defining the risks and identifying their probabilities of occurrence. Mitigating risks is the process of identifying the controls available to reduce them.

Management needs to define a security model based on recognised security frameworks, standards and toolsets. This security model needs to be able to measure existing security. The model must also provide the company with recommendations on where it needs to be. Any new security requirements must be accepted and adopted by management, IT, and of course employees. Finally, the security model needs to be both transparent and adaptable to a multitude of different smartphone devices that it will be required to secure.

1.1.1 Smartphone security solutions

The majority of literature focuses on the technical nature of smartphone security, and include issues of encryption, network protocols, communication protocols, operating system configurations and many other technical aspects. However, technical topics are outside the scope of this research.

Dunn (2007) mentions that smartphone security is still a largely neglected area. McCall (2006) agrees suggesting that although smartphones are used increasingly as organisational productivity tools, not all corporate network administrators have plans to safeguard the corporate data carried on these devices. Sharma (2007) adds that CIOs fail to consider smartphone devices in terms of their security and management strategies. The evidence suggests therefore that the security industry is currently paying too little attention to a technology that is real, and already becoming a major threat.

1.1.2 The COBIT 4.1 framework

IT governance integrates and institutionalises good practices to ensure that the organisation's IT supports the business objectives. The COBIT 4.1 framework meets this definition by "providing good practices across a domain and process framework which presents activities in a manageable and logical structure" (IT Governance Institute, 2007b, p. 5). The COBIT 4.1 framework contributes to the needs of delivering against business requirements through the following:

- Making a link to the business requirements;

- Organising IT activities into a generally accepted process model;
- Identifying the major IT resources to be leveraged;
- Defining the management control objectives to be considered (IT Governance Institute, 2007b, p. 5).

The process focus of COBIT 4.1 is illustrated by a process model, that subdivides IT in to four domains and 34 processes in line with the responsibility areas of plan, build, run and monitor. This end-to-end approach to the IT process provides management with a core foundation centred on solid accepted guidelines. The IT Governance Institute indicates that enterprises need an objective measure of where they are and where improvement is required. "Organisations need to implement a management tool kit to monitor this improvement (IT Governance Institute, 2007b, p. 6)".

COBIT 4.1 provides for the assessment of process capability, based on maturity models, which help to identify gaps in capability and then be demonstrated to management. Action plans can then be developed to bring these processes up to the desired capability target levels. This makes COBIT 4.1 perfect for assessing the gaps existing between the currently implemented security solution, and a COBIT 4.1 based smartphone security solution. COBIT 4.1 defines IT activities in a generic process model within four domains (IT Governance Institute, 2007b, p. 12). The four domains defined by COBIT 4.1 are Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. COBIT 4.1 explains that these domains map to I.T.'s traditional responsibility areas of plan, build, run and monitor. The COBIT 4.1 framework is especially well suited as it incorporates a common language for all sectors of the business involved in IT.

This research project will focus primarily on the Plan and Organise domain of the COBIT 4.1 framework. This is because the scope of this research project does not include the implementation aspects of a smartphone security solution. The IT Governance Institute describes the domain as one that covers strategy and tactics, and concerns the identification

of the way IT can best contribute to the achievement of the business objectives (IT Governance Institute, 2007b, p. 12). The IT Governance Institute further indicates that the realisation of the strategic visions needs to be planned, communicated and managed for different perspectives. Planning and organising provides the foundation for implementing a smartphone solution into the organisation. The proposed solution will cover the following key requirements:

- Aligning the smartphone business strategy with the overall business strategy;
- Plan for optimum use of enterprise resources;
- Providing a means for everyone in the organisation to understand the objectives of a smartphone security solution;
- Providing an understanding of the risks and their management;
- Determining whether the quality of the smartphone solution is appropriate for the business needs.

This study will assess each of the processes within the COBIT 4.1 frameworks. The IT Governance Institute recommends the use of maturity models, in order to establish how well IT is being managed, and what can be done to reach adequate maturity levels (IT Governance Institute, 2007b, p. 17). By using maturity models based on each of COBIT's processes, organisations are able to measure where the enterprise is situated in relation to the required levels of a smartphone security solution. Then the organisation can efficiently decide the direction in which it needs to move, and measure the progress made towards this goal.

1.1.3 The ISO27002 standards

The ISO27002 standards derive security requirements based on assessing risks to the organisation and by adhering to legal, statutory, regulatory and contractual requirements and a particular set of principles, objectives and business requirements (Standards South Africa, 2005). The international standard establishes guidelines and general principles for initiating, implementing and maintaining and improving information security management

in an organisation (Standards South Africa, 2005). The control objectives and controls in ISO27002 are implemented to meet the requirements identified by a risk assessment (Standards South Africa, 2005). This makes the ISO27002 standard a perfect complement to the risk analysis performed using the COBIT 4.1 framework. The ISO27002 provides a common basis and a practical guideline for developing organisational security standards. This includes effective security management practices to help build confidence in inter-organisational activities.

"The standard contains 11 security control clauses, collectively containing a total of 39 main security categories, and one introductory clause introducing risk assessment and treatment" (Standards South Africa, 2005, p. 4). This research project will also make use of existing COBIT 4.1 and ISO27002 mapping documents.

1.2 Statement of the problem

With the mass consumerism of the smartphone being driven aggressively by leading IT companies such as Apple, HTC and Microsoft, along with the continuous release of feature heavy handsets by manufacturers such as Nokia, Sony Ericsson, LG, HTC and others, many organisations are seeing the proliferation of smartphones into the workplace. Predictions have estimated this number to be as high as 30% globally year on year, for at least the next five years (Reardon, 2007). Yeo (2008) quotes a Gartner prediction that by 2012 half of all mobile employees will switch from laptops to more powerful and compact devices such as smartphones. Software consultancy organisations that do not prepare for the introduction of smartphones into their infrastructure will suffer the consequences of security vulnerabilities, and threats which exploit these vulnerabilities, being introduced by these devices. Many of these organisations do not have a concise and eligible model to measure and identify gaps or vulnerabilities existing between their current security solutions and an adequate smartphone security solution.

1.3 Research question

How can a software consultancy organisation measure the vulnerability gaps that exist between its existing security solution, and a smartphone security solution so it conforms to both the COBIT 4.1 framework and the ISO27002 standards?

A software consultancy organisation's existing security solution requires adjustment in order to encompass smartphone security requirements. This would include an analysis of the requirements of a smartphone security solution for a software consultancy organisation. These requirements when measured against an existing security solution will identify the vulnerabilities that exist in the security solution as it is. The IT Governance Institute (2007b) states that management is constantly on the lookout for benchmarking and self-assessment tools. They indicate the need for a tool to measure where the organisation is, where it needs to go, and how to measure progress against this goal. Vulnerabilities are the gaps between the existing security solution as it is, and the direction it needs to take. Figure 1 illustrates the gap between the existing security solution (right column) and a security solution that includes smartphone security component (left column).

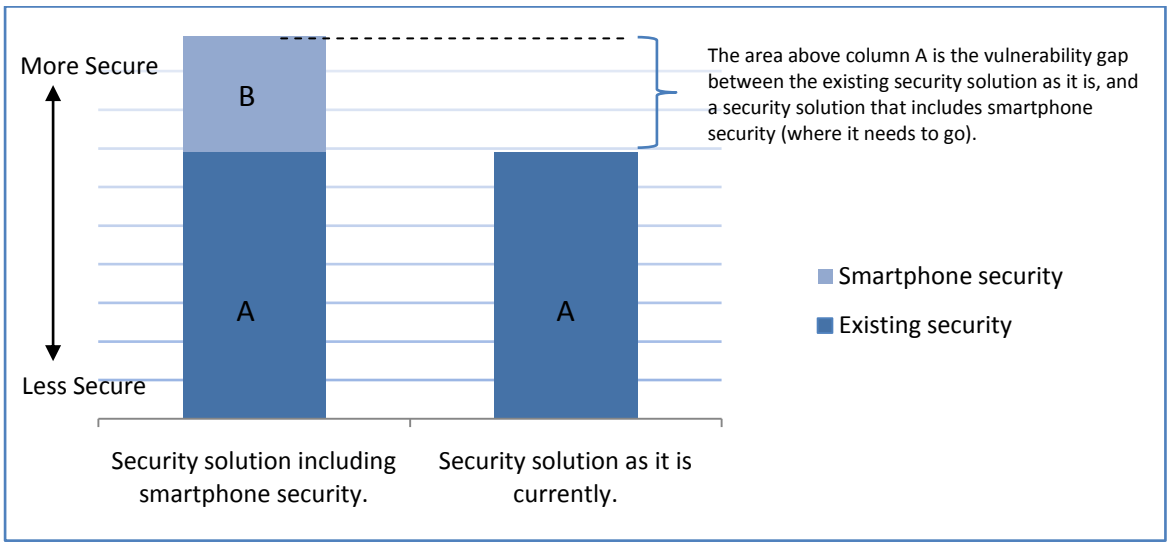


Figure 1 - The vulnerability gap

New controls and policies must be defined to minimise gaps once they are identified. Measuring the requirements of a new solution can be achieved by basing the analysis of the measurements on existing accepted frameworks and standards. Therefore, the COBIT 4.1 framework and ISO27002 standards have been selected, due to their recognition and acceptance by industry experts. This research project will define a model as the tool to identify the requirements of a software consultancy organisation's existing security solution. This solution will include smartphone security components and will aim to satisfy the security requirements of smartphone adoption in these organisations. The model will identify the gaps that exist between a software consultancy organisation's existing security model as it is, and that of a smartphone security model based on the COBIT 4.1 framework and ISO27002 standards. Using this model, organisations will be able to identify the vulnerabilities illustrated above in Figure 1 as area 'B'.

1.4 Sub-questions

What are the specific security requirements of smartphones in software consultancy organisations?

Software consultancy organisations, by their nature tend to have a significant mix of technology, and technology professionals; an extra level of vigilance to maintain smartphone security amongst skilled employees using advanced smartphone technologies, is required. Seventeen measurable components are identified in this research project in response to this research sub-question.

What components from the COBIT 4.1 framework and ISO27002 standards are most significant to a security solution that includes smartphone security?

The COBIT 4.1 framework and ISO27002 standards consist of a number of components aimed at a broad technology spread. Identifying the components most relevant to smartphone security is crucial in providing a solution that is both concise and focused. This

research highlights these components, and integrates them with other key smartphone security requirements in producing a solution to this research sub-question.

How can the gap between an existing security solution and one that conforms to both COBIT 4.1 *and ISO27002 be measured in a software consultancy organisation?*

Identifying a way to measure the gaps between an existing solution, and one that conforms to the COBIT 4.1 framework and ISO27002 standards, is a core focus of this research project. It will provide a software consultancy organisation with a starting point for the implementation of smartphone security, in a way that will not hamper its inception, or compromise existing security solutions. Measuring these gaps in a software consultancy organisation will present a unique set of requirements, risks as well as other factors to consider. A maturity model with adjustable targets is provided by this research project as a response to this sub-question.

1.5 Objectives of the study

The objective of this research project was to define a model. This model was expected to provide clear and concise guidelines to measure a software consultancy organisation's existing security solution against a solution based on the COBIT 4.1 framework and supported by the ISO27002 standards. The model solution will include a smartphone security component as a core requirement. Using this model, software consultancy organisations will be able identify vulnerabilities in their existing internal security controls. Consequently, goals can be established to reduce and remove these vulnerabilities. Maturity models can then be used to measure the progress made by these organisations in reducing or removing the weaknesses in their system of internal controls.

Brotby (2007, p. 2) states that "it is probable that recognising the value of an organisation's intangible assets and integrating information security governance with business strategy will be increasingly critical to ongoing corporate success". Thus, Brotby emphasises the

increasing importance of information as an intangible organisational asset. Protecting this asset is as important as the tangible assets of an organisation. Thus, the primary objective of securing smartphone usage is that of securing information assets.

1.6 Significance of the study

Dunn (2007) states that while personal smartphones have added complexity to the ongoing development of the IT landscape, smartphone security is still a largely neglected area. It is alarming to consider the potential for damage by both malicious and unintentionally motivated incidents because of users, who may or may not even be aware of the fact that their smartphone device is insecure. In fact the centre for public service innovation in South Africa, listed 'institutional readiness' as one of the leading factors to consider when implementing a mobile computing solution. They state that the real issue is one of management, rather than of technology (The centre for public service innovation, 2003, p. 28).

Kooser (2007) explains that when it comes to mobile security, prevention is definitely the key. According to Pironti (2005), users fail to appreciate the sensitivity of storing data on these devices. In addition, they do not understand how to secure data on these devices and even consider security mechanisms to be an inconvenience not worth having (Pironti, 2005). Dunn (2007) indicates that policies, although restrictive of an employee's use of a certain mobile computing platform, would be effective in securing data. However, these policies may be difficult to enforce remotely. In other words, acceptance from the end user of these policies is essential. Using the model from this research project, software consultancy organisations will now have a starting point from which they will be able to measure the success of their preparation for a smartphone security solution.

Following this study, these organisations will be able to design and implement a security solution and supporting policies. This solution must be specifically directed at closing the gaps identified within an organisation's existing security solution. This will assist in defining

the expansion of the existing security solution to accommodate for the requirements of a COBIT 4.1 and ISO27002 compatible solution. These solutions will be grounded on secure policies, which are in turn founded on an accepted security framework utilising accepted standards.

1.7 Research design

Congdon and Dunham (1999) point out that the probability of a successful project is greatly enhanced when the beginning is correctly defined as a precise statement of goals and justification. The research design describes the elements of the research and the methodology to be followed.

1.8 Research paradigm

The paradigm selected for this research project is interpretive using qualitative research methods. Myers (1997, p. 1) explains that, "qualitative research methods were developed in the social sciences to enable researchers to study social and cultural phenomena. Examples of qualitative methods are action research, case study research and ethnography". This approach is conducive in understanding the social constraints and opportunities in adapting towards a controlled smartphone security solution. Greenhalgh and Taylor (1997) add that qualitative research attempts to address and interpret phenomena in terms of the meanings that people bring to them. The underlying epistemology on which this research project is based, is that of an interpretive approach, where knowledge will be interpreted based on the researcher's experience. Myers (1997) states that interpretive studies are generally aimed towards understanding the phenomena, through the meanings that people assign to them.

Neill (2006) indicates that the interpretive approach allows one to gain insights through discovering meanings. Myers (1997) adds that interpretive methods of research in IS, are aimed at producing an understanding of the context of an information system, the process which itself influences that context. Gaining a subjective insight of the holistic impact of

smartphone security in the context of an existing security solution can be achieved using an interpretive approach. Neill (2006, p. 1) states that "a major strength of the qualitative approach is the depth to which explorations are conducted and descriptions are written, usually resulting in sufficient details for the reader to grasp the idiosyncrasies of the situation". He suggests that research should provide both a rich and deep exploration of a particular subject.

Collis and Hussey (2003) indicate that combining research strategies would allow one to take a broader view of the research problem. They suggest that few research projects would be compiled using one research paradigm. Due to the slant of this research project towards the managerial aspects of smartphone security, qualitative research methods will be predominant. However, analysis of these results will be quantified using quantitative methods in order to identify any possible trends. Combining qualitative and quantitative methodologies will allow the researcher to obtain a deeper understanding of the results. Collis and Hussey (2003) refer to this as research triangulation.

Figure 2 illustrates the extremes of the pure interpretive approach and the pure positivist approach.

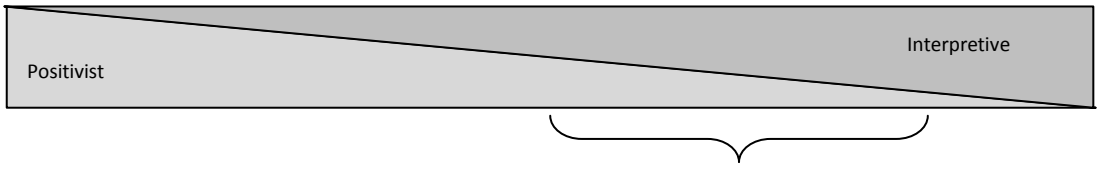


Figure 2 - Research methodology positioning

As one moves between the extremes the composition of the research consists of less of one approach and more of the other. This research project will be positioned as indicated towards the interpretive approach.

1.9 Research methodology

This research project will culminate in the development of a model. Olivier (2004, p. 45) explains that a model should "capture the essential aspects of a system or process, while it ignores the non-essential aspects". The model will be based on the following characteristics as defined by Olivier (2004, p. 49):

- It should be simple to understand;
- It should be comprehensive;
- It should be able to be applied generally;
- It should fit the problem exactly;
- It should be clear.

1.10 Data collection

Myers (1997) provides us with the following examples of qualitative data sources: observation and participant observation (fieldwork), interviews and questionnaires, documents and texts, and the researcher's impressions and reactions. The research instrument used to collect the data required for the model will be a questionnaire. Components will be selected from the COBIT 4.1 framework for inclusion in the questionnaire. The researcher will select the components according to their role in the COBIT 4.1 framework. Questions will be organised into managerial and operational smartphone security requirements. This will provide the researcher with subjective and quantifiable results, of the subjective opinions of the respondents of each questionnaire.

The questionnaire will be distributed to voluntary participating software consultancy organisations. The questionnaires will need to be completed by employees at various positions and in levels within the organisations. The questions will range from the operational to managerial levels. Questions will be structured in such a way as to be as subjective as possible. The questions will achieve subjectivity by utilising scaled response options. The respondents will be asked to indicate the level to which they consider the question statements importance to be, to smartphone security at their organisation. This

question structure is similar to that of the maturity model of the COBIT 4.1 framework. This approach allows each respondent to subjectively evaluate a similar set of structured question statements that can easily be quantified.

1.11 Data analysis

The data will be analysed using a spreadsheet tool for trends and patterns amongst the respondents. Graphs and charts will be generated in order to present trends graphically. All trends and patterns identified will then be incorporated into the development of the model.

1.12 Delimitation of the study

This research project is focused on providing a model. The model will assist in measuring software consultancy organisations security readiness for the adoption of smartphones. The primary focus will not contain technical implementation instructions. Instead, the solution will emphasise the requirements at a higher managerial level. Furthermore, the outcome will not provide an estimated period or budget for implementation of its recommendations, as these will depend on each individual organisation's circumstance.

The specific technical details of each smartphone device will not be considered for this research project. Integrating smartphone security into a software consultancy organisation's existing system of internal controls is the core focus of the model developed in this study. This model will be constructed from the specific smartphone security requirements of software consultancy organisations.

This research project will adopt a neutral stance regarding each device, device model, device manufacturer and device operating system. Software consultancy organisations will be able to use the outcome of this research project to make an informed managerial decision. This research project provides security solutions for devices that fall under the description of a smartphone. This description will be clearly defined in the research project. The results of this study would need to be reassessed for any possible implementation or adoption in other industries, organisations or government departments.

1.13 Outline of the research project

The research project begins with an introductory chapter. Chapter 1 provides a brief introduction to the topic and the problem within the context of a software consultancy organisation. Chapter 1 also provides an overview of the objectives, research methodology and delimitation of the study. Chapter 1 concludes with details of the outline of the research project.

Chapter 2, 3 and 4 provide the literature review section of this research project. Chapter 2 explains the importance of organisational information security. The role of information as an organisational asset is established, followed by the importance of an information security culture. Software consultancies and information workers are discussed in detail in Chapter 2.

Chapter 3 introduces the smartphone and establishes a definition for this research paper. Smartphone security weaknesses are defined and explored in detail. Finally, Chapter 3 concludes by contrasting the risk management and mitigation measures of smartphones against more traditional fixed computing devices. In Chapter 4, two industry leading information security frameworks are analysed as a basis from which the research model can be developed. These frameworks are then analysed to identify the components that are relevant to the requirements of smartphone security.

The research methodology, empirical framework and case study are discussed in Chapter 5. The chapter provides both the philosophical assumption and method of study used to address the research problem. The empirical framework and resulting case study are detailed in Chapter 5, including details of the primary and secondary data used.

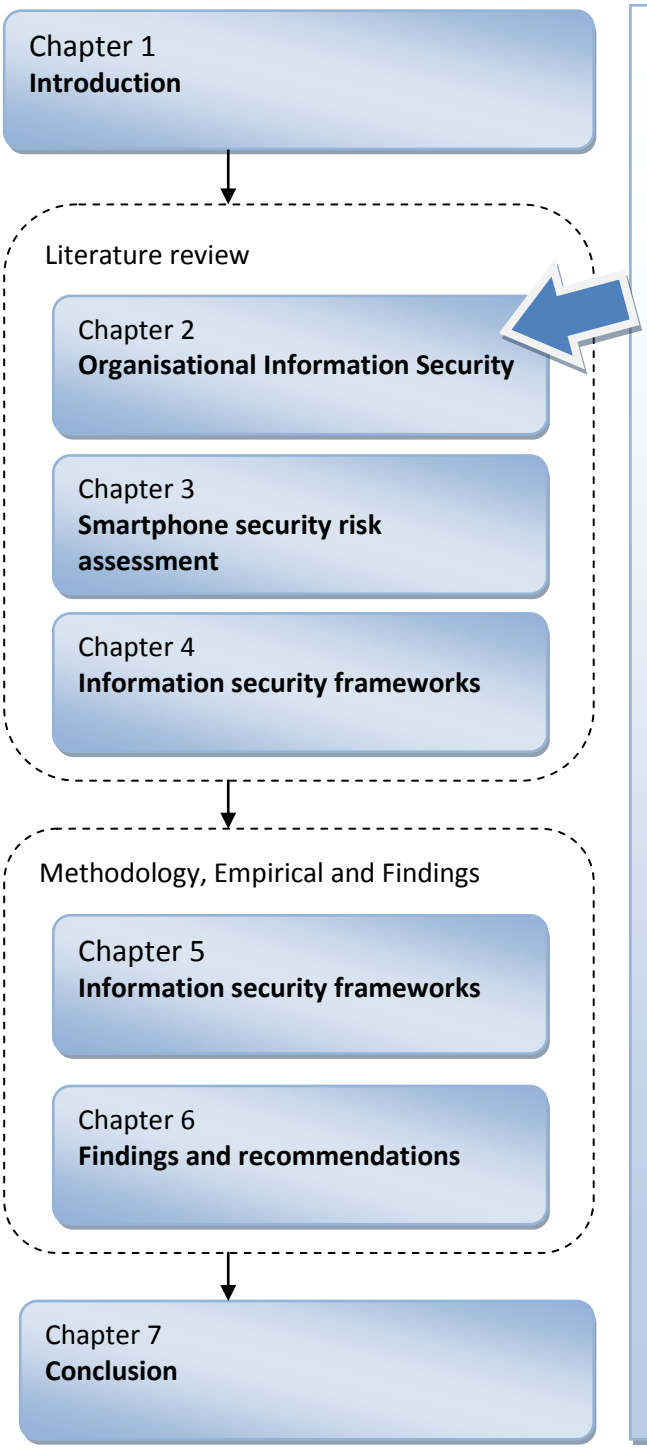
In Chapter 6 the findings of the research project are presented, followed by the recommendations. A model is presented in this chapter in response to the research

problem. Chapter 6 concludes with a detailed explanation of the recommendations and model.

Finally, Chapter 7 concludes this research project by providing an explanation of the contributions made by this research, an evaluation of the research outcomes and directions for future research.

2 Organisational Information Security

Chapter 2



2.1 Introduction

Information, and more importantly the security thereof, is the ultimate goal of smartphone security. Many organisations focus security efforts solely on the protection of physical assets. Certainly in the information technology (IT) department, hardware ranks as one of the most expensive investments an organisation makes. However, hardware investments are only there to serve information requirements.

Organisations need to recognise the importance of their information. They need to emphasise its protection, as the most important of all the assets of the IT department. Employees must be made aware, through education, of the importance of information. Section 2.2 introduces the concept of information as an asset, and organisational information security cultures. This becomes vital as we enter into an information centric age of business. Many companies have failed to recognise the increasing importance of information in their daily business procedures.

Section 2.3 explains the importance of information security, within the context of the organisation. Understanding the importance of information security ensures that a culture of information awareness, and acceptance, prevails. This is provided in section 2.4, which also covers the importance of ensuring that employees are at the centre of all efforts to maintain information security.

Section 2.5 of this chapter introduces the software consultancy organisational context of this research project, and provides an explanation of the reason that this context was chosen. Focus will be shifted to employees in section 2.6, only this time to understand the concept of an information workforce, and how information is driving a new era of information workers. Section 2.7 details the importance of acceptance towards information security by all employees. Finally, section 2.8 provides insight into the steps that security stakeholders can take to establish a security control mechanism, through a stringent awareness culture and widespread policy adoption.

Doherty and Fulford (2006) describe information as the lifeblood of an organisation. Information is redefining the way that we do business; in turn, we must redefine the way that we use and protect information. Organisational information security is not a new concept. It has existed in some form as long as business itself. However, technological advancements have completely changed both the importance, and definition of organisational information security. Finally, the term information, as provided in this chapter, refers to all forms of information such as data and knowledge.

2.2 Information as an asset

The protection of organisations' information assets is a complex task. Securing information means securing the repositories it is stored in, the channels it moves across and the systems that process it. Information is being exposed to an ever-growing number of threats and vulnerabilities (Standards South Africa, 2005). Information assets introduce many risks and complexities. An Information asset can comprise of a vast assortment of different forms and factors. Musaji (2006) indicates that information assets can include systems, data, images, text and voice. These assets are contained within the internal systems that support the company's business activities.

Kruger and Kearny (2008) point out that companies will often spend huge amounts of money and time on implementing technical solutions, while the human factor in information security receives relatively less attention. Protecting information is the responsibility of all employees, and not just those at managerial levels.

Employees do not tend to take as much care of information assets, as they would with a physical asset. They are often unable to place value on intangible concepts such as information. Kruger and Kearny argue that it is therefore important for human activities to be linked to security issues through the involvement of humans in information security. In order for security to become a priority concept, people need to be at the centre of its implementation.

As with physical assets, employees should be made aware of the value of the information that they might take for granted in an organisation. Information is an asset to the company. Senior management are ultimately responsible for educating all employees on the importance of protecting information, as if it were a regular physical asset. Strict policies and guidelines need to be identified and implemented. These must be introduced in such a way, as to not restrict the flow of information within the organisation. Businesses thrive on information. Restricting the flow of information would prove detrimental to the business and frustrating for employees.

There is no definitive description or example of an information asset. The value of an information asset can change depending on the context within which it exists. Often information is what uniquely positions most companies from their competitors. Today businesses are operating in markets that move more quickly than ever before; and information becomes key to detecting or predicting market movements. Companies that can harness their information to help them to react faster to these movements can achieve winning results. Ensuring that information is readily available and accurate, while at the same time remaining secure, is key to the importance of information security.

2.3 The importance of information security

The importance of protecting an organisation's security exists for a number of reasons. Organisational information that is compromised, stolen or lost can harm more than just the organisation. If an organisation maintains confidential third party information, the responsibility remains with the organisation to protect that information. Loss of information could result in damages to the organisation itself or third parties. This may be in the form of damaged reputations, loss of confidential information and trade secrets, or in extreme cases may result in threats to human life.

Information security threats can result from a number of different sources, and take many forms. Standards South Africa (2005) provides the following list of possible forms of threats to an organisation's information security:

- Computer-assisted fraud
- Espionage
- Sabotage
- Vandalism
- Fire or flood
- Malicious code
- Computer hacking
- Denial of service attacks

These, and other forms of threats are not only on the increase, but according to Standards South Africa (2005), are becoming both more sophisticated and ambitious. These security threats exist from both inside and outside the organisation, and they can be classified as intentional or accidental (Kritzinger & Smith, 2008).

Organisations however have traditionally focused on applying security to control external threats to information security. Often organisations are only seeking to mitigate internal malicious intentions when implementing internal controls. Table 1 indicates the primary and secondary focus areas for a majority of organisations.

Table 1 - Threat source security focus

	Internal Threats	External Threats
Malicious Intentions	Secondary Focus	Primary Focus
Accidental/Unintentional Actions	Minimum Focus	Secondary Focus

As indicated in the above table, the primary focus of traditional security solutions has been against the malicious actions of external threats such as hackers or viruses. Secondary focus is aimed at restricting external accidental information security breaches and malicious

internal breaches. Lastly, internal unintentional or accidental information security breaches traditionally receive relatively less or no attention.

Liginlal, Sim, and Khansa (2009) state that human error, as a cause of data breaches, has received very little attention from researchers. They found that internal accidental threats, such as human error, actually accounted for a large percentage of incidents over a period from January 2005 to June 2008 (Liginlal, Sim, & Khansa, 2009). This is especially true in smaller organisations that traditionally operate under the notion of absolute trust in employees. A trust that views employees as always acting within the best interest of the company.

Addressing each of these areas equally is imperative in ensuring that the security chain contains no weak links at any point. The traditional mindset of information security, as being a defence strategy from outside offenses, need to be updated or redefined to an offensive strategy on security weaknesses. This is especially important for smartphone security. Still in its infancy, smartphone security is at a higher risk from both internal and external threats, than more mature computing platforms.

The CIA triad (or triangle) is a widely known and accepted conceptualisation of the pillars of information security.

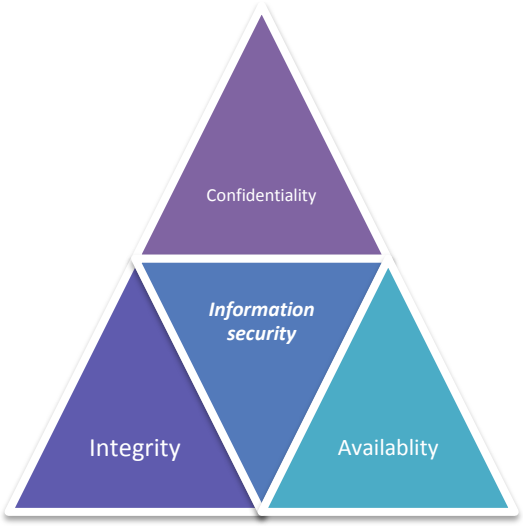


Figure 3 - The CIA Triad (Triangle)

The triangle indicates that information security can be broken up into three core components (the pillars): confidentiality, integrity and availability. The first component, confidentiality, centres on the restriction of access to information. Only authorised individuals should have access to confidential information. Confidentiality is a critical component of information security.

The restriction of access to information ensures that only authorised and authenticated users are able to view restricted organisational information. Authenticated users are users that are permitted to access the organisations information systems. Authorised users are authenticated users with the permission to access the information contained within these systems.

Confidentiality measures must be implemented across all mediums of information storage, communication and processing for true restriction of access to be enforced. Enforcing confidentiality is a complex task involving multiple technologies and communication methods. Without confidentiality, the integrity of information could become compromised.

Smartphones present confidentiality issues by virtue of their mobility. Confirming the identity of a smartphone user attempting to connect via an independent service provider, requires a heightened depth of security.

The second component in the CIA triangle, Integrity, is based upon the need for information to be accurate, authentic and trustworthy. Digital information can be easily modified. Modified information no longer provides the authenticity of its original state. Thus preventing the undesired modification of information is paramount to protecting its integrity.

Information must be maintained in the format that is best suited to the business context that it supports. Malicious or accidental modifications might result in information that is no longer able to provide a competitive advantage to the employees that use it. Integrity can be better protected by ensuring that the confidentiality of the information is maintained. Ensuring integrity, such as enforcing confidentiality, is complicated by the various forms of information available. In addition, smartphones often communicate this information on untrustworthy network channels. Untrustworthy channels are digital networks where the organisation does not have any control over the security controls, policies or implementation. Ensuring the integrity of the information received and sent on these networks is paramount to achieving adequate information security.

The final component, availability, indicates the importance of being able to access information when and where it is required. This component is often neglected by organisations that do not invest enough in technology capable of extending the access employees have to information. Availability, if adequately addressed, can provide a competitive advantage for employees. However often in order to achieve adequate levels of availability, organisations must make extensive use of untrustworthy networks.

When an employee is connected to a third party untrustworthy network, the organisation has limited to no control over the security deployed across that network. Adequate security for an organisation's information should provide mitigation strategies for untrustworthy communication channels. However, restricting access to these networks will reduce or halt productivity gains possible through smartphone use.

All information needs securing in such a way as to address each of the components of the triangle. Organisations that fail to address each of these components, will compromise the value of the information to the organisation. This can result in stagnation of the innovation and responsiveness of the organisation to its markets, suppliers and consumers. Al Aboodi (2006) adds that demonstrated information security, can add real value to an organisation, by contributing to the integration with trading partners, maintaining closer customer relationships, improving competitive advantage and protecting reputations.

Information security is vitally important. Employees should receive training and education in order to both understand and support this sentiment. To achieve the objectives of information security, an organisation-wide culture of information security must be nurtured. One in which all employees are tuned into the threats to their organisations information confidentiality, integrity and availability. One in which all employees are provided with the tools and knowledge to act on these threats accordingly. Organisational culture is discussed in the following section. Defining and installing this culture is the responsibility of organisational leaders and policy makers.

2.4 Establishing an information security culture

The most secure information security solution would be futile without the support of the employees with whom it is tasked to protect. Olzak (2006), states that one of the most important pieces of an effective information security solution is employee awareness. New employees might not be aware of existing policies, or the need for these information security policies. It becomes vitally important that employees are aware of such programs

at the initiation of their employment with the organisation. Existing employees require constant reminding, using both direct and indirect means of reinforcing that awareness.

Ruighaver, Maynard, and Chang (2007) found that there was no evidence that employees are intrinsically motivated to adopt secure practices. They argue that employees need to learn that security controls are necessary and useful, in order to discourage them from attempting to bypass these controls. Thus, employee motivation needs to be developed. Motivational rewards, such as money and recognition, can also be used to increase levels of participation.

Albrechtsen (2007) explains that a user's view on information security is created by several interlocking organisational, technological and individual factors. Any changes to the environment in which employees are familiar with, tends to be highly resisted. Thus introducing any policy of information security can be met with resistance from some employees. Unfortunately, security changes are usually forced on organisations, as they must adapt to external fluctuations in markets, technology and legislation.

Employees might not be aware of how these changes translate into changes that they are required to address. In fact, employees will tend to overlook security, if this allows them to ease their workload (Albrechtsen, 2007).

Rasmussen (1997) points to the existence of a natural migration of employees towards a boundary of acceptable performance. A natural human instinct is to find the easiest and most convenient way in which to complete work tasks. In Figure 4, this natural instinct is illustrated as a gradient towards the least effort. This gradient illustrates a natural resistance of workloads that are unacceptable, represented as the boundary of unacceptable workload. Pressure from management away from the boundary of economic failure, along the gradient of efficiency, provides a natural balance to the gradient of least effort. Acting against each other these gradients move towards a final gradient of functional

acceptance. At the extremes of functional acceptance (along its boundary), efficiency is maximised while workload is minimised.

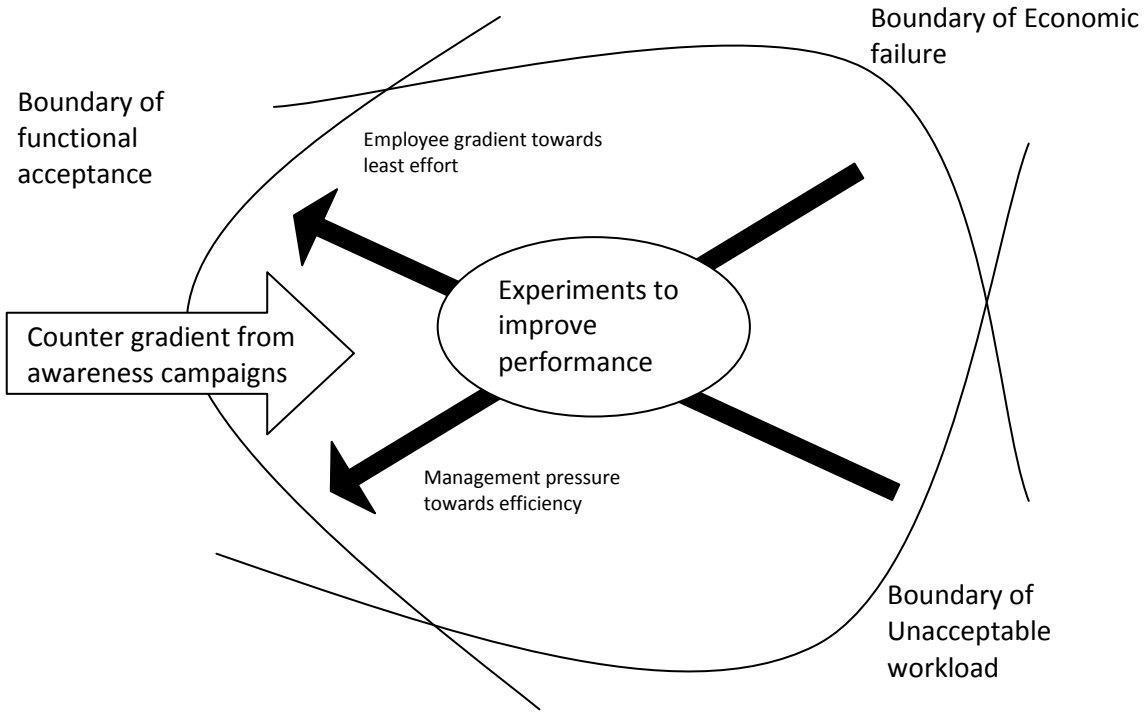


Figure 4 - Awareness boundaries (adapted from Rasmussen (1997, p. 189))

This model assists in understanding the role that information security awareness campaigns play in organisational security. If left unabated, either gradient would continue to cross the boundary of functional acceptance. Rasmussen (1997) indicates that at this point errors and accidents may occur. In the context of information security, this might result in a breach of the confidentiality, integrity or availability of organisational information security.

A natural employee focus on moving away from unreasonable workloads exists in each organisation. Employees perceive security measures as adding unnecessary effort to their work tasks. In contrast, management often strive to achieve the highest levels of efficiency. In order to achieve the highest levels of efficiency, management will often neglect security

measures. This results from management being primarily interested in resisting the boundary of financial failure.

Neither employees nor management should be able to increase pressure along their gradient, without at least some resistance from policy and awareness counter-pressures. This awareness might be in the form of policy or controls, but awareness of these policies and controls is vital to a counter gradient effort.

A culture of security awareness will counter the gradients of least effort and efficiency, maintaining a balance towards functional acceptance, but not breaching through. This awareness can be achieved through education and awareness programs. These awareness programs are a means of creating the initial awareness, for an information security culture defined by policies and controls.

The use of smartphones as a means of reducing work effort will increase pressure on the gradient of least effort. In contrast, management might introduce smartphones as a means to increase productivity. This will increase pressure along the gradient of efficiency. However, both management and employees in their efforts to maximise the pressure on these gradients, might neglect smartphone security considerations.

The quality of the information security management also affects users' awareness, motivation, and behaviour in some way (Albrechtsen, 2007). Albrechtsen provides a list of possible components of an information security awareness program:

- Information campaigns
- Education
- Rewards
- Technological / Physical measures
- Legislation

Kruger and Kearny (2008) add the following items to this list:

- Posters
- Presentations
- Brochures
- Intranet resources
- In-house magazines

Albrechtsen states that the field of information security has traditionally been directed towards technological problems and solutions, and has lacked socio-organisational and human aspects. Al Aboodi (2006) agrees, that in the past security decisions were based primarily on technology, and assigned to individuals with technical expertise. They add that because technology itself cannot provide all answers to all problems, managers at the highest level have to become more involved in the security strategy and its implementation. Creating this top-to-bottom awareness is the first step towards nurturing an organisational security culture.

According to Olzak (2006) the objective of awareness programs is to focus the attention of employees on maintaining confidentiality, integrity, and availability of information assets. Organisational culture as with any culture provides a platform to introduce a set of values, principles and expectations for all employees. It is essential that each employee recognise the importance of an organisational culture. The organisation needs to be centred on information security as a key component. Each employee must be given the opportunity to participate in the establishment of these values, principles and expectations. This will increase the likelihood of employees taking ownership of the initiative. Once employees have accepted the need for information security, implementing the support policies is greatly simplified.

2.5 Awareness culture and policy adoption

Martins and Eloff (2001, p. 1) indicate that, "the way in which people interact with information assets and how they behave in the working environment will in time become the way in which things are done in an organisation". They continue by explaining that the way people do things, becomes the organisational culture. Kruger and Kearny (2008) describe security awareness programs as a key defence against security incidents. They also indicate that awareness programs increase awareness of the importance of information security. Kruger and Kearny (2008) identified that awareness programs are normally focused on specific areas of concern and that they may include a variety of awareness materials such as posters, presentations and brochures.

Organisational culture provides an effective means of promoting the agenda of information security within software consultancies. Martins and Eloff indicate that organisational behaviour has an impact on the security culture within an organisation. They add that organisational behaviour focuses on three different levels, namely the individual, group and organisational levels (Martins & Eloff, 2001). Organisational security policy needs to be addressed across each of these levels. Martins and Eloff (2001) identified key aspects addressed across each of these levels. These aspects are illustrated below in Figure 5.

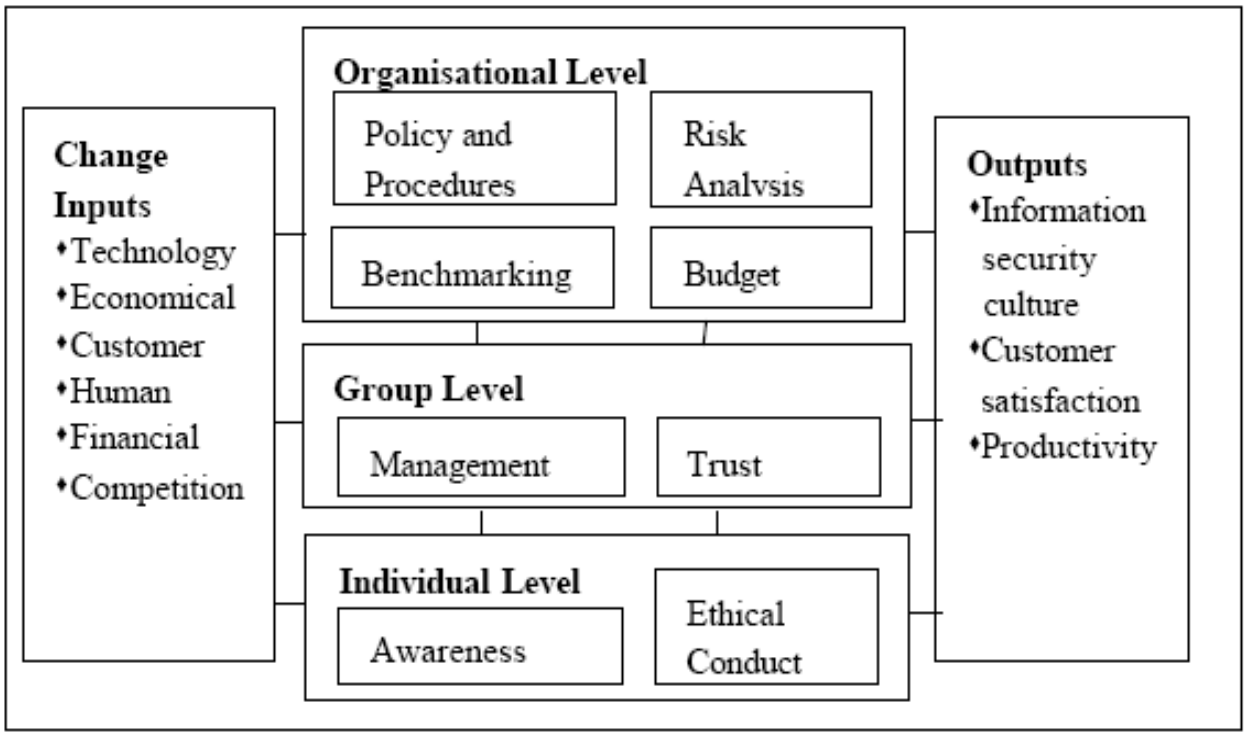


Figure 5 - Information security culture model (Martins & Eloff, 2001, p. 5)

The organisational level introduces all formal policies and procedures. These are the structures for providing the information security culture at a broader level. Martins and Eloff (2001) indicate that without these processes in place, employees might not know how to behave or what is expected of them, even though they may be willing to adhere to an information security policy. This implies that the formal policies and procedures actually should provide guidance as opposed to restrictions on employees. Finally, Martins and Eloff (2001) add that the responsibility of the organisational level is to provide awareness, education and training. They suggest that organisations benchmark themselves to other similar organisations and to international standards such as the ISO27002.

The group level relies on management and other influential employees to promote information security policy. Furnell and Thomson (2009) state that the culture of an organisation is not formed by what management preaches or publishes, but what it accepts in practice. Martins and Eloff (2001) insist that management should provide support and guidance in installing an environment of trust between the organisation and its employees.

This they suggest is achieved through the implementation of a vision and strategy required to protect information assets.

It is important to recognise that one of the outputs of an awareness culture is productivity gains. A healthy company culture will assist in promoting almost any productivity agenda that senior management requires. This is important when seeking to gain acceptance and trust from employees. A direct result of productivity gains could be an increase in customer satisfaction. Achieving this, while meeting information security obligations would be the best possible outcome of the organisation culture programs.

Trust becomes a very important issue in software consultancies, where often employees have elevated access to highly confidential trade information. Nurturing trust is one of the most important elements of information security culture at the group level.

Martins and Eloff (2001) describe the individual level as governed by the attitude of each individual. The processes and procedures defined at the organisational level, together with the guidance of managers and other influential individuals, shape this attitude. Individuals need to be enabled and equipped to form a culture of information security through awareness and training.

2.6 Software consultancies

This research project focuses on the software consultancy organisation for very specific reasons. Firstly, it is a highly information centred organisation. Information is a bedrock component of this organisation. Secondly, smartphones provide real benefits to software consultancy workers. Employees of such organisations can use smartphones extensively to perform their everyday work tasks. Finally, information security is more complicated in software consultancies, due to this reliance on information and technology, and compounded by a highly educated workforce.

The definition of a software consultancy varies widely. For the purposes of this research project, a software consultancy is limited to the following definition. A software consultancy is an organisation of people who collectively analyse business information requirements and problems to produce an information systems solution to address those requirements. It is important to note from this statement that the input into this organisation is information and the output from this organisation is an information processing system (or systems). Thus if we consider the process flow, illustrated in Figure 6 below, of a software consultancy business unit, we will note that business requirements are first translated into data, facts and other forms of information. Software consultancies would then analyse and process these to formulate an information systems solution designed to address and solve these requirements.

At all stages, information is both a key input and output parameter, and a key parameter to the success of the business. Producing the correct solution requires the most accurate and comprehensive information inputs. In software consultancies, it is evident that information is a key asset of this organisation. Dingsøyr (2002) points out that software engineering is a knowledge intensive task, frequently changing because of technological and market changes.

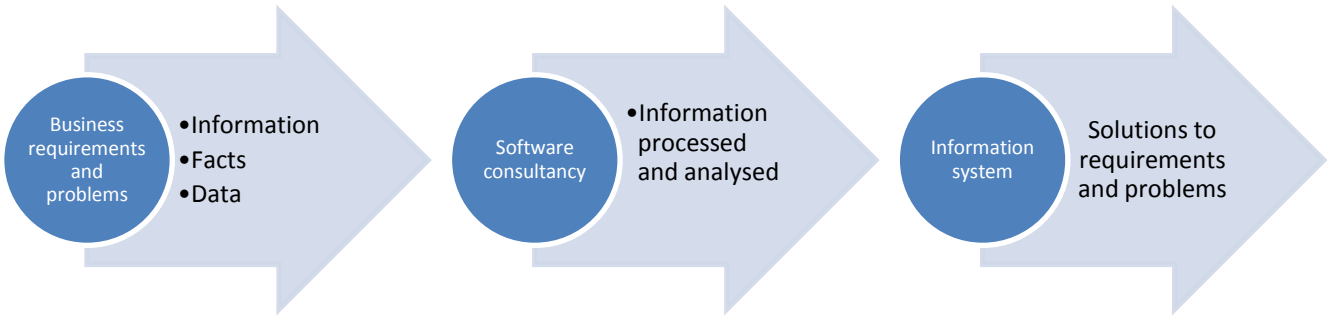


Figure 6 – Typical software consultancies' business process flow

Software consultancy organisations can be considered great knowledge factories. Employees are usually well educated and highly skilled. Processing the information requirements and problems of organisations that contract software consultancies requires a

highly skilled workforce. Often the clients of a software consultancy have complex requirements and problems that only specialised information processing can solve. Simple problems could be resolved using traditional 'off-the-shelf' software. This requires highly skilled employees.

One major factor that separates this type of organisation from its competitors is the employees that drive it. People, and the knowledge contained within these people, are the tools of the trade in software consultancy organisations. Hardware and software provide little competitive advantage in this industry. Instead, information and knowledge become the key competitive assets of this type of organisation.

Software consultancies rely on information systems to provide employees with the tools to access, store and process the information that they require. Information workers often require information as a tool to perform their work tasks. Information therefore becomes a critical component of their work. This requires information to be readily available when and where information workers require that information. Smartphones provide an excellent medium for accessing, storing and processing information, out of restrictions of time and location.

Storing, retrieving and transporting information assets, introduces various issues that are unique to this type of asset. In order to meet the objectives of this type of organisation, employees need to collaborate and share information freely. Decisions must be able to be made quickly. These decisions require accurate facts and information in order to produce the best results. The employees of software consultancies work collectively in processing this information. At the centre of this industry is a collection of people, who collectively are worth far more than the sum of their parts. This collection of people and the knowledge they possess are all part of the modern information workforce.

2.7 The information workforce

People are the ultimate source and destination of the information found within organisations. Information cannot act on itself. Employees act on information. Therefore, it is important for companies to recognise that the modern workforce is fuelled by information.

The security of information cannot be allowed to hamper the flow of information between employees. Post and Kagan (2007) point out that there must remain a balance between protecting information, and enabling authorised access. They continue to explain that tightening security by making systems more inaccessible can hinder employees while making them less productive. Thus striking this balance becomes vital to the success of the information security solution.

Another important factor to consider is that every year more and more millennium generation (generation Y) workers enter the workforce. These workers are comfortable using technology to address their information needs. Mahoney (2009) explains that this generation (generation Y), tends to be ambitious and idealistic, embracing new ideas and technologies. She adds that they are confident, flexible and collaborative. The adoption of new technologies is rapidly increasing with the proliferation of workers who view technology as a way to make business processes more effective, flexible and mobile, while increasing collaboration (Mahoney, 2009). It is vitally important that organisations factor this generation into future information policy considerations. This generation not only relies on information access, they expect it.

The ease at which modern employees are able to access information serves not only as excellent productivity tool, but also as a source of risk. Restricting access to information requires careful consideration. Employees must understand and accept the policies in place to protect organisational information. This is especially important as without education,

users may consider security measures cumbersome and annoying. Achieving employee acceptance greatly reduces resistance to information security provisions.

2.8 Information security acceptance

Information security acceptance will be achieved if employees understand the need for such. Hughes and Stanton (2006) explain that companies need to win the hearts and minds of their employees before policy will be adopted. They add that this will require more than simply lecturing people. Users need to completely understand the importance of what is being put in place, as well as the reasoning behind it (Hughes & Stanton, 2006). Furnell and Thomson (2009) found that people are often perceived as an obstacle rather than an asset to information security efforts.

Employees will naturally look for the easiest way to perform any task in front of them. Unfortunately, the easiest way to perform a task is usually very different to the most security conscious approach to performing the same task. Forcing employees to do a task a certain way for the sake of security, is often initially met with resistance.

Long established organisations, with legacy security policies, also need to accept the changing requirements of information security. Legacy security policies are long-standing, and generally accepted, security standards drafted at inception of an organisations' security policy, but not periodically updated. Existing policies might need to be completely re-engineered to address ever-changing security requirements. Long established security policies are being rendered inadequate by the changing landscape of information security threats. This has necessitated a response from senior levels of organisation across all business components.

It therefore becomes crucial for employees to both understand, and accept, the reasons for doing things in ways that embrace security. Employees will only accept information security

if they are aware of it, and they will only embrace it if it becomes embedded in the culture of the organisation (Hughes & Stanton, 2006).

2.9 Conclusion

The achievement of information security remains the core underlying focus of this study. This chapter provided us with an understanding of the context of information within the organisation. Information plays varying roles across all organisations. However, its security requirements remain the same across all organisations. The importance of this underlying concept remains at the centre of all arguments in this research project.

Information security is a complex topic to understand due to the natural intangibility of information. This can often be the cause of neglect towards such an important requirement of an overall security solution. It becomes vitally important that companies are able to provide comprehensive protection to IT investments, and the information that is transported, stored and processed in these systems. While information security is very often only achieved through the security of these IT systems, this is not the only area that requires security attention. As detailed in this chapter, it is important to understand that information security requires much more than simply securing the physical IT components. People must become a part of this security solution. Without their involvement, there would remain a critical weakness in the information security chain.

Information security awareness must form part of the organisational culture. Awareness programs and other means need to be applied in order to constantly re-enforce this message. The installation of an information security culture through awareness will encourage employees to recognise the true value of information as an asset.

In this chapter, it was established that information must receive the same level of asset classification as physical assets. Employees should ensure that they demonstrate similar levels of caution when dealing with information. The importance of information security

was highlighted in this chapter. Information security was identified as a means to protect information from numerous threats. These threats were identified as existing both within and outside of the organisation. It was established that information security should not only ensure protection of information from intentional threats, but also from unintentional threats.

In order to establish levels of acceptance towards security requirements, this chapter introduced the concept of the establishment of a security culture. This was identified as a culture in which security becomes an intrinsic consideration to all decisions.

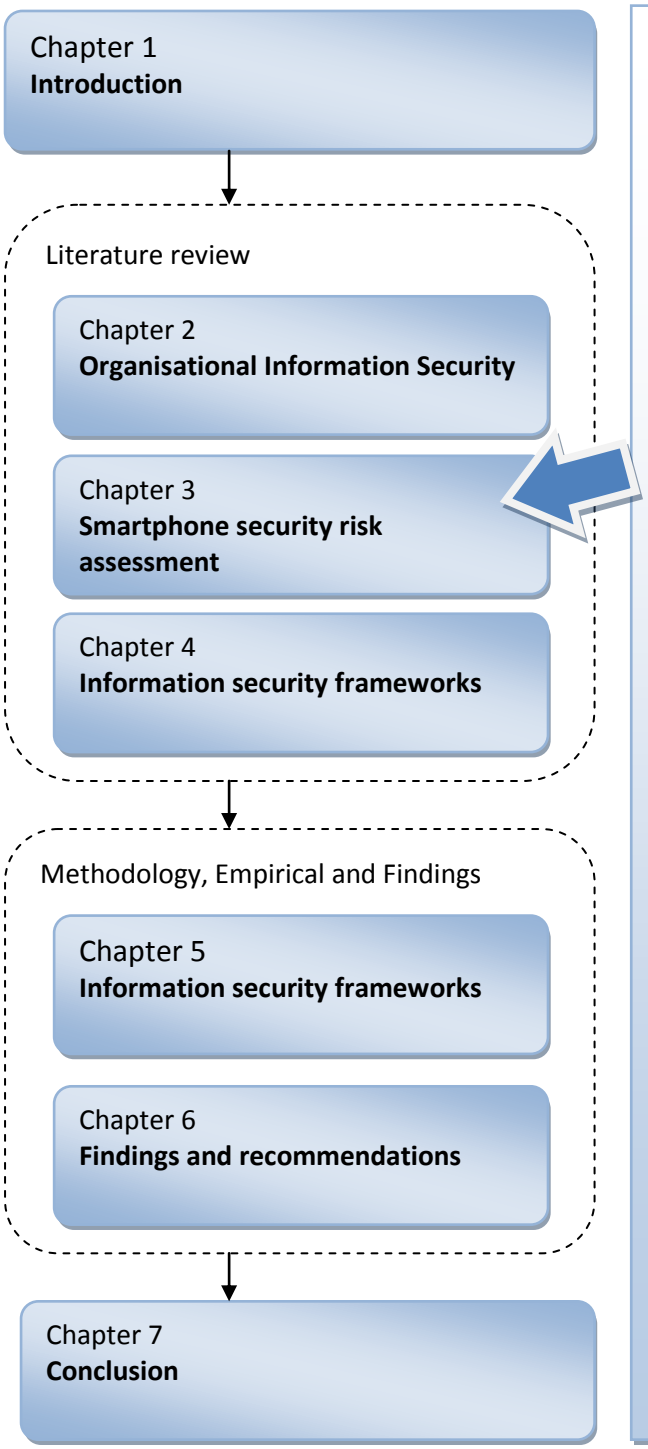
This chapter also highlighted the pressure that management and employees put on security components as they attempt to maximise efficiency and minimise workload respectively. Security was identified as often decreasing efficiency by increasing workload. Without awareness programs to explain the role and importance of security, the findings were that employees and managers would tend to place pressure on the boundary of functional acceptance. Beyond this boundary, it was established that undesirable results might occur.

In section 2.6, the role of information and its security within software consultancies was provided. Information was established as being a provider of business opportunity, but only if proper information security is provided. This chapter also highlighted the defining characteristics of the modern information workforce in section 2.7. As this chapter indicated, this is the majority of software consultancy employees.

The following chapter identifies the smartphone as one of the newest components of risk introduced into the IT department's portfolio. Smartphones introduce completely new threats to organisational information security. Chapter 3 will consider the risks and threats introduced through smartphone devices.

3 Smartphone security risk assessment

Chapter 3



3.1 Introduction

Smartphones have introduced an entirely new dimension of risk to organisational information security. In the past, security only needed to focus on devices that were physically tethered to the network of the organisation, or within its physical perimeter. Today smartphones introduce the need for wireless security, which according to Stanley (2004), are inherently less secure than their wired counterparts are. It is important to understand smartphone risks, and how smartphone security risks, differ from traditional security risks. Hunter (2008) states that, "IT departments already have processes to manage desktops and have usually extended these to laptops. Now it is equally vital that PDAs, smart phones, and other devices, are managed in the same way".

Chapter 2 introduced the concept of information as an asset of the organisation. Smartphones, themselves a company asset, are responsible for communicating, storing and processing organisational information. It is important to understand that smartphones are not simply physical assets of the organisation, but also repositories of information assets. The vulnerability of this information is defined by the vulnerability of smartphone devices.

In this chapter, smartphone security risks will be assessed in order to establish what risks organisations, and more specifically software consultancies, must begin to prepare for. Section 3.2 introduces the smartphone device. This section helps to establish a better description of what constitutes as a smartphone in the context of this research project. In section 3.3, the most prevalent or likely risks of smartphone devices are established. While not an exhaustive list, these provide the most likely risks to be encountered by regular organisational operation. Section 3.4 then places these risks into the context of a software consultancy organisation.

Before the risks associated with smartphones can be understood, it is important to provide an acceptable definition of a smartphone for the purposes of this research project. Once a

definition has been provided, the unique security challenges of the smartphone can be analysed within the context of the provided definition.

3.2 Introducing the smartphone

Gartner (2009) research group define the smartphone as a "large-screen, voice-centric handheld device designed to offer complete phone functions while simultaneously functioning as a personal digital assistant (PDA)". Palm provides the following definition, "a portable device that combines a wireless phone, e-mail and Internet access and an organiser into a single, integrated piece of hardware" (Elgan, 2007). These definitions provide a reasonable description of the operational facilities provided by these devices.

Figure 7 - The HTC HD2, Blackberry Storm and Nokia E72

The HTC HD2, Blackberry Storm and Nokia E72, pictured above, are examples of smartphone devices available from standard cellular retail stores. These devices all contain a large screen and keyboard for data input, display and processing. All of these devices are equipped with multiple wireless communication technologies.

Defining a device as a smartphone or regular mobile phone is often difficult. This research project does not wish to provide a definitive definition for what exactly constitutes as a smartphone. Any device displaying all of the characteristics identified in Table 2 below can be considered to be within the scope of the definition of a smartphone device for this study.

Table 2 - Smartphone characteristics (adapted from Gartner and Palm)

Characteristic	Considered a smartphone if...
Size	The device is compact; battery operated, easily transported and can be operated by hand (finger) or stylus.
Operating System	The device runs on an operating system that allows external (3rd party) applications to be installed and run on the device.
Connectivity	The device provides multiple methods (wired and wireless) of connecting to both the internet and other devices and networks.
Input	The device contains either a hardware or software based 'QWERTY' style keyboard, designed for extended data input.
Storage capacity	The device has a large and expandable storage facility.
Office functionality	The device provides the ability to perform basic office tasks such as email, take notes and word processing.
Calendar	The device includes a digital organiser and calendar.
Synchronisation	The device supports synchronisation of information with fixed desktop or laptop devices, or online web services.
Regular Phone Features	The device performs voice, text and multimedia message functions.

Some standard mobile phones provide one or more of the characteristics above, but only smartphones are capable of all. Therefore, any device that satisfies all of the criteria of each characteristic in Table 2 above can be considered a smartphone under this definition.

Devices that display these characteristics are likely to be used by information workers, to store, transport and process information. A device centred on other characteristics such as multimedia or photography is less likely to be used as business tools in organisations.

Regular mobile phones are not capable of storing and processing the same volumes of organisational information, thus rendering them as a lower risk to the organisation.

As devices become easier to operate, their uptake and acceptance will increase rapidly. Some estimates have predicted a 30% year-on-year growth in the sale of smartphones between 2007 and 2012 (Reardon, 2007). This, coupled with rapidly decreasing unit prices, has placed smartphones within reach of all employees.

3.3 Smartphone information security weaknesses

With ample storage capacity built into smartphone devices, and massive expansion capabilities available, employees are able to store large quantities of corporate information on these devices. This information forms part of the collective of information assets belonging to the organisation. While stored on smartphone devices, the information is often worth more than the unit cost of the smartphone itself. Therefore, the security of this information can be determined by assessing the risks of the smartphone device. Botha, Furnell and Clarke (2009) provide a list of smartphone security risk categories. These are discussed in this section.

3.3.1 Expandable storage

Botha, Furnell and Clarke (2009) point out that early generations of cell phones and PDA's had relatively little storage capability. Johnson (2009) indicates that today's generation of devices can be quickly and easily upgraded by adding additional storage cards.

Figure 8 - Storage expansion cards (Johnson, 2009)

However, very often these cards are not encrypted, and do not require separate authentication in order to access the information that they contain. This introduces an element of risk, should the device, stick or card fall into the wrong hands. Botha, Furnell and Clarke (2009) state that a malicious user would be able to insert unencrypted expansion media from a one device into another device in order to easily access that information.

3.3.2 Physical threats

Because of their mobile characteristics, smartphone devices are also more likely to be exposed to destructive elements such as sand, water or fire than fixed machines. Botha, Furnell and Clarke (2009) found that smartphones are more vulnerable to physical threats such as theft and accidental loss, than larger systems in fixed locations. Unfortunately, for organisations this has resulted in new components to their information security risk portfolio.

3.3.3 Configuration and users

One of the key challenges of smartphone security is that these devices can perform both personal and work related tasks. Quite often, the device belongs to the employee personally. Even where the device is company issued, employees will tend to personalise their device to their preferences. According to Botha, Furnell and Clarke (2009), this is has become a significant point of neglect by organisations, who have failed to acknowledge that users are often responsible for configuration of their smartphones, while administrators secure their desktops. They point out that end users may not possess the technical expertise to ensure that their devices be configured securely. Furnell, Josoh and Katsabas (2006) point out, that although some users will actively seek to overcome secure configurations, the most likely scenario is that security configurations will be unused or configured incorrectly.

3.3.4 Authentication

Botha, Furnell and Clarke (2009) also found that smartphone users are of the opinion that periodic re-authentication is intolerable on smartphone devices, but widely accepted on desktop machines. This they concluded was due to the way that smartphones are used versus desktop machines. Jürjens, Schrek and Bartmann (2008) explain that users tend to have a short and nomadic usage pattern with smartphones, leading to reduced acceptance of full-blown security checks for relatively low and spontaneous uses. Clark and Furnell (2007) add that existing PIN-based techniques are under-utilised, and provide an inadequte level of protection when compared to the sensitivity of data and services accessible through the devices.

Smartphone devices are usually used to perform a limited set of tasks in an equally limited period. In contrast, major undertakings are performed on the desktop machine over extended periods. Therefore, users would tend to configure their smartphone device to deliberately avoid periodic re-authentication for the sake of convenience.

3.3.5 Communication

Another unique challenge introduced with the smartphone, is that these devices are no longer limited to communicating over only the public cellular network. As previously pointed out, smartphones possess a number of available connectivity methods. Jürjens, Schrek and Bartmann (2008) explain that the difference in thoughput, latency, cost and availability justify having these alternatives. However, as Botha, Furnell and Clarke (2009) point out, smartphone users are required to configure network connection security settings for each network that they connect to.

The majority of users do not know appropriate security settings, and will connect to the least secure network, that requires minimal configuration. Jürjens, Schrek and Bartmann (2008) reiterate this by stating that this (multitude of device configurations) leads to various combinations depending on the set of requirements essential for the given usage scenario.

3.3.6 Applications

Mobile applications are rapidly becoming available for smartphone devices. These applications are targeted at providing access to the same information that users access on their desktop machines. While the level of sensitivity of the data remains the same, the security level of smartphone applications is usually much lower than the desktop version of the same application. Botha, Furnell and Clarke (2009) point out that the smartphone version of internet explorer, IE Mobile, has only three security options, compared to 45 on the desktop version. They also found, that the mobile version of Microsoft Word does not support some of the key security components of the desktop version. Jürjens, Schrek and Bartmann (2008) point out that the provision of patches, updates (such as virus signatures), is difficult on mobile platforms such as smartphones.

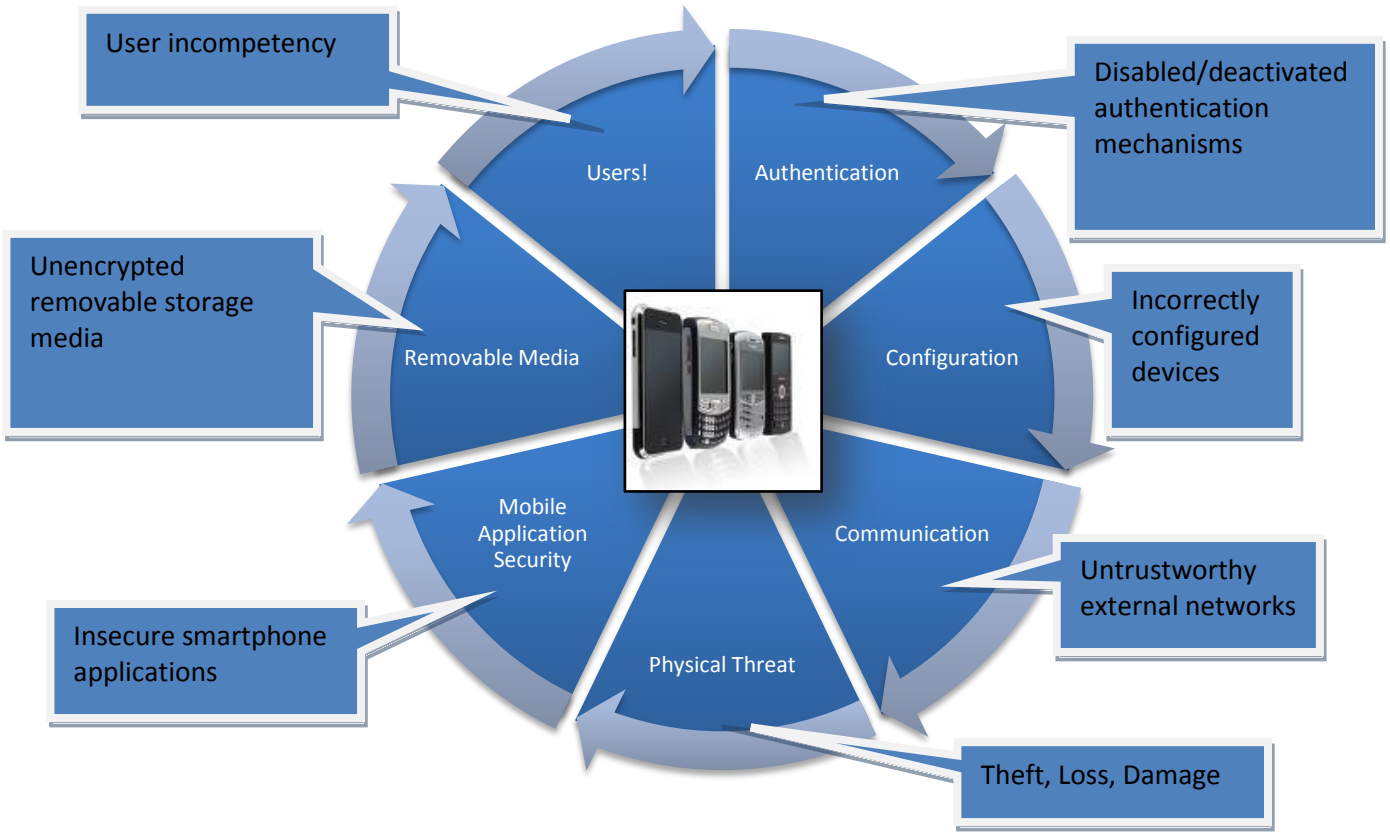


Figure 9 - Smartphone information security risks summary (Botha, Furnell, & Clarke, 2009)

Illustrated above are the key risk areas identified by Botha, Furnell, and Clarke. These risks need to be targeted in order to increase the security level of the information stored,

processed and transferred by these devices. Furnell (2005) states that antivirus protection is likely to become as important on mobile devices as it has become on desktop systems.

3.4 Smartphone risks in a software consultancy environment

Software consultancy organisations are perfectly positioned to take advantage of the benefits introduced by smartphone devices. They operate by identifying and implementing software based solutions, to business problems and requirements. As discussed in Chapter 2, software consultancies employ large numbers of information workers. The smartphone provides the perfect solution for management, and communication, of the information that drives these individuals.

There are numerous business cases for the smartphone device. A study conducted in 2005 by Cellcom found revenue generation of around $28 billion annually, as a result of the ability to receive data from anywhere with mobile broadband services (Pahl, 2009). However, as noted by Doherty & Fulford (2006) the risks to information on mobile computing platforms, such as smartphones, is exacerbated as staff are away from the normal in-house controls and monitoring regimes.

3.4.1 Smartphone information responsibilities in software consultancies

Software consultancy employees of all levels deal with vast amounts of information on a daily basis. This information is usually part of a collective effort towards achieving a work task. The work tasks processed by software consultancy organisations produce information deliverables. The information deliverables usually feed into other work tasks, effectively creating a chain of information flowing from customer requirements through to solutions development. Information becomes both an input and output of each process in this type of organisation.

Smartphones are capable of driving the flow of information between work tasks. Certain work processes might benefit from smartphone information communication and processing. With instant access from any location, these devices are capable of eradicating certain work

tasks completely, by routing information more responsively. Of course, with this comes an increase in the vulnerability of information.

Compromise to any of the three pillars of information security, (confidentiality, integrity or availability) would result in delays and threats to the entire process. At the same time, minimising the time it takes to make decisions based on information is key to optimising this process chain. Figure 10 below, displays the typical flow of information deliverables between work tasks. Conventional product driven manufacturing processes are often limited by physical constraints. In software consultancies, information is only limited by ability of the consultants to identify, store and communicate it.

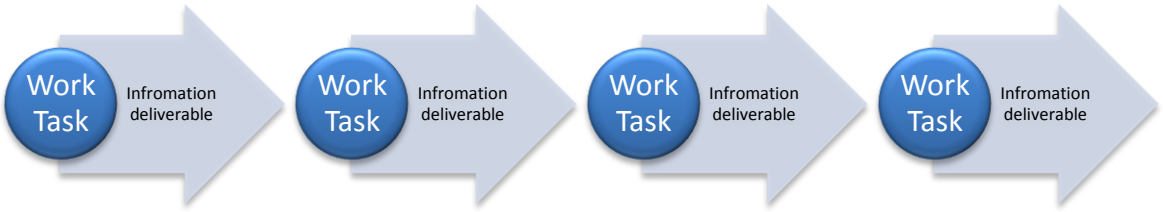


Figure 10 - Software consultancy process flow

Optimising the flow of information is achievable using many different techniques and technologies. One of which is the smartphone. Senior management should see it in their best interest, to ensure that the storage and transmission of information is as rapid and efficient as possible. Smartphone implementation can satisfy management's requirements, of an efficient medium of information storage and transmission, but only if done so in a secure manner.

Due to the nature of business in software consultancies, the information that is processed is highly confidential. This results from the business and trade secrets that are identified for inclusion in the information systems, and information deliverables, that are the outputs from software consultancies.

3.4.2 The perception created by smartphone security

Considering Rasmussen's (1997) model in Figure 4, smartphone implementation into software consultancy organisations, can be considered a movement away from the boundary of economic failure. This is due to increases in efficiency, which results in reducing operating costs, and increasing profit. As established in this model, employees will tend to migrate away from the boundary of unacceptable workload (Rasmussen, 1997). This means that employees will gradually reject components of smartphone devices, or their implementation, which can be perceived as adding unnecessary workload to their work tasks. This is often the perception created by smartphone security requirements.

As indicated previously, smartphone security is tolerated less than desktop security. This increases pressure on the gradient towards least effort, as employees attempt to reduce effort by neglecting security requirements. With both strong pressure from management towards increasing efficiency, and from employees towards least effort, pressure on the boundary of functional acceptance becomes intensified. Rasmussen (1997) indicates that if this pressure is allowed to breach through the boundary of functional acceptance, undesirable results may occur. Without security awareness to ensure that smartphone security risks are mitigated, software consultancy organisations would experience increased risk to their information assets.

Employees with technical expertise are capable of configuring devices to minimise the interruption of security components. Management similarly drive employees to ensure that they are as efficient as possible. This increases pressure towards the boundary of functional acceptance. Awareness programs, policies and other mitigating mechanisms would ensure that there is a balance maintained between each of the three boundaries.

3.5 Smartphone risk management and mitigation contrasts

Some of the key differences between smartphone security and security of other devices were outlined earlier in this chapter. These are summarised in Table 3.

Table 3 - Smartphone versus traditional security risks

Risk area	Traditional risk	Smartphone risk
Users	Users are more aware of security requirements of desktop and laptop devices.	Users do not understand security requirements of these devices. Users are less tolerant of security
Authentication	Authentication performed by a centralised network, configured and controlled, by the organisation. Authentication is usually performed once at the beginning of the working session.	Authentication must be performed by the device even when disconnected from the network. Authentication requested multiple times during the course of the working day.
Configuration	Typical security configuration is performed by network administrators. Machines are restricted by network security policies.	Devices are configured by employees according to personal preference. Far less security configuration options are available on mobile operating systems.
Communication	Traditional communications are performed across trusted wired or wireless networks. These networks are configured by internal system administrators.	Smartphone devices must be able to communicate regardless of position. This requires them to communicate through untrustworthy third party networks.
Physical Threat	Traditional computer equipment is less vulnerable to physical threats as it is secured by the perimeter defences of the organisation. Access controls can be easily installed to reduce the physical threat to equipment.	Smartphone devices are far more vulnerable to physical threats. Due to their mobility requirements and smaller physical form, these devices are much more difficult to protect from these threats. Devices are also much easier to misplace.
Application Security	Traditional applications execute on mature operating systems with more established security components. Applications are patched more frequently. Desktop machines are commonly equipped with anti-virus software and client firewalls.	Mobile applications are developed for operating systems that contain a subset of security components found in desktop operating systems. Most smartphone users neglect to install smartphone anti-virus software.
Removable media	Desktop machines are less likely to contain removable media. This reduces the chance of information being removed from the machine. Network administrators are easily able to restrict removable media from being connected to desktop and laptop devices if required.	It is highly likely to find removable media attached to these devices. This removable media usually does not share similar security restrictions with the device itself. Media can often be removed and accessed from other devices.

Managing organisational smartphones becomes complicated, as personal devices make their way into the corporate environment. In addition, smartphone devices found in companies might be from multiple different hardware manufacturers, with various operating systems and models.

As soon as smartphone devices become a security risk, management will take steps to restrict their usage. This would result in a loss of the advantages possible through proper smartphone integration. Khokhar (2006) and Davis (2006) point out increased productivity, greater job satisfaction and increased flexibility as a result of mobile usage. This is especially relevant to information industries such as software consultancies. Employees can increase productivity, by using smartphone devices to accelerate the capture and transmission of information. To avoid restrictions, proper procedure and control must be implemented. Smartphone users must be aware of these procedures and controls.

Management must obtain the support of smartphone users, as they are ultimately responsible for the proper configuration of their personal devices. Employees should be made aware of their security requirements and policy expectations. This will not only ensure better security of their devices and personal information, but that of the organisations information.

Where companies issue devices, employees must be understand the security capabilities and requirements of these devices. Employees must understand the risks to both the device and its information. Once employees are better equipped to manage their own device security, management will be able to manage the security of the information without restricting, or banning, smartphone usage.

3.6 Conclusion

In Chapter 3, the smartphone was comprehensively addressed. The security and risk profiles of smartphone devices were examined. Smartphones were also identified as a

means of providing a strategic enabling function to the flow of information within software consultancy organisations.

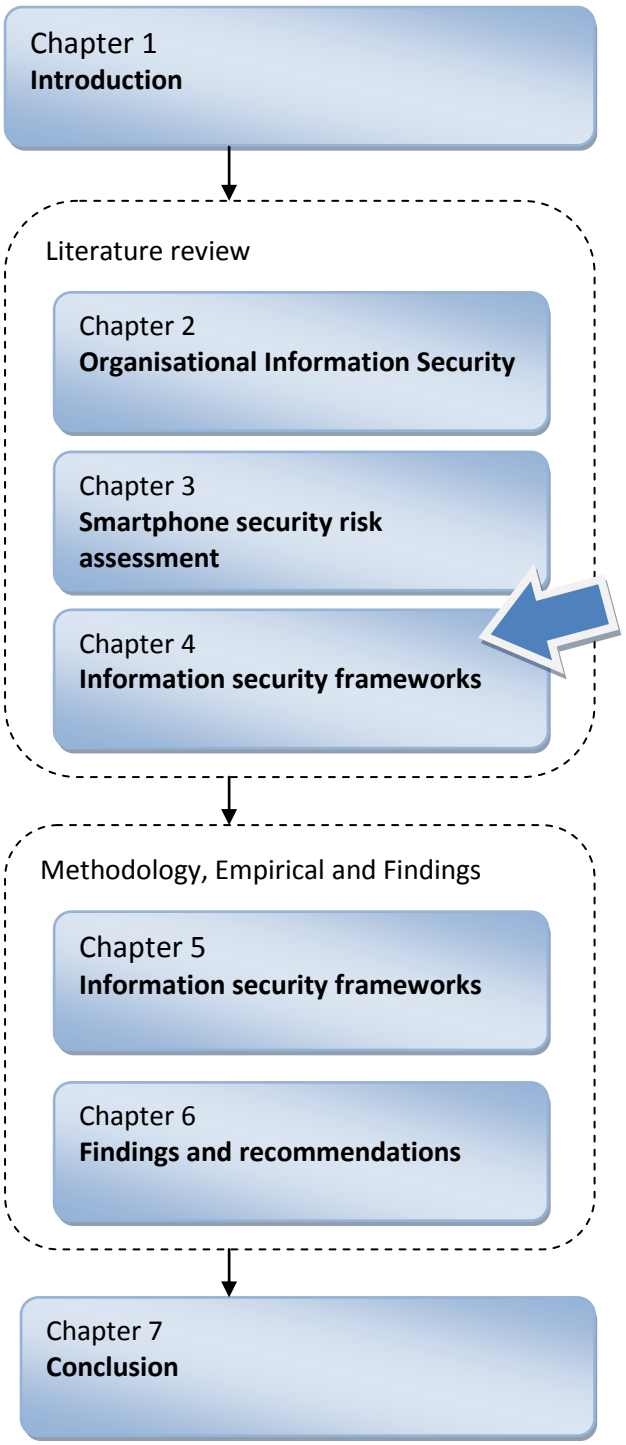
Section 3.2 provided the definition of a smartphone device for the purposes of this research project. This included a description of the characteristics typically found in smartphone devices. In the section 3.3, the security weaknesses inherit to smartphone devices were listed. This provides an answer to the first sub-question of this research project.

Section 3.4 placed these risks into the context of the software consultancy organisations, highlighting the concerns, which might be faced through the proliferation of smartphone devices into these organisations. Finally, some of the key differences between smartphone risks and traditional desktop risks were pointed out in section 3.5.

A set of controls needs to be established and installed, in order to mitigate against the risks introduced with smartphone implementation. Developing a basis from which these policies and controls can be composed, would prove overwhelming for an individual organisation. Software consultancy organisations should instead consider existing security frameworks, as a basis from which they can establish a smartphone security solution. Two such frameworks, discussed in the following chapter, are the COBIT 4.1 framework and the ISO27002.

4 Information security frameworks

Chapter 4



4.1 Introduction

Karyda, Kiountouzis, and Kokolakis (2005) state that the implementation of an IS security policy should be translated into guidelines, procedures and to-do lists that must be put into practice by information system users. The content of these policies according to them is dependent on the context of the organisation. Karyda, Kiountouzis, and Kokolakis (2005) reason that there is no single security solution or policy that can fit all organisations. This is in line with the interpretive paradigm used within this research project.

As highlighted in previous chapters, user adoption of policy is paramount in ensuring that it is successful. Organisations attempting to implement an authoritarian approach to security, risk losing support from end users. Karyda, Kiountouzis, and Kokolakis point out, that this might result in users circumventing security measures, in order to perform as efficiently as possible.

Considering Rasmussen's model from Figure 4, security policies supported by awareness programs will resist employee circumvention. For employees, the functional acceptance boundary does not include distracting security requirements. This is because security requirements are perceived by employees, to add additional steps to work tasks. It becomes important that user circumvention of these security requirements be avoided, through proper security awareness.

Accordingly, management should ensure that they do not simply seek the most efficient definition of working requirements. This would include the least amount of security possible, in order to maximise efficiency. Both employees and managers should subscribe to a common set of security requirements and policies. These policies are required in order to maintain a balance between employee, management and security requirements. This balance requires security experimentation to discover an optimum level of security and efficiency. This should be achievable through proper adaption of existing best practice approaches, to the context of smartphone security in software consultancy organisations.

In order to achieve this, best practice approaches must be indentified from existing security frameworks. Two such frameworks are the COBIT 4.1 framework and ISO27002. These security frameworks are both widely accepted and utilised in the information technology industry. Independent global groups manage them both, through continuous revision. They are also independent of organisational and industry constraints. Both were developed with best business practices at their core and by experts within the field of information security.

4.2 The COBIT 4.1 Framework

The most recent version of the COBIT 4.1 framework at the date this research project was compiled was version 4.1. All references to COBIT 4.1 in this research project refer to version 4.1 of that framework.

4.2.1 COBIT 4.1 Introduction

The COBIT 4.1 framework provides good practices across a domain, and process framework, and presents activities in a manageable and logical structure (IT Governance Institute, 2007a, p. 4). COBIT 4.1 is a representation, of the consensus of experts, in the domain of information governance (IT Governance Institute, 2007a).

This places the COBIT 4.1 framework in an excellent position to provide expert governance advice, for controlled implementation of new technologies such as smartphones. Implementing or preparing for any new technology introduces various unpredictable risks. It is impossible to predict all the risks that a new technology will introduce. Management must ensure that sufficient controls are in place to mitigate against as many risk possibilities as possible.

COBIT 4.1 provides a link between business requirements and information technology requirements, defining management control objectives to be considered. Employees need to be made aware of the possible areas of risk.

4.2.2 Content analysis

The COBIT 4.1 framework is illustrated by a process model that subdivides IT into 4 domains and 34 processes (IT Governance Institute, 2007a). Figure 11 below outlines the key principles of the COBIT 4.1 framework.

Managing IT investments through adequate process, delivers the enterprise information, which satisfies business requirements. COBIT 4.1 provides recommended control objectives, to assist in choreographing this effort. COBIT 4.1 also ensures that all stakeholder responsibilities are clear and adequate measurement devices available. Ongoing measurement is a key part of monitoring the control objectives.

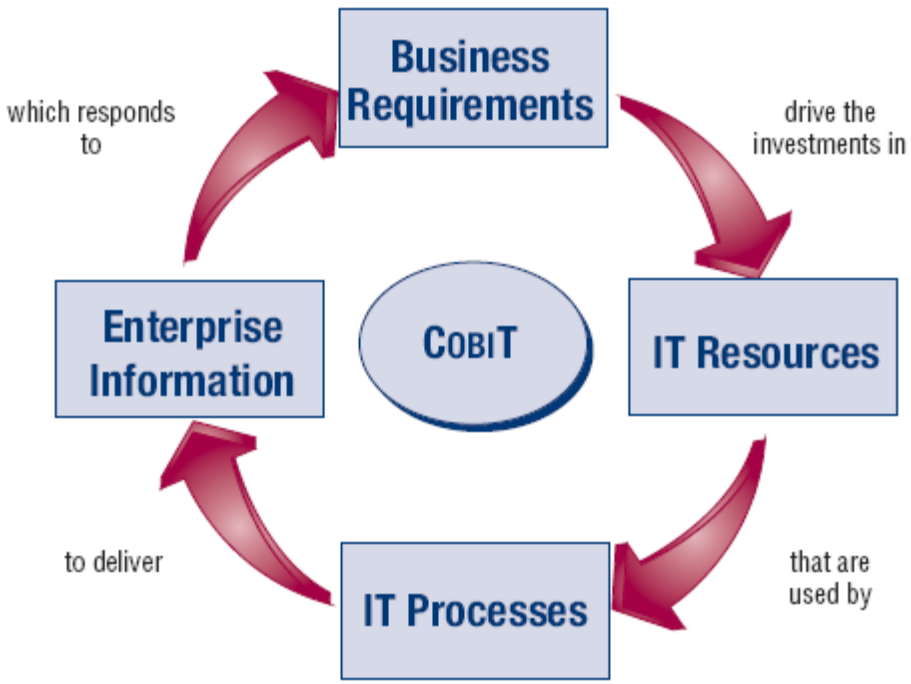


Figure 11- Basic principles of COBIT 4.1 (IT Governance Institute, 2007a)

From this cycle, the importance of these 34 processes in delivering enterprise information from IT resources is illustrated. These processes are organised into four separate domains. The four interrelated IT domains are illustrated in Figure 12.

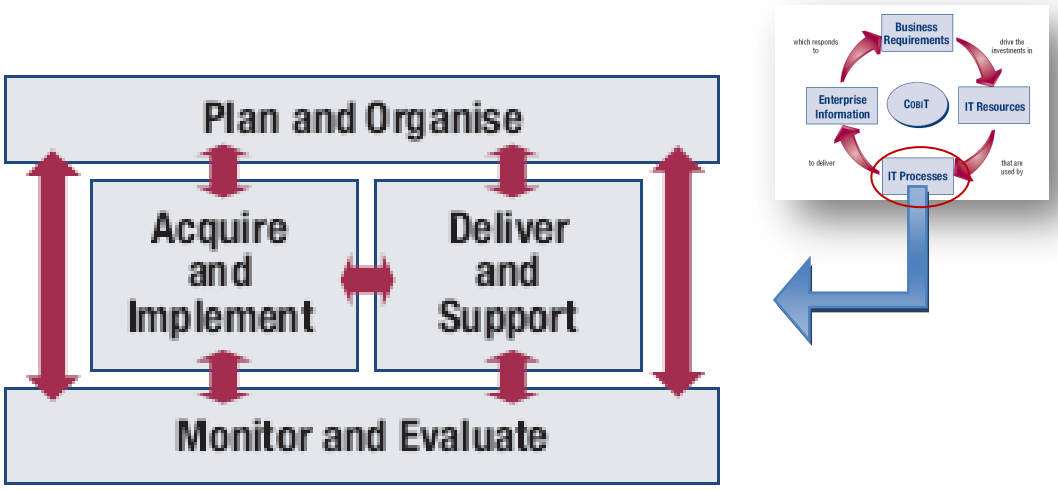


Figure 12 - The four interrelated domains of COBIT 4.1 (IT Governance Institute, 2007a)

The Plan and organise domain covers the strategic and tactical concerns, including the way in which IT can best contribute to the achievement of the business objectives (IT Governance Institute, 2007a). This domain addresses the strategic advantages of infrastructure investments. This domain further ensures optimum use of resources, and awareness of organisational IT objectives. Awareness covers the understanding and management of risks. Finally, this domain ensures that the quality of the IT systems, are appropriate for business needs.

The second domain, acquire and implement, addresses the solutions that need to be identified, developed or acquired, as well as implemented into the business process. Other items covered by this domain include changes to existing systems, new projects, new implementations and business continuity.

The deliver and support domain focuses on the actual delivery of required services. This includes the delivery, management of security and continuity, service support for users and management of data and operational facilities. For this domain, other items covered include, cost optimisation, service delivery, productivity and safety, and adequate information security (confidentiality, integrity and availability).

The final domain, monitor and evaluate, introduces the need for IT processes to be regularly assessed over time for their quality and compliance with control requirements. This domain

is concerned with issues such as performance management, monitoring and regulatory compliance. The task of this domain is to identify problems early, and ensure adequate information security. These domains work together to ensure that adequate controls are present across the entire organisation.

The COBIT 4.1 framework provides a complete set of high-level requirements to be considered by management, for effective control of each IT process (IT Governance Institute, 2007a). Due to the sheer number of different types of smartphones, operating systems and potential uses, management would not be able to provide a specific set of instructions. Instead, management must ensure that an adequate set of high-level controls are provided, in such a way that they generically cover as many possible security requirements as possible. Using the COBIT 4.1 framework, management can identify these high-level controls, and adapt the policies, procedures and practices mapped out in the framework, to the requirements of smartphone security. Finally, this can be adapted to the specific requirements found within software consultancy organisations.

The COBIT 4.1 framework introduces a measurement-driven approach in order to ensure that management can actively respond to process performance. The introduction of any new technology will need to be subjected to performance analysis, in order to ensure that there is a positive return on that investment. Maturity models of the COBIT 4.1 framework can assist in measuring the gap between where the organisation is, and where it needs to go.

The COBIT 4.1 framework covers five specific IT governance areas:

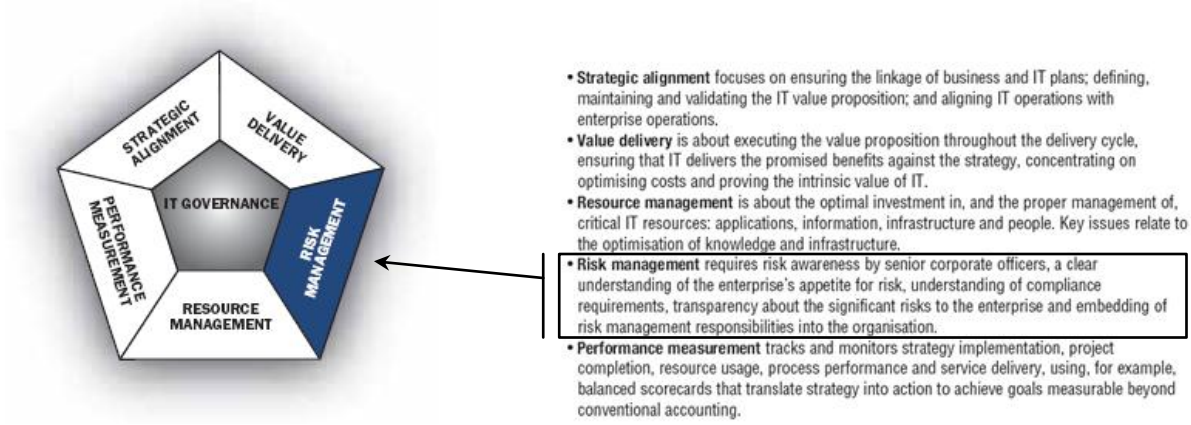


Figure 13 - IT Governance focus areas (IT Governance Institute, 2007a)

Of these five areas, this research project will only focus on COBIT 4.1 domain processes of which the area of "risk management" is the primary focus. This ensures that the solution focuses on providing a model that satisfies solely the requirements of measuring smartphone security readiness. Risk management is the most relevant governance area in relation to information security management. Risk management seeks to embed the responsibilities of security into the organisation. This is aligned to the main goal of this research project; measuring smartphone security risks.

The following table lists the COBIT 4.1 processes that target risk management:

Table 4 - Risk management focused COBIT 4.1 process items

COBIT 4.1 Process Code	Process description
PO4	Define the IT Processes, Organisation and Relationships
PO6	Communicate Management Aims and Direction
PO9	Assess and Manage IT Risks
DS2	Manage Third-party Services
DS4	Ensure Continuous Service
DS5	Ensure Systems Security
DS11	Manage Data
DS12	Manage the Physical Environment
ME2	Monitor and Evaluate Internal Control
ME3	Ensure Compliance With External Requirements
ME4	Provide IT Governance

The process items included in the table above provide strategies for the management of risk. These risk management controls will form a core part of a smartphone security readiness model. Three of the four domains are represented (plan and organise, deliver and support and monitor and evaluate), as these three each contain processes that target risk management as a primary objective. The acquire and implement domain does not have any processes which target risk management as a primary objective.

4.2.3 Risk management processes

The previous section outlined the 11 processes identified from the COBIT 4.1 framework, of which risk management is a primary objective. Further analysis of these processes, will assist in identifying how these are applicable to a possible smartphone security readiness model. From these processes, questions will be compiled, as part of the research instrument of this research project.

The COBIT 4.1 cube (Figure 14), summarises the organisation components addressed by each the COBIT 4.1 processes, and illustrates their relationship to each other. The cube presents three separate related, but disparate, organisational constructs.

The three faces are listed below:

- Business Requirements *(which drive investments in...)*
- IT Resources *(that are used by...)*
- IT Processes *(delivering information responding to the business requirements)*

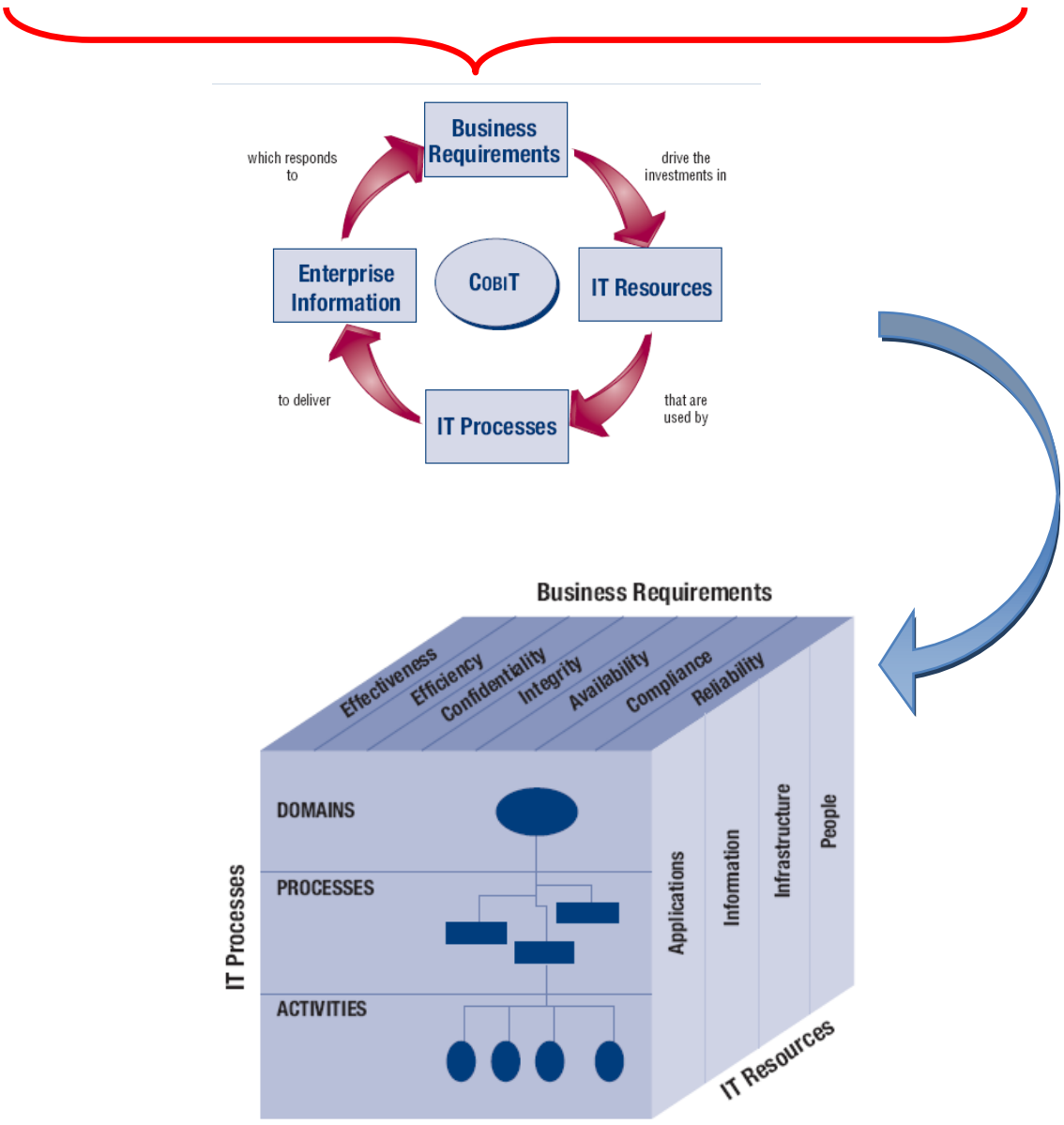


Figure 14 - The COBIT 4.1 cube (IT Governance Institute, 2007b)

On the front face of the cube, the IT processes are illustrated as belonging to a particular domain, and containing various activities. These processes are applied across the IT resources displayed on the face to the right hand side of the cube.

The IT resources provided by COBIT 4.1 are listed below:

- Applications
- Information
- Infrastructure
- People

Each of the processes provided to govern these resources, seeks to fulfil at least one of the business requirements. The business requirements are listed on the upper face at the top of the cube. The COBIT 4.1 framework identifies the primary business requirement satisfied by each process along with the key resources involved.

Using this, smartphone security risks can be placed into respective resource categories. Figure 15 categorises each of the smartphone security risks identified in Chapter 3. Each of these risks are then categorised under one primary resource area.

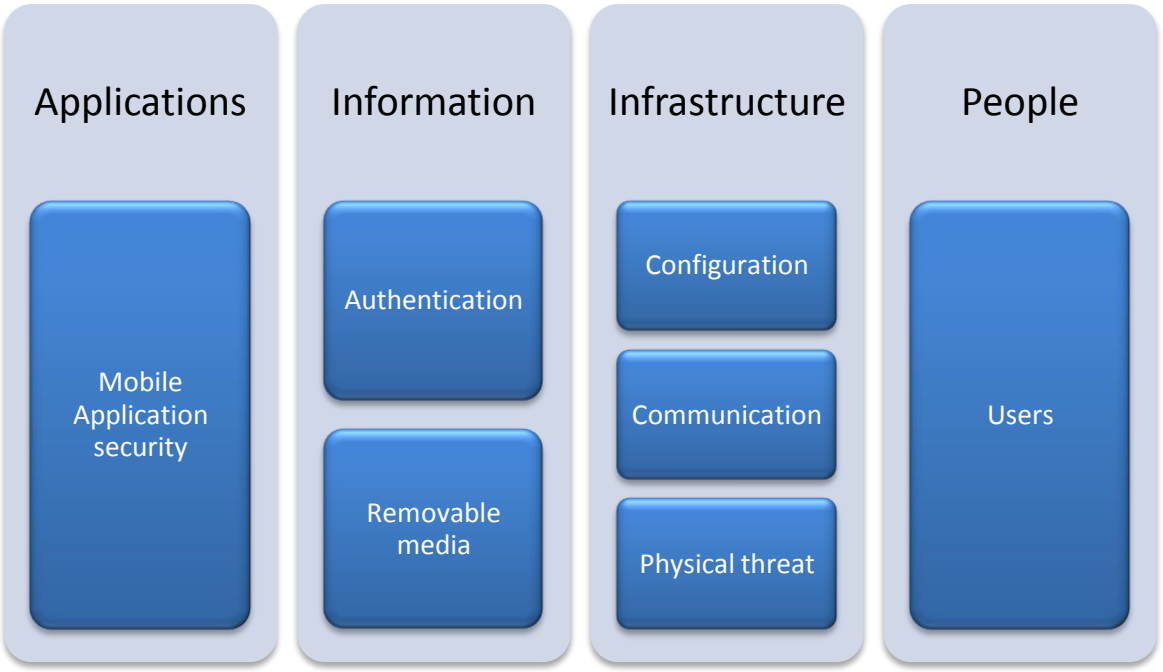


Figure 15 - Resource risk categories

The risk of mobile application security is categorised under the resource category of applications. Mobile application security was noted in Chapter 3 as being substandard, especially when compared with more mature desktop-based software. Within the resource category of information; authentication and the risk of removable media have been identified. The risk of authentication identified, is that information could be accessible by persons who are not or should not be allowed to access it.

Removable media in itself (its physical form) is a component of the infrastructure resource. However, the risk identified here relates to the information contained within the removable media. Removable media is therefore categorised under the category of information. The physical risk aspect of removable media is covered under the broader risk of physical threats.

The category of infrastructure includes configuration risk, communication risk and that of physical threats. Secure configuration of devices, requires security right through from the infrastructure level. Hardware and software configuration requires security management, and the support of existing infrastructure security measures. Communication between

device and organisational networks might not always be across trusted communication channels. It is important that the boundary infrastructure between these communications channels is secure.

Physical threats to smartphone devices are higher due to their small size and mobility characteristics. It might prove difficult to provide a level of infrastructure security on a device as small and as mobile as a smartphone. However, organisational infrastructure security should extend to secure smartphone devices, even when they are outside of organisational perimeter security controls. Finally, smartphone users appear under the people category.

Each smartphone risk is now associated as a risk belonging to a primary organisational resource. This will assist in mapping the relevant COBIT 4.1 process against each smartphone risk. Table 5 below lists the smartphone risk areas with their corresponding resource category, as defined in the COBIT 4.1 framework. These are mapped to the COBIT 4.1 process items, which target risk management as a primary concern as listed in

Table 4.

Table 5 - COBIT 4.1 smartphone risk process matrix (IT Governance Institute, 2007b)

Risk Area	Resource category	COBIT 4.1 Process										
		PO4	PO6	PO9	DS2	DS4	DS5	DS11	DS12	ME2	ME3	ME4
Application security	*Applications*			X	X	X	X			X	X	X
Authentication	*Information*		X	X	X	X	X	X		X	X	X
Removable media	*Information*		X	X	X	X	X	X		X	X	X
Configuration	*Infrastructure*			X	X	X	X		X	X	X	X
Communication	*Infrastructure*			X	X	X	X		X	X	X	X
Physical threat	*Infrastructure*			X	X	X	X		X	X	X	X
Users	*People*	X	X	X	X	X	X			X	X	X

Table 5 above, provides specific control objective mappings, for each of the identified smartphone risk areas from Figure 9. By combining the COBIT 4.1 process items and

resource categories, to each of these risk areas, appropriate risk mitigation controls can be identified and implemented. These can then be applied to each of the risk areas.

For each of the identified processes, COBIT 4.1 provides a list of implementation activities. These activities provide a list of actions to be implemented by various authority positions within the organisation. These activities are utilised in the empirical portion of this research project.

Goals and metrics are provided for each of the process items. These provide a mechanism for measuring whether the IT expectations from business are being met by IT. They indicate what process goals and metrics each process must deliver, so that it can support the objectives of IT. Finally, they indicate what must happen inside a process, in order to achieve the required performance, and how it can be measured (IT Governance Institute, 2007b).

4.2.4 COBIT 4.1 Conclusion

The strength of the COBIT 4.1 framework centres on the high-level strategic approach to risk management defined in the framework. It becomes easier to identify the core requirements for risk management of a new technology, when the COBIT 4.1 framework is adapted to the specific requirements of that technology. Using the COBIT 4.1 framework in conjunction with a supporting standard, such as the ISO27002, the high-level policy control objectives can be applied to best business practices.

4.3 The ISO27002 code of practice

The ISO27002 began as a code of practice for information security. The department of trade and industry in the United Kingdom developed it, first published in the early nineties. In 1995, it was re-published by the British Standards Institute (BSI) as the BS7799-1 (ISO 17799 News, 2006). In 1999, it underwent a major revision to significantly strengthen the standard. The standard set was fast-tracked through ISO within that year, and become known as the ISO 17799. Finally, in 2005, the standard was again republished as the

ISO27002 (ISO 17799 News, 2006). The reference version for this research project is the Standards South African version, which is identical in content to the original version.

4.3.1 ISO27002 Introduction

The purpose of the ISO27002 standard is to establish guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organisation (Standards South Africa, 2005). The guide provides guidance on the commonly accepted goals of information security. The control objectives outlined in the ISO27002 document seek to address the requirements identified in a risk assessment (Standards South Africa, 2005).

This document is also fully compatible with the control clauses contained within the COBIT 4.1 framework. Together they provide a formidable and complimentary approach to risk management.

4.3.2 Content analysis

The ISO27002 standard consists of 11 security clauses, which collectively contain 39 main security categories (IT Governance institute, 2006) .

The IT Governance institute provides a mapping document, which maps the components of the COBIT 4.1 framework, to that of the ISO27002 framework. Using this document, the components of the COBIT 4.1 framework selected as targeting risk management from

Table 4, can be mapped to the objectives of the ISO27002 standard.

Figure 16 - ISO27002 (IsecT Ltd., 2008)

Table 6, provides a list of the COBIT 4.1 framework processes, which target risk management, along with a list of ISO27002 objectives that map to these. The first column displays each of the COBIT 4.1 processes that target risk management as a primary objective. The right hand column lists each of the ISO27002 objectives that map to that process, according to the mapping document.

Table 6 – ISO27002 to COBIT 4.1 mapping items adapted from (IT Governance institute, 2006)

COBIT 4.1 Process Code	ISO27002 objectives mapped to COBIT 4.1 Process
PO4	6.1, 6.2, 7.1, 8.1, 9.1, 10.1, 10.6, 15.1 and 15.2
PO6	5.1, 6.1, 6.2, 7.1, 8.1, 8.2, 8.3, 9.1, 9.2, 10.7, 10.8, 10.9, 11.1, 11.3, 11.7, 12.3, 13.2, 15.1 and 15.2
PO9	5.1, 13.1 and 14.1
DS2	6.2, 8.1, 10.2, 10.8, 12.4, 12.5 and 15.1
DS4	6.1, 10.5 and 14.1
DS5	5.1, 6.1, 6.2, 8.1, 8.2, 8.3, 9.1, 9.2, 10.1, 10.4, 10.6, 10.7, 10.8, 10.9, 10.10, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 12.2, 12.3, 12.4, 12.6, 13.1, 13.2, 15.1, 15.2 and 15.3
DS11	9.2, 10.5, 10.7, 10.8, 12.4 and 15.1
DS12	6.2, 9.1 and 9.2
ME2	5.1, 6.1, 6.2, 10.2, 10.10, 15.2 and 15.3
ME3	6.1, 15.1 and 15.2
ME4	5.1, 6.1 and 10.10

These objectives must be satisfied, in order to satisfy the requirements of each of the COBIT 4.1 processes that primarily target risk management. This is based on the relationships defined by the mapping document. The following sections cover each of these objectives, and identify any relationships to smartphone security.

Objective 5.1) Information security policy

In section 2.5 of this research project, the need for the acceptance of security policy by employees is highlighted. The ISO27002 highlights this by indicating the importance of establishing a clear policy direction in line with business objectives, and the demonstration of support for this policy. In order to achieve adequate information security when implementing and using smartphone devices, a clear policy must be available. A

commitment to this policy is required, and regular policy maintenance must take place. Information security policy applies across each of the smartphone security risk areas identified in section 3.3.

Objective 6.1) Internal organisation

The ISO27002 indicates that an internal security framework group must be established to act within the organisation towards the establishment and implementation of security controls. Some of the roles identified for this framework include the management of security policy, assignment of security roles, co-ordination and review of security across the organisation. Internal organisation, as with security policy, applies through all the security risk areas of smartphones.

Objective 6.2) External Parties

Smartphone communication often occurs over third party networks. The ISO27002 highlights the importance of ensuring that all external party interaction with organisational information is both controlled and secured. Security policies must exist that protect the information sent, processed and stored by external networks and parties.

Objective 7.1) Responsibility for Assets

The ISO27002 indicates that appropriate protection of organisational assets must be achieved. This will assist in protecting the information stored on these devices. The ISO27002 points out the importance of keeping a register of all assets, such as smartphone devices that are issued to employees. Chapter two highlighted the importance of the information asset of smartphone devices, this needs to include the actual device itself. The protection of the device and its information must remain the responsibility of the employee who is in charge of that device. Extra care must be taken to include any removable media that the device includes.

Objective 8.1) Prior to Employment

Through this section, the ISO27002 stresses the importance of establishing that all potential employees, contractors and third parties are aware of security requirements prior to their employment. Future employees must be made aware of the sensitivity of organisational information that they will be working with.

Objective 8.2) During Employment

Section 8.2 ensures that during the course of employment, employees, contractors and third party users are aware of information security threats and concerns. During employment, employees must be made aware of their responsibilities and liabilities, and adequate levels of awareness, education and training in security should be provided. Finally, a formal disciplinary process for handling security breaches should be established.

Objective 8.3) Termination or change of employment

In section 8.3, the responsibility of ensuring that an employee's, contractor's or third party user's exit from the organisation is managed is highlighted. The removal of all equipment and access rights is vital to a successful and secure exit.

Objective 9.1) Secure Areas

The objective of section 9.1 is to prevent unauthorised physical access, damage, and interference to the organisation premises and information. Due to the mobility requirements of smartphone devices, section 9.1 is not targeted towards equipment that is intended to be operated outside of secure areas. However, smartphone devices must still be stored in secure areas, especially when travelling.

Objective 9.2) Equipment Security

Preventing loss, damage, theft or compromise of assets and interruption to the organisation's activities. This section highlights the importance of protecting equipment from physical and environmental threats. Section 9.2 states that protection of equipment reduces the risk of unauthorised access to information. Smartphone users must ensure that adequate security is applied to protect the device from unauthorised access. This section provides controls that are able to enforce measures that increase equipment security.

Objective 10.1) Operational procedures and responsibilities

Ensuring the correct and secure operation of information processing facilities is the objective of section 10.1. Through this section, segregation of duties is recommended to ensure that the risk of negligent or deliberate system misuse is mitigated. Smartphones might form part of an information processing facility. In such cases, controls must be applied to ensure that smartphones become a secure component of such facilities.

Objective 10.2) Third party service delivery management

In order to implement and maintain the appropriate level of information security and service delivery, section 10.2 indicates that third party service agreements should be implemented. Organisational checks must exist to ensure that the services delivered meet all requirements agreed with the third party. Smartphone usage usually includes communication over third party networks and software. It is important that controls are in place to ensure the security of these third party agreements and service contracts where they involve organisational information.

Objective 10.3) System planning and acceptance

This section states that provision must be made to minimise the risk of system failures. The ISO27002 standard states that advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance.

Objective 10.4) Protection against malicious and mobile code

The integrity of software and information is ensured in section 10.4. Precautions are provided to ensure prevent and detect the introduction of malicious code, and unauthorised mobile code.

Objective 10.6) Network security management

Section 10.6 focuses on ensuring the protection of information in networks, and the protection of the supporting infrastructure. As established in earlier chapters, smartphones often communicate information over public or third party networks. Section 10.6 provides controls to reduce the risk of information security breaches when using these networks.

Objective 10.7) Media Handling

One of the risk factors associated with smartphone devices included removable media. Section 10.6 provides that media must be controlled and physically protected. This includes all other types of media.

Objective 10.8) Exchange of Information

One of the advantages of smartphones identified in a previous chapter is the relative ease in which information can be achieved using these devices. Section 10.8 establishes that security must be maintained when exchanging information both within and outside of the organisation. Formal exchange policies should be established and carried out in line with exchange agreements and legislative requirements.

Objective 10.9) Electronic commerce services

Smartphone devices are perfectly positioned to make use of electronic services. Section 10.9 ensures that implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls are considered. This section targets both the integrity, and availability components of the information security triad first introduced in Chapter 2.

Objective 10.10) Monitoring

As with internal access to information systems, access from external devices such as smartphones must be monitored. All legislative requirements applicable to monitoring and logging activities must be applied to smartphone usage, as with desktop devices. Monitoring provides the ability to check the effectiveness of controls adopted to verify conformity to and access policy model.

Objective 11.1) Business requirements for access control

Section 11.1 is responsible for providing the controls to restrict access to information. The ISO27002 standard states that access to information, information processing facilities, and business processes should be controlled based on business and security requirements.

Objective 11.2) User access management

Formal procedures are highlighted in section 11.2 which specify that access rights to information systems and services must be controlled. These procedures must cover all stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

Objective 11.3) User responsibilities

In order to prevent unauthorised user access and compromise or theft of information and information processing facilities, section 11.3 stipulates that user cooperation is essential. Users are required to take ownership of the security requirements of smartphone usage. Access codes must remain strictly confidential.

Objective 11.4) Network access control

Network access controls prevent unauthorised access to networked services. This covers both internal and external networked services. This section adds that user access should not compromise the security of the network.

Objective 11.5) Operating system access control

Operating systems, including those on smartphone devices must prevent unauthorised access. Security facilities should be configured to restrict access by unauthorised users to operating systems.

Objective 11.6) Application and information access control

Section 11.6 indicates the need to prevent unauthorised access to information held in application systems. It is important that logical access to application software and information should be restricted to authorised users.

Objective 11.7) Mobile computing and teleworking

This section is focused on mobile devices of which smartphones are included. Specific controls targeted at protecting the information security of these devices are covered by section 11.7.

The ISO27002 (2005) specification states that mobile computing policy should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection.

Objective 12.2) Correct processing in applications

The objective of section 12.2 is to prevent errors, loss, unauthorised modification or misuse of information in applications. This section continues by adding that appropriate controls should be designed into applications, including user-developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

Objective 12.3) Cryptographic controls

Cryptographic controls protect the confidentiality, authenticity and integrity of information by cryptographic means. Policy is required to ensure that adequate cryptographic controls are utilised in smartphone security where feasible.

Objective 12.4) Security of system files

As established in earlier chapters, smartphones are capable of storing very large quantities of system files. Section 12.4 is responsible for providing controls to protect these files and those files that are accessible to smartphone users on system file serves.

Objective 12.5) Security in development and support processes

Project and support environments should be strictly controlled. This ensures that management are responsible for the security of the project or support environment. All proposed system changes need to be checked for security risks.

Objective 12.6) Technical Vulnerability Management

The importance of reducing risks from the exploitation of published technical vulnerabilities is covered in section 12.6. Considerations should be extended to included operating systems, and any other applications in use.

Objective 13.1) Reporting information security events and weaknesses

Section 13.1 ensures that information security events and weaknesses with information systems are communicated in a manner allowing timely corrective action to be taken. It is important that employees, contractors and third party users are aware of the procedure to follow when reporting any security events or weaknesses. Formal event reporting and escalation procedures should be established and put in place. Feedback forms a very important part of a successful security strategy.

Objective 13.2) Management of information security incidents and improvements

In earlier chapters, the importance of employees understanding their security responsibilities and procedures was introduced. A consistent and effective approach must be applied to the management of information security incidents.

Objective 14.1) Information security aspects of business continuity management

To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption (Standards South Africa, 2005). Smartphones are usually support devices as opposed to critical infrastructure, however, they must form part of continuity and contingency considerations.

Objective 15.1) Compliance with legal requirements

All company activities and equipment must be fully compliant with legislative requirements. This includes mobile devices and smartphones, which may contain or process confidential personal information. Section 15.1 highlights the importance of ensuring all statutory and legislative requirements are considered when designing and implementing a smartphone security solution.

Objective 15.2) Compliance with security policies and standards, and technical compliance

Once security policies and standards are established, it is important that employees comply with these. The importance of information systems should be regularly reviewed. Section 15.2 indicates that such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with the applicable security implementation standards and documented security controls.

Objective 15.3) Information systems audit considerations

Information systems must be audited regularly and the protection of the operational systems and audit tools is paramount in ensuring the integrity, and prevention of the misuse of audit tools.

4.3.3 Conclusion

The COBIT 4.1 framework was selected, as it is an industry accepted and respected guideline, in implementing IT governance measures. It was found to consist of 34 processes. In this chapter, 11 processes of the COBIT 4.1 framework of which risk management was a primary objective, were identified. Risk management was selected due to its focus on the management of risks associated with information technology governance.

The smartphone security weaknesses identified in section 3.3 could now be categorised into a IT resource category, and ultimately will become part of the final research model. This ensures that the security weaknesses are adequately addressed by the final research model. Furthermore, the information category provides assurance that the information security requirements identified in Chapter 2 will also be addressed.

This chapter also introduced the ISO27002 standards set. The standard was found to contain over 39 security categories. Using the COBIT 4.1 to ISO27002 mapping document, 28 of the 39 security categories were found to map to the 11 COBIT 4.1 processes identified.

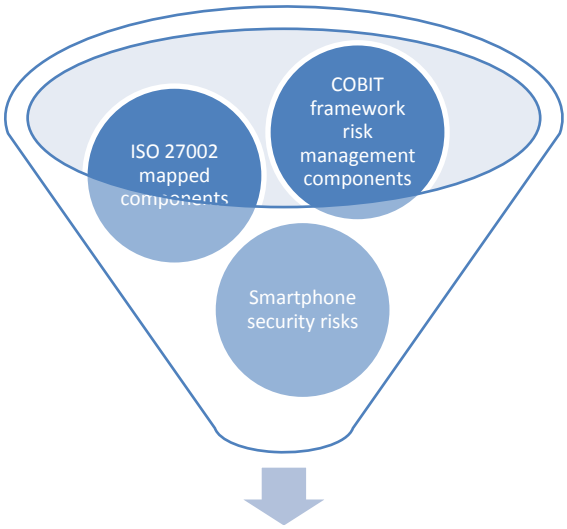


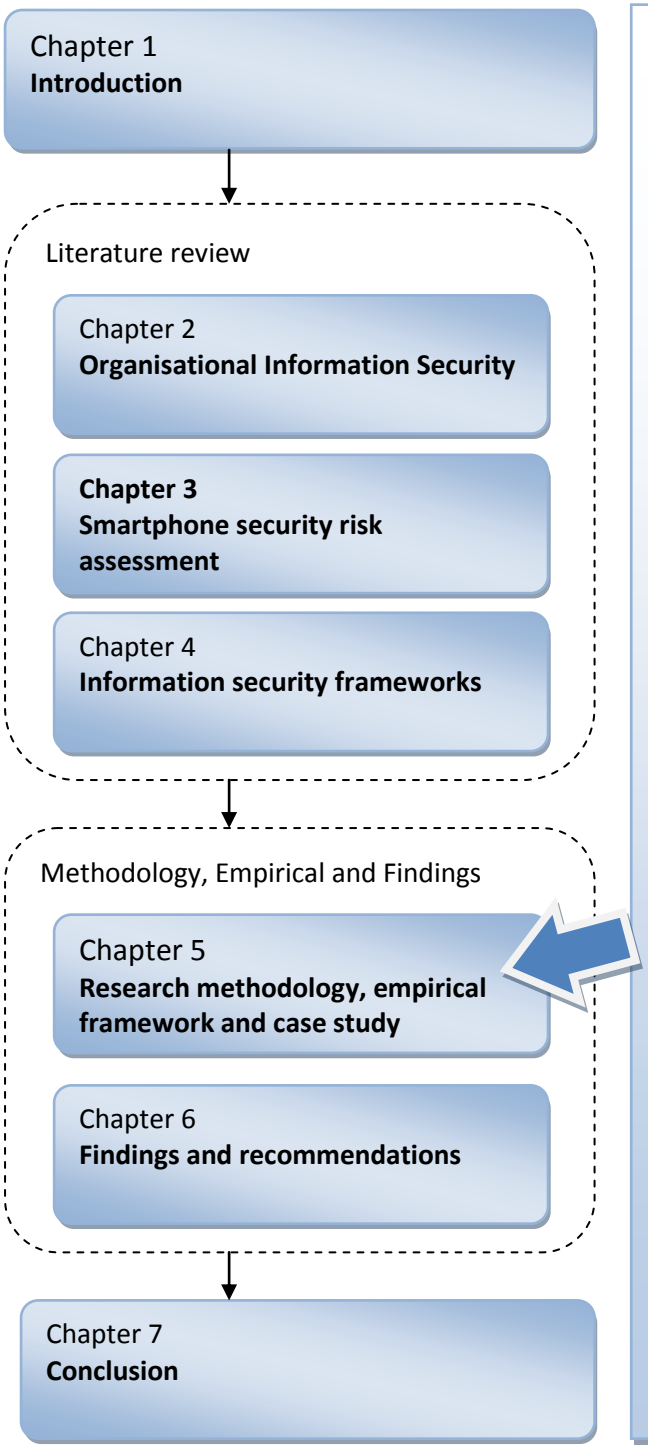
Figure 17 - Empirical framework composition

This process has streamlined both the components of the COBIT 4.1 framework and the ISO27002 standard to a reduced set of requirements from which a smartphone security model can be compiled. These processes will be included in the empirical framework in order to provide an answer to the second sub-question. When applied to the particular risks identified for smartphone devices, the requirements of the empirical framework can be compiled to include each of the required controls and processes.

The following chapter introduces the methodology, empirical framework and case study. By defining the specific components from each of the COBIT 4.1 framework and the ISO27002 standards set, a targeted subset of controls and processes have been indentified from which this methodology, empirical framework and case study will be developed.

5 Research methodology, empirical framework and case study

Chapter 5



5.1 Introduction

This chapter will introduce the methodology, empirical framework and case study. The qualitative and quantitative methodologies are contrasted, in order to establish which would be better suited to the requirements of this research project. Similarly, the research assumptions are contrasted, in order to determine the most suitable. The remainder of the chapter will focus on the method used to perform the empirical portion of the research project.

In the final sections of this chapter, the data collection method and research instrument is discussed. The chapter will conclude by indicating the results from the pilot study tests, of the case study data collection instrument. The changes due to recommendations from pilot study participants are highlighted before a brief section that introduces secondary data sources is provided.

5.2 Research methodology

Myers (1997) indicates that while research methods can be classified in various ways, one of the most common distinctions made is between qualitative and quantitative research methods. Myers (1997) adds that quantitative research methods were originally developed in the natural sciences to study natural phenomena. By contrast, qualitative research methods were developed in the social sciences to enable researchers to study both social and cultural phenomena.

Chapter three found, that the smartphone platform is not yet at the technical security maturity of desktop based systems. Chapter two of this research project pointed out that, people and organisational culture form a large part in establishing a successful smartphone security implementation. Myers (1997) states that the motivation for doing qualitative research comes from the observation that humans possess the ability to communicate. Myers indicates that humans have the ability to form both social and cultural constructs based on their interactions with each other. Morgan and Smirchich (1980, p. 498) add that

"once one relaxes the ontological assumption that the world is a concrete structure, and admits that human beings, far from merely responding to the social world, may actively contribute to its creation, the dominant methods [quantitative] become increasingly unsatisfactory, and indeed, inappropriate".

Qualitative research provides the facility for understanding the social components required, in developing information awareness in employees. Awareness programmes depend on successful communication in establishing or re-enforcing their messages. Qualitative research can assist in understanding how successful communication can lead to successful awareness programs. This helps mitigate the risks exposed by any immature levels of existing smartphone security.

Myers (1997) adds that researchers often combine both quantitative and qualitative methods in one research project. A method referred to as triangulation.

5.2.1 Philosophical assumption

Myers (1997) indicates that three distinct philosophical assumptions exist, into which all research projects can be classified. These are positivist, interpretive and critical. Myers cautions that the distinctions between these assumptions are often not always so clear-cut.

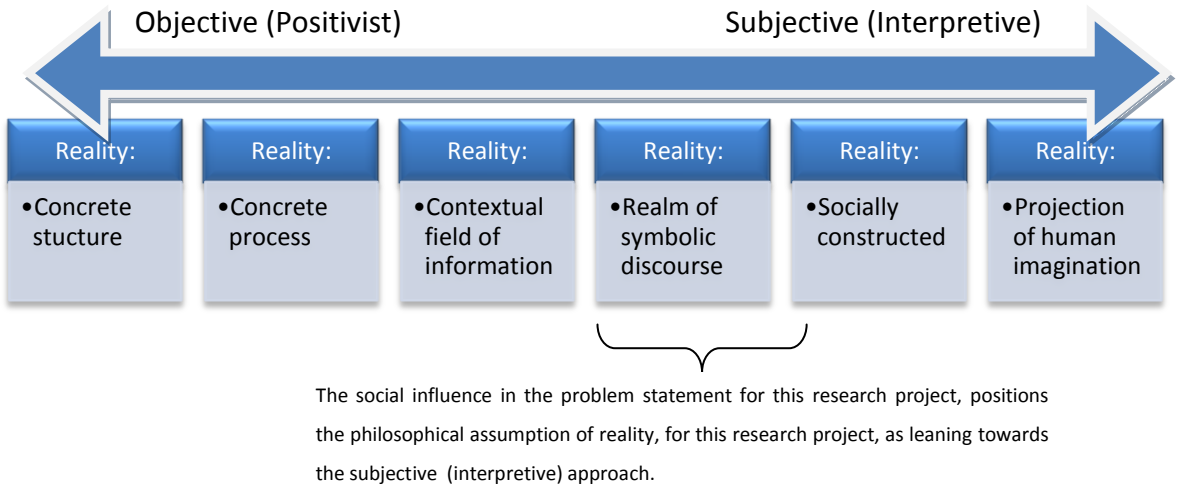


Figure 18 - Characterising the subjective-objective debate (adapted from Morgan and Smircich 1980 - Table 1)

Morgan and Smircich (1980) portray reality as a continuum between the extremes of objective and subjective assumptions (See Figure 18). This best illustrates the difficulty in cutting a clear distinction between the assumptions. Table 7 below, highlights the differences between three philosophical assumptions.

Table 7 - Philosophical assumptions (Myers, 1997)

Philosophical assumption	Description
Positivist	• Assumes that reality is objectively given and can be described by measureable properties, independent of the observer and his or her instruments. • Test theory, in an attempt to increase the predictive understanding of phenomena. • Evidence of formal propositions, quantifiable measures of variables, hypothesis testing, and the drawing of inferences about a phenomenon from the sample to a stated population.
Interpretive This research project leans towards the interpretive approach	• Reality is only through social construct such as language, consciousness and shared meaning. • Attempts to understand phenomena through meanings that people assign to them. • Aimed at providing an understanding of the context of the information system. • Influenced by the context. • Does not predefine dependant and independent variables, but focuses on the full complexity of human sense making the situation emerges.
Critical	• Assume that reality is historically constituted, produced, and reproduced by people. • The ability to consciously act to change social and economic circumstances is constrained by various forms of social, cultural and political domination. • Socially critical, restrictive and alienating conflicts and

	contradictions of the status quo are brought to light. • Focuses on the oppositions, conflicts and contradictions in contemporary society. • Seeks to eliminate the causes of alienation and domination.

This research project leans towards the interpretive approach. The questioning of personal subjective opinion within the context of the problem area will be used to formulate a model solution. Morgan and Smircich (1980, p. 498) point out that, "if one recognises that the social world constitutes some form of open-ended process, any method that closes the subject of study within the confines of a laboratory, or merely contents itself with the production of narrow empirical snapshots of isolated phenomena at fixed points in time, does not do complete justice to the nature of the subject."

5.2.2 Method of study

The method of study, according to Myers (1997), provides a strategy of inquiry that moves from the underlying philosophical assumptions to research design and data. Each method changes the manner in which the researcher harvests the data required for the research project. Myers (1997) adds that each method relies on different skills, assumptions and research practices. He lists the following qualitative research methods:

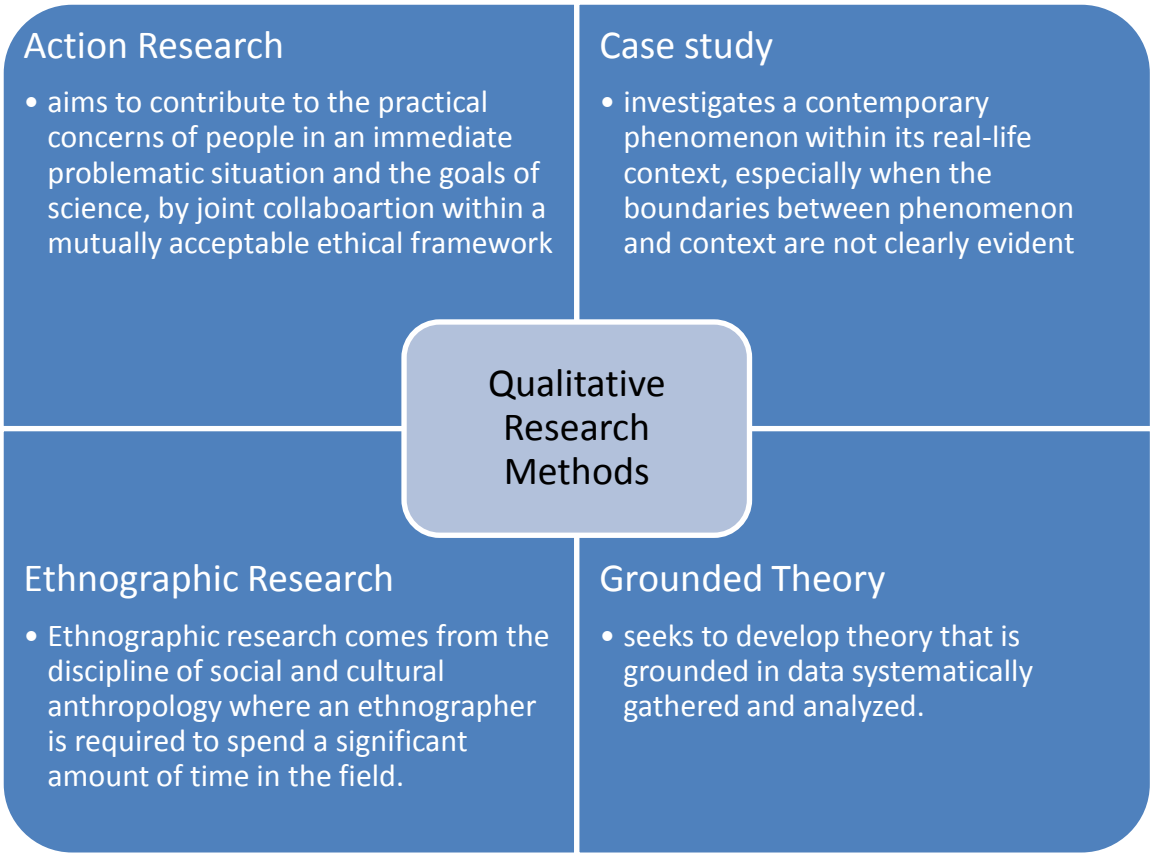


Figure 19 - Qualitative research methods (Myers, 1997)

The case study method is the most commonly used of the four qualitative methods above, however ethnographic and grounded theory methods are becoming more common (Myers, 1997). Based on the above definitions, the case study addresses the requirements of this research project. Myers (1997) states that, "case studies investigate a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident". Morgan and Smircich (1980, p. 498) note that researchers can no longer remain "external observers", but must move to investigate from within the subject of study and employ research techniques appropriate for such a task. Case studies can provide such a technique.

Using a case study, this research project addresses the context of existing security, by identifying the boundary between this context and the phenomenon introduced through

smartphone security risk. Due to the immaturity of smartphone security, these boundaries may not always be as evident as with other technologies.

5.3 Empirical framework

The empirical framework outlines the process by which the experimental or observable portion of the research method is to be completed. The empirical framework is tightly coupled to the underpinning research theories and paradigm. The researcher has selected multiple case studies utilising a questionnaire, to serve as the research instrument for primary data collection. In order to satisfy the requirements of a case study, a lengthy questionnaire will be utilised to in order to conduct an in depth study. The following section introduces the case studies, followed by the primary data collection process.

5.4 Case study

In order to gain insight into the security risks of smartphone devices, this study is performed as multiple case studies. Tellis (1997, p. 1) points out that, "multiple cases strengthen the results by replicating the pattern-matching, thus increasing confidence in the robustness of the theory". The case studies centre on a convenient multiple software consultancy organisations, randomly selected. The questionnaire is instructed to be answered within the context of the organisation at which the respondent is employed. Each software consultancy selected, displayed the following key characteristics:

1) Information services are the primary services offered by the organisation.

2) The organisation employs information workers to render these services.

These characteristics bring together key elements that must be consulted when identifying smartphone security requirements. These elements are the information and people of the organisation. Together, information and people form part of the bedrock of smartphone security requirements. It is important to point out that smartphone proliferation, of any percentage, or nominal value is not a pre-requisite for that organisation to participate.

Each case study is interpretive in its approach and seeks to identify the perceived smartphone security requirements of that organisation, even if they do not currently exist. This is achieved by asking each respondent what is important to their organisational context. As opposed to asking what is currently in use.

By requesting that respondents provide an interpretive opinion that is not influenced by any existing security measures, or lack thereof, the results from each case study provide a perceived set of best smartphone security requirements. This provides the specific requirements important to each respondent. The converse is that all items perceived to be of lower importance are also identified. Collectively, the case studies provide a set of comparative responses in which trends are identified. This provides the details for a model that is based on a collectively quantified best security approach across multiple organisational contexts.

5.4.1 Primary data collection

The primary data for this research project is the results returned by each of the questionnaires. Respondents were urged to provide their subjective opinion to all questions that they encountered on the questionnaire. In providing subjective opinions to the questions, the qualitative component of the research methodology is satisfied. Once the primary data collection was completed, analysis took place to reveal any trends and patterns that existed. This process introduces the quantitative component, together with the qualitative results. The triangulation of both research methodologies assists in establishing a sufficient quantity of qualitative results.

These results were used to identify the components required to design the assessment model output of this research project. Questionnaires were presented in the form of separate case studies. Each questionnaire sought to identify the perceived requirements of a respondent for their organisation. This allowed the respondents to provide their own

subjective perceptions of smartphone security requirements, within their organisations security requirements context.

The structure of the questionnaire is based on a Likert Scale question format. Each of the questions are phrased as a security requirement. This requirement effectively becomes a question statement. The statements are adapted from the activities recommended by each of the COBIT 4.1 processes identified in Chapter 4. 67 Question statements are included in the questionnaire. These activities are listed by each of the COBIT 4.1 processes that target risk management as a primary objective.

The question statements are a verbatim copy of the recommended COBIT 4.1 process activities, with the object or subject of that sentence re-phrased to represent either smartphones, or the role of smartphones. These altered statements will be scrutinised by pilot study participants, to ensure that the meaning or intention of those statements is not lost, by altering the statement. Appendix A provides a list of the original statements along with the altered statement. Two statements were omitted from the questionnaire as they targeted a specific security component, other than the smartphone.

The following table lists the COBIT 4.1 processes and their respective number of activities.

Table 8 - COBIT 4.1 Process activities

Processes that target risk management as a primary objective	Number of activities identified for the Questionnaire
PO4	5
PO6	3
PO9	10
DS2	6
DS4	11
DS5	7
DS11	5
DS12	5
ME2	7
ME3	5
ME4	5

The Likert Scale selected was the level of importance that respondents felt statement to have, within the context of their organisation. An example of a question statement, and its Likert Scale, is provided below in Table 9. Respondents were asked to read each statement as part of the question, "*how important is it to [their company] that ...*", followed by each statement. This made it easier, and clearer, for the respondent to understand what each statement was asking. It also reduced the amount of reading that needed to be done by the respondent. Reading the same opening question for each statement question might also fatigue the respondent. In addition, it provided a greater context for the statement.

Table 9 - Question example

A smartphone process framework has been developed.					
Very Unimportant	Unimportant	Neutral	Low Importance	Moderately Important	Very Important

When read with the previously provided prefix, the statement reads as follows: *how important is it to [your company] that a smartphone process framework has been developed.* The Linkert Scale requires respondents to provide an opinion as the answer. The provided answer is therefore the subjective opinion of the respondent, based on security requirements within the context of that organisation.

In addition to the statements, the following administrative, ethical and statistical questions were provided at the start of the questionnaire.

1) Would you prefer your company to be listed as an anonymous participant?
2) Are you directly responsible for the definition, implementation OR maintenance of the security requirements of your organisation?
3) Approximately how many workers are accountable to the information security requirements of your organisation?
4) Does your organisation's security policy specifically address any risks of smartphone computing?

5) Are smartphones generally considered as a strategic enabling technology within your organisation?
6) Are smartphones generally viewed as a risk to the information within your organisation?

These questions assist in providing an idea of the size, and basic smartphone security maturity at that organisation, separate to the perceived importance of the security statements that follow. The provided an additional context and dimension to the primary data that was collected. This additional context enhanced the trend analysis component of the data analysis further.

Finally, it is important to mention that all respondents that indicated that they wished for their organisation to remain anonymous had any identifiable information removed from the results. No personal information is required in the analysis of the data. Organisational security requirements are more important to this research project, than the identity of the organisation.

Fifty-eight (58) responses were received from the case study requests. These responses represent a convenient sample from an unknown population. The responses were imported into a database for safekeeping, and in order to provide an easy method of performing queries to the data. The data was imported directly from the online questionnaire service into the database; no modifications were made to the raw response data.

There were a small number of incomplete questionnaire responses, which were discarded as spoilt. These results were not included in any of the response data statistics. Responses from respondents, who indicated that they had misunderstood the requirements during the pilot study, were also removed from the final results. This ensured that the results reflected a universal understanding of the questionnaire requirements. The following section introduces the pilot study conducted prior to the primary data collection.

5.4.1.1 Pilot study

In order to ensure that the questionnaire provided the highest quality responses, a select number of respondents conducted a pilot study. The pilot study took place two weeks before the questionnaire was scheduled to be released. Pilot study participants were randomly selected. Pilot study participants were asked to complete the questionnaire, however they were given the following additional instructions:

1) Indicate approximately how long it takes you to complete the questionnaire?
2) Please mark any questions that you feel are unclear, ambiguous, and irrelevant or duplicate the recommendation of another question (also indicate whether you would recommend they be removed or modified)?
3) The flow of the questions (is the order logical, or would you have preferred a different or random ordering)?
4) Are the instructions clear?
5) Any additional comments or recommendations would be appreciated.

Initial responses from the pilot study revealed that respondents found some misinterpretations between the questionnaire instructions, and the requirements of the questionnaire. Based on these results, the instructions were updated, until respondents agreed that the instructions accurately explained the intentions of the researcher.

There was no negative feedback regarding the length or content of the questionnaire. The ethical, administrative and statistical questions were understood, and accepted, by all pilot study participants. As mentioned previously, pilot study results were discarded for all respondents that indicated that they had misinterpreted the initial instructions.

5.4.2 Secondary data

Secondary data will be comprised of information collected from various sources. Sources include the following:

- The COBIT Framework version 4.1
- The ISO27002 code of practice

- Articles from various academic journals
- Books
- Conference proceedings

Only the most recent data available was included. All secondary data is referenced, to ensure that the original author is accredited. All references are listed in full at the end of this research project.

5.5 Conclusion

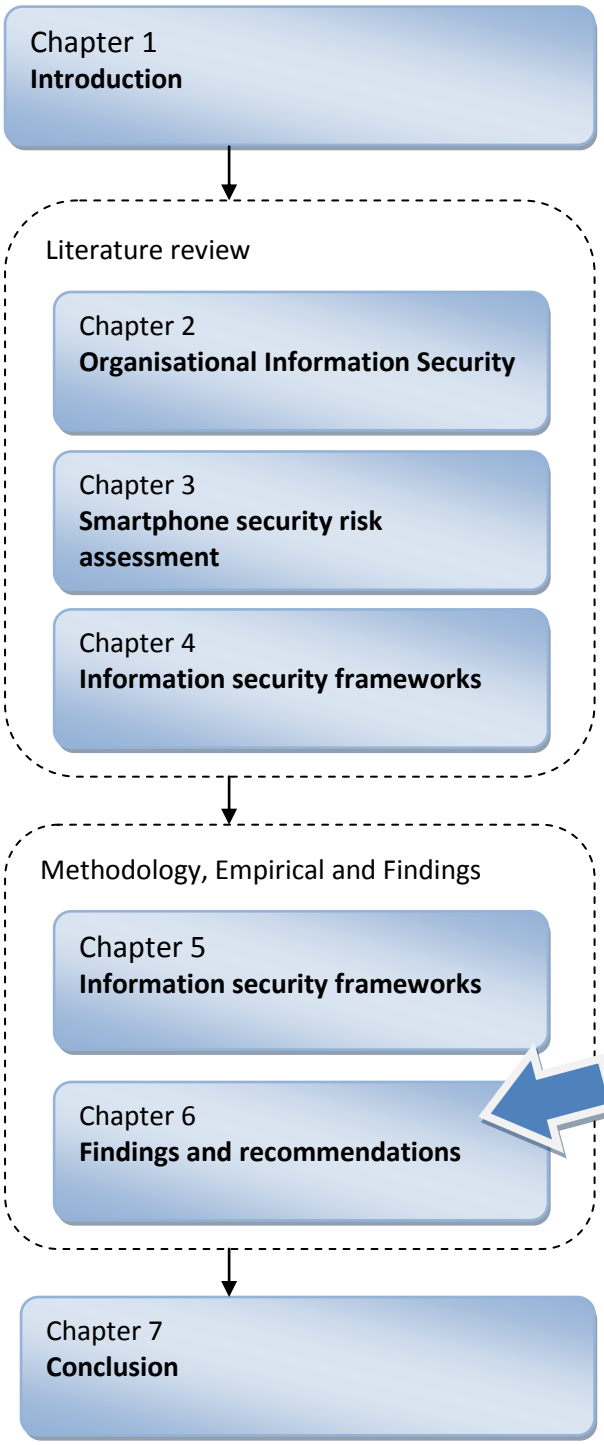
In this chapter, the research methodology for this research project was established as a triangulated combination of both the qualitative and quantitative methods. The qualitative approach was expected to take a larger role, due to the social and cultural influences around smartphone security requirements.

The philosophical assumption to this research project was established to be that of an interpretive approach. From this approach, the reality of the study would be based on social constructs. This enables respondents, through their subjective opinions, to interpret the security requirements of smartphone devices. This ties into the qualitative method through the Likert Scale questions utilised in the questionnaires of each case study. Collectively a quantitative analysis of these results would reveal trends in the opinions of respondents.

A questionnaire was developed as the research instrument for this research project. A pilot study was conducted, to ensure that the questions and instructions provided by the questionnaire resulted in accurate responses. Once the recommendations of pilot study participants were implemented, the questionnaire was circulated. The following chapter presents the results of the questionnaire, and introduces the resulting model.

6 Findings and recommendations

Chapter 6



6.1 Introduction

This chapter will introduce both the model and findings of this research project. Section 6.2 will provide a statistical analysis of the quantitative results of the case study responses. Any trends identified will be listed, and compared to the literature. Section 6.3 will thereafter propose the recommendations.

In order to enhance the comparative component of the analysis, the results will first be considered for all respondents; and then separately based on the respondents' response to the following question: "Are you directly responsible for the definition, implementation OR maintenance of the security requirements of your organisation?". This criterion was best suited to divide all respondents into one of the two gradients detailed by the awareness boundary model (detailed in Chapter 2) which is illustrated below. Nineteen (or 33%) of the 58 responses were from respondents that indicated that they were responsible for security policies at their organisation.

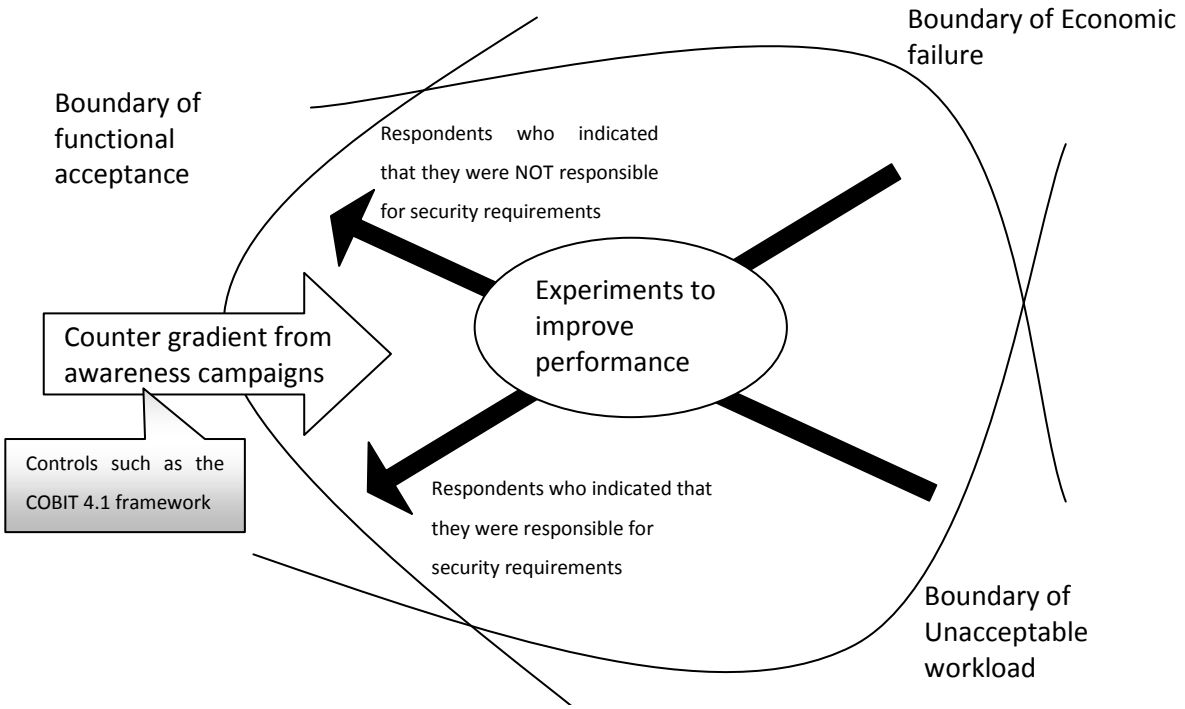


Figure 20 - Awareness boundaries (adapted from Rasmussen (1997, p. 189)) - Case study overlay

In Figure 20 above, the separate case study populations are transposed onto the awareness boundary model. Here it becomes easier to identify that respondents, who are not responsible for security requirements, are inclined to be moving away from the boundary of unacceptable workload. This is because these respondents would consider security requirements to be unnecessary extra workload (extra workload pushes them towards the boundary of unacceptable workload). This is confirmed in Chapter 2 by Ruighaver, Maynard, and Chang (2007). They found that there is no evidence that employees are intrinsically motivated to adopt secure practices.

Respondents responsible for implementing security requirements must do so in order to protect the organisation from anything that might result in economic failure. Therefore, those respondents who indicated that they were responsible for implementing security requirements move in the gradient away from the boundary of economic failure.

The question statements used in the case study questionnaire simulate a counter gradient provided by the recommendations of the COBIT 4.1 framework. By determining the optimum requirements of both gradients away from economic failure and unacceptable workload, each of these gradients can focus on pushing towards the boundary of functional acceptance. Any significant disparity between the gradients does not translate into an effort towards functional acceptance, but rather against each other.

6.2 Findings

In order to quantify the Likert Scale responses, each of the responses was allocated a score. The score allocated to the individual responses is detailed in the following table.

Table 10 - Likert scoring allocation

Likert scale answer	Scoring
Very Unimportant	-2
Unimportant	-1
Neutral	0
Low Importance	1
Moderately Important	2
Very Important	3

Scoring each of the response answers, allows an average score to be determined for each of the statements. The scores can be added together for each question, and averages can be easily calculated. The following ruler illustrates the scale used to illustrate answers:

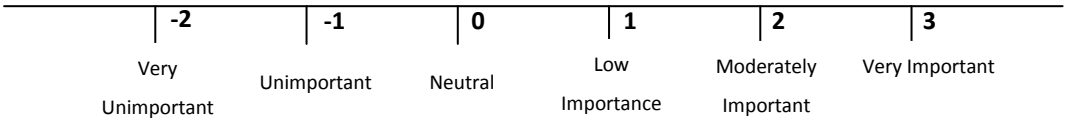


Figure 21- Answer scale ruler

The scale represents a range beginning at -2 (Very Unimportant) and ending at 3 (Very Important). This allows us to approximately position items at their actual position between the scale steps. Answers might lie at any position on the line.

The findings reveal a number of interesting results when the entire population is examined. The overall average importance for respondents across all questions was below 1 (between neutral and low importance) at 0.80 points. This supports the argument that employees do not perceive smartphone security to be of moderate or high importance to their organisation. The results indicated similar levels of perceived importance of smartphone security, regardless of whether or not respondents indicated that they were responsible for the security policies at their organisation.

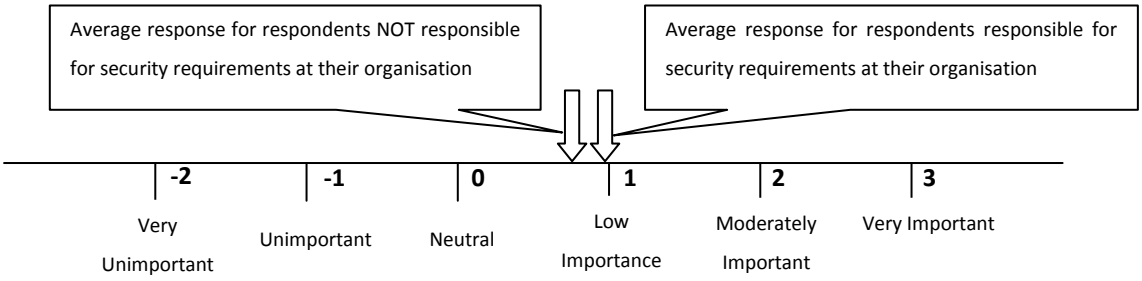


Figure 22 - Overall average selection, by responsibility of respondent

The results were analysed along the following criteria:

- Determination of the question statements that received the highest score ratings.
    - Overall
    - By respondents who were responsible for security policies.
    - By respondents who were not responsible for security policies at their organisation.
- Determination of the question statements that received the lowest score ratings.
    - Overall
    - By respondents who were responsible for security policies.
    - By respondents who were not responsible for security policies at their organisation.
- Determination of the question statements that yielded the greatest discrepancies between the respondents responsible for security policy, and those not responsible.
    - Above standard deviation.
    - Below standard deviation.
- Determination of the level of importance across each of the represented domains from the COBIT 4.1 framework.

By categorising and analysing the information according to these criteria, the trends were much easier to identify. The following graph (Figure 23) presents the overall average result across each question. The numbers along the vertical Y-axis directly correlate to the scale steps on the answer scale ruler. Interesting to note is how the average score for the first 18 questions is 1.08, which is higher than the overall average (0.80) for the entire answer set.

These question statements are from the Planning and Organising domain of the COBIT 4.1 framework. This is discussed in detail later in the chapter. In Chapter 4, three of the four domains from the COBIT 4.1 framework were identified which target risk management as a primary objective.

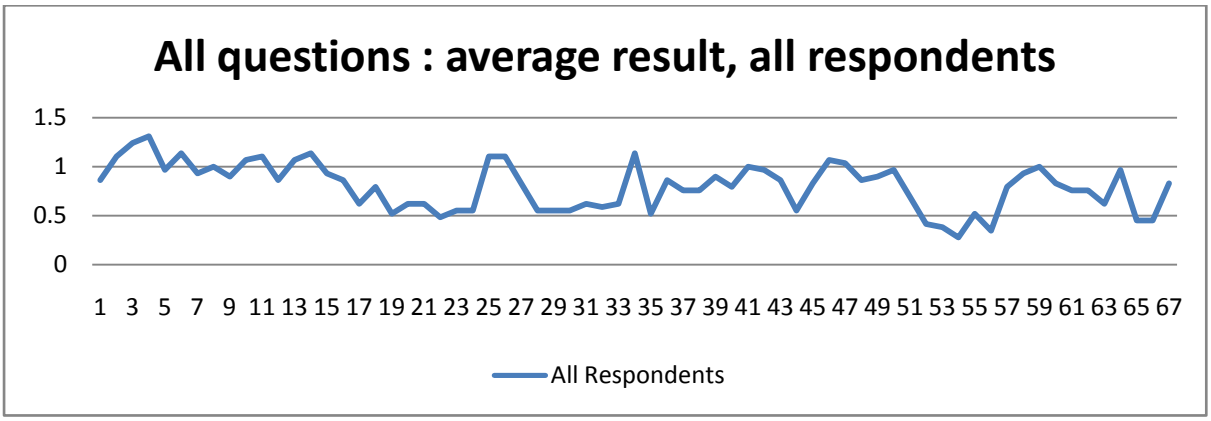


Figure 23 - All questions: average result, all respondents

The graph in Figure 23 highlights the distribution of importance levels across each of the 67 questions given to respondents. As discussed above, a breakdown of each of the components of the questions is provided in the following sections.

6.2.1 Highest scoring question statements

The following five question statements received the highest scores overall between all respondents:

Table 11 - Top five question statements, overall scores

Question	Question statement	Score
4 (PO4)	Smartphone users are aware of who owns the data processed and stored on their device.	1.31
3 (PO4)	Smartphone system owners have been identified.	1.24
6 (PO6)	A smartphone control environment and framework has been established, and is being maintained.	1.14
14 (PO9)	Smartphone risks associated with events have been assessed.	1.14

34 (DS4)	Smartphone information backup storage and protection has been planned for and implemented.	1.14

Four of the top five question statements selected by all respondents come from the Planning and Organising domain. The statement that received the highest overall level of importance was question statement four. Overall, respondents found that user awareness of the data stored and processed on smartphone devices to be of high importance. Olzak (2006) highlighted the importance of employee awareness in an effective information security solution.

Question 3 received the second highest rating of importance at 1.24. Respondents found that it is very important that smartphone system owners be identified. According to the IT Governance Institute (2007b), owners are responsible for classifying information and systems, and protecting them in line with this classification.

Three question statements received equal importance of 1.14. Question statement six, received a relatively high rating of importance. This question statement highlights the importance of implementation and maintenance, of a smartphone control framework. One aligned with the organisations' management philosophy and operating style.

The second question statement that received an importance level of 1.14 was question statement 14. This question statement highlights the importance of identifying possible risks to smartphone security.

Question statement 34 was the only question statement that was not from the Planning and Organising domain. It too received an importance level of 1.14. This question statement highlights the importance respondents placed on backup and security of the information on smartphone devices.

Table 12 - Top five question statements, respondents responsible for security requirements

Question	Question statement	Score
10 (PO9)	The relative strategic business objectives of smartphones are understood.	2.11
14 (PO9)	Smartphone risks associated with events have been assessed.	1.78
3 (PO4)	Smartphone system owners have been identified.	1.67
11 (PO9)	Relevant smartphone business process objectives are understood.	1.67
46 (DS11)	Smartphone data is backed up according to scheme.	1.67

When considered as a separate population, respondents that indicated they were responsible for security at their organisations selected a different top five. Only one item is from the Deliver and Support domain, the rest are from the Planning and Organising domain.

The most important question statement for this group is question statement 10. Question statement 10 received an importance of 2.11. This was the highest recorded for a single question statement across all respondents and population splits. This question statement involves understanding the relative strategic objectives of smartphones. In Chapter 2, Martins and Eloff (2001) indicated that without processes, employees might not know how to behave, or what is expected of them. A strategy must be defined, and then understood by all employees.

Question 14 was the second highest rating at 1.78. This question statement, along with question statement three, also appeared in the overall top five. Question three received and importance level of 1.67, along with two other question statements, 11 and 46. Question statement 11 is very similar to question statement 10. Both deal with strategic objectives. Question 11 differs in its focus on process level requirements as opposed to business level requirements. This does reinforce the importance of strategic objectives in smartphone security considerations.

Finally, question statement 46 echoes the sentiments of question statement 34. Both highlight the importance of ensuring that a backup policy exists. Question statement 46 adds the importance of defining a specific backup scheme to smartphone security requirements.

Table 13 - Top seven question statements, respondents not responsible for security requirements

Question	Question statement	Score
4 (PO4)	Smartphone users are aware of who owns the data processed and stored on their device.	1.30
6 (PO6)	A smartphone control environment and framework has been established, and is being maintained.	1.10
3 (PO4)	Smartphone system owners have been identified.	1.05
25 (DS4)	An IT continuity framework has been developed, and this framework includes smartphones.	1.05
8 (PO6)	Smartphone control frameworks, objectives and direction have been communicated to smartphone users.	1.00
13 (PO9)	Events associated with smartphone objectives have been identified.	1.00
34 (DS4)	Smartphone information backup storage and protection has been planned for and implemented.	1.00
39 (DS5)	Smartphone user access rights and privileges are periodically reviewed and validated.	1.00

Finally, Table 13 lists the responses that received the highest importance level, from respondents who indicated that they were not responsible for security requirements. This table contains the top seven responses. This is due to four statements sharing the fourth highest level of importance. Three items were from the Deliver and Support domain, the other four are all from the Planning and Organising domain.

Question statement four received the highest level of importance (1.30) for this population, similar to its position in the overall population. Question statement six received the second highest level of importance (1.10). This question also appears in the overall top five.

Following this, question statement three received an importance rating of 1.05, and is the only one to appear on all three lists.

Question statement 25 also received a rating of 1.05. This question statement is centred on the importance of developing an IT continuity framework, which includes smartphone devices. The next question statement, eight, is the first of four question statements to receive an importance rating of 1.00, by respondents who indicated that they were not responsible for security requirements. In question statement eight, respondents found that it is important for smartphone control frameworks, objectives and directions to be communicated to smartphone users.

Also receiving an importance rating of 1.00, question statement 13 highlighted the importance of identifying the events associated with smartphone objectives. Question statement 34, which appeared in the previous top five, also received an importance rating of 1.00 for this population group. Finally, question statement 39 was the final statement to receive an importance rating of 1.00. This question statement provides the importance of periodically reviewing and validating user access rights and privileges.

6.2.2 Comparison between population groups

Two distinct population groups were identified earlier in this chapter. These groups were then identified to align with one of the two gradients of the awareness boundary model. Figure 24 below provides a graph of the difference between the importance rating of respondents responsible for security requirements and those not responsible, for each question statement.

The difference between each question answered by both population groups falls within a standard level of deviation. From this graph, it is easier to identify those questions that fall outside of the standard deviation. These items present the most disparities between the two population groups. Establishing which items present the greatest disparities, assists in

identifying the factors that cause the gradients (population groups) to act against each other.

The standard deviation for the difference between each of the population groups is 0.35598. This creates an upper level of 0.61 and a lower boundary of -0.10. Any differential between each of the population groups that falls outside of this boundary will be considered a significant disparity. Figure 24, illustrates the standard deviation upper and lower boundaries, from which each of the items outside of these boundaries is revealed.

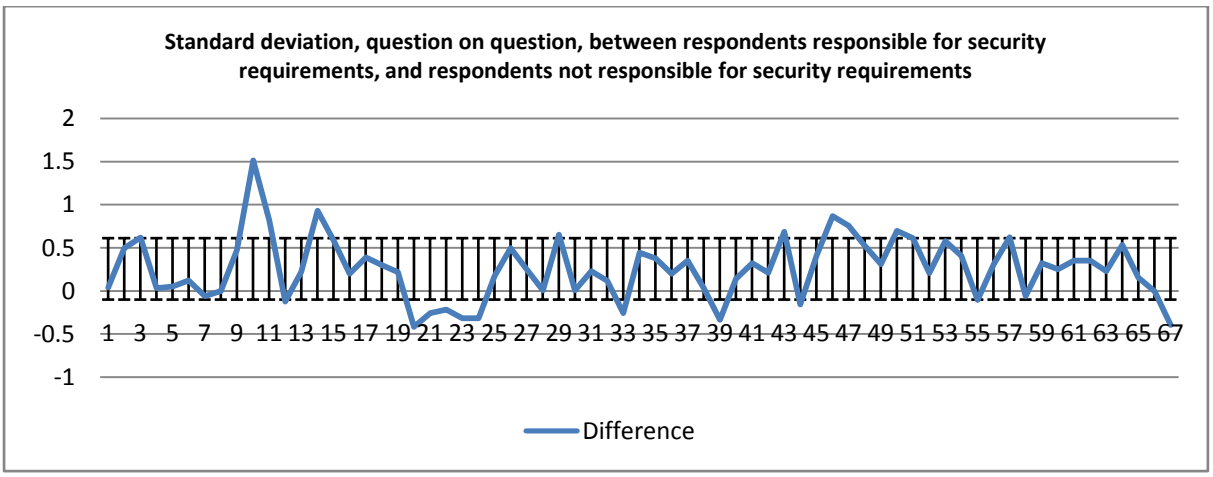


Figure 24 - Standard deviation between the two population groups

The following table lists the questions that display differences, which fall outside the standard level of deviation:

Table 14 - Question statements outside of the standard deviation level

Scope	Question Statement
Above the standard level of deviation	3, 10, 11, 14, 29, 43, 46, 47, 50, 57
Below the standard level of deviation	12, 20, 21, 22, 23, 24, 33, 39, 44, 55, 67

An even split is observed between those above and those below standard deviation. Twenty-one (21) question statements in total fall outside of the standard deviation level. This is just short of one in every three questions. Items above the standard deviation level are of greater importance to respondents responsible for security at their organisation. Items below this level are more important to respondents who are not responsible for security at their organisations.

6.2.2.1 Top five items above standard deviation

These items find particular support amongst respondents who indicated that they were responsible for security requirements at their organisations.

Question statement ten recorded the highest deviation between the groups. Strategic objectives for smartphones are found to be important to respondents who are responsible for security requirements, with an importance level of 2.11. This is not the case for respondents who are not responsible for security requirements. This population only recorded an importance level of 0.60.

Question statement fourteen displays the second highest level of deviation above standard. This indicates the importance of establishing the smartphone risks associated with events, if far greater to respondents responsible for security requirements. Question statement 46 follows in third position. The importance of establishing a set backup scheme displayed much greater significance to respondents responsible for security requirements.

Finally, question statements 11 and 47 provide the fourth and fifth highest level of deviation above the stand level. Respondents responsible for security place greater emphasis on the

relevance of business process objectives and data restoration procedures, than respondents who were not responsible.

6.2.2.2 Top five items below standard deviation

These items find particular support amongst respondents who indicated that they were not responsible for security requirements at their organisations.

Question statement 20 exhibited the greatest level of deviation below the standard level of deviation. Respondents not responsible for security requirements allocated this statement an importance of 0.75, versus 0.33 allocated by those respondents not responsible for security requirements. This question statement rates the importance of defining and documenting the supplier management processes.

Question statement 67, which deals with the IT governance report, receives much higher support from respondents not responsible for security than those who are responsible. This statement displays the second highest level of deviation below the standard level. The third highest level of deviation below the standard is question statement 39. This statement highlights smartphone user access rights and privileges.

Finally, question statements 24 and 23 respectively scored the fourth and fifth highest levels of deviation below the standard level. These items are concerned with both smartphone service delivery and relationships. This rates more importantly to respondents not responsible for security, than it does to respondents who are responsible.

6.2.3 Responses by COBIT 4.1 domain

Figure 25 displays a graph of each of the answer levels for only the question statements extracted from the planning and organising domain. As highlighted earlier, responses from this domain received a higher level of average importance (0.99) for each question statement that those of the other domains.

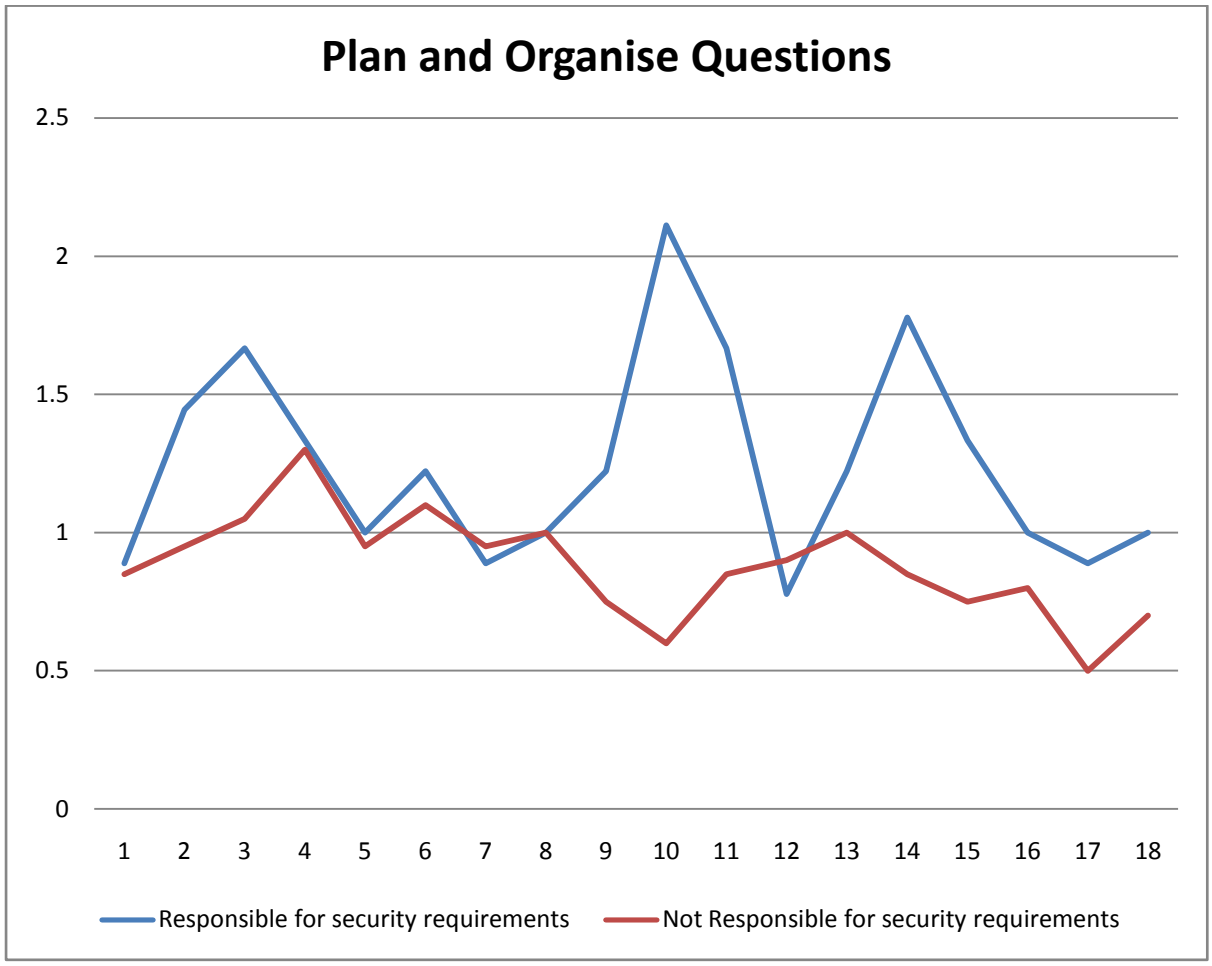


Figure 25 - PO importance levels

Figure 26 displays a graph of each of the answer levels for only the question statements extracted from the delivery and support domain. This domain provided the bulk of the question statements used in the questionnaire. Responses for this domain generally received a lower level of average importance (0.77) than those of the planning and organising domain.

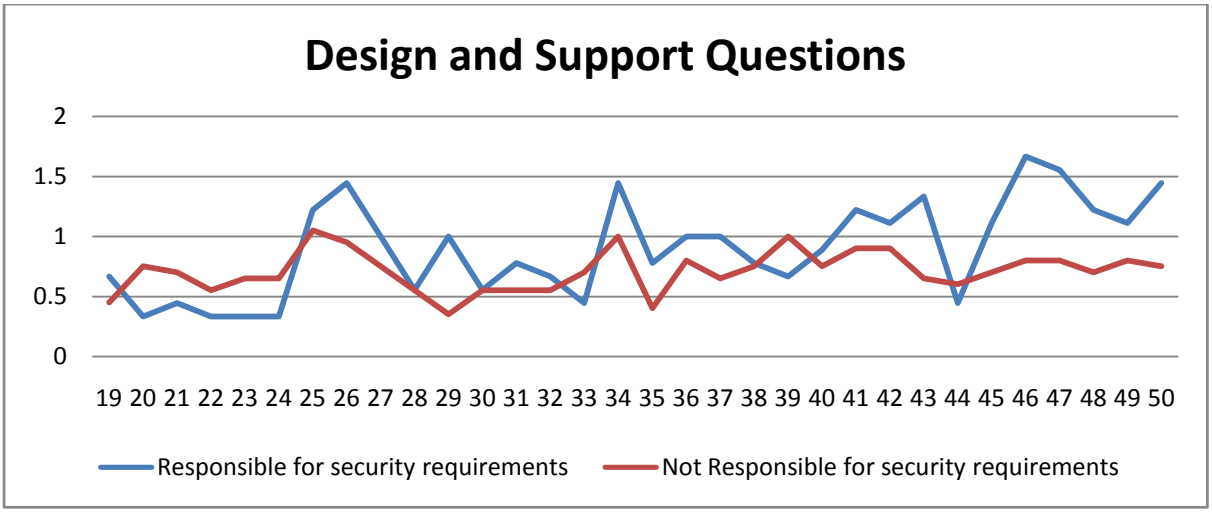


Figure 26 - DS importance levels

Figure 27 displays a graph of each of the answer levels for only the question statements extracted from the Monitor and Evaluate domain. Responses for this domain generally received the lowest average level of importance (0.65) across each of the represented domains.

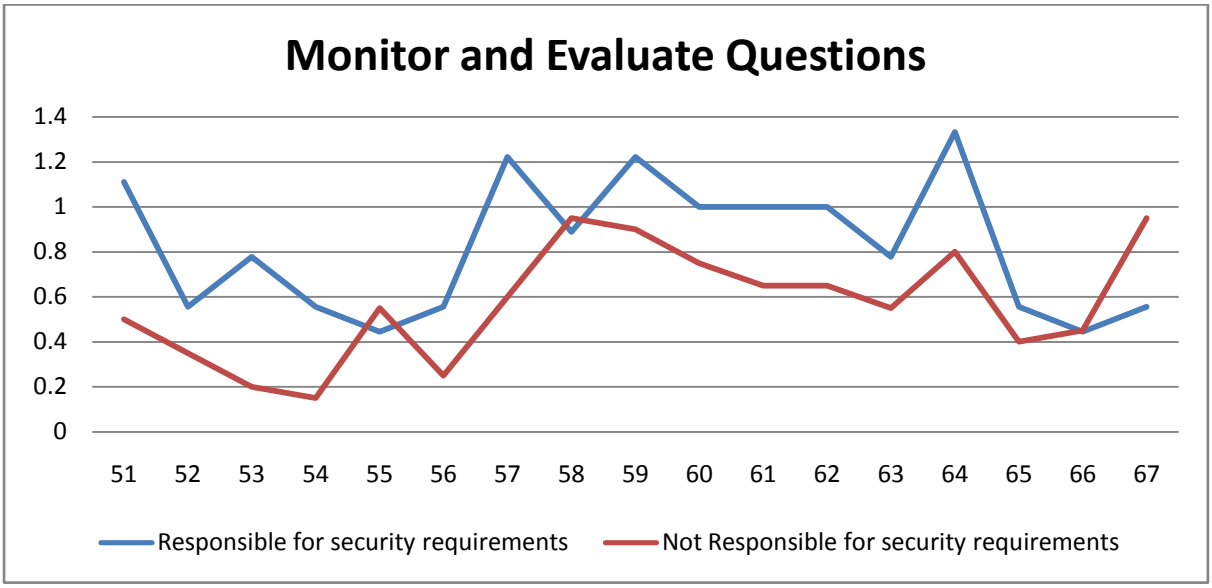


Figure 27 - ME importance levels

Only three of the four COBIT 4.1 domains are represented. The fourth domain (Acquire and Implement) does not target risk management as a primary objective. In this section, the

statements from the planning and organising domain were found to contribute the highest average overall level of importance for all respondents.

Table 15 below confirms that the separate population groups echo the sentiments of the overall averages highlighted above.

Table 15 - Average level of importance by respondent and domain

	Average level of importance		
Domain / **Respondent**	Plan and Organise	Deliver and Support	Monitor and evaluate
Responsible for security requirements	1.25	0.90	0.82
Not Responsible for security requirements	0.88	0.70	0.57

6.3 Recommendations and Model

The importance of protecting the information assets of an organisation is discussed extensively in Chapter 2. If the security risks of smartphones are not adequately measured and mitigated, they could present a considerable risk to the organisation. In order to ensure that adequate security is applied, management must be able to assess their current security position.

This section recommends a model, which can be applied to measure the security maturity currently operating at a software consultancy organisation. This model further provides a method of assessing the areas in which the current security solution does not adequately consider the security requirements for smartphone devices. The model is based on both the primary data collected, and the secondary data sources.

6.3.1 Purpose of the model

The model provided in this section is intended to meet the following key characteristics:

- Measure the current security solution.
- Identify the gaps that exist between this solution and one that encompasses smartphone security.

6.3.2 Model composition

The model for this research project is comprised of a number of components from the secondary data collected, and includes findings of the primary data collection. These items are all subjected to a maturity model scale.

6.3.2.1 The maturity scale

The COBIT 4.1 framework recommends the use of maturity models, which help to identify gaps in capability, and are easily demonstrable to management. Based on the key characteristics listed in the previous section, a maturity model based solution is best suited to providing the required gap analysis. COBIT 4.1 provides six maturity levels, with respective definitions.

Table 16 - Maturity levels (IT Governance Institute, 2007b)

Level	Title	Definition
0	**Non-Existent**	Complete lack of any recognisable processes. The enterprise has not even recognised that there is an issue to be addressed.
1	**Initial / Ad Hoc**	There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganised.
2	**Repeatable but Intuitive**	Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.
3	**Defined Process**	Procedures have been standardised and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
4	**Managed and Measurable**	Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5	**Optimised**	Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

This scale will provide the measurement and assessment component for the model. The scale is simple enough for comprehension by non-technical management. It provides a quick overview of areas in which smartphone security does not exhibit adequate protection.

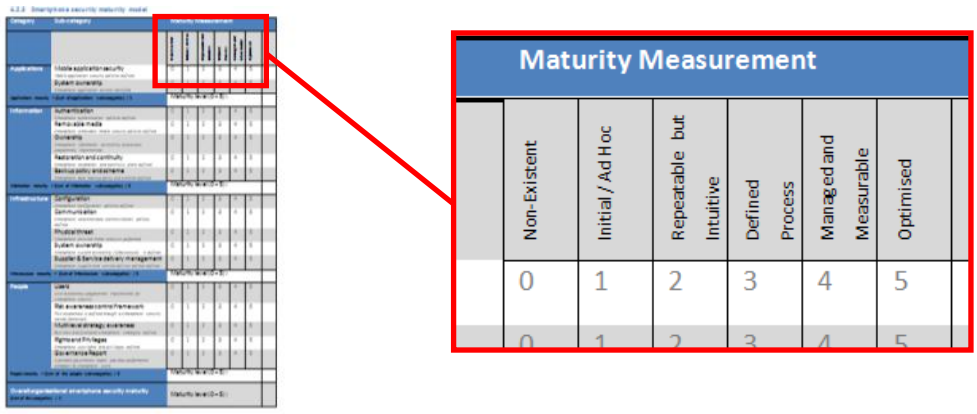


Figure 28 - Maturity scale

Illustrated above in Figure 28, the six maturity scale columns run down the right hand side of the model. For each of the components, a maturity level will be marked in one of these columns.

6.3.2.2 Measurable components

Figure 29 - Measurable components

The seventeen measurable components for the model are comprised of a combination of the seven smartphone risk items identified in the secondary data collection and ten items from the primary data collected. In Chapter 3, seven smartphone risks identified by Botha, Furnell and Clarke (2009) were presented in Figure 9 in Chapter 2. These are subsequently mapped to one of the IT Resource categories of the COBIT 4.1 framework. This mapping is illustrated in Figure 15 in Chapter 3. These items are included in the model, as they provide a measureable risk component across each of the smartphone security risks areas. However, this does not fully satisfy the IT governance requirements of smartphone security, according the COBIT 4.1 process requirements.

In order to ensure the solution satisfies smartphone security governance, items from the primary data collected, are incorporated into each of the categories. The items added are comprised of responses from the primary data collected, as detailed below in Table 17. This is illustrated in Figure 30. These items were also categorised under one of the IT Resource categories. The application category now contains two sub-categories; the other three categories now each contain five sub-categories.

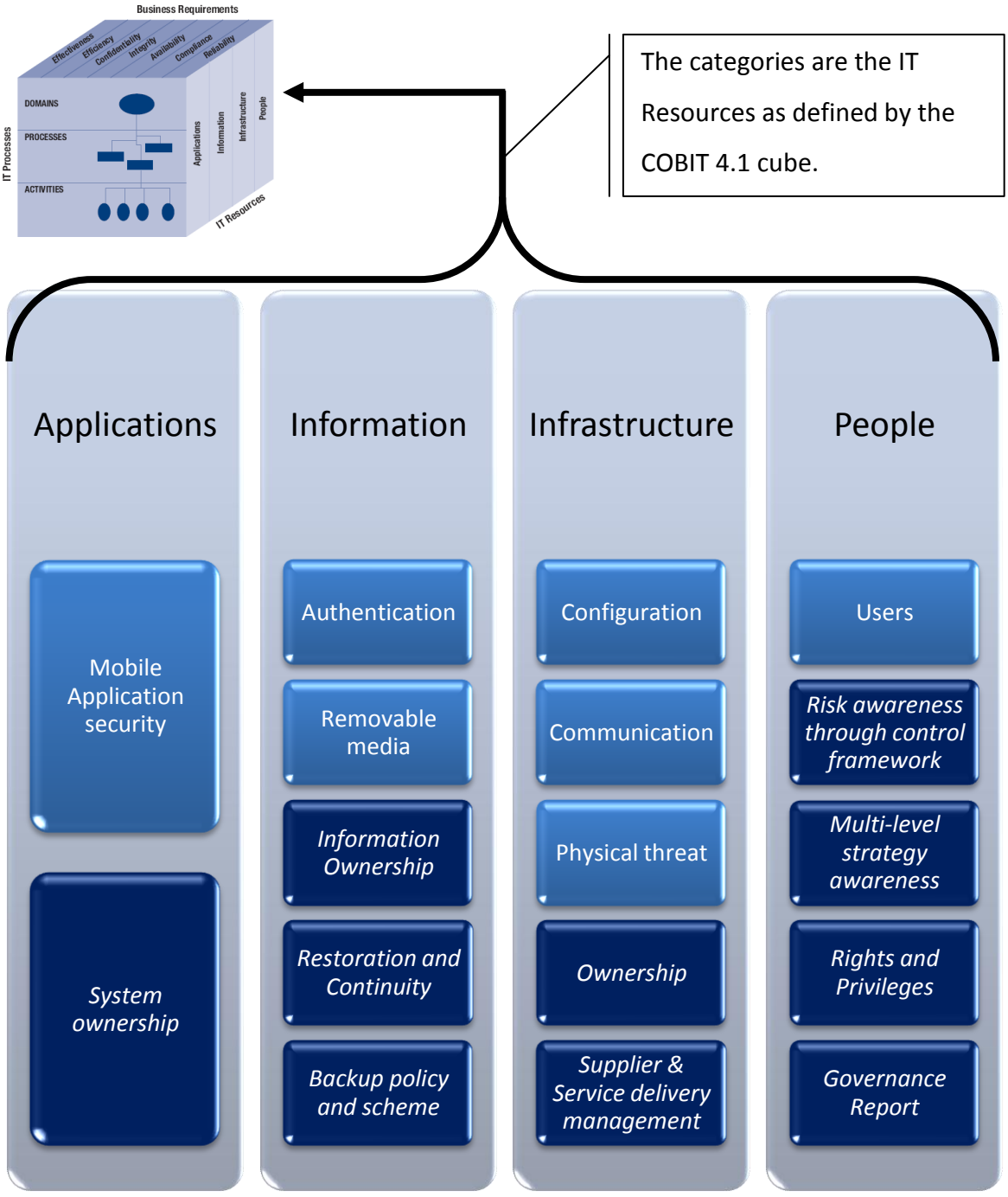


Figure 30 - Extended smartphone risk categorisation

The items displayed with the darkened background, and italic font style, are the question statements added to the original smartphone risks (lighter background) from Figure 15.

The items added from the primary data collection are from the five most important items to each population, and the items displaying the greatest deviation from the standard level of

deviation. The following table (Table 17) indicates which question statements from the primary data collected are added to each category.

The first column lists the population group, or groups, that highlighted the importance of the question statement. The second column provides the question statement number. The final two columns provide the category this item is added to, and the item name within that category.

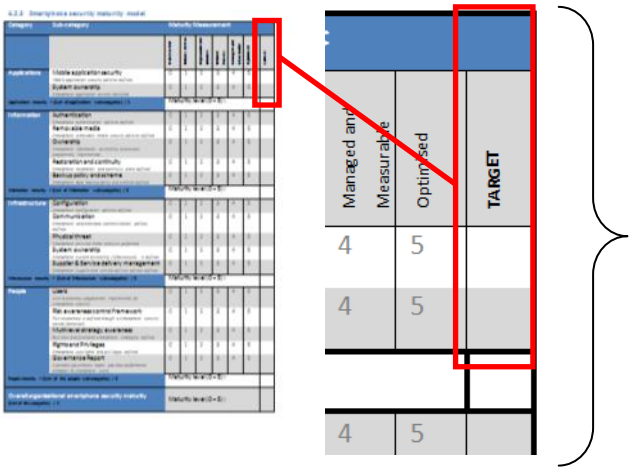
Table 17 - Items added to model from primary data

Concerned group(s)	Question statement	Category	Item
Overall top five, respondents responsible for security & respondents not responsible for security	3 (PO4)	Application and Infrastructure	System ownership
Overall top five & respondents not responsible for security	4 (PO4)	Information	Ownership
Overall top five & respondents not responsible for security	6 (PO4)	People	Risk awareness through control framework
Respondents not responsible for security	8 (PO6)	People	Multi-level strategy awareness
Respondents responsible for security & above standard deviation	10 (PO9)	People	Multi-level strategy awareness
Respondents responsible for security & above standard deviation	11 (PO9)	People	Multi-level strategy awareness
Respondents not responsible for security	13 (PO9)	People	Risk awareness through control framework
Overall top five, respondents responsible for security & above standard deviation	14 (PO9)	People	Risk awareness through control framework
Below standard deviation	20 (DS2)	Infrastructure	Supplier & Service delivery management
Below standard deviation	23 (DS2)	Infrastructure	Supplier & Service delivery management

Below standard deviation	24 (DS2)	Infrastructure	Supplier & Service delivery management
Respondents not responsible for security	25 (DS4)	Information	Restoration and Continuity
Overall top five & respondents not responsible for security	34 (DS4)	Information	Backup policy and scheme
Respondents not responsible for security & Below standard deviation	39 (DS5)	People	Rights and Privileges
Respondents responsible for security & above standard deviation	46 (DS11)	Infrastructure	Backup policy and scheme
Above standard deviation	47 (DS11)	Information	Restoration and Continuity
Below standard deviation	67 (ME5)	People	Governance Report

6.3.2.3 Organisational maturity targets

The model is designed for generic use across all types of software consultancies. For each software consultancy, the environment within which they operate is likely to be very different. For this reason, the model allows for a target maturity to be defined according to the specific requirements and priorities of the organisation that it is being used within. A committee of senior managers and security officers should be assembled to define the target maturity level for the specific organisation utilising the model.



The final column of the smartphone security maturity model provides a space to capture the target maturity level. This must be completed by a committee of senior managers and security officers, and is defined by each organisation according to its unique requirements and priorities. It might not be feasible for an organisation to achieve higher than a particular maturity level for certain items.

Figure 31 - Target maturity level

Any maturity scores below the target level identify gaps between the existing security solution, and one that encompasses an adequate smartphone security.

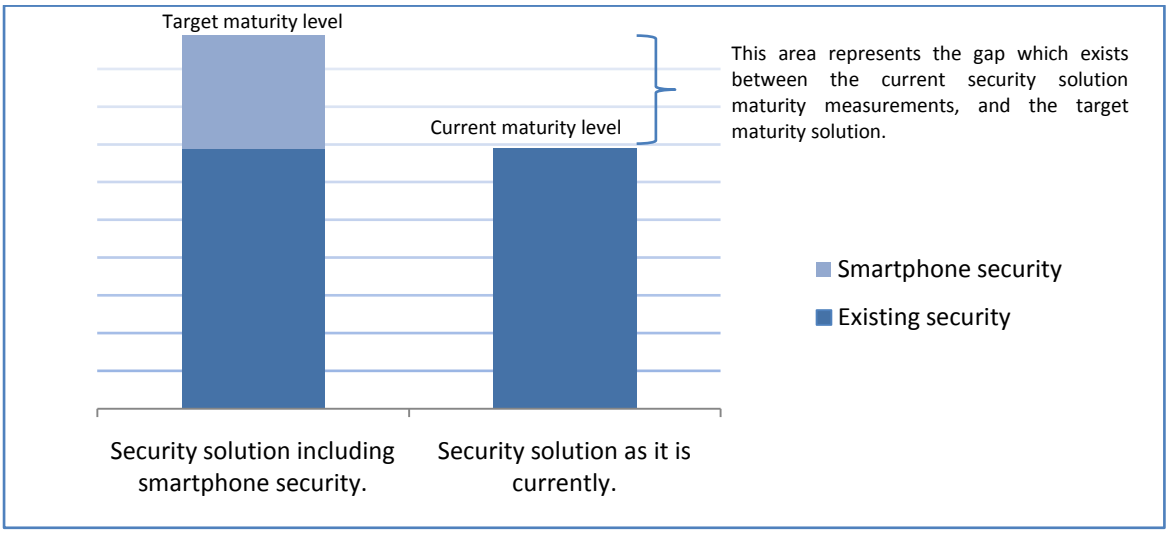


Figure 32 - The security maturity gap

Figure 33 on the following page presents the smartphone security maturity model.

6.3.3 Smartphone security maturity model

Category	Sub-category	Maturity Measurement						
		Non-Existent	Initial / Ad Hoc	Repeatable but Intuitive	Defined Process	Managed and Measurable	Optimised	TARGET
Applications	Mobile application security *Mobile application security policies defined*	0	1	2	3	4	5	
	System ownership *Smartphone application owners identified*	0	1	2	3	4	5	
Applications maturity = (Sum of applications sub-categories) / 2		Maturity level (0 – 5) :						
Information	Authentication *Smartphone authentication policies defined*	0	1	2	3	4	5	
	Removable media *Smartphone removable media security policies defined*	0	1	2	3	4	5	
	Ownership *Smartphone information ownership awareness programmes implemented*	0	1	2	3	4	5	
	Restoration and continuity *Smartphone restoration and continuity plans defined*	0	1	2	3	4	5	
	Backup policy and scheme *Smartphone data backup policy and scheme defined*	0	1	2	3	4	5	
Information maturity = (Sum of information sub-categories) / 5		Maturity level (0 – 5) :						
Infrastructure	Configuration *Smartphone configuration policies defined*	0	1	2	3	4	5	
	Communication *Smartphone recommended communication polices defined*	0	1	2	3	4	5	
	Physical threat *Smartphone physical threat analysis performed*	0	1	2	3	4	5	
	System ownership *Smartphone system ownership (infrastructure) is defined*	0	1	2	3	4	5	
	Supplier & Service delivery management *Smartphone supplier and service delivery polices defined*	0	1	2	3	4	5	
Infrastructure maturity = (Sum of infrastructure sub-categories) / 5		Maturity level (0 – 5) :						
People	Users *User awareness programmes implemented for smartphone security*	0	1	2	3	4	5	
	Risk awareness control framework *Risk awareness is defined through a smartphone security control framework*	0	1	2	3	4	5	
	Multi-level strategy awareness *Business and functional smartphone strategies defined*	0	1	2	3	4	5	
	Rights and Privileges *Smartphone user rights and privileges defined*	0	1	2	3	4	5	
	Governance Report *A periodic governance report provides performance feedback to smartphone users*	0	1	2	3	4	5	
People maturity = (Sum of the people sub-categories) / 5		Maturity level (0 – 5) :						
Overall organisational smartphone security maturity **(Sum of the categories) / 4**		Maturity level (0 – 5) :						

Figure 33- The smartphone security maturity model

The model should be used as a score sheet to assess the maturity of the organisational smartphone security maturity. Through each of the categories, each sub-category must be allocated a maturity level. Once all the sub-categories are allocated a maturity level, the category itself can be allocated a category maturity. This can be done by dividing the sum of the maturity levels by the amount of sub-categories. For example, in Table 18 below, the applications category has been completed, with a set of example target maturities (randomly selected) provided.

Table 18 - Category maturity example

Category	Sub-category	Maturity Measurement						
		Non-Existent	Initial / Ad Hoc	Repeatable but Intuitive	Defined Process	Managed and Measurable	Optimised	TARGET
Applications	Mobile application security *Mobile application security policies defined*	0	1	2 X	3	4	5	4
	System ownership *Smartphone application owners identified*	0	1	2	3 X	4	5	4
Applications maturity = (Sum of applications sub-categories) / 2		Maturity level (0 – 5) : **2.5**						4

The score for the applications maturity level is calculated as follows:

Applications maturity = (2 + 3) / 2 = 2.5

The maturity gap for this section is calculated as follows:

Applications maturity gap = (actual - target) = (2.5 – 4) = -1.5

Negative values indicate a gap; positive values indicate that maturity is currently above the target level.

Finally, if required, an overall organisational smartphone security maturity can be calculated by dividing the sum of all of the category maturities by four (the amount of categories). This

test can be completed quarterly, annually or as often as the organisation wishes to assess its smartphone security maturity.

6.3.3.1 Recommended measurement process

The recommended process for measuring the smartphone security maturity is illustrated in Figure 34. Begin by using the maturity model to perform an initial measurement, establishing the maturity scores as an initial benchmark. This benchmark is the current security maturity of the organisation. In conjunction, initial maturity targets must be set by senior managers and security officers.

Once a benchmark is established, gaps can be identified by comparing maturity levels to target maturity levels. A task team or individual, depending on the organisation, can be established in order to react to the security gaps identified. Recommended actions and policies must be defined and implemented (React), in order to move the current smartphone security maturity levels toward target levels.

Once this is completed, a new measurement using the model must be completed. Any items, which are now equal to, or above the target maturity level, must be incorporated into a maintenance plan. A new benchmark must be set and new gaps must be identified. The cycle should be repeated continuously according to the requirements of the organisation.

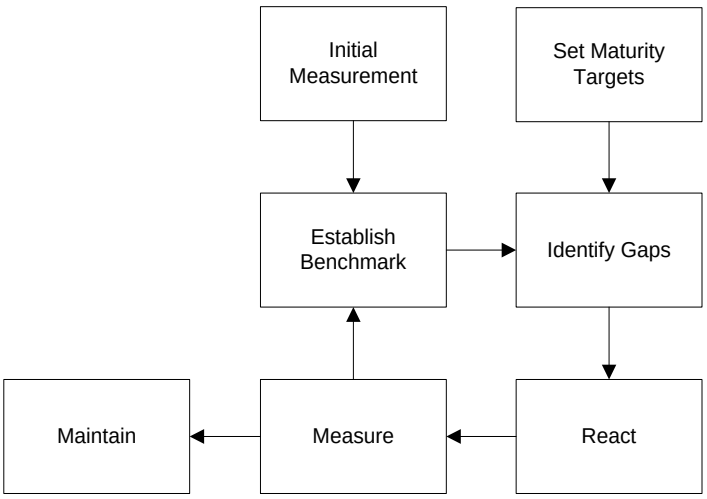


Figure 34 - The maturity measurement cycle

This measurement cycle is intended to provide one example of a recommended usage pattern for the model. Each organisation might customise this workflow according to their own strategic or legislative requirements.

Through repetitive measurement cycles, employee awareness of the smartphone security requirements will constantly become reinforced and eventually form a part of the security culture.

Once smartphone security becomes part of the organisational culture, an alignment between business and smartphone security objectives will begin to occur.

6.3.4 Strategic alignment of business and smartphone security objectives

By ensuring that each of the categories moves towards optimised maturity, each of the gradients of the awareness boundary model (detailed in Figure 4 in Chapter 2) will begin moving in a similar direction. They will then be working together to resist both economic failure and unacceptable workload. Together, their efforts to reach functional acceptance will be far greater and with rigid security in place, the counter gradients will ensure that functional acceptance is never breached.

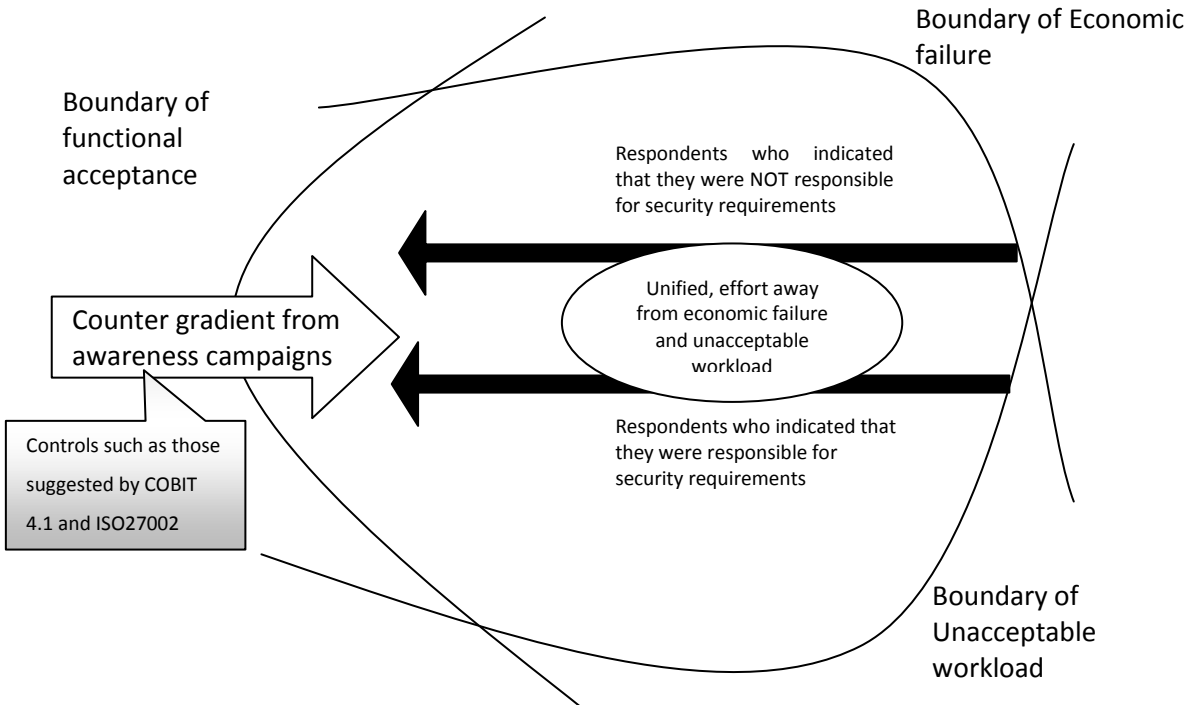


Figure 35 - Awareness boundary model, unified effort – adapted from Rasmussen (1997)

This represents an employee base, which is in tune with the requirements of the organisation. At the same time, management are aware of security requirements. Both groups are also aligned with the organisational security requirements, as opposed to only resisting their individual boundaries.

6.4 Conclusion

In this chapter, the results from the primary data collection were analysed. The results were analysed as a whole, and then separately by population groups defined by whether or not the respondent was responsible for security at their organisation. Interestingly there appears to be very little difference in the perception of smartphone security requirements between both population groups. Sacco (2008) pointed out that a study by CompTIA pointed out that less than a third of organisations had implemented measures to raise security awareness. This appears to correlate to the results of this study as it was found that employees who are responsible for security are similarly unconcerned about the security weaknesses of smartphone devices, as those respondents who indicated that they

were not responsible. Dunn (2007) agrees suggesting that smartphone security is a largely neglected area. From the results it would seem as though all employees, regardless of their responsibility for security at their organisations, view smartphone risks as negligible.

The results included a comparison between the two population groups in the form of a standard deviation test. This concluded that respondents share similar perceptions of importance for certain components of smartphone security, with only one third of the score differences falling outside of standard deviation.

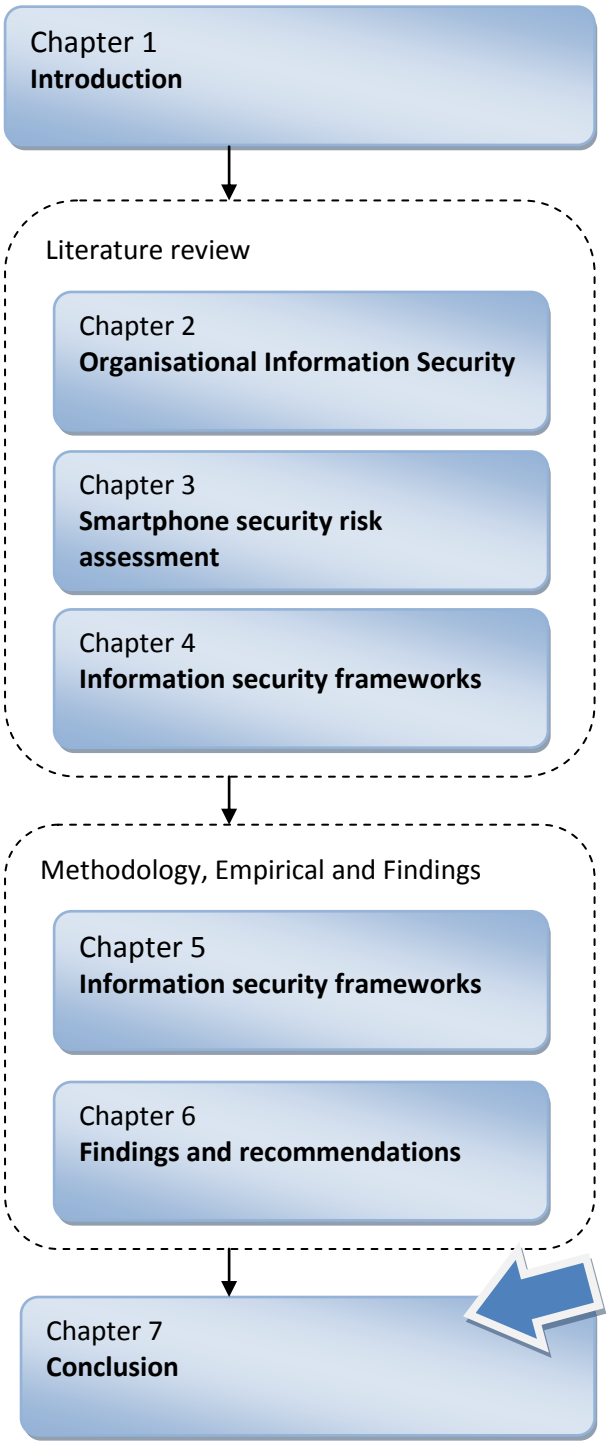
The final analysis performed was across each of the relevant COBIT 4.1 domains in order to establish which domain was the most important to respondents. The results point to the Planning and Organising domain as being the most relevant to smartphone security.

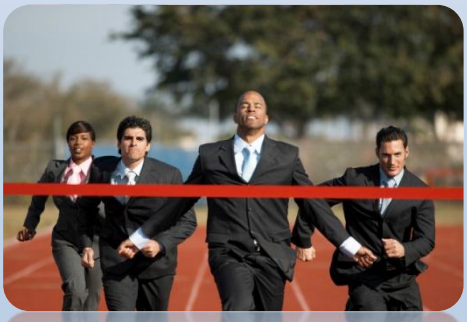
The chapter concluded with the model and recommendations. The purpose of the model is detailed before the actual model is provided. A detailed explanation of the maturity scale and measureable components of the model is provided. This included a recommended usage cycle.

This chapter highlighted the question statements that gained the highest importance levels across each of the population splits. From this, items that are important to each of the groups, even where they might disagree, can receive attention in the maturity measurement. This is important in ensuring that the requirements of each of these groups are satisfied. Once all population groups are satisfied, the chance of successfully gaining support for a smartphone security initiative is much higher. Chapter 7, the final chapter, provides the conclusion to this research project.

7 Conclusion

Chapter 7





7.1 Background

This chapter will provide a conclusive discussion to this research project. A brief background of the research will be presented followed the contribution made. In this section, an overview of all the chapters will be discussed. An evaluation of the research outcomes follows in section 7.3.

The following section, 7.4 provides future research recommendations. These recommendations provide direction in which future research could build on the work of this project. Finally, some concluding remarks are offered in section 7.5.

Proliferation of smartphones is set to catch many software consultancy organisations off-guard. While many organisations might take extreme measures to mitigate this risk, such as banning the use of smartphones for processing of organisational information, the potential strategic advantage of these devices cannot be overlooked.

The literature consulted in this research project suggests that organisations have not focused adequate resources on ensuring that security for these devices is at an acceptable level. In Chapter 3, it was established that security for other platforms has gradually matured over time; however, smartphone security remains relatively immature in comparison. This not only poses a real threat to an expensive piece of equipment (the physical device), but also puts an increasing amount of organisational information at risk.

In Chapter 2, the importance of information as an asset to the organisation is discussed. It was noted that organisations are increasingly reliant on confidential, reliable and readily available sources of strategic information. In order to satisfy this appetite for information employees have begun to move processing of this information to mobile smartphone devices. An information security driven organisational culture, provides a powerful method of ensuring that employees subscribe to the requirements of information security. This was found to provide employees with a sense of awareness of the requirements of information

security. Finally, Chapter 2 detailed the characteristics of a typical software consultancy worker.

In Chapter 3, the smartphone was subjected to a discussion of its security risk areas. Smartphones, because of their relatively young lifespan, were found to possess a number of areas in which their security level has not reached a similar level of maturity, as that found in regular computing devices. A definition for a smartphone device was provided, specifically for this research project, in order to minimise confusion.

At the end of Chapter 3, the specific risks exposed by smartphones were covered in detail. This covered the threat to information security in software consultancies, introduce by the proliferation of the smartphone. Chapter 4 provided the final chapter for the literature review section of this research project. In this section a base framework from which the research solution could be developed was introduced.

Chapter 4 introduced two major security frameworks. These frameworks provide an excellent platform to build a solution to the problem area. The core of the solution was achieved by decomposing the COBIT 4.1 framework, into parts that targeted risk management as a primary objective. Each of the smartphone security risk areas was mapped to a resource area of the COBIT 4.1 framework. Finally, the ISO27002 standards were mapped to the COBIT 4.1 components.

In Chapter 5, the research methodology was established to favour the interpretive approach. A questionnaire, as part of multiple individual case studies, provided an ideal research instrument. Both quantitative and qualitative methods were deployed in order to gain insight into the problem area. This was achieved by quantifying the results from the Linkert Scale responses of each case study.

Using a database in conjunction with a spreadsheet tool provided a method of dissecting and analysing multiple combinations of the results. The results were filtered based on the

respondents' responsibility for security at their organisation. Clear trends and patterns were identified. These were then analysed and incorporated into the research model. The findings and recommendations were presented in Chapter 6.

The resulting outcome of this research project is a model, which can be used to measure the smartphone security maturity of a software consultancy organisation. The following section will highlight the contributions made by the research project.

7.2 The contribution made by this research project

It was established that organisational smartphone security levels must be improved to prevent vulnerabilities or threats to information security. Existing security solutions were found to be lacking adequate security for smartphone devices. Employees were found to be driving an explosion of smartphone devices into the workplace. While this tendency is not confined to just the software consultancy organisation, due to the nature of this organisation it is set to suffer considerable harm in the event of a security breach. The reason for this is because of the heavy dependence on information and information workers, at this type of organisation.

A significant problem that required attention was that there was no clear and concise model for measuring which areas of an organisation's current security solution were inadequately prepared, for the risks introduced by smartphone devices. From this research project, a model has been presented which seeks to fulfil this requirement. Software consultancy organisations can now utilise this model in order to determine which areas of smartphone security need to be adequately addressed.

Smaller software consultancies are able to set separate maturity targets to larger consultancies with bigger budgets and requirements, using the same model. This model can be customised to measure the maturity requirements at any software consultancy by

adjusting the target maturities. Furthermore, this model provides a methodology of measuring progress and areas, which have regressed.

This model provides each of the most important measurable factors for adequate smartphone security assessment. The model takes the form of a maturity measurement tool. One that can be completed by security personnel, and easily understood by executive managers who might not be proficient in the area.

This research project highlighted areas of smartphone security, which were important to the following respondents:

- Users responsible for security at their organisations.
- Users not responsible for security at their organisations.
- Both groups (collectively).

Procedures of the COBIT 4.1 framework which targeted risk management as a primary objective were identified. Each of the objectives of the ISO27002 standard which mapped to these procedures were also identified. This provided a detailed starting point, from which security users are able to begin implementing security requirements. The planning and organising domain of the COBIT 4.1 framework was found to be the most important to all respondents.

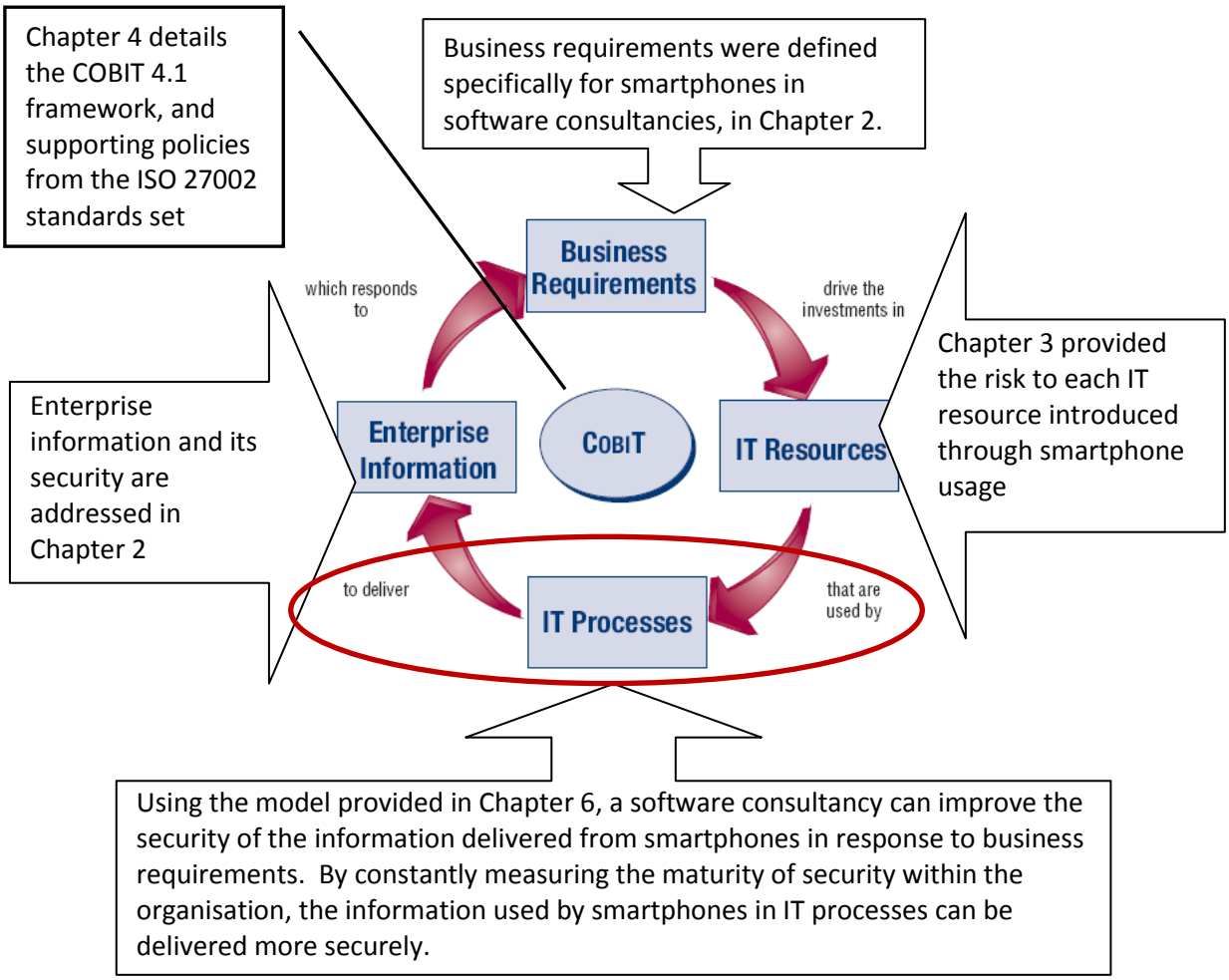


Figure 36 - Research project outcomes

In Figure 36 above highlights key chapters of this research project are presented where they focus on one of the major principles of the COBIT 4.1 framework.

7.3 An evaluation of the research outcomes

At the onset of this research project, three research questions were provided in section 1.3 and 1.4. These questions have remained the guiding focus, for the direction in which every step of this project has taken. Topics which were not found to be adding value to one of these questions were either removed or refocused. In order to evaluate the success of this research project, an assessment of each of these questions was undertaken. If each of these questions has been answered, then the research project has fulfilled its original intentions.

The primary research question is:

> *How can a software consultancy organisation measure the vulnerability gaps that exist between its existing security solution, and a smartphone security solution so it conforms to both the COBIT 4.1 framework and the ISO27002 standards?*

This question is asked as the primary question for this study. The answer to this question forms the primary output for the research project. In response, a model was developed, which seeks to provide the answer to this question. The model allows a software consultancy to measure any gaps that exist between its current security solution and one that encompasses components from both the COBIT 4.1 framework and ISO27002 standards. Through the model, a solution has been provided which satisfies this question.

Secondary research questions directly related to the primary question were identified. These questions complemented the solution and formed a significant part of the research project.

The first research sub-question is:

> *What are the specific security requirements of smartphones in software consultancy organisations?*

By combining the findings of both the primary and secondary data collection, a specific set of security requirements of smartphones, within software consultancy organisations, was established. The literature survey identified generic risk areas for smartphone devices, while the primary data collected from each of the case study respondents provided an insight into the specific requirements of software consultancies.

The question asks what the specific security requirements of smartphones in software consultancies are. The findings of the empirical study provide ample evidence of the specific requirements for all areas of risk management of smartphone devices. This

question has been comprehensively covered from a generic smartphone security requirement level, and all the way through to the specific requirements of software consultancy organisations.

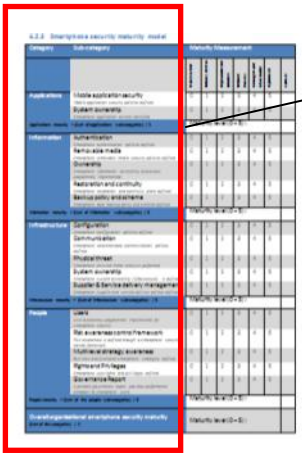
Seven specific requirements were identified in Chapter 3. The specific requirements were found to consist of the following:

- Mobile application security
- Authentication
- Removable media
- Configuration
- Communication
- Physical threat
- Users

The second research sub-question is:

> *What components from the COBIT 4.1 framework and ISO27002 standards are most significant to a security solution that includes smartphone security?*

This question seeks to identify only the components, from each of the frameworks, which are significant to smartphone security. In order to achieve this, the COBIT 4.1 framework processes that target risk management as a primary objective were identified. These processes were then mapped to the ISO27002 control objectives using the official mapping document provided by COBIT 4.1.



The most relevant components to smartphone security were combined from both the primary and secondary data sources. These items are the measurable component of the maturity model.

Figure 37 - Components identified

From this, the relevant objectives from the ISO27002 standard were identified. Finally, the activity statements for each of these COBIT 4.1 processes were adapted to place the smartphone as the focus of each activity. This allowed the most significant components to be identified using a questionnaire as part of each of the case studies conducted.

Items from the following COBIT 4.1 processes were identified for incorporation into the model: PO4, PO6, PO9 DS2, DS4, DS5, DS11 and ME5. ISO27002 items mapped to these processes are listed in

Table 6. Thus, this sub-question has been successfully answered in this research.

The third research sub-question was:

> *How can the gap between an existing security solution and one that conforms to both COBIT 4.1 and ISO27002 be measured in a software consultancy organisation?*

The maturity measurement scale provided in the research model allows software consultancy organisations to measure their current security solution as it is. Targets can be set to give the organisation an idea of where it needs to be, in order to provide adequate levels of smartphone security. When used as part of a continuous measurement and improvement programme, such as the recommended measurement process, this provides a formidable method of closing such a gap.

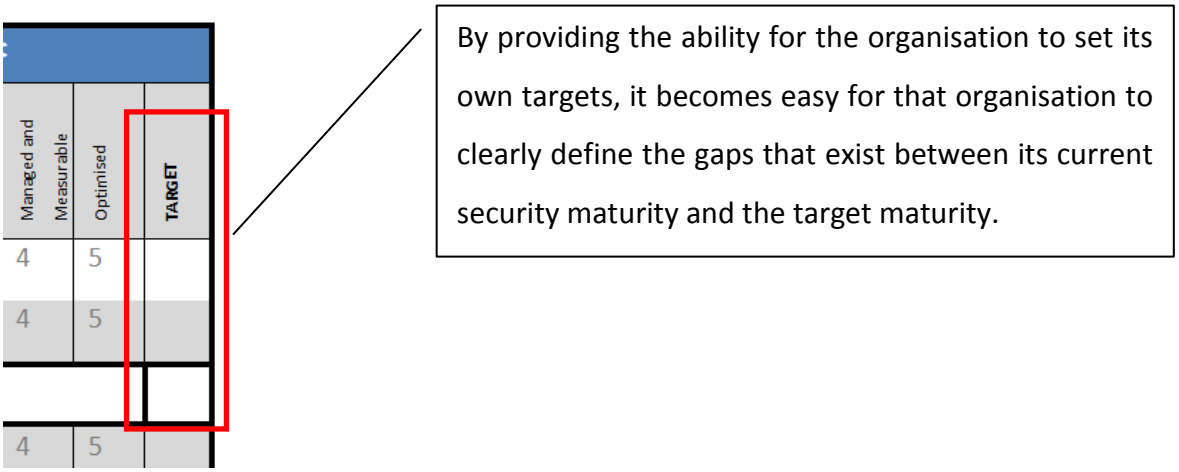


Figure 38 - Measuring maturity gaps

Each of the questions set out at the onset of this research have therefore been adequately addressed by the research project.

7.4 Directions for future research

There were many directions in which this research project might have digressed, had the main research question not maintained focus. This section will detail a number of areas in which future research might be able to build upon this research project.

The research model provides a method of measuring the maturity level of various components of smartphone security. Future research could be focused towards identifying the COBIT 4.1 processes, and ISO27002 control objectives, which best raise the maturity level of each of the measurable items of the model. This would provide users, of the model, with a defined set of activities that could be performed to assist in archiving target maturity for that measureable.

Providing specific instructions for increasing the maturity of each of the measureable components of the maturity model is a natural progression for this research topic. Specific actionable instructions would remove the requirement of interpreting the instructions of the COBIT 4.1 framework, and ISO27002 standard, for smartphone security.

Future research might be directed at translating each of the action statements of the COBIT 4.1 processes and ISO27002 control objectives to specifically target smartphone security. These frameworks provide generic security recommendations, often difficult to apply to smartphone security requirements. Research in this area might assist in providing specific instruction for smartphone security so that compliance with these framework recommendations is achieved.

Future research could be directed at refining the model through a deeper analysis of the recommendations of the ISO27002 processes provided in Chapter 4. This would provide a detailed set of instructions for the 'react' component of the recommended maturity process.

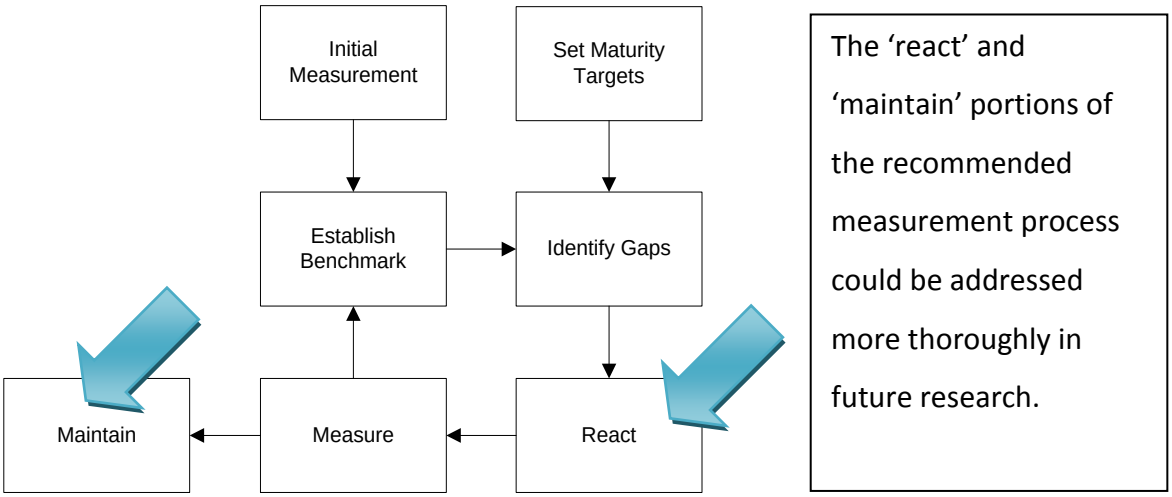


Figure 39 – Measurement process enhancements

Employee awareness is highlighted as a critical factor in ensuring the success of a security solution. Future research could be targeted at formulating strategies to enhance employee awareness of the security measurable highlighted in the model. The ability to measure these components is provided in the model, and people form a core part of the measurable components. However, maintaining the awareness of security in employees, and translating this into a security culture, is an excellent direction in which future research could be focused.

In conclusion, the following suggested directions for future research are:

- Identifying components from each of the framework documents most significant to maturing each of the measureable components.
- Translate each actionable recommendation of both frameworks, such that they provide smartphone specific security recommendations.
- Enhance the model further through the recommendations of the processes from the ISO27002 standard, which were identified in Chapter 4.
- Employee awareness of the purpose and requirements of the model and its components as a direction of future study.

7.5 Concluding note

This research project provided a model for measuring the maturity of smartphone security in software consultancy organisations. This model provides an excellent method of measuring the maturity of smartphone security at these organisations. Software consultancy organisations can use this model to identify which components of their smartphone security are not meeting their target maturity level.

Ensuring that smartphones are not a weak link in the chain of security at an organisation is paramount to the protection of the information at that organisation. Regular assessment of all security components is vital in ensuring an ongoing security solution. Using the model provided by this research project, the smartphone component is capable of active ongoing maturity measurement.

Finally, employees, management, clients and customers will only benefit by efforts to improve smartphone security. Through the work of this research project, smartphone security in software consultancies can be both measured and improved. Software consultancies can now embrace this innovative and exciting technological advancement, without fearing it.

Reference list

Al Aboodi, S. S. (2006). A New Approach for Assessing the Maturity of Information Security. *Information Systems Control Journal , 3* (1), 1-4.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers and Security , 26* (4), 276-289.

Best, J. (2006, February 13). *Analysis: What is a smart phone?* Retrieved August 14, 2008, from Silicon.com: http://networks.silicon.com/mobile/0,39024665,39156391,00.htm

Botha, R., Furnell, S., & Clarke, N. (2009). From desktop to mobile: Examining the security experience. *Computers & Security , 28* (3-4), 130-137.

Brotby, K. (2007). Information Security Governance: Who Needs It? *Information Systems Control Journal , 2* (1), 1-2.

Clarke, N., & Furnell, S. (2007). Advanced user authentication for mobile devices. *Computers and Security , 26* (2), 109-119.

Collis, J., & Hussey, R. (2003). *Business Research: A practical guide for undergraduate and postgraduate students* (2nd Edition ed.). New York: Palgrove Macmillan.

Congdon, J., & Dunham, A. (1999). Defining the Beginning:The Importance of Research Design. (K. Eckert, K. Bjorndal, F. Abreu-Grobois, & M. Donnelly, Eds.) *Research and Management Techniques for the Conservation of Sea Turtles , 1*, pp. 1-5.

Davis, A. (2006). Information security can enable mobile working. *Infosecurity Today , 3* (4), 42.

Dingsøyr, T. (2002). Knowledge Management in Medium-Sized Software Consulting Companies. *Empirical Software Engineering , 7* (4), 383-386.

Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers and Security , 25* (1), 55-63.

Dunn, D. (2007). Mobility: Securing devices on the run. (P. Watson, E. Feretic, & E. Cone, Eds.) *Innovations , 2007* (5), pp. 18-19.

Elgan, M. (2007, March 12). *It's time we stopped talking about "smartphones"*. Retrieved May 05, 2009, from techworld.com: http://www.techworld.com/mobility/features/index.cfm?featureid=3204

Furnell, S. (2005). Handheld hazards: The rise of malware on mobile devices. *Computer Fraud & Security , 2005* (5), 4-8.

Furnell, S., & Thomson, K.-L. (2009). Recognising the varying user acceptance of IT security. *Computer Fraud & Security* (2), 5-10.

Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers and Security , 25* (1), 27-35.

Garbani, J.-P., Koetzle, L., & Powell, T. (2006, April 26). *ITIL, CoBIT and ISO: Overlap Or Complement?* Retrieved July 11, 2008, from IT Service Today: http://itservicetoday.blogs.com/itil/2006/04/itil_cobit_and_.html

Gartner. (2009). *Gartner Glossary*. Retrieved December 7, 2009, from Gartner: http://www.gartner.com/6_help/glossary/GlossaryS.jsp

Greenhalgh, T., & Taylor, R. (1997, September 20). *How to read a paper: Papers that go beyond numbers (qualitative research)*. Retrieved August 05, 2008, from BMJ: http://www.bmj.com/cgi/content/full/315/7110/740

Hughes, M., & Stanton, R. (2006). Winning security policy acceptance. *Computer Fraud & Security , 2006* (5), 17-19.

Hunter, P. (2008, June 6). *Central support goes into the field.* Retrieved December 16, 2009, from The Institution of Engineering and Technology: http://kn.theiet.org/magazine/issues/0801/mobile.cfm

Isaksen, A. (2004). Knowledge-based Clusters and Urban Location: The Clustering of Software Consultancy in Oslo. *Urban Studies , 41* (5/6), 1157-1174.

IsecT Ltd. (2008). *ISO/IEC 27002 code of practice*. Retrieved August 2, 2009, from isect.com: http://www.iso27001security.com/html/27002.html#39controlObjectives

ISO 17799 News. (2006). *ISO17799 News. A Short History of ISO 17799.* Retrieved June 24, 2009, from ISO 17799 News: http://17799-news.the-hamster.com/issue10-news7.htm

IT Governance Institute. (2007b). *COBIT 4.1.* Rolling Meadows: IT Governance Institute.

IT Governance Institute. (2007a). COBIT 4.1 Executive Summary. Rolling Meadows, Illinois, USA.

IT Governance institute. (2006). *Mapping of ISO/IEC 17799:2005 with COBIT 4.0.* Rolling Meadows, IL: IT Governance institute.

Johnson, J. (2009). *Memory Cards for Your PDA; Expand Your PDA's Storage Potential*. Retrieved July 21, 2009, from About.com: http://palmtops.about.com/od/accessoriesperipherials/ss/flashcards.htm

Jürjens, J., Schrek, J., & Bartmann, P. (2008). Model-based Security Analysis for Mobile Communications. *International Conference on Software Engineering* (pp. 683-692). Leipzig, Germany: Association for Computing Machinery (ACM).

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: a contextual perspective. *Computers and Security , 24* (3), 246-260.

Khokhar, R. (2006). Smartphones – a call for better safety on the move. *Network Security , 2006* (4), 6-7.

Kooser, A. C. (2007, August). Safe Trip. *Entrepreneur Magazine , 1*, p. 28.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security , 27* (5-6), 224-231.

Kruger, H. A., & Kearny, W. D. (2008). Consensus ranking – An ICT security awareness case study. *Computers and Security , 27* (7-8), 254-159.

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers and Security , 28* (3-4), 215-228.

Lim, E. (2007, December). Security policies must keep pace with business mobility. *Network World Asia , December 2007*, p. 12.

Mahoney, C. (2009, January). Talk Generation Y's Language. *HR Magazine , January 2009*, p. 25.

Martins, A., & Eloff, J. (2001). *Information security culture.* Retrieved February 18, 2009, from Rand Afrikaans University: http://etd.rau.ac.za/theses/available/etd-04292004-110222/restricted/SEC2002FinalVersion.pdf

McCall, M. (2006, April 01). *Industry grapples with smartphone security*. Retrieved August 05, 2008, from Wirelessweek.com: http://www.wirelessweek.com/industry-grapples-with-smartphone.aspx

Morgan, G., & Smircich, L. (1980). The case for qualitative research. *The academy of management review , 5* (4), 491-500.

Musaji, Y. (2006). A Holistic Definition of IT Security—Part 2. *Infromation Controls Journal (ISACA)* .

Myers, M. D. (1997, May 20). *Qualitative Research in Information Systems*. Retrieved July 22, 2008, from MISQ Discovery: http://www.misq.org/discovery/MISQD_isworld/

Neill, J. (2006, July 05). *Analysis of Professional Literature Class 6: Qualitative Research I*. Retrieved August 05, 2008, from Wilderdom.com: http://www.wilderdom.com/OEcourses/PROFLIT/Class6Qualitative1.htm

Olivier, M. (2004). *Infromation Technology Research* (2nd Edition ed.). Pretoria, South Africa: Van Schaik.

Olzak, T. (2006, April). *Strengthen Security with an Effective Security Awareness Program.* Retrieved February 15, 2009, from Adventuresinsecurity.com: http://adventuresinsecurity.com/Papers/Build_a_Security_Awareness_Program.pdf

Pahl, A. (2009, April/May). *The business case for smartphones.* Retrieved May 26, 2009, from titletown.org: http://www.titletown.org/resources/bbjtechwatch.pdf

Pironti, J. (2005, April). Minimizing New Risks the Old-Fashioned Way. *Wireless Week , April 2005*, p. 31.

Post, G. V., & Kagan, A. (2007). Evalutating information security tradeoffs: Restricting access can interfere with user tasks. *Computers and Security , 26* (3), 229 - 237.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science , 27* (2), 183-213.

Reardon, M. (2007, November 13). *Smartphone sales skyrocket*. Retrieved July 02, 2008, from CNet.com: http://news.cnet.com/8301-10784_3-9816072-7.html

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers and Security , 26* (1), 56-62.

Sacco, A. I. (2008, February 15). Remote workers pose rising security threat. *CIO , 21* (9), p. 12.

Sharma, B. (2007). Mobile management beyond the office walls. *Siliconindia , July 2007*, 28-29.

Standards South Africa. (2005). *SANS 17799:2005.* Pretoria: Standards South Africa.

Stanley, R. (2004). Security, Audit and Control Issues for Managing Risk in the Wireless LAN Environment. *Infromation Systems Control Journal , 3* (1).

Stephen, L. (1868). *Cornhill Magazine* (Vol. XVII). London: Smith, Elder & Co.

Sweren, S. H. (2006). ISO 17799: Then, Now and in the Future. *Information Systems Control Journal , 1* (1), 34-37.

Tellis, W. (1997). Introduction to case study. *The Qualitative Report , 3* (2), 1.

The centre for public service innovation. (2003). *Government unplugged.* South African Government, State Information Technology Agency. World Wide Worx.

Yeo, V. (2008, April 14). *Tech-savvy workers to make IT decisions in future*. Retrieved July 11, 2008, from Silicon.com: http://management.silicon.com/careers/0,39024671,39187852,00.htm

Yusuf, M. (2006). A Holistic Definition of IT Security. *Information Systems Control Journal , 3* (1).

Glossary

Word	Meaning
Acceptance	The act of accepting with approval; favourable reception
Accessibility	The quality of being at hand when needed
Authentication	Validating the authenticity of something or someone
Availability	The quality of being at hand when needed
Confidentiality	Discretion in keeping secret information
Control	The activity of managing or exerting control over something
Deviation	A variation that deviates from the standard or norm
Domain	The content of a particular field of knowledge
Framework	A hypothetical description of a complex entity or process
Governance	The act of governing; exercising authority
Integrity	An undivided or unbroken completeness or totality with nothing wanting
Maturity	State of being mature; full development
Paradigm	The generally accepted perspective of a particular discipline at a given time
Patch (software)	A short set of commands to correct a bug in a computer program
PIN	A number you choose and use to gain access to various accounts
Qualitative	Relating to or involving comparisons based on qualities
Quantitative	Relating to the measurement of quantity

Appendix A – Question statements

Question number	COBIT process	Original question statement and altered statement below in bold
1	PO4	Establish IT organisational structure, including committees and linkages to the stakeholders and vendors. **An IT organisational structure, including committees and linkages to smartphone stakeholders and smartphone vendors, has been established.**
2	PO4	Design an IT process framework. **A smartphone process framework has been developed.**
3	PO4	Identify system owners. **Smartphone system owners have been identified.**
4	PO4	Identify data owners. **Smartphone users are aware of who owns the data processed and stored on their device.**
5	PO4	Establish and implement IT roles and responsibilities, including supervision and segregation of duties. **IT roles and responsibilities have been established, that include the supervision and segregation of duties when using smartphones and smartphone applications.**
6	PO6	Establish and maintain an IT control environment and framework. **A smartphone control environment and framework has been established, and is being maintained.**
7	PO6	Develop and maintain IT policies.

		Smartphone policies have been developed and are being maintained.
8	**PO6**	Communicate the IT control framework and IT objectives and direction. **Smartphone control frameworks, objectives and direction have been communicated to smartphone users.**
9	**PO9**	Determine risk management alignment (e.g., assess risk). **A smartphone risk assessment (risk management alignment) has been determined.**
10	**PO9**	Understand relevant strategic business objectives. **The relative strategic business objectives of smartphones are understood.**
11	**PO9**	Understand relevant business process objectives. **Relevant smartphone business process objectives are understood.**
12	**PO9**	Identify internal IT objectives, and establish risk context. **The internal objectives of smartphones have been identified, and a smartphone risk context has been established.**
13	**PO9**	Identify events associated with objectives **Events associated with smartphone objectives have been identified**
14	**PO9**	Assess risk associated with events. **Smartphone risks associated with events have been assessed.**
15	**PO9**	Evaluate and select risk responses.

		Smartphone risks responses have been selected and evaluated.
16	**PO9**	Prioritise and plan control activities. **Smartphone control objectives have been planned and prioritised.**
17	**PO9**	Approve and ensure funding for risk action plans. **Funding for smartphone risk action plans has been approved and ensured.**
18	**PO9**	Maintain and monitor a risk action plan. **A smartphone risk action plan is being maintained and monitored.**
19	**DS2**	Identify and categorise third-party service relationships. **Third party smartphone service relationships have been identified and categorised.**
20	**DS2**	Define and document supplier management processes. **Smartphone supplier management processes have been defined and documented.**
21	**DS2**	Establish supplier evaluation and selection policies and procedures. **Smartphone supplier evaluation and selection policies and procedures have been established**
22	**DS2**	Identify, assess and mitigate supplier risks. **Smartphone supplier risks have been identified and mitigated.**
23	**DS2**	Monitor supplier service delivery. **Smartphone supplier service delivery is monitored.**

24	**DS2**	Evaluate long-term goals of the service relationship for all stakeholders. **The long-term goals of the smartphone service relationship for all stakeholders has been evaluated.**
25	**DS4**	Develop an IT continuity framework. **An IT continuity framework has been developed, and this framework includes smartphones.**
26	**DS4**	Conduct a business impact analysis and risk assessment. **A business impact analysis and risk assessment has been conducted for smartphone devices.**
27	**DS4**	Develop and maintain IT continuity plans. **IT Continuity plans which include the role of smartphones, have been developed, and are being maintained.**
28	**DS4**	Identify and categorise IT resources based on recovery objectives. **Smartphone resources that are based on recovery objectives, have been identified and categorised.**
29	**DS4**	Define and execute change control procedures to ensure that the IT continuity plan is current. **Change control procedures that ensure the role of smartphones in the IT continuity plan are current, have been defined, and are being followed.**
30	**DS4**	Regularly test the IT continuity plan. **The smartphone component of the IT Continuity plan is regularly tested.**
31	**DS4**	Develop a follow-on action plan from test results.

		A follow-on action plan for smartphones from test results has been developed.
32	**DS4**	Plan and conduct IT continuity training. **The role of smartphones in IT Continuity training is planned for and conducted.**
33	**DS4**	Plan IT services recovery and resumption. **The role of smartphones in IT services recovery and resumption has been planned for.**
34	**DS4**	Plan and implement backup storage and protection. **Smartphone information backup storage and protection has been planned for and implemented.**
35	**DS4**	Establish procedures for conducting post-resumption reviews. **Procedures for conducting post-resumption reviews of the role of smartphones have been established.**
36	**DS5**	Define and maintain an IT security plan. **The role of smartphones is defined in an IT security plan.**
37	**DS5**	Define, establish and operate an identity (account) management process. **An identity management process for smartphone devices has been defined and established, and is in operation.**
38	**DS5**	Monitor potential and actual security incidents. **Potential and actual smartphone security incidents are being monitored.**
39	**DS5**	Periodically review and validate user access rights and privileges.

		Smartphone user access rights and privileges are periodically reviewed and validated.
40	**DS5**	Establish and maintain procedures for maintaining and safeguarding cryptographic keys. **Procedures for maintaining and safeguarding cryptographic keys used for smartphone information have been established and are being maintained.**
41	**DS5**	Implement and maintain technical and procedural controls to protect information flows across networks. **Technical and procedural controls to protect the flow of information from smartphones across networks, are implemented and are being maintained.**
42	**DS5**	Conduct regular vulnerability assessments. **Smartphone vulnerability assessments are regularly conducted.**
43	**DS11**	Translate data storage and retention requirements into procedures. **Smartphone information data storage and retention requirements have been translated into procedures.**
44	**DS11**	Define, maintain and implement procedures to manage the media library. **Procedures to maintain the smartphone media library have been defined, maintained and implemented.**
45	**DS11**	Define, maintain and implement procedures for secure disposal of media and equipment **Procedures for the secure disposal of smartphone media and equipment have been defined, maintained and implemented.**

46	**DS11**	Back up data according to scheme. **Smartphone data is backed up according to scheme.**
47	**DS11**	Define, maintain and implement procedures for data restoration. **Procedures for smartphone data restoration have been defined, maintained and implemented.**
48	**DS12**	Define the required level of physical protection. **The required level of physical protection of smartphone devices has been defined.**
49	**DS12**	Implement physical environment measures. **Measures have been implemented within the physical environment to mitigate smartphone risk.**
50	**DS12**	Define and implement procedures for physical access authorisation and maintenance. **Smartphone physical access authorisation and maintenance procedures have been defined and implemented.**
51	**ME2**	Monitor and control IT internal control activities. **Smartphone internal control activities are monitored and controlled.**
52	**ME2**	Monitor the self-assessment process. **Smartphone self-assessment processes exist and are monitored.**
53	**ME2**	Monitor the performance of independent reviews, audits and examinations. **Independent smartphone reviews, audits and examinations are monitored.**

54	**ME2**	Monitor the process to obtain assurance over controls operated by third parties. **The process of obtaining assurance over smartphone controls operated by third parties is monitored.**
55	**ME2**	Monitor the process to identify and assess control exceptions. **The process to identify and assess smartphone control exceptions is monitored.**
56	**ME2**	Monitor the process to identify and remediate control exceptions. **The process to identify and remediate smartphone control exceptions is being monitored.**
57	**ME2**	Report to key stakeholders. **The role of smartphones is reported to key stakeholders.**
58	**ME3**	Define and execute a process to identify legal, contractual, policy and regulatory requirements. **The process to identify legal, contractual, policy and regulatory requirements of smartphones, has been defined and executed.**
59	**ME3**	Evaluate compliance of IT activities with IT policies, plans and procedures. **Smartphone activities are evaluated for compliance with IT policies, plans and procedures.**
60	**ME3**	Report positive assurance of compliance of IT activities with IT policies, plans and procedures. **Positive assurance of smartphone compliance of IT activities, with IT policies, plans and procedures is reported.**
61	**ME3**	Provide input to align IT policies, plans and procedures in response to compliance

		requirements. **Input is provided to align smartphone policies, plans and procedures in response to compliance requirements.**
62	**ME3**	Integrate IT reporting on regulatory requirements with similar output from other business functions. **Smartphone reporting on regulatory requirements with similar output from other business functions is integrated.**
63	**ME5**	Establish executive and board oversight and facilitation over IT activities. **Executive and board oversight, and facilitation over smartphone activities, is established.**
64	**ME5**	Review, endorse, align and communicate IT performance, IT strategy, and resource and risk management with business strategy. **Smartphone performance, smartphone strategy and smartphone resource and risk management is reviewed, endorsed, aligned and communicated with business strategy.**
65	**ME5**	Obtain periodic independent assessment of performance and compliance with policies, plans and procedures. **Independent assessment of smartphone performance and compliance with policies, plans and procedures is periodically obtained.**
66	**ME5**	Resolve findings of independent assessments, and ensure management's implementation of agreed-upon recommendations. **Independent smartphone assessments are resolved, and management implement agreed upon recommendations.**

67	**ME5**	Generate an IT governance report. **An IT governance report has been generated and includes feedback on the performance of smartphones.**
Omitted questions below		
68	**DS12**	*Select and commission the site (data center, office, etc.).*
69	**DS12**	*Manage the physical environment (maintaining, monitoring and reporting included).*

Appendix B – Response scores by question (Rounded)

Question	All Respondents	Responsible for security requirements	Not Responsible for security requirements
1	0.86	0.89	0.85
2	1.10	1.44	0.95
3	1.24	1.67	1.05
4	1.31	1.33	1.30
5	0.97	1.00	0.95
6	1.14	1.22	1.10
7	0.93	0.89	0.95
8	1.00	1.00	1.00
9	0.90	1.22	0.75
10	1.07	2.11	0.60
11	1.10	1.67	0.85
12	0.86	0.78	0.90
13	1.07	1.22	1.00
14	1.14	1.78	0.85
15	0.93	1.33	0.75
16	0.86	1.00	0.80
17	0.62	0.89	0.50
18	0.79	1.00	0.70
19	0.52	0.67	0.45
20	0.62	0.33	0.75
21	0.62	0.44	0.70

22	0.48	0.33	0.55
23	0.55	0.33	0.65
24	0.55	0.33	0.65
25	1.10	1.22	1.05
26	1.10	1.44	0.95
27	0.83	1.00	0.75
28	0.55	0.56	0.55
29	0.55	1.00	0.35
30	0.55	0.56	0.55
31	0.62	0.78	0.55
32	0.59	0.67	0.55
33	0.62	0.44	0.70
34	1.14	1.44	1.00
35	0.52	0.78	0.40
36	0.86	1.00	0.80
37	0.76	1.00	0.65
38	0.76	0.78	0.75
39	0.90	0.67	1.00
40	0.79	0.89	0.75
41	1.00	1.22	0.90
42	0.97	1.11	0.90
43	0.86	1.33	0.65
44	0.55	0.44	0.60
45	0.83	1.11	0.70
46	1.07	1.67	0.80
47	1.03	1.56	0.80

48	0.86	1.22	0.70
49	0.90	1.11	0.80
50	0.97	1.44	0.75
51	0.69	1.11	0.50
52	0.41	0.56	0.35
53	0.38	0.78	0.20
54	0.28	0.56	0.15
55	0.52	0.44	0.55
56	0.34	0.56	0.25
57	0.79	1.22	0.60
58	0.93	0.89	0.95
59	1.00	1.22	0.90
60	0.83	1.00	0.75
61	0.76	1.00	0.65
62	0.76	1.00	0.65
63	0.62	0.78	0.55
64	0.97	1.33	0.80
65	0.45	0.56	0.40
66	0.45	0.44	0.45
67	0.83	0.56	0.95