

**A STRUCTURED APPROACH TO THE IDENTIFICATION OF THE SIGNIFICANT
RISKS RELATED TO ENTERPRISE MOBILE SOLUTIONS AT A MOBILE
TECHNOLOGY COMPONENT LEVEL**

by

Lize-Marie Sahd

*Thesis presented in partial fulfilment of the requirements for the degree of Master of
Commerce (Computer Auditing) in the Faculty of Economic and Management
Sciences at Stellenbosch University*



Supervisor: Riaan J Rudman

March 2015

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

Date: 3 November 2014

ACKNOWLEDGEMENTS

It is with the most sincere gratitude that I want to thank the following:

- My Father, for being true to Your word and directing my paths.
- My parents, for giving me wings. Your endless faith, support and guidance throughout my academic career has made all of this possible.
- My husband, Monty, for supporting and loving me unconditionally and for being my ever-needed voice of reason, my rock and my quiet place.
- My daughter, Nina, for being my inspiration and the giggle at the end of every long day.
- My study leader, Riaan, for selflessly sharing your experience and knowledge with me over the years.

ABSTRACT

The consumerisation of mobile technology is driving the mobile revolution and enterprises are forced to incorporate mobile solutions into their business processes in order to remain competitive. While there are many benefits relating to the investment in and use of mobile technology, significant risks are also being introduced into the business. The fast pace of technological innovation and the rate of adoption of mobile technology by employees has, however, created an environment where enterprises are deploying mobile solutions on an *ad hoc* basis. Enterprises are only addressing the risks as they are occurring and resulting in losses. The key contributing factor to this lack of governance and management is the fact that those charged with governance do not understand the underlying mobile technology components.

The purpose of this research is to improve the understanding of the underlying components of mobile technology. The research further proposes to use this understanding to identify the significant risks related to mobile technology and to formulate appropriate internal controls to address these risks. The findings of the research identified the following underlying components of mobile technology: mobile devices; mobile infrastructure, data delivery mechanisms and enabling technologies; and mobile applications. Based on an understanding of the components and subcategories of mobile technology, a control framework was used to identify the significant risks related to each component and subcategory. The significant risks identified included both risks to the users (including interoperability, user experience, connectivity and IT support) as well as risks to the enterprise's strategies (including continuity, security, cost and data ownership). The research concludes by formulating internal controls that the enterprise can implement to mitigate the significant risks. This resulted in two matrixes that serve as quick-reference guides to enterprises in the identification of significant risks at an enterprise specific mobile technology component level, as well as the relevant internal controls to consider. The matrixes also assist enterprises in determining the best mobile solutions to deploy in their business, given their strategies, risk evaluation and control environment.

UITTREKSEL

Die mobiele revolusie word deur die verbruiker van mobiele tegnologie aangedryf en, ten einde kompetender te bly, word ondernemings gedwing om mobiele tegnologie in hul besigheidsprosesse te implementeer. Terwyl daar baie voordele verbonde is aan die investering in en gebruik van mobiele tegnologie, word die besigheid egter ook blootgestel aan wesenlike risiko's. Die vinnige tempo waarteen mobiele tegnologie ontwikkel en deur werknemers aangeneem word, het egter 'n omgewing geskep waarin ondernemings mobiele tegnologie op 'n *ad hoc* basis ontplooi. Besighede spreek eers die risiko's aan nadat dit reeds voorgekom het en verliese as gevolg gehad het. Die hoof bydraende faktor tot die tekort aan beheer en bestuur van mobiele tegnologie is die feit dat diegene verantwoordelik vir beheer, nie onderliggend mobiele tegnologie komponente verstaan nie.

Die doel van hierdie navorsing is om die begrip van die onderliggende komponente van mobiele tegnologie te verbeter. Die navorsing poog verder om die wesenlike risiko's verbonde aan mobiele tegnologie te identifiseer en om toepaslike interne beheermaatreëls te formuleer wat die risiko's sal aanspreek. Die bevindinge van die navorsing het die volgende onderliggende komponente van mobiele tegnologie geïdentifiseer: mobiele toestelle; mobiele infrastruktuur, data aflewering-meganismes, en bemagtigende tegnologieë; en mobiele toepassings. Gebaseer op 'n begrip van die komponente en subkategorieë van mobiele tegnologie, is 'n kontrole raamwerk gebruik om die wesenlike risiko's verbonde aan elke komponent en subkategorie van die tegnologie, te identifiseer. Die wesenlike risiko's sluit beide risiko's vir die gebruiker (insluitend kontinuïteit, gebruikerservaring, konektiwiteit en IT ondersteuning) sowel as risiko's vir die onderneming se strategieë (insluitend kontinuïteit, sekuriteit, koste en data eienaarskap) in. Die navorsing sluit af met die formulering van die beheermaatreëls wat geïmplementeer kan word om die wesenlike risiko's aan te spreek. Dit het gelei tot twee tabelle wat as vinnige verwysingsraamwerke deur ondernemings gebruik kan word in die identifisering van wesenlike risiko's op 'n onderneming-spesifieke tegnologie komponentvlak asook die oorweging van relevante interne beheermaatreëls. Die tabelle help ondernemings ook om die beste mobiele tegnologie vir hul besigheid te implementeer, gebaseer op hul strategie, risiko evaluering en beheeromgewing.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION AND RESEARCH OBJECTIVE	1
1.1 Introduction and background	1
1.2 Problem statement and research objective	2
1.3 Scope limitations	3
1.4 Organisational structure of the research	3
CHAPTER 2: RESEARCH DESIGN AND METHODOLOGY	5
CHAPTER 3: LITERATURE REVIEW	8
3.1 Historic review of prior research	8
3.2 Mobility and the mobile enterprise	10
3.3 Benefits of mobile technology to the enterprise	11
3.4 Considerations in the deployment of mobile solutions	12
3.5 Corporate governance and the governance of mobility	13
3.5.1 Corporate governance	13
3.5.2 IT governance	14
3.5.3 IT gap	16
3.5.4 Alignment	16
3.5.5 Governance of mobility	17
3.6 Control frameworks	17
3.6.1 Considerations when implementing control frameworks	17
3.6.2 Control frameworks reviewed	18
3.6.3 An overview of COBIT	18
3.6.4 An overview of ITIL	20
3.6.5 An overview of the ISO/IEC 27000-series	21
3.6.5.1 ISO/IEC 27000:2014	22
3.6.5.2 ISO/IEC 27001:2013	22
3.6.5.3 ISO/IEC 27002:2013	22
3.6.5.4 ISO/IEC 27005:2011	24
3.6.5.5 ISO/IEC 27014:2013	24

3.6.6	Benefits and limitations of the reviewed control frameworks	25
3.6.7	Framework selected for the purposes of this research	26
3.7	Summary and conclusion	26
CHAPTER 4: MOBILE SOLUTION COMPONENTS		27
4.1	Mobile devices	28
4.1.1	Types of mobile devices	28
4.1.2	Categories of mobile devices	30
4.1.2.1	Corporate owned business only (COBO)	30
4.1.2.2	Corporate owned personally enabled (COPE)	31
4.1.2.3	Bring your own device (BYOD)	32
4.1.3	Comparison of mobile device deployment categories	33
4.2	Infrastructure, delivery mechanisms and enabling technologies	34
4.2.1	Mobile networks	34
4.2.1.1	Categories of mobile networks	34
4.2.2	Data delivery mechanisms	35
4.2.2.1	Data delivery connections	35
4.2.2.2	Categories of data delivery mechanisms	36
4.2.3	Enabling technologies	37
4.2.3.1	Synchronisation technologies	37
4.2.3.2	Virtualisation technologies	37
4.2.3.3	Cloud technologies	38
4.3	Mobile applications	39
4.3.1	Mobile operating systems and platforms	39
4.3.1.1	Types of mobile operating systems	40
4.3.1.2	Categories of mobile operating systems	42
4.3.2	Application frameworks	43
4.3.3	Mobile applications	43
4.3.3.1	Types of mobile applications	44
4.3.3.2	Mobile application categories	45
4.4	Summary and conclusion	47

CHAPTER 5: RISKS RELATED TO THE DEPLOYMENT OF MOBILE SOLUTIONS	48
5.1 Inadequate governance and management of mobile solutions	48
5.2 Significant risks on an operational level	49
5.2.1 Interoperability	49
5.2.2 User experience	50
5.2.3 Connectivity	51
5.2.4 IT support	52
5.2.5 Continuity	52
5.2.6 Security	53
5.2.7 Cost	56
5.2.8 Data ownership	57
5.3 Less significant risks	58
5.3.1 Licensing	58
5.3.2 Litigation	58
5.3.3 Data retention	58
5.4 Summary and conclusion	58
CHAPTER 6: CONTROLS IN A MOBILE ENVIRONMENT	61
6.1 Mobile solution governance	61
6.1.1 Mobile strategy and related policies	62
6.1.2 Training	64
6.2 Mobile solution management systems	64
6.2.1 Enterprise mobility management system (EMM system)	64
6.3 Mobile solution operational control techniques	66
6.3.1 Mobile device controls	66
6.3.2 Communication controls	68
6.3.3 Application and other software controls	70
6.3.4 Data controls	72
6.4 Summary and conclusion	73
CHAPTER 7: CONCLUSION	79
REFERENCES	81

LIST OF FIGURES, TABLES AND APPENDICES

Figures

Figure 1: The core components of mobile solutions	27
Figure 2: The building blocks of mobile application layer	39

Tables

Table 1: The benefits and limitations of COBIT, ITIL and the ISO/IEC 27000-series	25
Table 2: A comparison of BYOD, COPE and COBO approaches to mobile device deployment	33
Table 3: The characteristics of push and pull data delivery mechanisms	37
Table 4: The significant characteristics of mobile operating systems	42
Table 5: Types of mobile applications	44
Table 6: The characteristics of leading mobile operating systems	45
Table 7: A comparison of the benefits and limitations of mobile application development categories	47
Table 8: A risk-component matrix: linking the underlying components of mobile technologies to the relevant significant risk it gives rise to	60
Table 9: A risk-control matrix: linking the significant mobile solution risks to the relevant mitigating internal controls	74

Appendices

Appendix A: A summary of COBIT's detailed processes	92
Appendix B: The benefits and limitations of reviewed control frameworks	97
Appendix C: Using COBIT to identify significant mobile solution risks	101

CHAPTER 1: INTRODUCTION AND RESEARCH OBJECTIVE

1.1 Introduction and background

Mobile technology is not a new innovation. The unprecedented rate at which mobile technology is developing, and the extent of its proliferation has, however, started a new phenomenon, referred to by IFS (2013) as the '*mobile revolution*'. From this revolution, the mobile enterprise is emerging and it is fundamentally changing communication, collaboration and the way business is conducted (Basole, 2007). The number of mobile devices in use has been steadily increasing for decades and in 2012 the number of mobile devices (estimated at 7.3 billion) exceeded the number of people on earth (estimated at 7 billion according to the World Bank) (Forrester, 2013a). The number of mobile devices and mobile users continues to grow, with 120 million new mobile subscriptions during the first quarter of 2014. Ericsson (2014) estimates that mobile subscriptions will reach 9.2 billion by the end of 2019.

Mobile data traffic is also growing exponentially with a 65% increase in mobile data traffic between quarter one in 2013 and quarter one in 2014. Mobile data traffic in quarter one of 2014 alone exceeded total mobile traffic in 2011 (Ericsson, 2014). It is, however, the change in composition of the mobile device market, marked by a decrease in the use of traditional mobile devices such as laptops, that is giving rise to the mobile enterprise. The Personal Computer (PC) market, including traditional PCs, laptops and notebooks is expected to decrease from an already low 13.6% in 2013 to 12.2% in 2015. This decrease is offset by the corresponding increase in the tablet, smartphone and other ultramobile market from 86.4% in 2013 to 87.8% in 2015 (Gartner, 2014). Ericsson (2014) estimates that the majority of mobile subscribers currently still use basic mobile phones, but that by 2016, smartphone subscriptions are expected to surpass basic mobile phone subscriptions.

The mobile revolution is driven by consumer behaviour and continuous innovation (Akella, Brown, Gilbert & Wong, 2012). It is evident that mobile technology has infiltrated the consumer market and these consumers (including employees, customers and suppliers) increasingly expect to have ubiquitous access to personal, as well as enterprise data and tools. The consumerisation of mobile solutions is creating a form of business operations where personal and enterprise information is shared, communicated, collaborated and accessed via wireless technologies, social

media, mobile applications and mobile commerce from multiple devices and any location (Gartner, 2012a). For enterprises a new employee profile is evolving: the anytime, anywhere, multi-device, multi-locational worker (Forrester, 2013b).

Despite the benefits derived from the use of mobile technology and the new opportunities and innovations that have been made possible, a problem has arisen. Since the mobile enterprise is driven by consumerisation and because of the rate of change and innovation within the technology trends, businesses are adopting mobile solutions on an *ad hoc* basis. These solutions are being deployed in business operations, but management do not understand the technology on a component level, and the IT technicians implementing the technology do not understand its impact on the business model (Rudman, 2010). This is creating what is commonly referred to as the 'IT gap'. Significant risks and weaknesses are being introduced into business operations through the *ad hoc* adoption of mobile solutions, and businesses are, often inadvertently, exposed due to poor IT governance. Businesses require a structured approach to identify and address significant risks relating to the adoption of mobile solutions on a mobile technology component level. The purpose of this research is to provide such a structured approach and thereby assist businesses in appropriately governing and managing their mobile solution investments and use.

1.2 Problem statement and research objective

The adoption of mobile solutions in any business exposes the business to significant IT strategic and operational risks at a technology component level (Boshoff, 2013). In practice mobile solutions were initially adopted on an *ad hoc* basis and these significant IT risks and weaknesses often remained unidentified or were only addressed after they had taken effect and losses had already been incurred. This has given rise to a current trend where enterprises have realised the potential impact of and vulnerabilities exposed by mobile solutions and are attempting to manage the technology and its deployment through a checklist method on a strategic level. The full impact of mobile solutions on the enterprise's operations and growth is not understood by all stakeholders on an operational and technical level and the risks related to the deployment of mobile solutions are still not appropriately identified and addressed. The current approach adopted by most businesses in the implementation

of mobile solutions involves an unstructured and ungoverned approach. This research proposes to provide management with practical and structured guidelines in order to address this problem by:

1. Identifying and understanding the underlying components of mobile technology;
2. Identifying the significant risks related to these components; and
3. Formulating appropriate controls to address these risks in order to adequately govern an enterprise's investment in mobile solutions and mitigate the significant risks.

1.3 Scope limitations

The research will focus only on significant risks and complexities related to the identified components of mobile solutions and does not propose to create an exhaustive list of all risks and complexities that may arise from the adoption of mobile solutions in business. In line with this, only significant internal control techniques will be formulated to address the identified risks.

The underlying components of mobile solutions (mobile devices, mobile infrastructure, delivery mechanisms and enabling technologies as well as mobile applications) will be defined and categorised. It is not the purpose of this research, however, to incorporate technical discussions on the design, development, programming and functionality of these components.

For the purposes of this research, the definition of a mobile device is intended to only include devices with computing, storage and communication capabilities. Storage devices used exclusively for the storage, transport and location-independent access to data and information, such as e-readers, portable drives and CD's, are excluded from the definition.

1.4 Organisational structure of research

This research is presented in seven chapters. Chapter 2 describes the design and methodology of the research and includes a discussion of the process followed in performing the review of prior literature. Chapter 3 contains the literature review and focuses on defining the theoretical concepts that will form the basis for the findings in Chapters 4 to 6. This includes the definition of mobility and the mobile enterprise, an investigation and definition of corporate, IT and mobile governance as well as the

review of relevant control frameworks with the intent of using the most appropriate framework in the identification of significant mobility risks. Chapter 4 investigates the underlying components in a mobile solution environment and defines and categorises each component. This understanding of the make-up of mobile solutions provides the foundation for the identification and definition of the significant risks related to the deployment of mobile solutions in Chapter 5. The conclusion of Chapter 5 contains a risk-component matrix, linking the significant risks identified to the relevant mobile technology component identified in Chapter 4. Chapter 6 formulates the appropriate internal control techniques to mitigate the risks identified in Chapter 5. The chapter concludes with a risk-control matrix that serves as a quick-reference guide to the risks that are addressed by each control. Chapter 7 provides an overview of the research, summarising the key findings of the research and concludes with the identification of potential areas for future research in the field of mobile solution risk management.

CHAPTER 2: RESEARCH DESIGN AND METHODOLOGY

In order to obtain a comprehensive understanding of mobile technology and to identify the significant risks and related controls, a non-empirical, qualitative study was performed. The following methodology was employed to address the research objectives:

1. An understanding of mobile technology was obtained. Based on this understanding, a definition for mobile technology was formed and its components were identified and classified.
2. Through a thorough investigation of the content, objectives, benefits and limitations of selected control frameworks, including Control Objectives for Information and Related Technology 5 (COBIT 5, hereafter referred to as COBIT), IT Information Library (ITIL) and the ISO/IEC 27000-series, an appropriate framework for the identification of risks relating to the use of mobile technology was selected. COBIT was identified as the most appropriate control framework for the objectives of this research.
3. The detailed processes of COBIT were reviewed to identify the processes applicable to the management of mobile technology on a component level.
4. These processes were used to identify significant risks relating to each process and the related mobile technology on a component level. A risk-component matrix was compiled, linking each mobile technology component to the significant risks it gives rise to.
5. Based on the significant risks identified, internal controls were formulated to adequately mitigate the risks. A risk-control matrix was compiled, linking each significant risk with the controls that can be implemented to mitigate the risk.

A literature review formed the foundation of the research. The review of prior literature relevant to an academic subject is a crucial part of research and forms the basis for new knowledge creation (Webster & Watson, 2002:xiii). Both Webster and Watson (2002:xiii) and Sylvester, Tate and Johnson (2010:1199) found that a literature review detects and recognises the gap in current knowledge that the research will address and differentiates the contribution of the current research from historic research. It characterises the research and places it in an academic context. Fink (2005) as cited in Okoli and Schabram (2010) identifies four characteristics of a rigorous literature review. It should be: (i) systematic in following a structured

approach; (ii) explicit in its description of the processes applied; (iii) comprehensive in its scope by taking into account all relevant subject matter; and thereby (iv) create a reproducible study. According to Rousseau, Manning and Denyer (2008:479) a systematic approach, as called for by Fink (2005), is the “*comprehensive accumulation, transparent analysis, and reflective interpretation*” of literature. In order to achieve this, Sylvester *et al.* (2010:1203-1205) suggests a five stage process whereby the initial selection criteria for the identification of relevant subject matter is purposefully wide and general, with the focus of the search narrowing and becoming more specified as the stages progress. Four stages were considered relevant to this research and were used:

- 1. The searching stage:** The initial approach to the search for relevant literature was broad and generic. Search terms used included: “mobility”, “defining mobility”, “mobile technology”, “IT governance”, “corporate governance”, “control frameworks” and “risks related to mobility”. The sources for literature reviewed included physical and electronic books, theses, organisational white papers, scholarly articles published in peer reviewed international and local academic journals, databases (such as IEEE (Institute for Electrical and Electronics Engineers), Elsevier, Gartner) and informal web articles. In the beginning of this stage, the review was performed to obtain an indication of the scope of knowledge on the subject and the quality, academic value and reputation of the literature was not taken into account. Towards the end of the stage, the search was more defined, focusing on influential contributors to the field and literature with solid academic backing and peer reviewed sources. This searching stage yielded 268 articles.
- 2. The mapping stage:** During the searching stage, recurring themes were observed and keywords and phrases were identified. These themes and keywords included “COBIT”, “ITIL”, “ISO 27000”, “benefits of mobility”, “enterprise mobility”, “categories of mobility”, “mobile applications”, “mobile devices” and “mobile security”. During the mapping stage, a more detailed review of articles, abstracts, introductions and conclusions was performed. The result of this stage was a clear understanding of the extent to which each theme should be discussed in the research. The original results of 268 articles were narrowed down to 132 relevant articles.

- 3. The appraisal stage:** Each article, chapter and paper was read in full and contributions to the identified themes were annotated. The most significant and fundamental concepts, as well as themes addressing the risks arising from the deployment of mobile solutions and the related control techniques, were identified and grouped together.
- 4. The synthesis stage:** Relevant literature grouped together during the appraisal stage was integrated, re-worked, adapted and simplified in order to formulate a structured and coherent document and reach the conclusions of this research.

The literature review conducted in the four stages as described provided a strong theoretical basis for an understanding of mobility, mobile solutions and the mobile enterprise; corporate and IT governance; as well as control frameworks as a tool for implementing IT governance.

This methodology provided the foundation for the identification of the components of mobile technology, the identification of significant risks related to the implementation of mobile solutions and the formulation of relevant controls that will mitigate enterprises' exposure to these risks. The research ultimately produced two quick-reference matrixes: the first linking the mobile technology components to the significant risks it gives rise to, and the second linking the significant risks to the relevant internal control techniques.

CHAPTER 3: LITERATURE REVIEW

3.1 Historic review of prior research

From a review of literature, it was established that extensive research has been conducted on mobility as a trend and the emerging mobile technologies. Current research focuses on three areas: (i) quantitative research with regards to the adoption of mobile technologies within enterprises internationally; (ii) studies that address mobile solution strategies, procedures and approaches on a high-level, often focusing on selected risks arising from the deployment of mobile solutions; and (iii) technical research that concentrates on the design, development, programming, and functionality of the underlying components of mobile technology.

Quantitative research is mostly conducted by corporations such as Forrester Research Inc., Ericsson and Gartner Inc. and includes findings on the rate of adoption of mobile technologies and the mobile technologies that are gaining popularity among users. Studies by these research companies also investigate the perspectives of boards of directors and Chief Information Officers (CIOs) regarding the benefits of and barriers to the deployment of mobile solutions as well as the risks enterprises are exposed to.

In the field of mobile solution strategies, studies such as Oracle (2014), Ernst & Young (2012), Gartner (2012a), Modus Associates (2012) and Sybase (2011) are sponsored by role-players in mobile solution management and explore the effect of mobile technology on business operations in the field of mobile solution management. These studies include mobile strategy considerations and the phases in mobile strategy implementation. Academic, peer reviewed research has also been conducted. A study by Sterk and Spruijt (2013) considers the definitions of enterprise mobility management systems and its subcategories, and reviews the products available on the market as well as the vendors offering these products. Studies by Akella *et al.* (2012), Wright, Mooney and Parham (2011), Sathyan and Sadasivan (2010) and Basole (2007) investigate risks related to mobile solutions, but focus mainly on the security risks and related control techniques. Deepak and Pradeep (2012) researched other non-security risks and Akella *et al.* (2012) and Basole (2007) also identify the inadequate governance and management of mobile solutions as an area of exposure.

On a technical level, databases such as IEEE and Elsevier contain wide-ranging studies on the technical functionality of mobile and related technologies. Themes that are extensively documented include studies in designing mobile infrastructure and wireless network architecture, developing communication protocols as well as mobile application development and mobile operating system platforms and frameworks. Specific studies reviewed include a study by Gavalas and Economou (2011) addressing the architecture of mobile applications on a programming and design level, application layer protocols that will enhance security and application security. Gavalas and Economou (2011) explore technical development platforms for applications such as Java ME, .NetCF, Adobe Flash Lite and Android. A study by Renner (2011) investigates the architecture of mobile operating systems including Android, Blackberry, iOS and Windows Phone. Arokiamary (2008) authored a book that includes the technical investigation and discussion of wireless communications infrastructure, telecommunications, wireless local area networks as well as the architectural layers of wireless networks.

Some studies attempt to provide a comprehensive overview of mobile technology, its development and its components, while also addressing the business consequences of adopting the technology. These include the book by Sathyan, Anoop, Narayan and Vallathai (2012) that addresses a wide range of mobility themes. They investigate and define mobility concepts such as the enterprise mobility landscape and the layers, architecture and enabling technologies of mobile solutions on a high level. The book includes case studies of the specific adoption of mobile solutions in industries such as retail, transportation, manufacturing and health. A master's thesis by Garcia (2013) also defines enterprise mobility and addresses the high-level components of mobile solutions as well as the challenges related to mobility. The latter part of the study focuses on the phases of enterprise mobility management strategy development. Fling (2009) authored a book that focuses on mobile technology design and development, including mobile application types and categories, mobile application development, design considerations, mobile web development, iPhone application development and adapting applications to mobile devices.

From the literature review conducted it appears that a gap in research still exists. On the one end of the spectrum, research is focused on mobile solution policies and

procedures on a high level and selected risks arising from the adoption of mobile solutions. On the other end of the spectrum, literature concentrates on the technical design, programming and functionality of the underlying components of mobile technology. This research proposes to address this gap in research by linking the significant risks related to mobile technology deployment, as identified using recognised frameworks, to the underlying technology on a component level.

3.2 Mobility and the mobile enterprise

Wilkins (2014) defines mobility as “*the movement of an organisation’s information and technology outside its physical facility for the purposes of accomplishing the daily activities and tasks required of employees.*” This definition is purposefully wide, and Wilkins (2014) argues that the obvious operational technologies, such as phones and tablets, constitute only a portion of an enterprise’s mobile landscape. Storage technologies and other technologies, such as virtual desktop infrastructure, that provide the basis for mobile functionality and other mobility techniques also fall within the scope of this definition. For the purposes of this research, the terms ‘mobility’, ‘mobile technology’ and ‘mobile solutions’ are used interchangeably to refer to all technology, mechanisms and techniques used and deployed in order to facilitate mobile functionality within the enterprise.

The most fundamental impact and principal contribution of mobile solutions within the enterprise is the initiation of ubiquity (Walters, 2012). Ghoda (2009:249) reiterates this concept by stating that mobility presents enterprises with the ability to transform traditional organisational structures into virtual structures through wireless network systems and services. This in turn enables global access to enterprise information allowing for ubiquitous collaboration and processing of corporate information, as well as the pervasive execution of corporate functionality.

The mobile enterprise is an organisational form that has emerged as a product of the consumerisation of mobile technology within the enterprise and the related transformation in the way business is conducted (Basole, 2007). Simply deploying mobile technology within an enterprise to execute basic operational functions does not constitute a mobile enterprise. The mobile enterprise is defined by the shift in the way the enterprise operates (Basole, 2007). This research is aimed both at enterprises deploying *ad hoc* mobile solutions to derive specific or isolated benefits

in its day-to-day operations as well as the mobile enterprise that extensively deploys mobile solutions and has adopted a ubiquitous business model.

3.3 Benefits of mobile technology to the enterprise

The deployment of mobile solutions has the potential to generate significant benefits within an enterprise if it is effectively and appropriately governed and managed (Wright *et al.*, 2011:14-15; ISACA, 2010). The following benefits can be derived from an investment in mobile solutions:

- **Increased employee productivity:** Mobile solutions facilitate remote access to the corporate network as well as its resources, allowing employees to continue work off-site and outside of office hours. Mobile solutions result in increased employee productivity, both in terms of an increase in output as well as improved employee collaboration (IFS, 2013; Cisco IBSG, 2012; Akella *et al.*, 2012; Wright *et al.*, 2011:15; ISACA, 2010; Basole, 2007).
- **Improved communication:** Greater access to company data and resources, coupled with a greater diversity in communication possibilities through voice, video and messaging, facilitates more spontaneous and timely communication (Akella *et al.*, 2012).
- **Improved quality of information:** Reducing reliance on paper-based processes results in an increase in the accuracy and integrity of data. Information is also analysed and received in real-time, furthering better and more timely decision-making (IFS, 2013; Basole, 2007).
- **Process improvement:** Mobile solutions create the opportunity for enterprises to automate and streamline business processes (Akella *et al.*, 2012; Basole, 2007). Revenue cycles are, for example, shortened by accelerated order capturing and a decrease in the time between order and shipment (Wright *et al.*, 2011:15; ISACA, 2010).
- **Lower costs:** Enterprises deploying mobile solutions experience cost savings by (i) replacing expensive computing equipment with lower cost mobile devices or employees funding their own mobile devices; (ii) improving business processes; (iii) increasing the quality of information; and (iv) increasing productivity (IFS, 2013; Cisco IBSG, 2012; Basole, 2007).

- **Competitive advantage:** Mobile technology has changed customer expectations and mobility has become a necessity in remaining relevant and improving customer satisfaction (Wright *et al.*, 2011:15; ISACA, 2010). Mobility also creates opportunities for enterprises to increase market share and explore new markets, while increasing the number and depth of customer connections. This will result in improved customer engagement (Gartner, 2012b; Akella *et al.*, 2012; Basole, 2007).
- **Attracting and retaining talent:** Employees are increasingly demanding the use of mobile technology in their professional lives, making mobile solutions a necessity to attract suitable staff (Akella *et al.*, 2012). Performing work remotely improves employees' work-life balance and, in turn, results in better staff retention (IFS, 2013; Wright *et al.*, 2011:15; ISACA, 2010).
- **Employee driven innovation:** As consumerisation is a major driver in the adoption of mobile solutions, employees often determine the best use of devices, applications and mobile services, allowing enterprises to identify value and capitalise on opportunities (Cisco IBSG, 2012).
- **Employee security and safety:** Employees are constantly connected and this may serve as a safety mechanism in terms of locating, tracking and assisting travelling employees (Wright *et al.*, 2011:15; ISACA, 2010).

3.4 Considerations in the deployment of mobile solutions

Walters (2012) acknowledges mobility as a powerful platform for innovation, but argues that pronouncing the end of the personal computer and fixed web is premature. The forced prioritisation of mobile solutions, without consideration of its context and relevance, may overlook the following key factors:

- **Early development:** Mobile device platforms are still in the early stages of development and have not reached their projected future capabilities.
- **Operational platforms:** The platform selected for performing operational activities is dictated by the nature of the activity. Personal computers (PCs) currently still provide the best and most effective platform for most day-to-day activities.

- **Communication platforms:** Mobility numbers are growing, but a significant portion of internet traffic still occurs on non-mobile platforms and will continue to do so in the near future.

Walters (2012) also argues that consumers and corporate management perceive the current mobile adoption rates and the level of innovation in mobile solutions as a movement away from one type of computer delivery channel to another. The infiltration of mobile solutions in an established PC and web domain does not constitute the replacement of one channel with another, but rather an expansion of opportunities within IT communication and usage.

3.5 Corporate governance and the governance of mobility

Mobile solutions, like all strategic assets, need to be governed through appropriate policies and procedures. The governance of IT requires those charged with governance to specifically tailor a governance system for IT assets, ensuring alignment with business strategies. The governance of mobility, as an IT asset, requires specific considerations due to the nature of the technology.

3.5.1 Corporate governance

Corporate governance comprises the policies, procedures, processes and systems according to which an enterprise is directed and controlled (Krechovská & Procházková, 2014:1145; Zalewska, 2014:2). The effective governance of an enterprise is achieved by incorporating responsibility, accountability, fairness and transparency into these policies, procedures, processes and systems, and specifically also decision-making processes (IODSA, 2009). The fundamental objective of corporate governance is the achievement of the long term strategic objectives of the enterprise by taking into consideration the expectations of shareholders and all other stakeholders, including regulators, auditors and corporate stakeholders (Grose, Kargidis & Vasilios, 2014:370; Bai, Liu, Lu, Song & Zhang, 2003:603).

In order to continue remaining relevant, enterprises need to adapt their corporate governance systems to changes in the business environment. Current movements, such as changes in technology and the related globalisation of corporations, need to be taken into consideration when formulating corporate governance systems

(Krechovská & Procházková, 2014:1145). Responding to these changes as well as the rapid rate of development in IT and its growing influence on business, the King Code of Governance for South Africa (2009) (King III) specifically addresses IT governance in its third report. In this report, it is argued that IT used to be viewed as an enabler in meeting the enterprise's strategic objectives, but that it has now become such an integral and pervasive part of business that IT, in itself, has become a strategic asset that needs to be governed (IODSA, 2009).

The core characteristics and nature of IT, as well as the rate at which technology is advancing, opens the enterprise up to new, incremental and complex risks and exposes new areas of vulnerability. IODSA (2009) refers to the use of control frameworks and guidelines as a tool to assist the board in systematically and adequately governing IT. In addition, enterprises need to identify and manage specific incremental risks and address these risks through adequate control techniques (IODSA, 2009).

3.5.2 IT governance

IODSA (2009) describes IT governance as an ever-evolving subject. A literature review of various researchers and studies established that IT governance can be analysed based on two characteristics: its scope and content and its objectives. With reference to its scope and content, IT governance is the responsibility of the board of directors and is considered to be a subset discipline of corporate governance (Rudman, 2008a; Webb, Pollard & Ridley, 2006; ITGI, 2003; Brisebois, Boyd & Shadid, 2001). IT governance is achieved through leadership and organisational structures, as well as a framework of best practices that encourages an established pattern of desirable behaviour for both users and administrators in order to direct, manage, control and maintain IT investments and the application and use of IT (Rudman, 2008a; ITGI, 2003; Brisebois *et al.*, 2001).

Effective and adequate IT governance needs to address both the enterprise's investment in IT as well as the operational use of IT. IT demand-side governance (ITDG) refers to the effective evaluation, selection, prioritisation and financial support of IT investments as well as the management and administration of its implementation and the realisation of measurable benefits from investments. IT supply-side governance (ITSG) refers to ensuring that the IT function is used

effectively, efficiently and appropriately and that it complies with all relevant policies and regulations (Gartner's IT Glossary, 2014).

With reference to its objectives, IT governance aims to achieve the following objectives:

- **Strategic alignment:** Ensuring that IT investments and its use supports and extends the strategic performance and sustainability objectives of the enterprise.
- **Value delivery:** Delivering value through IT in the form of timely, within-budget and quality information, financial benefits, the enablement of innovation and expansion, increasing competitive advantage and meeting all stakeholder expectations by utilising opportunities and maximising benefits.
- **Risk management:** Including IT as an integral part of the enterprise's risk management strategy and processes in order to appropriately and comprehensively identify and address IT related risks and exposures. This ensures that IT assets are safeguarded, functions as intended and that disaster recovery procedures are in place.
- **Accountability:** Assigning responsibility for the implementation of an IT governance framework and the day-to-day management of the IT function.
- **Performance management:** Monitoring, measuring and assessing the use and functioning of IT investments and projects in order to identify weaknesses and areas for improvement.
- **Resource management:** Managing all resources employed in IT including people, technology, facilities, data and applications to optimise the IT investment and maximise efficiency.

(Zhang & Le Fever, 2013:391; SAICA, 2010; IODSA, 2009; Webb *et al.*, 2006; Hardy, 2006:56-57; Symons, 2005; ITGI, 2003)

In order to meet the stated objectives of IT governance, the enterprise needs to implement structures and mechanisms tailored to the specific technology deployed.

3.5.3 IT Gap

The board of directors is charged with the implementation and maintenance of control frameworks and other mechanisms in order to govern IT investments and use. IT professionals are tasked with the implementation of control techniques to execute the objectives set by management, using these control frameworks. This segregation of responsibilities leads to the 'IT gap' (Rudman, 2010). Those charged with governance often do not understand the underlying technology and its technical design, whereas those charged with the implementation of the technology do not understand the framework and strategic objectives within which IT needs to be governed. As a direct consequence, what the board expects in terms of IT governance is often far removed from the actual controls implemented by the IT department. Rudman (2010) suggests that risks and weaknesses are not introduced into an IT system because of a lack of policies and procedures, but rather because governance policies and procedures are not merged with the technical operations to form an integrated risk management unit.

3.5.4 Alignment

With the purpose of bridging the IT gap, the board of directors needs to ensure that the business strategies and IT investments are aligned. Business/IT alignment is achieved when IT investment and the delivery of IT services are driven by business strategies and when business strategies are influenced by an understanding of IT capabilities and limitations (Macehiter Ward-Dutton, 2005). Alignment is, therefore, the degree of integration and correlation among business strategy, IT strategy, business infrastructure and IT infrastructure (Henderson & Venkatraman, 1999:472). These definitions highlight two important considerations. It emphasises that decisions regarding IT investment and management, that have traditionally resided with IT practitioners, should now be governed in the same manner as other strategic business assets (Macehiter Ward-Dutton, 2005). As with all strategic assets, it is when IT investments are shaped by business objectives, that corporate spending is more likely to enhance business value, growth and competitiveness (Krivida, 2008). It also highlights that those charged with governance can no longer steer a business successfully without a clear understanding of the technical IT implications of strategic decisions (Macehiter Ward-Dutton, 2005).

3.5.5 Governance of mobility

Akella *et al.* (2012) states that the deployment of mobile solutions as part of the enterprise strategy will affect application development, technical infrastructure and networks as well as operational processes in all enterprise departments. In order to ensure alignment of the enterprise's investment in mobile solutions with business strategy, those charged with governance will need to consider the specific characteristics of mobile technology such as the continuous changes in the technology, the incremental risks related to mobile solutions and its technical design and functionality. In order to achieve alignment, an active, flexible strategy and cross-functional governance structure needs to be put in place (Akella *et al.*, 2012).

3.6 Control frameworks

Control frameworks make IT governance achievable by providing those charged with governance with a structure to systematically, comprehensively and effectively govern IT systems. Control frameworks provide the basis for identifying and addressing risks related to the use of and investment in IT (Rudman, 2010).

3.6.1 Considerations when implementing control frameworks

Enterprises need to consider their approach to the adoption and implementation of multiple frameworks and standards in order to sufficiently address all areas of IT governance. Where each standard is implemented separately, this leads to a silo approach with duplicate controls. This creates an inefficient control structure and an unnecessarily complex system of controls that inhibits a clear and comprehensive understanding of the enterprise's risk exposure and related control structure (Anisingaraju, 2013).

Another consideration when implementing control frameworks is the use of external IT service providers. Because of the complexity of many frameworks and standards, the amount of detail and the level of understanding required to implement the frameworks, this process is often outsourced. Contracted service providers frequently create a standard and repeatable approach to the implementation of processes in order to streamline their service. This may cause misalignment as the processes implemented are not driven by each enterprise's specific business strategies (Overby, 2012).

3.6.2 Control frameworks reviewed

According to Nicho and Fahkry (2011:55), Control Objectives for Information and Related Technology (COBIT), IT Information Library (ITIL) and ISO/IEC 27002 are the most relevant and commonly adopted IT control frameworks and standards for the governance, management, maintenance and security of IT. According to their study, each framework or standard provides a different value to its users: COBIT is generally used as a benchmark framework and for audits, ITIL is used for the description and design of IT processes and ISO/IEC 27002 for security issues and the mitigation of specified risks. King III also specifically makes reference to ISO/IEC 38500:2008: Corporate governance of information technology. This standard is a high-level advisory standard that provides broad guidance on IT governance and ensures the board's involvement in the governance of IT (Wilkin & Campbell, 2010:100; ISO/IEC, 2008). The standard requires boards to govern IT by evaluating the current and future use of IT, aligning IT with enterprise strategies and monitoring compliance with relevant policies and regulation and the standard itself encourages the use of control frameworks to reinforce and apply these processes (ISO/IEC, 2008).

Based on the study by Nicho and Fahkry (2011:55) and the broad nature of ISO/IEC 38500:2008, COBIT, ITIL and the ISO/IEC 27000-series were selected for review. These frameworks and standards were reviewed in detail in order to identify the most appropriate framework for the identification of operational and strategic risks related to mobile solutions.

3.6.3 An overview of COBIT

Control Objectives for Information and Related Technology (COBIT) is an internationally accepted framework for the governance and management of the use of and investment in enterprise IT (ISACA, 2012a; Radovanović, Radojević, Lučić & Sarac, 2010:1137). COBIT is a generic yet comprehensive framework that optimises the value derived from IT investments and its use by promoting a balance between IT related risk and benefits. The framework is published by ISACA and the latest version of the framework, COBIT 5, was released in 2012 (ISACA, 2012a). COBIT 5 consolidates several of ISACA's information assets into one comprehensive framework. Previous publications integrated in the COBIT 5

framework include COBIT 4.1, Val IT (a framework for the creation of value from IT investments and innovation), Risk IT (a framework providing a comprehensive overview of IT related risks), BMIS (Business Model for Information Security), ITAF (the IT Assurance Framework), TGF (Taking Governance Forward) and the Board Briefing on IT Governance, 2nd edition (Zhang & Le Fever, 2013:392).

COBIT is based on five principles, as identified by ISACA (2012a):

1. Considering and meeting all stakeholder requirements by converting enterprise goals into actionable IT goals.
2. Covering the enterprise end-to-end, not only focusing on IT governance in isolation but integrating it into corporate governance as a whole.
3. Applying a single, integrated framework that operates as an overarching framework for the implementation of other frameworks.
4. Enabling a holistic approach to achieve effective and efficient IT governance through categorised enablers.
5. Separating governance from management. The two disciplines meet different enterprise needs and operate through different organisational structures.

The core framework of COBIT includes five domains, divided between the governance and management of IT. Governance ensures the achievement of enterprise strategies by evaluating stakeholder expectations and needs; establishing direction through prioritisation and regulation; and monitoring performance, compliance and progress against pre-approved requirements. Management includes the planning, developing, operating and monitoring of activities that are aligned with enterprise strategies and objectives (ISACA, 2012a). Each domain is broken down into processes that assist the enterprise in achieving its control objectives (ISACA, 2012a). The five domains are:

- **Evaluate, direct and monitor (5 processes):** This domain requires establishing a governance framework and monitoring processes and systems to ensure that IT governance objectives are met.
- **Align, plan and organise (13 processes):** This domain requires the development of an aligned IT strategy, the development of an appropriate organisational and IT infrastructure to support this strategy, the

implementation of a comprehensive risk assessment and the management of all related resources.

- **Build, acquire and implement (10 processes):** This domain addresses the development and implementation of the necessary IT solutions at an operational level. This includes the acquisition, installation, configuration and maintenance of IT assets as well as the management of any changes and modifications.
- **Delivery, service and support (6 processes):** This domain focuses on the actual delivery of IT services and addresses day-to-day operational and data management, security and continuity as well as user support.
- **Monitor, evaluate and assess (3 processes):** This domain requires the implementation of performance management and monitoring systems as well as structures of internal control, regulatory compliance and governance to ensure compliance with control objectives.

The detailed processes of COBIT were reviewed and summarised in Appendix A.

3.6.4 An overview of ITIL

IT Information Library (ITIL) is a widely adopted framework that defines best practices for IT service management and its support processes, recognising the management of IT services as a primary driver of quality enterprise information and business-IT alignment. The most recent version of the framework is ITIL version 3 (ITIL, 2011).

ITIL does not provide an overarching framework for IT governance as a whole but focuses on operational and detailed processes. The framework provides comprehensive guidance on the planning, design and implementation of IT service delivery and includes detailed operational considerations such as roles, responsibilities and functions (Zhang & Le Fever, 2013:392; Radovanović *et al.*, 2010:1139).

The content of ITIL is organised around the IT service life-cycle and comprises a series of eight books, five of which each cover a core stage in this life cycle (Zhang & Le Fever, 2013:392; Arraj, 2013; ITIL, 2011):

- **Service strategy:** This phase addresses the development of a service strategy based on stakeholder expectations and requirements. It also addresses financial management and requires an analysis of the organisational design and infrastructure needed to achieve the strategy.
- **Service design:** This area addresses the design of a specific service solution to deliver the service strategy and meet user expectations. It defines service delivery requirements and considers continuity and security management.
- **Service transition:** This section provides guidance on the implementation of the service design, change management, control over IT assets and configuration items, service validation and user support.
- **Service operation:** This phase addresses the day-to-day management of the service, monitoring of performance and incident management.
- **Continual service improvement:** This area focuses on maintaining value for stakeholders through the measurement and improvement of service levels and technology.

3.6.5 The ISO/IEC 27000-series

The ISO/IEC 27000-series, as published by the International Organization for Standardization (ISO) in partnership with the International Electrotechnical Commission (IEC), includes twenty five published standards and twelve proposed standards addressing information security management systems, best practices and controls (ISO 27001 Security, 2014).

The complete list of ISO/IEC 27000-series standards was reviewed and five standards were identified that are relevant to the identification of risks arising from the adoption of mobile solutions. These standards were found to specifically address the governance of information security as well as the identification of risks and controls within an Information Security Management System (ISMS). According to Nicho and Fahkry (2011:57) these standards also address ISMS management at an IT component level which relates to one of the objectives of this research.

3.6.5.1 ISO/IEC 27000:2014 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

ISO/IEC 27000 provides an overview of the complete ISO/IEC 27000-series and an introduction to information security management systems (ISMS). It further includes a glossary defining and explaining essential terms (ISO 27001 Security, 2014).

3.6.5.2 ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements

ISO/IEC 27001 is an internationally accepted best-practice standard that provides guidance on the development and maintenance of a comprehensive ISMS (IT governance, 2014). An ISMS is defined as a methodical approach to the management of enterprise data in order to ensure its availability to authorised users and its confidentiality and integrity. It serves as a framework for the identification and mitigation of IT security risks (IT governance, 2014; ISO 27001 Security, 2014).

The standard does not provide the specific controls to be adopted as part of the ISMS but provides detail on the following best practices relating to the development of an ISMS:

- Assessment of all stakeholder needs and defining the scope of the ISMS;
- Leadership and commitment to the ISMS from top management;
- Planning risk management;
- Support through competent resources and proper documentation;
- Assessment and mitigation of security risks and the day-to-day operation of the ISMS, including change management;
- Performance evaluation of the ISMS through monitoring, measurement and review; and
- Continuous improvement of the ISMS based on review findings (ISO 27001 Security, 2014).

3.6.5.3 ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls

ISO/IEC 27002 is a guideline that contains a list of practicable best practices in order to meet the objectives of an ISMS (ISO 27001 Security, 2014; Zhang & Le Fever,

2013:392). ISO/IEC 27001 formally defines the requirements of an ISMS whereas ISO/IEC 27002 serves as a guideline that includes security control recommendations (ISO 27001 Security, 2014).

ISO/IEC 27002 contains 14 sections of security considerations and controls, specifying 35 control objectives and 114 controls in total (ISO 27001 Security, 2014). The objective of each section is summarised as follows:

- **Information security policies:** Define a set of policies to achieve the information security strategy.
- **Organisation of information security:** Define and assign roles and responsibilities for information security and address specific policies and controls for mobile devices and teleworking.
- **Human resource security:** Outline security considerations and responsibilities during the recruitment, employment and termination or change of employment of all employees.
- **Asset management:** Catalogue all information assets (including physical assets, information assets and storage media), assign ownership and the related responsibilities and document policies regarding its use.
- **Access control:** Document an enterprise access control policy, manage user access rights and restrictions to information, systems and applications and communicate user responsibilities.
- **Cryptography:** Develop and document a policy on the management and use of encryption and other integrity controls.
- **Physical and environmental security:** Protect physical areas against unauthorised entry and other damages and protect and secure information on equipment, utilities and cabling, both on and off-site.
- **Operations management:** Document and manage operational responsibilities and procedures. This includes malware protection, backups, logging and monitoring of activities, exceptions and incidents, software installation, technical vulnerability management and IT audits.
- **Communications security:** Manage network and information transfer security.
- **System acquisition, development and maintenance:** Determine the security control requirements of information systems, including web

applications and transactions. Develop policies that govern secure systems development, modifications, outsourcing and testing.

- **Supplier relationships:** Create awareness of and policies on enterprise information available to third parties and the management of all service deliveries by third parties.
- **Information security incident management:** Manage, document and improve on security incidents.
- **Information security aspects of business continuity management:** Integrate policies for information security continuity into the enterprise's business continuity systems and create adequate redundancy.
- **Compliance:** Identify legal and contractual compliance responsibilities including an external independent review and audit of the enterprise's systems (ISO 27001 Security, 2014).

3.6.5.4 ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management

ISO/IEC 27005 supports ISO/IEC 27001 by providing guidelines on the implementation of a risk management approach. The standard provides a structured and systematic approach to risk analysis and mitigation but does not require any specific method.

The standard promotes a risk management process that identifies information assets exposed to risk, identifies the potential threats and vulnerabilities and considers the effect if the risk is realised (ISO 27001 Security, 2014).

3.6.5.5 ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security

ISO/IEC 27014 provides guidance on the governance of information security through a framework of six governance principles: (i) establishing enterprise-wide information security; (ii) adopting a risk based approach; (iii) directing investment decisions; (iv) compliance with internal and external requirements; (v) creating a secure environment; and (vi) performance review (ISO 27001 Security, 2014). The standard also details five governance processes to ensure appropriate governance of IT security. These include the evaluation of strategic objectives, providing general

direction, monitoring the process, communicating with stakeholders and obtaining assurance through independent reviews and audits (ISO 27001 Security, 2014).

3.6.6 Benefits and limitations of the reviewed control frameworks

The benefits and limitations of control frameworks were investigated and considered as part of the process of determining the most applicable control framework to apply in the identification of risks related to mobile solutions. Table 1 summarises the benefits and limitations of the control frameworks reviewed. The detail of the benefits and limitations identified are included in Appendix B.

Table 1: The benefits and limitations of COBIT, ITIL and the ISO/IEC 27000-series

	COBIT	ITIL	ISO/IEC 27000-series
Benefit			
Improves alignment	X	X	
Comprehensive framework	X		
Adaptable to enterprise size	X	X	X
Integrates international control frameworks	X		
COSO compliant	X		
Cost saving	X	X	X
Improves user and customer satisfaction	X		
Detailed processes		X	X
Consistent processes and terminology		X	
Statement of commitment to IT security			X
Promotes constant revision and improvement of IT processes		X	X
Limitations			
Complex and not easy to understand	X	X	X
Resource intensive	X	X	
Lacks guidance on practical implementation	X	X	
Lacks detailed processes	X		
IT security not addressed	X		
Cost management not addressed			X
Leads to inter-departmental conflict		X	X
IT governance as whole is not addressed			X

(Babb, 2014; ISO 27001 Security, 2014; Standards Consultants, 2014; Anisingaraju, 2013; Arraj, 2013; Zhang & Le Fever, 2013:392-393; Oliver & Lainhart, 2012; Goosen, 2012:24; ITIL, 2011; Mataracioglu & Ozkan, 2011; Oliver & Lainhart, 2011; Henry-Stocker, 2010; Rudman, 2008b; Sahibudin, Sharif & Ayat, 2008:749-752; Fry, 2005)

3.6.7 Framework selected for the purposes of this research

The three selected frameworks and standards were considered for use as the potential basis from which risks arising from the deployment of mobile solutions within an enterprise will be identified. COBIT was selected as the most appropriate basis as it provides the most comprehensive approach to IT governance and addresses not only the IT function, but all areas in the enterprise affected by the investment in and use of IT solutions. ITIL and the ISO/IEC 27000-series were not used as a basis to identify significant risks. They are more detailed in terms of guidance and processes, but were considered to be too narrow for the purposes of identifying the significant risks relating to mobile solutions. ITIL focuses only on IT service delivery and the ISO/IEC 27000-series focuses only on IT security.

3.7 Summary and conclusion

The literature review conducted in Chapter 3 created the foundation for the definition of mobile technology and an understanding of its benefits. This knowledge formed the basis for the identification, classification and definition of mobile technology components in Chapter 4. The understanding of corporate governance, IT governance and the role of control frameworks in governance directed the research into a review of relevant control frameworks to be used for the identification of significant mobility risks and the related mitigating. COBIT was selected as the most appropriate control framework, and its detailed processes formed the basis for the identification of significant risks related to the deployment of mobile solutions in Chapter 5 and the formulation of mitigating controls to the address these risks in Chapter 6.

CHAPTER 4: MOBILE SOLUTION COMPONENTS

COBIT was selected as the most appropriate framework for the identification of significant risks relating to the deployment of mobility within an enterprise. In order to effectively apply this framework to mobile technology at a detailed category level, the underlying components of mobile solutions need to be identified, defined and categorised. Studies by Basole (2008:1), Deepak and Pradeep (2012:178), Fling (2009:13) and Sathyan *et al.* (2012:65) have classified mobile solutions into various components. Based on the recurring concepts and models identified in these studies, the following principal components were identified as the core elements of mobile solutions:

- devices;
- infrastructure, delivery mechanisms and enabling technologies; and
- applications.

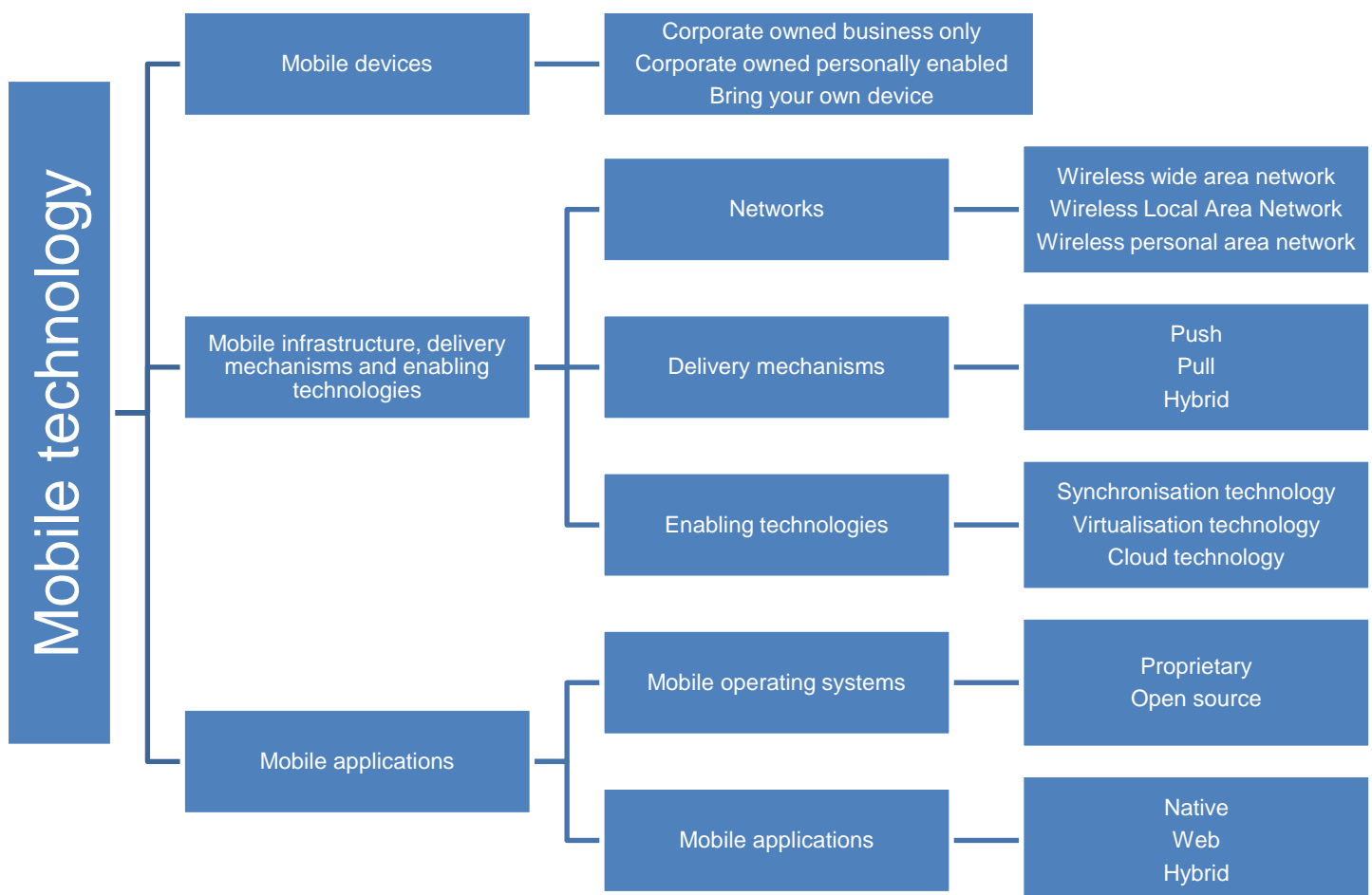


Figure 1: The core components of mobile solutions

In order to obtain a comprehensive understanding of the components, each component is defined and placed in context in terms of its role within mobile solution delivery. Where relevant, the types of technology that is included in each component is identified and defined. Lastly, each component is subdivided in its main categories and, where applicable, the benefits of each category are considered. The limitations of each of the categories give rise to the significant risks related to mobile solutions and will be considered in Chapter 5.

4.1 Mobile devices

The term “mobile device” is a generic and broad term for a diverse collection of devices that allow access to data and/or functionality from any location. For the purposes of this research, a mobile device is defined as a compact and portable device that specifically has computing, storage and communication capabilities. These devices often have a display screen with either touch input, a small keyboard or both (Wilkins, 2014; Wright *et al.*, 2011:14).

4.1.1 Types of mobile devices

According to Sathyan *et al.* (2012:66), mobile devices can be grouped into three levels:

- **Legacy devices:** This level includes technologically lower level and traditional devices with limited browser capabilities and with data exchange limited to text and images. Web pages are simple text pages and do not have the ability to run applications capable of functioning independently, known as thick applications. The device primarily runs native applications, or utilities, installed by device manufacturers.
- **Mediocre devices:** Devices in this level have more advanced browser capabilities and web execution can facilitate drop-down and other media presentation controls. These devices are, however, still limited to manufacturer installed applications.
- **Advanced devices:** This level of devices provides an enhanced user experience with advanced communication, computing and operational functionality. These devices offer superior web browsing capabilities, the ability to download applications and mobile techniques such as synchronising capabilities.

Although enterprises often have employees that own devices from all three levels of mobile devices, the consumerisation of mobile solutions is driven mainly by advanced mobile devices. This research focuses on this level specifically. Advanced mobile devices include the following significant types of mobile devices (Pinola, 2014; Sathyan *et al.*, 2012:66-67; ISACA, 2010):

- **Portable digital assistants (PDAs):** Portable digital assistants (PDAs) are considered the original palm-sized mobile devices and function as personal information managers and organisers. They have basic mobile phone capabilities but also allow for web browsing and office and productivity applications. PDAs are comparable to smartphones in terms of size. PDA features vary extensively and input mechanisms include keyboard and or stylus input, and more recently touch input. The active development of PDA technology has, however, slowed down significantly, mostly as a direct consequence of advancements in smartphone technology. Examples of PDAs: Dell Axim, HP iPaq, Palm Pilot.
- **Mobile personal computers (PC):** Laptops are regarded as the original mobile device. Laptops, in comparison to other advanced mobile devices, have the most computing power as they were initially developed specifically to execute all functionalities that are executable with a desktop PC, but from any location. They are however the least portable. Notebooks and netbooks are included in this category, with size being the main differentiator. The notebook is often smaller and lighter than the laptop, followed by the netbook. Laptops, notebooks and netbooks have traditional keyboard input and touch mouse input. Ultra mobile PCs also fall into this category. They offer the traditional desktop version of computing in the smallest available package with keyboard, touchscreen or stylus input. Examples of mobile PC manufacturers: Acer, Apple, Dell, Lenovo, HP.
- **Tablet personal computer (tablets):** This type of mobile device is often smaller and lighter than the mobile PC, offering better portability but is typically more limited in terms of processing power. Tablets are normally contained in a single panel and are moving away from running traditional desktop software to running mobile operating systems. The tablet's most distinguishable feature is not its size but its input mechanism. This tends to be

a combination of a touchscreen, stylus input and the option of an external keyboard. Examples of Tablet PCs: iPad, Samsung Galaxy tab, Lenovo Miix, Asus MeMO Pad.

- **Smartphone:** Smartphones are mobile phones built on a mobile platform with advanced features and computing capabilities (Song & Lee, 2012). Smartphones are generally smaller than tablets making these devices the most portable. Smartphones do, however, have the least processing power when compared to the mobile PC and tablet. The current input mechanism of the smartphone is mostly touch input, but this is often combined with keyboard input. The development and use of voice input as the next level input mechanism is, however, growing. Display screens are larger than traditional mobile phones, but are smaller than tablets. Examples of smartphones: iPhone, Samsung Galaxy, HTC One, Nokia Lumia, Sony Experia, Blackberry.

4.1.2 Categories of mobile devices

Enterprises that seek the benefits of mobile solutions need to consider basic categories of mobile device deployment: (i) a model where the device is owned by the enterprise and intended only for business purposes; (ii) a model where the enterprise owns the device but allows personal use of the device; and (iii) a model where the employee uses his/her own device to access corporate information and functionality.

4.1.2.1 Corporate owned business only (COBO)

Blackberry (2014) defines corporate owned business only (COBO) as a mobile solution approach where an enterprise issues mobile devices to its employees that are dedicated exclusively to work related computing and communication activities. The enterprise bears the cost of investment in the device but cost savings are possible through bulk purchase options.

Blackberry (2014) and Zscaler (2013) highlight the following benefits of a COBO approach to the deployment of mobile devices:

- **Homogeneous devices:** The enterprise selects and distributes devices creating a homogeneous device landscape that simplifies device management, upgrades and support.
- **Control:** The enterprise has maximum control over corporate content and functionalities. This also offers additional security benefits as users can access networks securely.
- **Management:** Enterprises have the opportunity to develop and implement a centralised governance and management policy, applicable to all corporate devices.

4.1.2.2 Corporate owned personally enabled (COPE)

COPE (corporate owned personally enabled) is a mobile solution where the enterprise pre-selects and supplies its employees with mobile devices that are owned by the enterprise but configured to allow for personal computing and communication use in addition to corporate use (Blackberry, 2014; Garcia, 2013:5). Most COPE policies also allow employees to, within reason, install personally selected applications on the device (Rose, 2013:328). The cost implications are similar to that of a COBO model.

In addition to the benefits of a COBO solution, Blackberry (2014), Samsung (2013) and Rose (2013:328) identify the following benefits relating to a COPE solution:

- **Control over corporate data and information:** The configuration of devices with secure containers that separate corporate and personal data continues to give enterprises maximum control over corporate information and functionality.
- **Flexibility:** COBO provides flexibility by allowing enterprises to implement a variation of the solution that suits their risk tolerance levels and business model. Enterprises can find the appropriate balance between management and security risks on the one side and business enablement and user satisfaction on the other.
- **User satisfaction:** By offering a range of supported devices, users can select the device best suited to their purpose and productivity requirements. This also serves as a recruitment driver attracting skills and staff.

- **Litigation:** By partitioning corporate and personal data, employees have reasonable assurance that personal data will remain secure, reducing the risk of litigation.

4.1.2.3 Bring your own device (BYOD)

Bring your own device (BYOD) is a mobile solution that allows employees the use of a personally selected and acquired mobile device to perform corporate computing and communication activities by executing enterprise applications and accessing enterprise data (Blackberry, 2014; Gartner, 2013). BYOD also introduces Bring Your Own Apps (BYOA), where employees not only use personal devices for corporate purposes, but also select the software and application best suited to their operational requirements (Rose, 2013:327).

BYOD is being driven by consumerisation (CDW, 2012). The trend where one user will interchangeably connect to the enterprise network with multiple devices for both personal and corporate use, is occurring whether it is approved by the enterprise or not (Rose 2013:328; Aruba Networks, 2012). BYOD, as a mobile solution, acknowledges this trend and creates an opportunity for enterprise IT to manage, support and secure corporate data as well as enable productivity on personally owned devices (Garcia, 2013:4). The model typically allows users specified access rights to enterprise applications and data, subject to enterprise security and management policies. IT may also pre-authorise a specified list of acceptable devices and may provide partial or full support for device access and applications (Gartner, 2012a).

The following benefits can be derived from a BYOD model:

- **Cost savings:** Cost savings are considered the principle reason for adopting a BYOD solution and are realised through a reduction in hardware investments; the transferral of running and replacement costs to the employee; and a reduction in support costs.
- **New technology:** Employees are faster to upgrade hardware and explore and deploy the latest software innovations allowing the enterprise to leverage the advantages of innovative and new technology.

- **Employee satisfaction:** Employees experience greater flexibility as they are able to select the technology that best supports and improves their functions and responsibilities. BYOD policies encourage motivated and more creative employees and consequently staff retention also improves.
- **Competitive advantage:** BYOD has become an expectation of potential employees and deploying the solution increases an enterprise's competitive advantage with regards to staff recruitment.

(Blackberry, 2014; Glasshouse, 2013; Pillay, Diaki, Nham, Senanayake, Tan & Deshpande, 2013)

4.1.3 Comparison of mobile device deployment categories

The following table summarises the most significant similarities and differences between the COBO, COPE and BYOD models (Garcia, 2013:5):

Table 2: A comparison of BYOD, COPE and COBO approaches to mobile device deployment

	BYOD	COPE	COBO
Device Ownership	User	Enterprise	Enterprise
Hardware Cost	Rests with the user	Bulk buying	Bulk buying
Devices Landscape	Very heterogeneous	Homogeneous	Homogeneous
Integration with Enterprise Services	Not ensured	Ensured	Ensured
IT Support	Difficult	Easy	Easy
User satisfaction	Good	Limited	Very limited
Control over device and content	Limited to user rights	Space Fully Managed	Space Fully Managed

From the table it appears that the most fundamental difference between a COPE and COBO model is the user's satisfaction. As the adoption of mobile solutions within an enterprise is primarily consumer driven, this is a significant aspect for enterprises to consider. The table also illustrates that as user independence and flexibility increases, control over the device and its content decreases (Sterk & Spruijt, 2013). Garcia (2013:5) states that the core decision driver for enterprises in deciding the

solution to deploy, is weighing up management and security exposure against flexibility and productivity.

4.2 Infrastructure, delivery mechanisms and enabling technologies

Mobile infrastructure, delivery mechanisms and enabling technologies provide the structure and foundation that facilitate mobility and its benefits (Gartner, 2012b; Yunos, Gao & Shim, 2003:34).

4.2.1 Mobile networks

The primary characteristic of mobile solutions is the user's ability to access data and functionality from any location. Wireless networks form the core component of mobile infrastructure that enables the delivery of this characteristic (Sathyan *et al.*, 2012:68). Wireless networks constitute wireless communications technologies that facilitate the communication between one or more mobile devices without a tangible wired connection. Data is transmitted across these wireless technologies through radio frequency (Verizon, 2012).

4.2.1.1 Categories of mobile networks

Wireless mobile networks can be categorised according to various characteristics including the area of coverage, type of modulation used, speed of data transfer, type of switching, bandwidth and type of interface used for data transfer between elements (Sathyan *et al.*, 2012:68). For the purposes of this research, area of coverage is considered the most appropriate grouping and three categories have been identified: wireless personal area networks (WPAN), wireless local area networks (WLAN) and wireless wide area networks (WWAN) (Verizon, 2012).

- **Wireless wide area networks (WWAN):** WWANs use cellular technologies to provide broadband data networks with broader coverage and range. The network allows mobile devices to connect to wireless broadband networks through the commercial carrier's network (Verizon, 2012). Examples of WWAN technologies include second generation standards (2G) such as General Packet Radio Service (GPRS), and Enhanced Data rates for GSM Evolution (EDGE), third generation standards (3G) such as High Speed Packet Access (HSPA) and Universal Mobile Telecommunications System

(UMTS) as well as fourth generation standards (4G) such as LTE (Fling, 2009:17; Verizon, 2012). Virtual private networks (VPNs) are included in this category and use public or shared telecommunication infrastructure, such as the internet, to provision remote or mobile users with secure private network services. A VPN is essentially a WAN, and where used by mobile users, a WWAN (Lewis, 2006:5).

- **Wireless local area networks:** A WLAN facilitates connections through devices such as routers and switches that were intended to connect devices to wired networks. In a WLAN, devices connect wirelessly to wireless access points that are connected to local networks via wired connections such as Ethernet cables. A single access point covers a certain area within which users can move without losing connectivity (Verizon, 2012). The most widely used form of WLAN is Wi-Fi. Wi-Fi is the common term for a set of standards established by the Institute of Electrical Engineers Standards Association to define wireless LANs (Verizon, 2012).
- **Wireless personal area networks:** A WPAN provides *ad hoc* network connections to devices at close range. The networks are defined as *ad hoc* as they operate without connecting to network infrastructures (Verizon, 2012). Bluetooth is the most commonly used WPAN network standard (Verizon, 2012).

4.2.2 Data delivery mechanisms

Data delivery mechanisms ensure the transmission of data across wireless networks in a wireless mobile environment and the two fundamental data delivery mechanisms used by wireless data applications are point-to-point access and broadcasting (Arokiamary, 2008:6-5).

4.2.2.1 Data delivery connections

A wireless mobile computing environment operates as a distributed system where components on the network communicate through the exchange of messages. Wireless applications primarily exchange messages via two types of connections. In a point to point connection, queries or messages are sent from the user to server and returned to the user. In a broadcast connection, queries and messages are simultaneously transmitted to all users within the broadcast (Arokiamary, 2008:6-5).

4.2.2.2 Categories of data delivery mechanisms

Mobile applications often use especially broadcast data delivery connections in the transmission of data. Broadcasting data delivery mechanisms can be grouped in the following categories (Arokiamary, 2008:6-6; Yunos *et al.*, 2003:34; Franklin & Zdonik, 1998:517):

- **Push** (also referred to as the publish-subscribe model): The server transmits information before the receipt of a request. The server initiates the transfer and perceives perpetual queries from users through their subscription and a single distribution addresses all queries in the broadcast.
- **Pull** (also referred to as the on-demand model): The server locates and broadcasts information on request from a user. It is responsive and reacts to the receipt of a query.
- **Hybrid**: This model integrates push and pull technology. In this model the user receives pull data items on request and push data items spontaneously.

According to Franklin and Zdonik (1998:517), an enterprise needs to take the following two characteristics of push and pull mechanisms into consideration when selecting the most appropriate mechanism for its data delivery:

- **Aperiodic and periodic**: Push and pull mechanisms can transmit data either periodically or a-periodically. A-periodic transmissions are activated by an event. In a pull model this means that a data request is sent in response to user action and in a push model a transmission is transmitted on data update. Periodic transmissions are delivered according to a schedule.
- **Unicast and 1-to-N**: In unicast communication, information is transmitted from a server to one identified user. In a 1-to-N communication, data is sent to multiple recipients.

Each data delivery mechanism has its own characteristics and possible consequences as described by Arokiamary (2008:6-6) and Franklin and Zdonik (1998:517-518). These are summarised in Table 3:

Table 3: The characteristics of push and pull data delivery mechanisms

	Push	Pull
Users are required to know the location of information	x	✓
Simultaneous transmission to multiple devices	✓	x
Server interruption and overload due to frequent user requests	x	✓
Inappropriate and irrelevant data distributed to users	✓	x
Intrusive transmission of data	✓	x

4.2.3 Enabling technologies

Enabling technologies are the technologies that allow users to maximise the benefits of mobile solutions. A review of literature (including Gartner (2012b), Akella *et al.* (2012) and Yunos *et al.* (2003)) identified the following as the predominant technologies applied by mobile users:

4.2.3.1 Synchronisation technologies

Synchronisation technology is a form of embedded middleware that facilitates the update of data between two or more devices, automatically updating for any changes on all the synchronised devices ensuring that the data sets are constantly identical (Gartner's IT Glossary, 2014; Yunos *et al.*, 2003:35). This is a practical technology in mobile solutions for employees that use more than one device for corporate functionality to ensure that information on all devices are consistently up-to-date. This eliminates double entries and duplicate work.

4.2.3.2 Virtualisation technologies

Gartner (2012b) recognises wireless network technology as the foundation of mobile infrastructure but also identifies the importance of virtualisation technology in delivering the benefits of mobile solutions. Virtualisation refers to the abstraction of IT resources, such as servers, storage, networks, applications or clients, and covers the physical limitations of the resources (Gartner's IT Glossary, 2014).

A prevalent virtualisation technology employed in a mobile environment is a server hosted virtual desktop (SHVD) (Gartner, 2012b). Desktop virtualisation separates a

PC desktop from the physical device, stores it on a centralised server and allows remote or mobile access to the desktop via a network (Gartner's IT Glossary, 2014).

4.2.3.3 Cloud technologies

Akella *et al.*, (2012) identifies cloud technologies as a significant enabling technology supporting the growing use of mobile devices by overcoming their inherent limitations with regard to storage capacity and other functionalities. Cloud technology is a computing model that facilitates ubiquitous, flexible and on-demand access to a shared pool of computing resources such as networks, servers, storage, applications and services that are instantaneously delivered to users via internet technologies (Enslin, 2012:9). Cloud services are provided in the form of three service models:

- **Software as a Service (SaaS):** is a model that provisions applications to users.
- **Platform as a Service (PaaS):** is a solution that provides the platform, including the databases, middleware and development tools, required for the development and deployment of applications.
- **Infrastructure as a Service (IaaS):** is a model that provides full IT infrastructure to users including servers, storage and virtualised networking hardware (Oracle, 2010).

Mobile users mostly download and execute SaaS applications to support and assist them in performing work functions. In order to control the use of cloud technologies by employees, the enterprise should consider the four deployment models of cloud services and select the appropriate model for the access, storage and use of its data and other functionalities:

- **Private clouds:** are used exclusively by one enterprise and hosted in private data spaces.
- **Public clouds:** are used by multiple enterprises and the general public and hosted and managed by external service providers.
- **Community clouds:** are used by a group of associated enterprises with shared interests.
- **Hybrid clouds:** are used by one enterprise that employs both private and public clouds (Enslin, 2012:7-8; Oracle, 2010).

4.3 Mobile applications

The application layer of mobile solutions includes mobile applications and mobile operating systems and provides the user with an interface to operate the mobile device (Sathyan *et al.*, 2012:72).

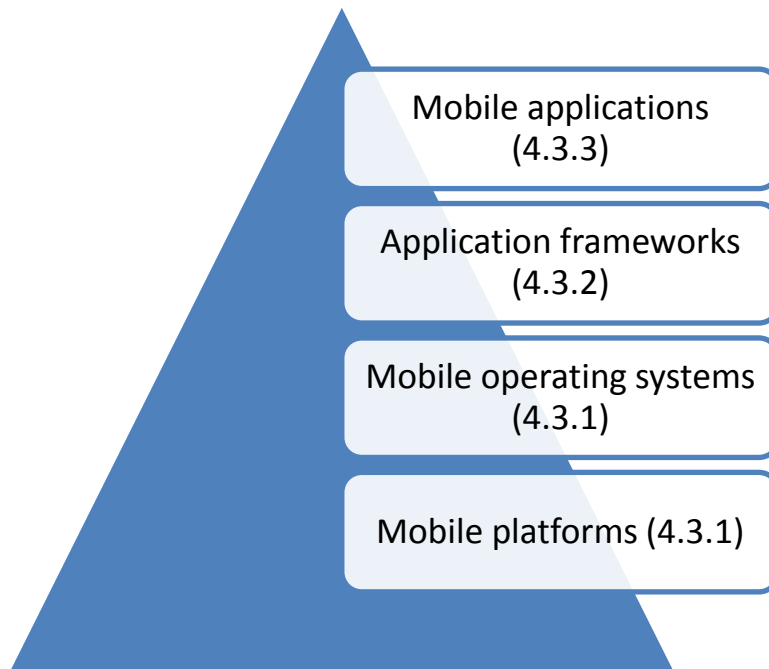


Figure 2: The building blocks of mobile application layer

4.3.1 Mobile operating systems and platforms

A mobile operating system is the principal software element on a processor-based mobile device (Juniper, 2009). The mobile operating system manages and operates hardware and software resources within the mobile device and serves as the platform on which other programmes run (Sathyan *et al.*, 2012; Renner, 2011; Juniper, 2009). It executes and manages basic tasks within the mobile device. These include receiving and identifying input from the keyboard, stylus or touch pad; delivering output to the mobile device screen; and managing device memory (Juniper, 2009). Furthermore, the mobile operating system is loaded by the device manufacturer and determines which applications can be executed on the device (Sathyan *et al.*, 2012:72). Core toolkits included in the mobile operating system manages communication between applications and ensures that applications and programmes operate without obstructing each other (Juniper, 2009; Fling, 2009:22).

4.3.1.1 Types of mobile operating systems

Mobile operating systems that once had significant market share, but that have become less relevant include Blackberry OS, Symbian and Palm OS (Gartner, 2013). Gartner's (2013) prediction of international device shipments by operating system shows that the operating systems that will have the biggest market share by 2017 include: Android 49.5%, Windows Phone 19.2%, iOS 17.0% and Blackberry OS 0.81%. Based on these findings, the following three operating systems were analysed:

- **Android:** Android is an operating system specifically developed for mobile devices by Google and the Open Handset Alliance (Renner, 2011). It is an open source operating system with a large group of developers developing applications that continuously expand and improve functionalities of mobile devices on this operating system. The system architecture consists of:
 - i. **Linux kernel:** Contains the drivers that control and communicate with device hardware. Android is built on the Linux kernel with some architectural modifications.
 - ii. **Android's native libraries:** Contain open source libraries coded in C or C++ that enable the mobile device to process and manage various types of data.
 - iii. **Android Runtime:** Draws from core libraries to deliver the key functions of Java. It also includes Dalvik virtual machine, a Java virtual machine (JVM) or abstraction layer between the application and the underlying platform, to execute applications.
 - iv. **Application framework:** Executes basic functions, services and libraries that run in Java for application development.
 - v. **Applications:** Operate on the Android operating system (Android-App-Market, 2012; Renner, 2011).
- **Windows Phone:** Windows Phone is a proprietary operating system developed by Microsoft. It runs on a modified Windows kernel. (Windows Phone, 2014; Renner, 2011). At its base layer, Windows Phone uses the Core Services. This is a minimal Windows system that executes basic operating system functionality. As the operating system is used across various devices, the Core system is supplemented by a set of binaries, specific to Windows

Phone, that form the Mobile Core (Windows Phone, 2014). The next layer of architecture includes the system services that run on top of the kernel. Included in this layer are, among others, services for the management of data, telephony, media and graphics (Windows Phone, 2014). The top layer contains programming frameworks and is used to develop applications. Application programming interfaces (APIs) in this layer include for example Silverlight, Common Language Runtime and JavaScript that support .Net applications (Windows Phone, 2014; Renner, 2011).

- **iOS:** iOS is a proprietary mobile operating system developed by Apple specifically for Apple's mobile devices. The operating system architecture is layered and the first two layers contain fundamental services and technologies, while the last two layers contain more sophisticated services and technologies.
 - i. **Core OS:** This layer is the kernel of the operating system and contains the basic frameworks that other technologies are built on.
 - ii. **Core services:** This layer is based on Objective-C and contains fundamental system services in the form of various frameworks. It also includes individual technologies that support features such as networking and social media.
 - iii. **Media services:** This layer contains the graphics, audio and video technologies used in application development.
 - iv. **Cocoa touch:** This layer is Objective-C based and contains the core frameworks and functionalities for developing iOS applications. (Apple, 2013; Renner, 2011)

Android, Windows Phone and iOS use a model of application sandboxing whereby each application is assigned a unique identity and all data, processes and permissions are assigned specifically to that application. Data assigned to one application has no access to the data of the next (Renner, 2011).

The significant characteristics of each type of mobile operating system are summarised in Table 4:

Table 4: The significant characteristics of mobile operating systems

Platform	Maintained by	Programming language	Example of device	Category
Android	Google/Open Handset Alliance	Java	Samsung galaxy	Open source
Windows phone	Microsoft	C#	Dell, HP, Motorola, Nokia	Proprietary
iOS	Apple	Objective-C	iPhone, iPad	Proprietary

(Holzinger, Tretler & Slany, 2012:179; Renner, 2011; Gavalas & Economou, 2011:78; Fling, 2009:22)

4.3.1.2 Categories of mobile operating systems

Based on the analysis of the characteristics of the three mobile operating systems, the following two categories of mobile operating systems were identified:

- **Proprietary:** Proprietary operating systems are licensed systems that are developed, owned and regulated by the developing company. Users pay royalties for right of use and the developing company provides support and updates (Juniper, 2009). Users that develop applications, including device manufacturers and operators, use Software Development Kits (SDKs), including APIs and other utilities, to support and facilitate code development. These developers access the operating system code through development partnership programmes (Juniper, 2009). The proprietor of the operating system has complete control over who develops applications. As they define the APIs, they also determine the features and functionalities of the operating system that are accessible (Juniper, 2009).
- **Open source:** The source code to an open source operating system is published and made available to the public to download and modify, allowing them to develop their own applications executable on the operating system (Fling, 2009:21). The code is often developed through the collaborative efforts

of programmers, and the code is continuously improved and updated (Juniper, 2009). No royalties are payable for the use of open source code and the community that maintains the system is often supported by stakeholders such as manufacturers, operators and software developers (Juniper, 2009).

4.3.2 Application frameworks or application programming interface

Application frameworks or application programming interfaces (APIs) are sets of programming instructions, protocols, tools and routines used to develop applications by opening up a programme's internal functionality. In the mobile technology context APIs run on top of the mobile operating system and operates as a software-to-software interface by linking the mobile application and the mobile operating system and allowing communication between the software (IBM, 2012; Fling, 2009:25). APIs, in the context of mobile application development, can be divided into two levels:

- **Low-level APIs:** Mobile applications use low-level APIs to access the basic features and functionalities of the mobile device. Some functionalities available to an application via low level APIs include interacting with the touch screen and keyboard, delivering graphics, connecting to networks, playing sounds through the device speaker or headphones and receiving images and videos from the camera (IBM, 2012).
- **High-level APIs:** In addition to the lower level hardware access required by mobile applications, high-level APIs facilitate more advanced functionality to the user. These services include web browsing, managing information and data as well as sending and receiving messages and making phone calls (IBM, 2012).

4.3.3 Mobile applications

Mobile applications are relatively small, separable software units with limited functionality developed specifically to run on mobile devices. Mobile applications are enabling the shift away from the traditional integrated software systems by providing users with the flexibility to determine the specific functionality of their mobile devices by installing selected mobile applications (Techopedia, 2014).

4.3.3.1 Types of mobile applications

A review of relevant literature revealed a range of diverse classification models for mobile application types (Unhelkar & Murugesan, 2010:34-35; Gasimov, Chuan-Hoo, Chee Wei & Sutanto, 2010:75; Fling, 2009:79-87). Based on the review, and the common characteristics identified, the following mobile application types were identified:

Table 5: Types of mobile applications

	Objective	Information flow	User interaction and input	Examples
Content and information application	<ul style="list-style-type: none"> Broadcast user requested information 	One directional	Little/ none	<ul style="list-style-type: none"> News applications such as BBC and NY Times Marketing applications and online directories E-books such as iBooks Video applications such as Netflix Music applications such as Pandora
Transactional application	<ul style="list-style-type: none"> Provide information and services Enable and execute financial transactions 	Multi directional	High	<ul style="list-style-type: none"> Banking applications Online booking applications
Collaborative applications	<ul style="list-style-type: none"> Facilitate user collaboration Provide rich user experience 	Multi directional	High	<ul style="list-style-type: none"> Social networking such as Facebook, Twitter, Linked-in, Pinterest, Instagram, Foursquare, Youtube Messaging applications such as Whatsapp Gaming applications
Productivity applications	<ul style="list-style-type: none"> Support task performance Deliver information and services Includes utilities 	Utilities: One directional Other: multi directional	Utilities: Little Other: High	<ul style="list-style-type: none"> E-mail applications Content management applications such as Evernote and Dropbox Voice recorder Utilities such as flashlight, calculator, weather applications as well as clock and time applications

4.3.3.2 Mobile application categories:

The development of mobile applications is classified into three categories (Budiu, 2013; IBM, 2012; Fling, 2009:70):

- Native applications:** Native applications have binary executable files that are downloaded directly onto the mobile device and reside locally on the device (IBM, 2012). These applications are developed and compiled specifically for one mobile platform and have full access to all device features and functionalities (Budiu, 2013; Fling, 2009:77). Native applications are installed through application stores or operating portals and the installation process is initiated by either the end user or IT department (Budiu, 2013; IBM, 2012; Fling, 2009:78). Once it is installed, the applications interface directly with the mobile operating system through APIs, without an intermediary (IBM, 2012). Before developing a native app, the enterprise needs to consider the device that will host the application; the availability of the skills and resources to test and certify the application; and the method of distribution (Fling, 2009:78). The developer of a native application uses tools, or the software development kits (SDKs) that are platform and language specific to each mobile operating system, to compile source code and create executables in binary form. These executables are packaged with additionally developed resources (such as images and audio segments) and distributed (IBM, 2012). Table 6 presents the different tools, languages, formats and distribution channels of mobile applications associated with the leading mobile operating systems (IBM, 2012).

Table 6: The characteristics of leading mobile operating systems

	Apple iOS	Android	Windows Phone
Languages	Objective-C, C, C++	Java (some C, C++)	C#, VB.NET and more
Tools	Xcode	Android SDK	Visual Studio, Windows Phone development tools
Packaging format	.app	.apk	.xap
Application store	Apple App Store	Google Play	Windows Phone Marketplace

- **Web applications:** Web applications are essentially websites delivered to a mobile device over the internet. Because of the powerful browsers run by advanced mobile devices, these rich browser-based applications produce native-like functionalities but are not installed on the device (Budiu, 2013; IBM, 2012; Fling, 2009:75). Access to web applications is instantaneous and installation on a mobile device only requires the user to navigate to the URL and create a bookmark (Budiu, 2013). Web applications are developed using web technologies such as HTML 5, Cascading Style Sheets 3 (CSS3) and advanced Java Script (IBM, 2012). Web application developers have a broad spectrum of options with regards to the nature of a web application. The two opposing ends of this spectrum are:
 - **Mobile optimised websites:** Mobile websites that recognise when it is accessed by a mobile device and present HTML pages adapted to the user interface of the mobile device.
 - **Mobile websites:** Appear to be native applications that are initiated from a shortcut similar to a native icon (IBM, 2012).
- **Hybrid applications:** Hybrid applications are accessed through mobile device browsers and combine the capabilities of native applications, that run on the mobile device, and multi-platform web technologies. Significant parts of the application are developed using web technologies but the applications retain access to the API for some functionalities (Budiu, 2013; IBM, 2012). The application operates by using the specific operating system APIs to create an embedded HTML rendering engine through the native portion of the application. This creates a bridge between the device APIs and the web browser. Developers can code their own bridge or use off-the-shelf options such as Phone-Gap (Budiu, 2013; IBM, 2012). The native portion of the application can be developed separately but solutions often include native containers that allow the development of an advanced application by accessing and leveraging device features using web language. The web portion is either a web page on the enterprise server or a set of web technologies bundled into application code and stored locally (IBM, 2012).

Each mobile application development category and its related benefits and limitations are set out in Table 7. The enterprise should select the most appropriate

category based on considerations such as financial constraints, IT infrastructure, required application functionality, timeframe, intended users and skill resources (Budi, 2013; IBM, 2012).

Table 7: A comparison of the benefits and limitations of mobile application development categories

	Native	Web	Hybrid
Platform independent	No	Yes	Yes
Development cost	High	Low	Low
User experience	Exceptional	Good	Good
Offline	Yes	Limited	Limited
Access to device features	Yes	No (very limited)	Yes (may be limited)
Installation	Effort	Instant access	Effort
Maintenance and upgrades	Complicated	Simple	Simple

(Budi, 2013; IBM, 2012; Fling, 2009:75-77)

4.4 Summary and conclusion

The investigation of mobile technology and its functionality identified three main components: (i) mobile devices; (ii) mobile infrastructure, data delivery mechanisms and enabling technologies; and (iii) mobile applications. The analysis of these components formed the basis for an understanding of the role of the various mobile technology components in enterprise operations. This understanding and the use of the detailed processes of COBIT, facilitated the identification of the significant risks that the enterprise is exposed to in Chapter 5.

CHAPTER 5: RISKS RELATED TO THE DEPLOYMENT OF MOBILE SOLUTIONS

The adoption and deployment of mobile solutions within an enterprise cannot be administrated and managed as a technical event in isolation. Mobile solutions are pervasive and it influences the flow of information within the entire enterprise, modifies the business processes and affects the operations of employees (ISACA, 2010). Mobile solutions affect business functions and as a result it introduces risk into all aspects of the business.

In order to apply a structured approach to risk identification, and to ensure that all significant risks are identified, the detailed processes of COBIT were applied to a mobile solution environment. The detailed considerations are documented in Annexure C and the significant risks were identified and grouped in two levels: risks arising from inadequate governance and management of mobile solutions and risks arising on an operational level.

5.1 Inadequate governance and management of mobile solutions

For many enterprises the deployment of mobile solutions is a reactive strategy to the consumerisation of mobile technology, and not a proactive strategy in order to fully utilise all mobile solution benefits. Mobile solution deployment is, therefore, often not adequately governed to ensure that all IT governance objectives are met. One of the key shortfalls of mobile solution strategies is board level involvement in the formulation of strategies and policies. Strategies and policies are also not sufficiently monitored for effectiveness and performance. A lack of appropriate, comprehensive mobile solution strategies and policies may expose the enterprise in the following areas:

- **Alignment:** The investment in and use of mobile solutions may not be aligned with enterprise strategies.
- **Value delivery:** The cost of mobile solution investments and use may exceed its benefit. In addition, opportunities to advance enterprise operations may be missed.
- **Risk assessment:** Mobile solution risk exposure may exceed the enterprise's risk tolerance levels and all risks that the enterprise is exposed to may not be identified. This will lead to insufficient mitigating controls and financial and other losses.

- **Resource management:** Resources may not be sufficient in meeting the enterprise's objectives for mobile solutions and may not be effectively and adequately employed. This may lead to excessive costs and the misallocation of resources.
- **Communication:** Communication with all stakeholders, including the board, management, IT staff, users, customers and suppliers, may not be sufficient to ensure the efficient deployment of mobile solutions and that the technology functions, and is used, as intended.
- **Ownership:** Ownership of mobile solution strategies and policies, if unassigned, may lead to miscommunication, undetected inefficiencies and inadequate incident management.
- **Relevance:** Mobile solution strategies and policies may become obsolete in a mobile environment where the technology advances at a rapid rate.
- **Change management:** Insufficient change management policies, for both planned and emergency changes, may lead to significant business continuity exposure.

5.2 Significant risks on an operational level

Risks at an operational level were identified using the detailed processes of COBIT and can be grouped in two classifications:

1. Risks that affect the users and the mobile technology's ability to function as intended. These include interoperability; user experience; connectivity; and IT support.
2. Risks that affect the enterprise strategies and objectives. These include continuity; security; cost; and data ownership.

These risks are discussed in the following sections.

5.2.1 Interoperability

ETSI (2008) defines interoperability as the ability of multiple systems within an infrastructure with diverse components to exchange data and intercommunicate using the same communication protocol. The core characteristics of an interoperable system are data or knowledge interchange, coordinated behaviour and cooperative problem solving (Wong, Ray, Parameswaran & Strassner, 2005:2058). Bentley (2013) and ETSI (2008) concluded that interoperability within a system is obstructed

by three main features: (i) hardware and software differences preventing compatibility and machine-to-machine communication; (ii) differences in data formats and data storage methods; and (iii) complex relationships between mobile components. Due to its nature, mobile solutions often present challenges on all three levels.

A mobile solution landscape is often a heterogeneous environment with diverse types and versions of mobile devices; software platforms and related programming languages; APIs and operating system architectures; and networking technologies (Abolfazli, 2014). In addition, the structure and composition of a mobile system often includes islands of activity and functionality which creates a complex system (ETSI, 2008). These characteristics of mobile solution environments create barriers to interoperability, leading to mobile solutions not functioning as intended (ETSI, 2008).

5.2.2 User experience

The performance requirements of the mobile user are productivity, convenience and on-demand and personalised functionality. The user interface creates the environment in which the mobile user transacts, communicates and locates information on a mobile device and dictates whether user requirements are met (Gansemer, Groner & Maus, 2007:699; Venkatesh, Ramesh & Massey, 2003:54).

Mobile devices contain inherent limitations that restrict the realisation of user expectations in terms of performance:

- **Visual output interface:** Mobile devices have small screens, sometimes with limited resolution that inhibits the optimal performance of tasks. Web sites accessed via mobile devices are often designed for desktop PCs or larger screens and users often have substandard experiences when accessing these websites using mobile devices.
- **Input interface:** Mobile devices, such as tablets and smartphones, often have small keyboards or are reliant on haptic or touch input, leading to cumbersome input. Furthermore, business applications, especially productivity and transactional applications often require mouse input, a feature not common in mobile devices such as smartphones and tablets.

- **Specifications:** Mobile devices often have a limited memory size, limited battery life and lower processor speeds than their desktop counterparts. These limitations are, however, increasingly addressed with the development of new devices.

(IFS, 2013; Gartner, 2012b; Sathyan *et al.*, 2012:31; Unhelkar & Murugesan, 2010:35; Gansemer *et al.*, 2007:699; Venkatesh *et al.*, 2003:54)

5.2.3 Connectivity

In the context of a mobile environment, connectivity refers to a user's ability to access data and functionality or transfer data from any location. Users of enterprise networks do not differentiate between wired and wireless networks. Mobile users have come to expect the same reliable connectivity, pervasive service and fast response times they have traditionally received from wired networks, of the wireless networks used in mobile solutions (Cisco and Citrix, 2014; Gartner, 2012a; CDW, 2012). Wireless networks often underperform when compared to their wired counterparts.

The inherent design of wireless networks often creates a barrier to its performance. Wireless systems were traditionally not built for ubiquitous mobility or the delivery of imperative services to critical business operations. They were initially intended to serve as temporary connectivity alternatives (Gartner, 2012a). In addition, the design of current wireless networks constitutes interconnected systems of servers (physical, virtual and cloud based), communication channels with mobile and fixed endpoints, as well as wired, WPAN, WLAN and WWAN networks run by different organisations. The enterprise often does not own one or more of the components of its wireless system but still needs to ensure reliable service delivery and support (Gartner, 2012a).

In addition, the demands on wireless networks and bandwidth have increased with the growth in the number of connected devices, the prevalence of data rich and real-time collaborative mobile applications as well as the increase in communication traffic (Cisco and Citrix, 2014; Gartner, 2012a; Deepak & Pradeep, 2012:179). These changes have created bandwidth bottlenecks and unreliable networks, often unable to deliver the quality of service required by mobile users to optimally use mobile solutions. Other barriers to the delivery of reliable, high performance connectivity

include signal disturbances and interference that cause loss of connectivity and coverage dead zones (Sathyan *et al.*, 2012:31; CDW, 2012; Deepak & Pradeep, 2012:179).

Infrastructure vendors have identified the challenges in building and maintaining wireless networks capable of providing high quality service to mobile users. The solutions offered by these vendors, however, often work in a siloed approach focusing on network policies and solutions per type of device. In a heterogeneous mobile environment, this provides a costly and complex solution to the enterprise (Aruba Networks, 2012).

5.2.4 IT support

Enterprises deploying mobile solutions regularly experience insufficient IT support due to the following characteristics of the mobile environment:

- the use of more than one device for both personal and corporate functionality;
- the variety of mobile devices and related operational platforms;
- the frequency with which users upgrade or change devices;
- the users' expectations of instant service delivery; and
- the increase in required configuration, help-desk and network support.

(Cisco and Citrix, 2014; Aruba Networks, 2012).

Renner (2011) also emphasises that in order to manage the risks inherent to mobile operating systems, the enterprise needs to understand the workings of all operating systems. The process of acquiring and maintaining these skills is costly and the lack of these skills leads to insufficient support for mobile solutions. In addition, mobile solution management is often outsourced to external service providers or vendors where the enterprise has insufficient internal resources or skills. The risk exists that external service providers do not provide aligned services and that all enterprise and user requirements are not met.

5.2.5 Continuity

Business continuity refers to the ability of an enterprise to continue its core business operations at an acceptable level during a time of interruption and disruption of services (ISO/IEC, 2012). Verizon (2008) identifies the six major IT threats to

business continuity as hardware failure, software failure, security events, network transmission, change management error and human error. The following three threats were identified as significantly threatening to business continuity specifically in a mobile environment (Apperian, 2013; Storagecraft, 2012; Sybase, 2011):

- **Security events:** In a mobile environment, corporate information assets are more susceptible to malware, hacker and cyber attacks and consequently, the enterprise's exposure to business continuity risks is increased. These risks include the increased likelihood of disruption of services due to malicious attack, but also the loss of competitive advantage and reputational damage in the instance of a material security breach.
- **Network transmission:** Continuous network access is critical for users of mobile solutions to operate optimally. Unstable wireless networks and disruption of connectivity in a mobile environment exposes the enterprise to business continuity risks as critical operations may come to a standstill.
- **Human error:** Mobile devices are specifically vulnerable to loss or theft. The loss of corporate data associated with the loss of a device may expose the enterprise to continuity risk.

Enterprise exposure to business continuity risk is further increased as traditional business continuity plans, involving off-site redundancy controls, are not appropriately revised to address the requirements of a mobile environment. Recovery time under traditional plans could take up to 72 hours and these turnaround times are considered inadequate in a mobile environment where users and customers expect real-time recovery and responses (Verizon, 2008).

5.2.6 Security

Information security refers to the safeguarding of data integrity and the protection of data from unauthorised access, use, distribution and modification while maintaining accessibility to authorised users (Gartner, 2012a). Mobile solutions have not changed the nature of information security risks, but introduce new developments to existing IT security risks (Sterk & Spruijt, 2013; Gartner, 2012b).

The deployment of mobile solutions introduces the following significant information security risks:

- **Device loss or theft** : Due to the nature and size of mobile devices, they are more susceptible to loss and theft than their desktop counterparts. This risk compromises the security of data stored on the device but also leads to loss of critical data if it is not stored on corporate servers (Akella *et al.*, 2012; Madgwicks, 2012; Wright *et al.*, 2011:17; Sybase, 2011).
- **Unauthorised data access and sharing**: This risk refers specifically to the unauthorised access to data by a seemingly authorised user where employees use one device for both personal and corporate use (Sybase, 2011). The risk also exists that authorised users upload sensitive or confidential data to cloud or website storage without enterprise knowledge or authorisation (Blackberry, 2014).
- **Transmission of data**: Mobile wireless networks are often more vulnerable to malicious attack and interception than wired networks. This affects both the confidentiality and integrity of data transmitted across wireless networks (Unhelkar & Murugesan, 2010:36).
- **Intentional security breaches**: Much like desktop computers, mobile devices are exposed to malicious attacks such as viruses, malware, Trojan horses, malicious applications, spam, phishing, spoofing and worms (Wright *et al.*, 2011:17). Mobile solutions, however, also introduce the following unique threats:
 - **Device cloning**: The electronic identity and information on a mobile device is cloned onto a second unofficial device. Access is gained to the device information and transactions and operations performed by the cloned device are then billed to the original device's owner.
 - **Jailbreak software**: Using specific coding, unauthorised access is gained to the device and all its content.
 - **Keystroke logging**: A type of malware is loaded onto the mobile device that records keystrokes to capture sensitive information.
 - **Zero-day exploit**: This attack takes advantage of security vulnerabilities on a mobile device before an update or patch is made available.

- **Bluetooth based attacks:** Bluebugging, bluejacking and blue snarling are examples of unauthorised access and the distribution of unsolicited messages using Bluetooth connections.
- **Wi-Fi sniffing:** Data is intercepted while it is sent to or from a mobile device over a non-secure network.
- **Automatic connectivity:** Mobile devices often have the capability to connect automatically to unknown Bluetooth devices in close vicinity or to unsecured Wi-Fi. This creates unmanaged connections and gives attackers access to device data and functionality.
- **Man-in-the-middle attack:** This attack intercepts and extracts information between two authorised users. The attacker orchestrates operations by connecting with two parties on both ends of a conversation or transaction, creating the impression that they are dealing with each other.
- **Eavesdropping:** This is the process of intercepting voice transmissions or transactions and listening in without consent of the conversing parties.
- **Malicious applications:** Applications on open platforms often have hidden functionality that harvest user data or act as hosting applications with administrative remote command execution capability.
- **Unauthorised location tracking:** The positioning capabilities on mobile devices allow for the tracking of their location and content for malicious purposes.

(GAO, 2012; Ernst & Young, 2012; Wright *et al.*, 2011:17; Sathyan & Sadasivan, 2010:3)

- **Gaps in mobile device management and security policy enforcement:** The management of mobile devices and the enforcement of security policies in a mobile environment are often inadequate due to the following factors:
 - Mobile devices are often not present in order for security software to be loaded.
 - The diverse landscape of mobile devices and operating systems as well as the rate of the introduction of new devices create a challenge in their management.

- The applications used for the access, storage and modification of business data have increased exponentially and each application includes its own distinct security protocols and data access capabilities (Sybase, 2011).
- **Out-dated software:** Old versions of mobile operating systems, plug-in software and application versions create a basic security risk on mobile devices. In BYOD environments, especially, it becomes impossible for enterprises to control whether users are running the latest versions of software and whether security patches and fixes are installed by the user. Out-dated mobile software versions expose the device to security vulnerabilities (Zscaler, 2013; GAO, 2012).

5.2.7 Cost

Deploying mobile solutions as part of an enterprise's operational activities may lead to significant cost implications for the enterprise. A study conducted by Akella *et al.*, (2012) found that 41% of CIOs consider these cost implications to be the critical challenge in the adoption of mobile solutions. Cost implications that need to be considered before deploying mobile solutions include:

- **Device costs:** In a COPE or COBO environment the enterprise carries the cost of investment in devices. In a BYOD environment the employee or user carries device cost, but other costs, identified below, are still influenced.
- **Software costs:** Software costs are increased by a number of investments that are necessary to effectively operate mobile solutions. These costs include the cost of developing and maintaining applications, the cost of enabling mechanisms such as desktop virtualisation, and the cost of management software such as mobile device management systems.
- **Connectivity costs:** Bandwidth costs increase considerably in a mobile environment primarily due to an increase in network traffic. In addition, the applications most frequently used by mobile users are often media rich and these applications and push delivery notifications cause further increases in connectivity costs.
- **Infrastructure and operational costs:** Mobile solutions require an investment in infrastructure modifications and upgrades as well as day-to-day

costs to support and maintain operations. The costs involved include the cost of wireless networks, the expansion of data storage and transmission capacity, the management costs of devices and applications, IT support costs, and the cost of user self-support tools.

- **Security costs:** Mobile solutions introduce incremental security risks and the controls implemented to mitigate these risks involve significant costs. These costs include, but are not limited to, the costs of authentication and encryption software, content protection, containerisation of data as well as the resources employed in the management and monitoring of security risks. Security breaches also lead to costs such as data remediation and the possible loss of competitive advantage.

(Cisco IBSG, 2012; Akella *et al.*, 2012; Gartner, 2012a; Sybase, 2011)

5.2.8 Data ownership

Loshin (2002) defines data ownership as both the possession of and responsibility for data. The responsibility for data assumes the control of data as an enterprise asset and this includes the ability to access, modify, create, remove and sell data as well as the right to assign these abilities. Mobility creates uncertainty in both areas of data ownership as corporate data is often communicated, stored, accessed and used on devices not owned by the enterprise.

The possession of the data is often not controlled as data is easily and informally shared and used in a mobile environment. The movement of data between devices and other IT components, that were previously protected by firewalls, is now unrestricted. Rights to data use are also exercised without clear allocation and assigning of such right (Oracle, 2014).

Intellectual property rights, similarly, have become unclear. Rights to content created on corporate devices were definite and clear and where an employee created content on enterprise-owned devices, the enterprise had a valid claim to the content. The risk, however, increases in an environment where content is created on personal devices outside of working hours (Madgwicks, 2012).

5.3 Less significant risks

In addition to the significant risks that affect the user and the enterprise strategies, enterprises need to be aware of other risks need to be considered when mobile technology is deployed. These risks are not considered to be as significant in affecting enterprise operations, but they need to be addressed to mitigate the consequences.

5.3.1 Licensing

Software licensing may create exposure for enterprises in situations where license terms apply only to corporate owned or leased devices and may not cover the use by employees of applications across multiple mobile devices. Conventional license agreements may also be specified on a per user or per device basis. This may create exposure in terms of breach of licensing contracts (Madgwicks, 2012).

5.3.2 Litigation

The consumerisation of mobile technology creates an environment where personal devices are used for corporate operations and enterprises need to consider litigation risk with regards to access to employees' private information, specifically also in terms of the Protection of Personal Information Act of 2013 (Madgwicks, 2012). In addition, enterprises need to consider all relevant regulations in terms of data safeguarding, data storage, data structuring and data extraction contained in acts such as the Sarbanes-Oxley Act of 2002.

5.3.3 Data retention

In mobile environments where corporate data is stored on personal or moving devices, enterprises may experience exposure in terms of regulations relating to the retention of corporate data (Madgwicks, 2012).

5.4 Summary and conclusion

The detailed processes of COBIT, as applied in Annexure C, identified significant risks related to the deployment of mobile solutions on a governance and management as well as an operational level. The mobile solution components identified and defined in Chapter 4 are associated with specific mobile solution risks

as summarised in Table 8. The risks identified in this chapter, if unaddressed, could have severe repercussions for the enterprise. Chapter 6 aims to identify and describe the mitigating control techniques that enterprises can implement to address the risks identified.

Table 8: A risk-component matrix: linking the underlying components of mobile technologies to the relevant significant risk it gives rise to

		Governance and management	Interoperability	User Experience	Continuity	Connectivity	Security	Data ownership	Cost	IT support
Devices	COBO	X		X	X		X		X	
	COPE	X		X	X		X		X	
	BYOD	X	X		X		X	X		X
Networks	WWAN	X		X	X	X	X		X	X
	WLAN	X		X	X	X	X		X	X
	WPAN	X		X	X	X	X		X	
Delivery mechanisms	Push	X	X	X					X	
	Pull	X	X							X
Enabling technologies	Synchronisation	X				X				
	Virtualisation	X	X			X			X	X
	Cloud	X	X			X	X	X		
Operating systems	Proprietary	X	X				X		X	
	Open source	X	X				X			
Applications	Native	X	X		X		X	X	X	X
	Web	X		X	X		X	X		

CHAPTER 6: CONTROLS IN A MOBILE ENVIRONMENT

Despite the significance of the risks that enterprises are exposed to when deploying mobile solutions, the controls to address and mitigate these risks are often not methodically planned and implemented. According to Sybase (2011) most enterprises deploying mobile solutions are implementing controls disjointedly and that the following factors contribute to this approach to risk mitigation:

- Enterprises are unprepared for the rate at which mobile devices and other mobile technology are developed.
- The shift to mobile solutions is driven by consumerisation, not corporate policies. This leads to a fragmented approach to risk mitigation.
- The implementation of controls is complicated by the number of devices that employees bring into the workplace.
- The ease of access to and the proliferation of mobile applications create a barrier to the management and control of risks.
- Enterprises perceive the adoption of a comprehensive mobility strategy to be too costly, complicated and challenging.

In order to mitigate the risks related to the deployment of mobile solutions, enterprises need to implement sufficient and appropriate controls on a governance, management and operational level. In terms of governance, the enterprise should develop and implement a customised and practicable mobile strategy as well as a set of comprehensive policies with best practices to ensure that the strategy is realised. At a management level, the enterprise needs to implement management systems that run mainly automated controls that would assist in the control, administration and monitoring of mobile solutions. At an operational level, the enterprise should implement both automated and manual control techniques at a technology component level to detect and mitigate risk exposure.

6.1 Mobile solution governance

In order to ensure the alignment of mobile solutions and business strategy, enterprises need to identify all internal and external factors influenced by mobile solutions, define their mobile objectives and formulate a mobile solution strategy and related policy documents that support these objectives (Oracle, 2014). A governance

system needs to be developed and implemented, taking the following important factors into consideration:

- **Board involvement:** The board needs to direct the system of mobility governance and designate roles, responsibility and decision-making authority.
- **Monitoring and reporting:** A system of governance monitoring needs to be developed and there needs to be sufficient reporting on governance efficiency and effectiveness.
- **Value contribution:** Regular cost-benefit analyses need to be compiled and analysed at board level.
- **Risk analysis:** The governance system should include a comprehensive risk management system that establishes enterprise risk tolerance levels, develops risk identification processes, addresses changes in technology risk profiles and assigns responsibility for risk identification and mitigation. This will include, where appropriate, a risk management team.
- **Communication:** All stakeholders need to be identified as part of the governance system and a communications policy should be developed and implemented.
- **Change management:** Policies, that address both planned changes and incident management, need to be developed and implemented.

6.1.1 Mobile strategy and related policies

The process of development of a mobile strategy needs to take into consideration all stakeholder requirements and expectations, including both the company and users, and facilitate the identification of new opportunities to advance business requirements (Akella *et al.*, 2012; Modus Associates, 2012). Gartner (2012a) identifies that enterprises often erroneously focus on only one mobility issue when defining and developing their mobile policies. Designing controls for one area of risk or exposure without understanding the overall effect or consequence may expose the entity to other risks. Another fundamental error that enterprises make, is the development of multiple mobile policies. It is important to have a single primary policy from which sub-policies are developed, ensuring consistency in support of all device types and applications as well as covering all user profiles, data, applications and software (Cisco IBSG, 2012; Sybase, 2011).

According to ISACA (2010), the characteristics of effective, executable mobile strategies and policies are: simplicity and ease of implementation; flexibility in order to adapt to changes in stakeholder requirements; auditability; and reliability under abnormal circumstances. Other considerations that enterprises need to take into account when developing a mobile strategy and related policies include:

- determining whether mobile solutions will be outsourced or developed and maintained in-house;
- considering the feasibility analysis per enterprise division, including cost analyses, consideration of the requirements for mobile technology as well as policies on cost monitoring and reporting;
- determining the resources and specific project plans necessary to migrate existing systems onto mobile systems;
- allocating specific responsibilities and decision-making authorities for mobile technology investments and its use;
- establishing performance measures for IT services, both outsourced and in-house, compiling and reviewing service level agreements with external service providers and evaluating internal IT staff performance regularly;
- establishing a programme for the continuous monitoring and evaluation of new and emerging threats in mobile platforms;
- maintaining and continuously updating existing strategies or developing new strategies to adapt to the introduction of new mobile devices, platforms and solutions;
- developing channels for the identification of areas of innovation;
- taking the full device life cycle into account, including the provisioning, production and decommissioning phases;
- defining and identifying allowable and approved devices and device types and applications. These restrictions should be broad enough to satisfy user requirements for productivity but narrow enough to reduce IT support workload. Determining the configuration specifications for each device, operating system and application type;
- defining the nature of services that are available on mobile devices;
- identifying and classifying both authorised or unauthorised uses of mobile devices by employees;

- specifying the storage and transmission procedures for enterprise information;
- including back up and redundancy policies; and
- establishing change controls.

(Blackberry, 2014; Oracle, 2014; Gartner, 2012a; Ernst & Young, 2012; Wright *et al.*, 2011:19; ISACA, 2010)

6.1.2 Training

The process of rolling out mobile policies should involve sufficient communication with all stakeholders. Application developers need to be trained in coding specifically for mobile device platforms (Ernst & Young, 2012) and IT personnel need regular refresher courses in terms of updated software versions, new security risks and technical developments. Users should be trained in the appropriate use of mobile devices including:

- awareness of security threats and securing of physical devices;
- regularly updating passwords;
- regularly updating applications and anti-virus or malware patches;
- not storing sensitive data on mobile devices;
- awareness of the appropriate channels for reporting problems and requesting IT support;
- reporting lost or stolen devices immediately;
- vigilance when opening e-mails and attachments on mobile devices or calling numbers on unsolicited sms's;
- limiting unnecessary applications; and
- limiting the use of public Wi-Fi for sensitive data.

(GAO, 2012; Madgwicks, 2012; Wright *et al.*, 2011:19).

6.2 Mobile solution management systems

6.2.1 Enterprise mobility management system (EMM system)

According to Garcia (2013:8) and Sterk and Spruijt (2013), the term enterprise mobility management (EMM) refers to the resources and processes employed to manage mobile devices, applications and data. EMM systems are software solutions that have been developed to assist the enterprise in effectively managing mobile solutions.

An important feature of an appropriate EMM system is that it is device and operating system independent in order to ensure continuity in support and management regardless of changes in technology. Another key characteristic of an EMM system is that it needs to provide an entire lifecycle management solution including configuration, provisioning, securing, support, monitoring and decommissioning of mobile solutions (Garcia, 2013:9). EMM systems are supported by mobile device management (MDM), mobile application management (MAM), mobile information management (MIM) and mobile expense management (MEM) systems.

- **Mobile Device Management (MDM):** MDM solutions are management and configuration tools that manage and administrate mobile devices as well as the related business resources by monitoring mobile device statuses and controlling functionality remotely via wireless communication technology (Sterk & Spruijt, 2013; Rhee, Jeon & Won, 2012:353). Most MDM solutions operate on diverse mobile devices and related operating systems (Sophos, 2013) and features of MDM solutions include policy enforcement, asset management, administration and reporting, help-desk tools, and the facilitation of software updates, data back-up and application installation (CDW, 2012). MDM solutions operate by registering the mobile device and user on the MDM system and configuring the specified policy for each device or device group. This allows IT to observe activity, application installation and data flow on the mobile device through an MDM application or agent. An MDM agent is installed on the mobile device either through an application store or in-house deployment. Instructions are sent to the MDM agent from the MDM server according to the configured policy and the MDM agent reports results in turn (Rhee *et al.*, 2012:354). According to Sterk and Spruijt (2013), MDM solutions contain inherent limitations as most users may not be content with locked devices and inaccessible functionality. In addition, mobile operating systems include contain their own APIs and mobile devices run different operating systems. The APIs per operating system determine whether MDM solution capabilities, such as restrictions, are supported and whether they are enforceable. Lastly, MDM solutions only address and manage the device and are not comprehensive tools for the management of all mobile solution complexities and exposures.

- **Mobile Application Management (MAM):** MAM tools are software systems that manage and administrate enterprise software on employee owned or corporate mobile devices and enable the secure provisioning of native applications. MAM systems facilitate enterprise software delivery, application configuration, application maintenance, usage tracking and policy enforcement. The usefulness of MAM solutions is limited, however, as it cannot manage mobile applications from public application stores. These public applications are isolated by closed mobile operating systems that prevent access to the MAM technology (Garcia, 2013:10; Sterk & Spruijt, 2013).
- **Mobile information management (MIM):** MIM focuses on the management and administration of data. Through the implementation of policies, IT manages the security and integrity of data regardless of the applications used. Off-the-shelf MIM system solutions have limited functionality in a diverse mobile landscape due to the closed architecture of mobile operating systems (Sterk & Spruijt, 2013).
- **Mobile Expense Management (MEM):** MEM solutions monitor and manage mobile data usage and trends. Features of MEM systems include the provision of information on the use of data and the sending of warnings to users when certain thresholds are reached (Sterk & Spruijt, 2013).

6.3 Mobile solution operational control techniques

Operational controls for mobile technology need to be designed and implemented on a component level in order to systematically mitigate all risk exposure. Enterprises should consider (i) mobile device controls; (ii) communication controls; (iii) mobile application and other software controls; and (iv) data controls.

6.3.1 Mobile device controls

Depending on the model of mobile device deployment, the devices used to access corporate information and functionality will either be the property of the employee or the enterprise. In both instances, however, the enterprise needs to ensure that sufficient security controls are in place. In a mobile environment, security policies can often be deployed through-the-air via remote configurations using MDM system software (Sophos, 2013; Sybase, 2011) and include:

- **Configuration controls:**
 - Configuring of browser security settings.
 - Enabling auto-lock where the device automatically locks after a certain lapse of time, requiring a password or passkey to regain access.
 - Disabling autocomplete functions that recollect usernames and passwords.
 - Setting requirements for complex passwords.
- **User authentication:** Requesting password login to access enterprise applications and data.
- **Remote lock:** Remote disabling of the device, rendering it inoperable.
- **Remote wipe:** Deleting device content selectively or completely and deactivating device functionality.
- **Data control:** Deleting data or blocking access to corporate e-mail when the user is not connected to the network for a certain time. This is done by the device itself.

(Sterk & Spruijt, 2013; Cisco IBSG, 2012; GAO, 2012; Sybase, 2011; Wright *et al.*, 2011:18)

Another control technique that can secure the content and functionality of mobile devices is dual identity whereby mobile device manufacturers enable two instances of the same operating system on one mobile device. One instance is enabled for corporate data and functionality and one for personal data and functionality. This is done through two types of hypervisors that enables virtual machines to operate. Type 1 (native or bare metal) hypervisors are hardware based technologies that create a duplicate copy of an operating system and runs both instances in two separate areas of the processor. On the other hand, Type 2 hypervisors run as a guest operating system on top of the host operating system and access the hardware by communicating through the host operating system (Rose, 2013:329). In addition to these security controls, enterprises can implement physical security controls such as cable locks for laptops and device tracking on all mobile devices, using GPS coordinates or tracking software to further protect mobile devices. In terms of the administration of mobile devices, enterprises should consider using a tiered approach to the provisioning of services and devices to users. This involves defining user groups and providing only the necessary functionality to each group. As an example, only basic services, such as corporate e-mail, are provided to the

broader user population and more extensive application resources are only provided to high value adding groups (Akella *et al.*, 2012). Device administration is further improved through device activity monitoring and logging which identifies issues, breaches and automates access control (Sybase, 2011).

6.3.2 Communication controls

Depending on current enterprise infrastructure, enterprises deploying mobile solutions will either build new or upgrade existing wireless mobile networks. In order to ensure appropriate and reliable service delivery and to maximise the enterprise investment, enterprises need to consider the following:

- **Establish requirements:** Consult all stakeholders and determine coverage, security level and availability requirements.
- **Managed wireless products:** Employ wireless controller technology that considers the network as a single component. This simplifies the management and configuration process as each wireless access point is not managed and configured separately.
- **Prioritise usage:** Ensure that critical corporate applications are prioritised through configuration management and firewalls. This will limit the automatic consumption of bandwidth even if the network is not actively used.
- **Develop a guest policy:** Include a guest policy that provides guest connections to the enterprise network through the use of automated guest provisioning systems. This will ensure that valuable IT department time is not spent connecting guests (CDW, 2012).

A significant challenge for enterprises using wireless networks is the development of secure networks and the maintenance of data integrity during transmission. Data integrity can be controlled using the following techniques:

- **Mutual authentication:** An authentication process where the communicating parties authenticate each other before any transaction is concluded.
- **Digital signature:** Validates the authenticity of information by confirming that messages were created by a known sender and that it was not altered during transmission. An example of this is the use of Public Key infrastructure where digital certificates are maintained that digitally signs and encrypts e-mails.

Most mobile devices have a set of public certificates depending on the platform.

- **Encryption:** Secures sensitive information during transmission. Enterprises need to assess the options available in terms of encryption on its various supported devices.
- **Secure Socket Layer (SSL):** A standard security technology for internet transmissions that ensures endpoint authentication and confidential transmissions through cryptography.
- **Disable wireless networks:** Disabling of Wi-Fi, Bluetooth and infrared when not in use.
- **Mobile VPN network:** Increase in the security of connections.
- **Settings:** Changing of settings of Bluetooth devices to non-discoverable to make them invisible to unauthenticated devices when not in use.
- **Network filters:** Monitoring the identity of users attempting access to the corporate network and blocking users that do not run the enterprise MDM software.

(GAO, 2012; Cisco IBSG, 2012; Wright *et al.*, 2011:18; Sathyan & Sadasivan, 2010:3)

In terms of implementing controls addressing the administration, cost and support of wireless mobile networks, Gartner (2012b) advises that a system management team is established to monitor and support these complex communication systems. This team should gather and store relevant, accurate and timely data on the performance of enterprise networks that will enable them to:

- assist in optimising the enterprise's investment in network technology;
- assist in meeting the necessary and expected performance requirements;
- ensure user productivity by increasing network availability; and
- ensure that incidents are detected and managed more timeously.

In addition, enterprises should consider automating the authentication and on-boarding process of employees and guests in order to self-register devices on secure wireless networks as well as VPNs in order to relieve the support duties of the IT department (Aruba Networks, 2012). The use of converged networks,

especially networks that integrate cellular and Wi-Fi transmissions, will further reduce costs and will be able to handle an increase in mobile device connections.

6.3.3 Application and other software controls

Mobile platforms were not originally developed for corporate use (Ernst & Young, 2012) but corporate functionalities have systematically been integrated on personal devices and, therefore, need to be administrated and managed through:

- **Application delivery:** The enterprise determines the circumstances and requirements that need to be met before an application can be run by a user or device.
- **Over-the-air provisioning:** IT remotely configures and updates applications.
- **Application blacklisting:** Unsecured or unsupported applications are listed and prevented from being run by mobile devices. This is a functionality often provided by MAM solutions. Alternatively, enterprises can use application whitelisting in which authorised applications are listed and, on initiation of an application, it is compared to the list and prevented from functioning if not found.
- **Limiting installation:** Corporate software can be accessed via mobile devices, but not locally installed and the corporate data does not leave the premises.
- **Updates:** All applications and software need to be regularly updated. This can be achieved through automatic updates, facilitated by MAM solutions or application configuration.
- **Software licensing:** Review agreements and update or renegotiate terms to support the enterprise's mobile solution landscape.

(Garcia, 2013:10; Sterk & Spruijt, 2013; Sophos, 2013; Akella *et al.*, 2012; Madgwicks, 2012; Wright *et al.*, 2011:18; Sybase, 2011; Sathyan & Sadasivan, 2010:3)

Virtualisation technologies allow for the efficient, secure and managed provisioning of corporate functionality on mobile devices. Two approaches to virtualisation should be considered:

- **Desktop virtualisation:** Creating a virtual desktop containing all authorised data and applications regardless of location or device. Data is transmitted directly from the corporate server to the device. IT supports and manages corporate software and applications centrally, while the user takes responsibility for device support (Cisco IBSG, 2012).
- **Application virtualisation:** Using user-centric application delivery, the application is delivered to the user and not the device. This requires investment in virtualisation technologies such as server hosted virtual desktops (SHVD) (Gartner, 2012b).

Another significant area of control over corporate applications is the testing of the applications. The different categories of mobile applications expose both the device and enterprise to different risks and they should, therefore, be tested for vulnerabilities and risks separately. The following test methods are applicable to native and web applications respectively:

- **Native applications:** Testing should be performed through the use of simulators contained within the SDK as provided by the application developers. These simulators allow the IT department to analyse and test applications in a variety of configurations and devices. Native applications should also be tested on the physical device to test features such as SMS, GPS, camera and Bluetooth that are not available through a simulator.
- **Web applications:** Testing should be done both as an anonymous user and as an authenticated user as web applications are accessible through the internet. Testers should also use traditional web browsers and standard application security assessment tool sets. During assessments, testers should scan web servers for infrastructure level risks and employ manual techniques to test for vulnerabilities that automated tools miss (Ernst & Young, 2012).

Protecting the security and integrity of corporate data is a priority for most enterprises, and this can be achieved through management of the applications that access, use, modify and store the data. MAM solutions are often used to facilitate these security controls by allowing the enterprise to monitor, administrate and control the functionalities of applications. The following are security controls that assist the enterprise in maintaining secure applications:

- **Segregating corporate functionality:** Designating corporate applications and data on the mobile device and controlling these according to mobile solution policies.
 - **Application access:** Restricting and preventing access to applications by unauthorised users via user authentication and password controls.
 - **Managing application capabilities:** Determining which applications access sensitive data and increasing access controls for these applications.
 - **One time password:** Allowing only single access and regenerating a password for every request for access to sensitive information.
 - **Out-of-band authentication:** Using a different channel to authenticate the user than the channel that the transaction is initiated in.
 - **Application wrapping:** Wrapping or containerising applications in order to separate corporate and private data. This allows IT to manage corporate data within an application without affecting personal information.
 - **Selective wipe:** Wiping corporate applications on the decommissioning of mobile devices.
 - **Third party e-mail clients:** Containing third party e-mails in a sandbox and encrypting messages and attachments.
 - **Anti-virus software:** Installing and regularly updating anti-virus software.
- (Sybase, 2011; Garcia, 2013:10; Sterk & Spruijt, 2013; Sophos, 2013; Sathyan & Sadasivan, 2010:3; Wright *et al.*, 2011:18)

6.2.4 Data controls

Enterprise data is being accessed, modified, created and stored on both corporate and personal mobile devices and this has created exposure in terms of the integrity of the data. Data can be safeguarded by:

- **Remote data wipe:** All corporate data is removed remotely.
- **Data fading:** In cases where a device is not connected to the enterprise network, data is automatically removed after a specific lapse of time.
- **Poison pill:** A message is sent that destroys data on the device and renders the device useless.
- **Data encryption:** Certain data on the mobile device is encrypted and encryption/ decryption mechanisms are password protected.

- **Full disk encryption:** All data on the mobile device is encrypted.
- **Data storage:** Managing, encrypting and establishing access controls over stored and backed-up data.
- **Thin mobile client models:** Data is stored and managed centrally, limiting the data stored on each device.

(Garcia, 2013:10; Sterk & Spruijt, 2013; Cisco IBSG, 2012; Wright *et al.*, 2011:18; Sybase, 2011; Sathyan & Sadasivan, 2010:3-4)

Another technique of securing corporate data is data containerisation. This is a security method provided by some MDM solutions that operates independently from the actual device by separating corporate and personal data and functionality on mobile devices. All information within the container is protected through user authentication and or encryption. The container is centrally managed allowing the enterprise to set all configurations. Information within the container can also be removed without affecting any other data in other containers (Garcia, 2013:10; Gartner, 2012b).

In terms of data ownership and legal rights to data, enterprises need to seek legal advice on existing employment contracts to ensure that intellectual property created by employees fall under corporate ownership regardless of location or device (Madgwicks, 2012).

6.4 Summary and conclusion

Enterprises deploying mobile solutions often unintentionally expose themselves to incremental risks that are not appropriately mitigated. Following a structured approach in terms of the formulation of governance, management and operational controls will ensure that enterprise exposure is limited and the full benefits of mobile solutions can be extracted. Table 9 summarises the specific control techniques that can be employed for every specific risk identified.

The columns of the table contain the significant risks and related detailed risks, as identified in Chapter 5 and based on the mobile technology components deployed by the enterprise, as in Table 8. The rows of the table formulate the internal control techniques that will mitigate the risks and link these controls to the specific risks they address.

Table 9: A risk-control matrix: linking the significant mobile solution risks to the relevant mitigating internal controls

		Governance	Inter-operability		User	Continuity		Connectivity		Security					Data ownership		Cost			IT support	
		Inadequate governance	Hardware and software non-compatibility	Differences in data formats	Inherent device limitations	Significant loss or disruption	Inadequate business continuity plans	Unreliable connectivity and performance	Bandwidth bottlenecks	Device loss or theft	Unauthorised access	Intentional security breaches	Insufficient management	Out-dated software	Possession and control of data	Intellectual property rights	Device, software and infrastructure costs	Transmission costs	Security costs	Insufficient support	External service providers
Governance	Develop and implement governance system	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Develop and implement a mobile strategy	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Develop and implement mobile solution policies	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Training	X	X	X	X	X		X	X	X	X	X	X	X		X	X	X	X		
Management systems (EMMS)	Mobile device management systems	X	X			X	X			X	X	X	X	X					X	X	
	Mobile application management systems	X	X	X							X	X	X		X				X	X	
	Mobile information management systems	X		X							X	X	X		X				X	X	
	Mobile expense management systems	X															X	X		X	

			Governance	Inter-operability		User	Continuity		Connectivity		Security					Data ownership		Cost			IT support	
			Inadequate governance	Hardware and software non-compatibility	Differences in data formats	Inherent device limitations	Significant loss or disruption	Inadequate business continuity plans	Unreliable connectivity and performance	Bandwidth bottlenecks	Device loss or theft	Unauthorised access	Intentional security breaches	Insufficient management	Out-dated software	Possession and control of data	Intellectual property rights	Device, software and infrastructure costs	Transmission costs	Security costs	Insufficient support	External service providers
Operational control techniques	Mobile device controls	User authentication								X	X	X		X								
		Remote wipe					X			X	X	X		X								
		Remote lock								X	X	X										
		Configuration controls: browser security, enabling auto-lock, password requirements, disabling auto-complete	X					X			X	X	X		X					X		
		Dual identify										X		X	X	X	X				X	
		Physical security					X				X	X										
		Tiered approach to service delivery								X								X	X		X	
		Device activity monitoring and logging										X	X	X					X		X	

		Governance	Inter-operability		User	Continuity		Connectivity		Security					Data ownership		Cost			IT support	
		Inadequate governance	Hardware and software non-compatibility	Differences in data formats	Inherent device limitations	Significant loss or disruption	Inadequate business continuity plans	Unreliable connectivity and performance	Bandwidth bottlenecks	Device loss or theft	Unauthorised access	Intentional security breaches	Insufficient management	Out-dated software	Possession and control of data	Intellectual property rights	Device, software and infrastructure costs	Transmission costs	Security costs	Insufficient support	External service providers
Communication controls	Use managed wireless products							X								X	X		X		
	Prioritise usage through configuration							X	X								X				
	Manage guest connections															X	X		X		
	Mutual authentication									X	X										
	Digital signatures and PKI									X	X										
	Encryption and SSL									X	X										
	VPN networks		X	X		X				X	X							X	X		
	Disable wireless networks									X	X							X			
	Wireless network settings undiscoverable									X	X							X			
	Network filters									X	X	X									
	Establish systems management team					X		X	X			X						X		X	
	Automate authentication and on-boarding									X										X	
	Use converged networks								X	X							X	X		X	

		Governance	Inter-operability		User	Continuity		Connectivity		Security				Data ownership		Cost			IT support			
		Inadequate governance	Hardware and software non-compatibility	Differences in data formats	Inherent device limitations	Significant loss or disruption	Inadequate business continuity plans	Unreliable connectivity and performance	Bandwidth bottlenecks	Device loss or theft	Unauthorised access	Intentional security breaches	Insufficient management	Out-dated software	Possession and control of data	Intellectual property rights	Device, software and infrastructure costs	Transmission costs	Security costs	Insufficient support	External service providers	
Application/ software controls	Application management		X	X																X		
	Over the air provisioning												X						X	X		
	Application blacklisting and whitelisting		X	X						X	X	X								X		
	Installation management								X	X				X								
	Regular software updates												X						X			
	Review and update of software licensing												X			X						
	Virtualisation technologies									X		X		X						X		
	Testing applications		X			X							X									
	Segregating corporate functionality										X		X			X					X	
	One time passwords									X	X											
	Out-of-band authentication										X	X										
	Application wrapping										X		X			X					X	
	Sandboxing										X	X			X							
	Anti-virus software										X	X		X								

		Governance	Inter-operability		User	Continuity		Connectivity		Security				Data ownership		Cost		IT support			
			Inadequate governance	Hardware and software non-compatibility		Differences in data formats	Inherent device limitations	Significant loss or disruption	Inadequate business continuity plans	Unreliable connectivity and performance	Bandwidth bottlenecks	Device loss or theft	Unauthorised access	Intentional security breaches	Insufficient management	Out-dated software	Possession and control of data	Intellectual property rights	Device, software and infrastructure costs	Transmission costs	Security costs
Data controls	Data fading										X				X						
	Poison pill					X				X	X	X			X						
	Managing data storage						X				X				X					X	
	Containerisation of data					X				X	X				X	X				X	
	Legal advice on employee contracts															X					

CHAPTER 7: CONCLUSION

The consumerisation of mobile technology is driving the expansion of mobile solutions in business operations at an exponential rate. The benefits derived from mobility are also driving enterprises to adopt mobile technology as part of their operations. Due to the nature of mobile solutions and the nature of its underlying components, however, significant incremental risks are being introduced into the business. Enterprises are often unaware of all the risks that they are exposed to when deploying mobile solutions and are not developing and implementing comprehensive systems of internal control to mitigate these risks. The process of deploying mobile solutions, for many enterprises, comes down to an *ad hoc* approach where the technology is used to address short-term requirements and not as part of the long term enterprise strategy. The objective of this research was to address this problem using a structured approach and to develop a risk matrix that would assist enterprises in evaluating their risk exposures from the mobile technology components deployed. In order to achieve this, the research aimed to (i) understand the technology and its underlying components; (ii) identify the significant risks relating to mobile solutions on a component level; and (iii) design appropriate controls to address these risks. From a review of relevant frameworks and standards, COBIT was selected as the most appropriate control framework to use for the identification of significant risks. Using the relevant processes of the framework, the significant risks were identified and mapped to appropriate controls to mitigate the risks.

The research found that mobile solutions mainly consist of three core components:

1. **Mobile devices:** Enterprises adopt different strategies in the use of mobile devices, ranging from device ownership that resides with the employee to corporately owned devices made available to the employee.
2. **Mobile infrastructure, delivery mechanisms and enabling technologies:** The functioning of mobile solutions is greatly dependent on wireless network technology to facilitate the location-independent use of mobile devices. These networks are classified based on their area of coverage. Delivery mechanisms determine how information is communicated to mobile devices via the wireless networks and enabling technologies support the delivery of maximum benefits from mobile operations.

3. **Mobile applications:** These include mobile platforms, mobile operating systems, mobile application interfaces and mobile applications. Mobile operating systems are mainly classified as open source or proprietary and mobile applications are classified as native, web or a combination of the two.

A review of prior literature found that research has been mainly focused on security as a significant risk related to the deployment of mobile solutions. This research, however, found that the significant risks that enterprises are exposed to are linked to the components of the mobile technology deployed and the following risks were identified using COBIT: interoperability, user experience, connectivity, IT support, continuity, security, cost and data ownership.

In order to address the identified risks, enterprises need to follow a methodical approach incorporating three levels of internal controls:

1. **Mobile solution governance:** The development and implementation of mobile solution strategies and policies, ensuring alignment with business strategies. This level includes the sufficient training of all stakeholders.
2. **Management systems:** The implementation of manual or software systems that support the control of the components of mobile solutions and provide management with information on the use of the technology.
3. **Operational control techniques:** The design and implementation of detailed control techniques on a mobile device, communication, application and data controls level.

The research focused on producing a theoretical basis for the identification of mobile solution risks and related internal controls, given the specific mobile technology component landscape of an enterprise. An area of future research is the application of both the risk and component and the risk and control matrixes to local and international enterprises. A specific area of potential research is the application of the matrixes to small and medium sized entities in the South African context to determine the practical results of its application. The aim would be to establish whether previously unidentified risks are identified and whether existing internal control systems are improved through the use of the matrixes.

REFERENCES

- Akella, J., Brown, B., Gilbert, G. & Wong, L. 2012. Mobility disruption: A CIO perspective. [Online]. Available: http://www.mckinsey.com/insights/business_technology/mobility_disruption_a_cio_perspective [Accessed: 14 May 2013].
- Android-App-Market. 2012. Android Architecture – The Key Concepts of Android OS. [Online]. Available: <http://www.android-app-market.com/android-architecture.html> [Accessed: 23 July 2014].
- Anisingaraju, S. 2013. What does COBIT 5 mean for your business? *COBIT Focus*, 4, October 2013. [Online]. Available: <http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Pages/COBIT-Focus-Volume-4-October-2013.aspx> [Accessed: 17 June 2014].
- Apperian. 2013. Addressing Enterprise Mobility and Continuity Challenges. [Online]. Available: <http://www.apperian.com/addressing-enterprise-mobility-and-continuity-challenges/> [Accessed: 5 August 2014].
- Apple. 2013. iOS Technology Overview. [Online]. Available: <https://developer.apple.com/library/ios/documentation/Miscellaneous/Conceptual/iPhoneOSTechOverview/iOSTechOverview.pdf> [Accessed: 23 July 2014].
- Arokiamary, V.J. 2008. Mobile computing. Pune, India: Technical Publications.
- Aruba Networks. 2012. Conquering today's bring-your-own-device challenges: A framework for successful BYOD challenges. [Online]. Available: http://www.arubanetworks.com/pdf/technology/whitepapers/WP_BYOD.pdf [Accessed: 26 February 2013].
- Arraj, V. 2013. ITIL: The basics. [Online]. Available: http://www.best-management-practice.com/gempdf/itil_the_basics.pdf [Accessed: 26 February 2013].
- Babb, S. 2014. Are COSO 2013 and COBIT 5 Compatible?. *COBIT Focus*, 3, July 2014. [Online]. Available: <http://www.isaca.org/COBIT/focus/Pages/Are-COSO-2013-and-COBIT-5-Compatible.aspx> [Accessed: 22 July 2014].
- Bai, C., Liu, Q., Lu, J., Song, F.M. & Zhang, J. 2003. Corporate governance and market valuation in China. *Journal of Comparative Economics*, 32:599-616.
- Basole, R.C. 2007. The Emergence of the Mobile Enterprise: A Value-Driven Perspective. *Sixth International Conference on the Management of Mobile Business*. 9-7 July, 41. Toronto, Canada. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4278584> [Accessed: 15 May 2013].
- Basole, R.C. 2008. Enterprise Mobility: Researching a new paradigm. *Information Systems Management*, 7:1-7.

Bentley. 2013. Interoperability Platform. [Online]. Available: ftp://ftp2.bentley.com/dist/collateral/Web/Platform/WP_Interop_Platform.pdf [Accessed: 22 July 2014].

Blackberry. 2014. Making the case for COPE. [Online]. Available: <http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/Case-for-COPE-Whitepaper.pdf> [Accessed: 2 July 2014].

Boshoff, W.H. 2013. Masters in Accounting (Computer Auditing). Unpublished lecture slides. Stellenbosch: University of Stellenbosch.

Brisebois, R., Boyd, G. & Shadid, Z. 2001. What is IT Governance and why is it important for the IS auditor?. [Online]. Available: http://www.intosaitaudit.org/intoit_articles/25_p30top35.pdf [Accessed: 17 June 2014].

Budiu, R. 2013. Mobile: Native Apps, Web Apps, and Hybrid Apps. [Online]. Available: <http://www.nngroup.com/articles/mobile-native-apps/> [Accessed: 12 June 2014].

CDW. 2012. Wi-Fi: Far and Wide. [Online]. Available: <http://www.opus1.com/www/whitepapers/WirelessInfrastructure2012.pdf> [Accessed: 8 May 2013].

Cisco IBSG. 2012. BYOD: A global perspective. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf [Accessed: 27 February 2013].

Cisco and Citrix. 2014. Cisco and Citrix for Productive and Secure Enterprise Mobility. [Online]. Available: <http://www.cisco.com/c/dam/en/us/solutions/enterprise-networks/mobile-workspace-solution/citrix-cisco-mobility-wp.pdf> [Accessed: 2 July 2014].

Deepak, G. & Pradeep, B.S. 2012. Challenging issues and limitations of mobile computing. *International Journal of Computer Technology & Applications*, 3(1):177-181. [Online]. Available: <http://www.ijcta.com/documents/volumes/vol3issue1/ijcta2012030132.pdf> [Accessed: 18 June 2014].

Enslin, Z. 2012. Cloud computing: COBIT-mapped benefits, risks and controls for consumer enterprises. Unpublished master's thesis. Stellenbosch: University of Stellenbosch.

Ericsson. 2014. Ericsson Mobility Report: On the pulse of the networked society. [Online]. Available: <http://www.ericsson.com/res/docs/2014/ericsson-mobility-report-june-2014.pdf> [Accessed: 31 October 2014].

Ernst & Young. 2012. Mobile device security: Understanding vulnerabilities and managing risks. [Online]. Available: [http://www.ey.com/Publication/vwLUAssets/EY_Mobile_security_devices/\\$FILE/EY_Mobile%20security%20devices.pdf](http://www.ey.com/Publication/vwLUAssets/EY_Mobile_security_devices/$FILE/EY_Mobile%20security%20devices.pdf) [Accessed: 2 July 2014].

ETSI. 2008. Achieving Technical Interoperability – the ETSI approach. [Online]. Available: <http://www.etsi.org/WebSite/document/whitepapers/IOP%20whitepaper%20Edition%203%20final.pdf> [Accessed: 22 July 2014].

Fling, B. 2009. Mobile design and development. California, United States of America: O'Reilly Media.

Forrester. 2013a. The Forrester Wave: Enterprise Mobility Services, Q1 2013. [Online]. Available: <https://www.forrester.com/The+Forrester+Wave+Enterprise+Mobility+Services+Q1+2013/fulltext/-/E-RES87581> [Accessed: 14 May 2013].

Forrester. 2013b. 2013 Mobile Workforce Adoption Trends. [Online]. Available: https://www.vmware.com/files/pdf/Forrester_2013_Mobile_Workforce_Adoption_Trends_Feb2013.pdf [Accessed: 20 May 2013].

Franklin, M. & Zdonik, S. 1998. Data in your face: push technology in perspective. *ACM SIGMOND Record*, 27(2):516-519.

Fry, M. 2005. Top ten reasons organizations are unsuccessful implementing ITIL. [Online]. Available: http://i.zdnet.com/whitepapers/ITIL_Malcolm_Top_Ten.pdf [Accessed: 11 June 2014].

Gansemer, S., Groner, U. & Maus, M. 2007. Data classification of mobile devices. *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*. 6-8 September, 699-703. Dortmund, Germany. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4488513> [Accessed: 27 June 2014].

GAO. 2012. Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. [Online]. Available: <http://www.gao.gov/assets/650/648519.pdf> [Accessed: 2 July 2014].

Garcia, D.A. 2013. Study, analysis and implementation of an Enterprise Mobility Management System. Unpublished master's thesis. Barcelona: Universitat Politècnica de Catalunya.

Gartner. 2012a. Bring Your Own Device: New Opportunities, New Challenges. [Online]. Available: <http://www.gartner.com/id=2125515> [Accessed: 26 February 2013].

Gartner. 2012b. Enterprise Mobility and Its Impact on IT. [Online]. Available: <http://www.gartner.com/id=1985016> [Accessed: 20 May 2013].

Gartner. 2013. Gartner predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes. [Online]. Available: <http://www.gartner.com/id/2466615> [Accessed: 20 May 2013].

Gartner. 2014. Gartner says worldwide traditional PC, Tablet, Ultramobile and Mobile Phone Shipments to Grow 4.2 Percent in 2014. [Online]. Available: <http://www.gartner.com/newsroom/id/2791017> [Accessed: 31 October 2014].

Gartner's IT glossary. 2014. [Online]. Available: <http://www.gartner.com/it-glossary/> [Accessed: 30 June 2014].

Gasimov, A., Chuan-Hoo, T., Chee Wei, P. & Sutanto, J. 2010. Visiting mobile application development: What, how and where. *2010 Ninth International Conference on Mobile Business and 2010 Ninth Global Mobility Roundtable*. 13-15 June, 74-81. Athens, Greece. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5494784> [Accessed: 12 June 2014].

Gavalas, D. & Economou, D. 2011. Development platforms for mobile applications: status and trends. *IEEE Software*, 28(1):77-86.

Ghoda, A. 2009. *Pro Silverlight for the Enterprise*. New York, United States of America: Apress.

Glasshouse. 2013. Is your BYOD Plan Exposing You to Risk?. [Online]. Available: <http://www.thedatachain.com/materials/byodplanrisk.pdf> [Accessed: 2 July 2014].

Goosen, R. 2012. The development of an integrated framework in order to implement information technology governance principle at a strategic and operational level for medium- to large-sized South African business. Unpublished master's thesis. Stellenbosch: University of Stellenbosch.

Grose, C., Kargidis, T. & Vasilios, C. 2014. Corporate Governance in practice. The Greek case. *Procedia Economics and Finance*, 9:369-379. [Online]. Available: http://ac.els-cdn.com/S2212567114000380/1-s2.0-S2212567114000380-main.pdf?_tid=07e50188-718c-11e4-86f9-00000aab0f6c&acdnat=1416580877_a8085273ad48001706bbd6d2008997e1 [Accessed: 17 July 2014].

Hardy, G. 2006. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Information Security Technical Report*, 11:55-61.

Henderson, J.C. & Venkatraman, N. 1999. Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 38(2-3):472-484.

Henry-Stocker, S. 2010. What Does ISO 27001 Mean to You?. [Online]. Available: <http://www.itworld.com/article/2761833/security/what-does-iso-27001-mean-to-you-.html> [Accessed: 23 June 2014].

Holzinger, A., Treitler, P. & Slany, W. 2012. Making Apps Usable on Multiple Different Mobile Platforms: On Interoperability for Business Application Development on Smartphones, in G. Quirchmayr, J. Basl, I. You, L. Xu & E. Weippl (eds).

Multidisciplinary Research and Practice for Information Systems. Berlin, Germany: Springer. 176-189.

IBM. 2012. Native, Web or Hybrid mobile-app development. [Online]. Available: www01.ibm.com/common/ssi/cgibin/ssialias?infotype=SA&subtype=WH&htmlfid=WSW14182USEN#loaded [Accessed: 7 July 2014].

IFS. 2013. The business benefits of enterprise mobile solutions. [Online] Available: [file:///C:/Users/Isahd/Downloads/White%20paper%20The%20business%20benefits%20of%20enterprise%20mobile%20solutions_004265%20\(1\).pdf](file:///C:/Users/Isahd/Downloads/White%20paper%20The%20business%20benefits%20of%20enterprise%20mobile%20solutions_004265%20(1).pdf) [Accessed: 8 May 2013].

Institute of Directors Southern Africa (IODSA). 2009. King Code of Governance for South Africa 2009. [Online]. Available: <http://african.ipapercms.dk/IOD/KINGIII/kingiiiireport/> [Accessed: 7 July 2014].

ISACA. 2010. Securing Mobile Devices. [Online]. Available: http://www.isaca.org/knowledge-center/research/documents/securemobiledevices_whp_Eng_0710.pdf?id= [Accessed: 9 June 2014].

ISACA. 2012a. COBIT 5:A Business Framework for the Governance of Enterprise IT. United States of America.

ISACA. 2012b. COBIT 5: Process Reference Guide. United States of America.

ISO/IEC. 2012. ISO 22301: Societal security – Business continuity management systems – Requirements. Switzerland.

ISO/IEC. 2008. ISO/IEC 38500: Corporate Governance of information technology. Switzerland.

ISO 27001 Security. 2014. [Online]. Available: <http://www.iso27001security.com/> [Accessed: 31 October 2014].

IT governance. 2014. ISO 27001 & Information Security. [Online]. Available: <http://www.itgovernance.co.uk/iso27001-kw.aspx#.U5WjnfIQtkU> [Accessed: 6 June 2014].

IT Governance Institute (ITGI). 2003. Board Briefing on IT Governance, 2nd Edition. [Online]. Available: http://wikimp.mp.go.gov.br/twiki/pub/EstruturaOrganica/AreaMeio/Superintendencias/SINFO/Estrategia/BibliotecaVirtual/MaterialExtra/26904_Board_Briefing_final.pdf [Accessed: 18 June 2014].

ITIL. 2011. An Introductory Overview of ITIL 2011. Norwich: United Kingdom.

Juniper. 2009. Open Source OS – The Future for Mobile?. [Online]. Available: <http://www.juniperresearch.com/whitepaper/open-source-OS-the-future-for-mobile> [Accessed: 17 July 2014].

Krechovská, M. & Procházková, P. T. 2014. Sustainability and its Integration into Corporate Governance Focusing on Corporate Performance Management and Reporting. *Procedia Engineering*, 69:1144-1151. [Online]. Available: http://ac.els-cdn.com/S187770581400349X/1-s2.0-S187770581400349X-main.pdf?_tid=f684d5de-718c-11e4-9db3-00000aab0f01&acdnat=1416581277_1d7ed0e3af4214419aa42383c171ea1f [Accessed: 24 June 2014].

Krivida, C.D. 2008. 6 Business imperatives: Gartner's Mark A Beyer outlines the drivers of IT initiatives. *Teradata Magazine*, 8(2). [Online]. Available: <http://apps.teradata.com/tdmo/v08n02/Features/BusinessImperatives.aspx> [Accessed: 19 June 2014].

Lewis, M. 2006. Comparing, Designing, and Deploying VPNs. Indianapolis, United States of America: Cisco Press.

Loshin, D. 2002. Knowledge Integrity: Data Ownership. [Online]. Available: jbutler.biz/mis/Ownership.doc [Accessed: 4 August 2014].

Macehiter Ward-Dutton. 2005. On IT-business alignment. [Online]. Available: <file:///C:/Users/Isahd/Downloads/on-it-business-alignment.pdf> [Accessed: 18 June 2014].

Madgwicks. 2012. Bring your own device. [Online]. Available: <http://madgwicks.com.au/files/file/PUBLIC/News/Whitepaper%20-%20BYOD%20%20September%2017%202012.pdf> [Accessed: 26 February 2013].

Mataracioglu, T. & Ozkan, S. 2011. Governing information security in conjunction with COBIT and ISO 27001. [Online]. Available: <http://arxiv.org/abs/1108/1108.2150.pdf> [Accessed: 18 June 2014].

Modus Associates. 2012. The Mobile Strategy Guide. [Online]. Available: http://modusassociates.com/downloadables/Modus_MobileStrategyGuide.pdf [Accessed: 2 June 2014].

Nicho, M. & Fahkry, H. 2011. An Integrated Security Governance Framework for Effective PCI DSS Implementation. *International Journal of Information Security and Privacy*, 5(3):50-67. [Online]. Available: <http://www.igi-global.com/article/integrated-security-governance-framework-effective/58982> [Accessed: 2 July 2014].

Okoli, C. & Schabram, K. 2010. A Guide to Conducting a Systematic Literature Review of Information System Research. *Sprouts: Working Papers on Information Systems*, 10(26). [Online]. Available: <http://sprouts.aisnet.org/10-26> [Accessed: 27 June 2014].

Oliver, D. & Lainhart, J. 2011. *COBIT Focus*, 3, July 2011. [Online]. Available: <http://www.isaca.org/COBIT/COBIT-focus/Documents/COBIT-Focus-Vol-3-2011.pdf> [Accessed: 12 June 2014].

- Oliver, D. & Lainhart, J. 2012. COBIT 5: Adding value through effective GEIT. *The EDP Audit, Control and Security Newsletter*, 46(3). [Online]. Available: <http://www.tandfonline.com/doi/pdf/10.1080/07366981.2012.706472> [Accessed: 11 June 2014].
- Oracle. 2010. Oracle Cloud Computing. [Online]. Available: <http://www.oracle.com/us/technologies/cloud/oracle-cloud-computing-wp-076373.pdf> [Accessed: 21 July 2014].
- Oracle. 2014. The New Perimeter: Keeping Corporate Data Secure in the Mobility Era. [Online]. Available: <http://www.oracle.com/us/products/middleware/identity-management/mobile-security/transformation-perimeter-wp-2199245.pdf> [Accessed: 21 July 2014].
- Overby, S. 2012. Adopting ITIL, COBIT is not always the best practice. [Online]. Available: <http://www.cio.com/article/2399188/it-organization/adopting-til-cobit-is-not-always-the-best-practice.html> [Accessed 11 June 2014].
- Pillay, A., Diaki, H., Nham, E., Senanayake, S., Tan, G. & Deshpande, S. 2013. Does BYOD increase risks or drive benefits?. [Online]. Available: https://minerva-access.unimelb.edu.au/bitstream/handle/11343/33345/300314_2013_Tan_Risk.pdf [Accessed: 3 July 2014].
- Pinola, M. 2014. Mobile Computing Devices. [Online]. Available: <http://mobileoffice.about.com/od/mobile-devices/a/mini-computers-and-mobile-devices.htm> [Accessed: 7 February 2014].
- Radovanović, D., Radojević, T., Lučić, D., Sarac, M. 2010. IT audit in accordance with COBIT standard. *MIPRO 2010 Proceedings of the 33rd International Convention*. 24-28 May, 1137-1141. Opatija, Croatia. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5533627> [Accessed: 12 June 2014].
- Renner, T. 2011. Mobile OS - Features, Concepts and Challenges for Enterprise Environments. [Online]. Available: https://www.snet.tu-berlin.de/fileadmin/fg220/courses/SS11/snet-project/mobile-os-features_renner.pdf [Accessed: 9 July 2014].
- Rhee, K., Jeon, W. & Won, D. 2012. Security Reuiqirements of a Mobile Device Management System. *International Journal of Security and Its Applications*, 6(12):353-358. [Online]. Available: http://www.sersc.org/journals/IJSIA/vol6_no2_2012/49.pdf [Accessed: 27 June 2014].
- Rose, C. 2013. Corporate Owned Personally Enabled (COPE): the superior paradigm for smartphones in the enterprise. *The Clute Institute International Academic Conferences*. 3-5 January, 327-328. Maui, Hawaii.
- Rousseau, D.M., Manning, J. & Denyer, D. 2008. 11 Evidence in Management and Organizational Science: Assembling the Field's Full Weight of Scientific Knowledge

Through Syntheses. *The Academy of Management Annals*, 2(1):475-515. [Online]. Available: <http://www.tandfonline.com/doi/pdf/10.1080/19416520802211651> [Accessed: 27 June 2014].

Rudman, R.J. 2008a. IT Governance: A New Era. *Accountancy SA*, March 2008:12-14.

Rudman, R.J. 2008b. Demystifying COBIT. *Accountancy SA*, April 2008:22-24.

Rudman, R.J. 2010. Framework to identify and manage risks in Web 2.0 applications. *African Journal of Business Management*, 4(13):3251-3264. [Online]. Available: http://www.academicjournals.org/article/article1380697598_Rudman.pdf [Accessed: 17 June 2014].

Sahibudin, S., Sharifi, M. & Ayat, M. 2008. Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. *Second Asia International Conference on Modelling & Simulation*. 13-15 May, 749-753. Kuala Lumpur: Malaysia. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4530569> [Accessed: 17 June 2014].

SAICA. 2010. What is IT Governance?. [Online]. Available: <https://www.saica.co.za/Members/GovernIT/WhatisITGovernance/tabid/2270/language/en-ZA/Default.aspx> [Accessed: 5 February 2014].

Samsung. 2013. Samsung Knox Value Proposition in the BYOD/COPE market. [Online]. Available: http://www.samsung.com/uk/business-images/resource/case-study/2014/04/Samsung_KNOX_Value_Proposition_BYOD_COPE_2013-0.pdf [Accessed: 3 July 2014].

Sathyan, J. & Sadasivan, M. 2010. Multi-layered collaborative approaches to address enterprise mobile security challenges. *2010 IEEE 2nd Workshop on Collaborative Security Technologies (CoSec)*. 15 December, 1-6. Bangalore, India. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=5730691> [Accessed: 15 May 2013].

Sathyan, J., Anoop, N., Narayan, N. & Vallathai, S. K. 2012. A comprehensive guide to enterprise mobility. Florida, United States of America: CRC Press.

Song, Y. & Lee, J. 2012. Mobile device ownership among international business students: a road to the ubiquitous library. *Reference Services Review*, 40(4):574-588.

Sophos. 2013. Sophos Mobile Control. [Online]. Available: <http://www.sophos.com/enus/medialibrary/PDFs/factsheets/sophosmobilecontroldna.pdf?la=en> [Accessed: 5 8 July 2014.]

Standards Consultants. 2014. Benefits of Certification to ISO/IEC 27001. [Online]. Available: <http://www.standardsconsultants.com/benefits-of-isoiec-27001> [Accessed: 23 June 2014].

Sterk, P. & Spruijt, R. 2013. Enterprise Mobility Management Smackdown. [Online]. Available: <http://www.pqr.com/enterprise-mobility-management-smackdown> [Accessed: 2 April 2014].

Storagecraft. 2012. Mobile device backup key for overall business continuity. [Online]. Available: <http://www.storagecraft.com/blog/mobile-device-backup-key-for-overall-business-continuity/> [Accessed: 5 August 2014].

Sybase. 2011. Mobility Advantage: Why Secure your Mobile Devices?. [Online]. Available: www.sybase.co.za/files/White.../Sybase_Afaria_WhySecurity_wp.pdf [Accessed: 9 May 2013].

Sylvester, A., Tate, M. & Johnstone, D. 2010. Beyond Synthesis: re-presenting heterogeneous research literature. *Behaviour & Information Technology*, 32(12): 1199-1215.

Symons, C. 2005. IT Governance Framework. [Online]. Available: <http://i.bnet.com/whitepapers/051103656300.pdf> [Accessed: 12 June 2014].

Techopedia. 2014. Mobile applications. [Online]. Available: <http://www.techopedia.com/definition/2953/mobile-application-mobile-app> [Accessed: 14 July 2014].

Unhelkar, B. & Murugesan, S. 2010. The Enterprise Mobile Application Development Framework. *IT Professional*, 12(3):33-39.

Venkatesh, V., Ramesh, V. & Massey, A.P. 2003. Understanding usability in mobile commerce. *Communications of the ACM – Mobile computing opportunities and challenges*, 46(12):53-56. [Online]. Available: <http://dl.acm.org/citation.cfm?id=953488> [Accessed: 11 June 2014].

Verizon. 2008. Business Continuity Management and the Extended Enterprise. [Online]. Available: http://www.verizonenterprise.com/resources/whitepapers/wp_business-continuity-management-and-the-extended-enterprise_en_xg.pdf [Accessed: 12 August 2014].

Verizon. 2012. The Verizon Wireless 4G LTE Network: Transforming Business with Next-Generation Technology. [Online]. Available: http://business.verizonwireless.com/content/dam/b2b/resources/LTE_FutureMobileTech_WP.pdf [Accessed: 12 August 2014].

Walters, T. 2012. Understanding the “Mobile Shift”: Obsession with the Mobile Channel Obscures the Shift to Ubiquitous Computing. [Online]. Available: <http://www.idgconnect.com/download/13186/understanding-mobile-shift-obsession->

mobile-channel-obscures-shift-ubiquitous-computing?contact_id=512df0e2252e2e681a54a9ead26c1fa8&source=intl031513idgce®ion=africa [Accessed: 19 March 2013].

Webb, P., Pollard, C. & Ridley, G. 2006. Attempting to define IT Governance: Wisdom or Folly?. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*. 4-7 January, 194a. Kauai, Hawaii. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1579684> [Accessed: 5 February 2014].

Webster, J. & Watson, R.T. 2002. Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*. 26(2):xiii-xxiii.

Wilkin, L.C. & Campbell, J. 2010. Corporate Governance of IT: a Case Study in an Australian Government Department. *Pacific Asia Conference on Information Systems*. 9-12 July, 98-109. Taipei: Taiwan. [Online]. Available: <http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1009&context=pacis2010> [Accessed: 12 June 2014].

Wilkins, B.R. 2014. Tips for Implementing Mobility Programs. @ISACA, 13. [Online]. Available: http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Documents/2014/at-ISACA-Volume-13_nlt_Eng_0614.pdf [Accessed: 19 June 2014].

Windows Phone. 2014. Windows Phone architecture overview. [Online]. Available: http://dev.windowsphone.com/it-it/OEM/docs/Getting_Started/Windows_Phone_architecture_overview [Accessed: 24 July 2014].

Wong, A.K.Y., Ray, P.K., Parameswaran, N. & Strassner, J. 2005. Ontology mapping for the interoperability problem in network management. *Journal on selected areas in Communications*, 23(10):2058–2068. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1514535> [Accessed: 19 March 2013].

Wright Jr., H.R., Mooney, J.L. & Parham, A.G. 2011. Your firm's mobile devices: How secure are they?. *Journal of Corporate Accounting and Finance*. 22(5):12-21. [Online]. Available: <http://onlinelibrary.wiley.com/doi/10.1002/jcaf.20701/abstract> [Accessed: 2 July 2014].

Yunos, M., Gao, J.Z. & Shim, S. 2003. Wireless advertising's challenges and opportunities. *Computer*, 36(5):30-37. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1198234> [Accessed: 2 July 2014].

Zalewska, A. 2014. Challenges of Corporate Governance: Twenty years after Cadbury, ten years after Sarbanes-Oxley. *Journal of Empirical Finance*, 27:1-9.

Zhang, S. & Le Fever, H. 2013. An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model. *Journal of Economics*,

Business and Management, 1(4):391-395. [Online]. Available: <http://www.joebm.com/papers/84-M021.pdf> [Accessed: 17 June 2014].

Zscaler. 2013. Enabling Seamless & Secure Mobility in BYOD, Corporate-Owned and Hybrid Environments: Efficiently and Cost-Effectively Managing Mobility Risks in the Age of IT Consumerization. [Online]. Available: <http://www.zscaler.com/pdf/whitepapers/wp-mobile-security-enabeling-byod-corp-hybrid-0613.pdf> [Accessed: 4 July 2014].

APPENDIX A: A SUMMARY OF COBIT'S DETAILED PROCESSES

Domain	Process	Process description
Evaluate, Direct Monitor (EDM)	EDM01 Ensure Governance Framework Setting and Maintenance	Analyse and formulate IT governance requirements, implement and maintain effective structures, principles, processes and practices to achieve the enterprise's strategic objectives, assign responsibilities and authority.
	EDM02 Ensure Benefits Delivery	Optimise value from IT enabled initiatives and assets, implement cost-effective service and solution delivery and apply cost-benefit analyses.
	EDM03 Ensure Risk Optimisation	Analyse, understand and communicate the enterprise's risk appetite and tolerance levels and identify and manage risks related to the use of IT.
	EDM04 Ensure Resource Optimisation	Ensure the availability of sufficient and appropriate IT support (people, processes and technology) at optimal cost.
	EDM05 Ensure Stakeholder Transparency	Ensure that IT performance measurement takes into account all stakeholder objectives and that reporting and corrective actions are transparent.
Align, Plan and Organise (APO)	APO01 Define the IT Management Framework	Define the strategic IT objectives. Implement appropriate mechanisms and authorities. Continuously improve the structures and consider business-IT alignment.
	APO02 Define Strategy	Prepare a broad and comprehensive view of the IT environment, its course for the future and define the initiatives necessary to achieve this. Build on existing enterprise

		architecture and infrastructure to enable agile, reliable and efficient responses to strategic objectives.
	APO03 Manage Enterprise Architecture	Determine a framework for the effective and efficient achievement of IT strategies. The framework should include business processes, information, data and all technology involved. The framework should define requirements for classifications and categorisation, standards, guidelines, procedures, templates and tools. Consider the use of existing components to save costs, improve alignment, increase agility and improve information quality.
	APO04 Manage innovation	Maintain awareness of IT trends, identify opportunities for innovation and align innovations with enterprise strategy. Drive enterprise strategic and infrastructure decisions by identifying opportunities for innovation from emerging technologies, IT-driven business innovation and IT process innovation based on existing technologies.
	APO05 Manage Portfolio	Align IT investments with enterprise strategy, define the categories of investments and consider resource and financial constraints as well as risk exposure. Evaluate, prioritise and implement designated investments, monitor performance and adapt to any changes in strategy.
	APO06 Manage Budget and Costs	Manage the cost of IT in both business and IT functions through budgets, cost-benefit analyses, spending prioritisation and cost allocation. Consult with all stakeholders to determine full cost and true benefit and create scope for adjustments as required.
	APO07 Manage Human Resources	Ensure the optimal structuring and use of skills through clear definition of roles and responsibilities, development plans, performance expectations and competent support.

	APO08 Manage relationships	Manage the IT- business relationship to ensure alignment within risk and budgetary constraints through transparent communication and clear assignment of ownership and authority.
	APO09 Manage Service Agreements	Ensure alignment of IT services. Identify, design and monitor services.
	APO10 Manage Suppliers	Manage third party service providers through establishing selection, review and monitoring processes.
	APO11 Manage quality	Define and communicate all quality requirements including controls and the use of frameworks and standards.
	APO12 Manage risk	Continually identify, assess and mitigate IT risks.
	APO13 Manage security	Establish, maintain and monitor an information security management system.
Build, Acquire and Implement (BAI)	BAI01 Manage Programmes and Projects	Coordinate all IT programmes and projects through planning, control, risk management and post-implementation review.
	BAI02 Manage Requirements Definition	Analyse business requirements for all applications, information, infrastructure and services before investment and review possible solutions for cost-benefit and risk exposure.
	BAI03 Manage Solutions Identification and Build	Align design, development, installation, procurement, configuration, testing and monitoring off IT technologies with business strategy.
	BAI04 Manage Availability and Capacity	Optimise current and future business requirements through planning, assessments, forecasting and risk assessment.

	BAI05 Manage Organisational Change Enablement	Prepare for organisational change by taking into account risk, sustainability considerations and stakeholders.
	BAI06 Manage Changes	Control standard and emergency changes through policies, procedures, prioritisation, reporting and documentation.
	BAI07 Manage Change Acceptance and Transitioning	Accept and implement new solutions through planning, testing, communication, support and process review.
	BAI08 Manage Knowledge	Identify, organise, maintain use and store information.
	BAI09 Manage Assets	Manage IT assets to ensure physical protection, value delivery, effective operation, reliability and availability.
	BAI10 Manage Configuration	Define and maintain a configuration model, baseline and repository, compile configuration reports and review the integrity of the repository.
Deliver, service and support (DSS)	DSS01 Manage Operations	Coordinate and execute IT activities.
	DSS02 Manage Service Requests and Incidents	Ensure timely and effective response to user requests and incident resolution including appropriate documentation.
	DSS03 Manage Problems	Identify and categorise the source of problems to resolve incidents effectively and recommend improvements.
	DSS04 Manage Continuity	Establish and maintain a business continuity plan to ensure continued operation of core business processes and the availability of information.
	DSS05 Manage Security	Protect business information and manage responsibilities, policies and standards.

	Services	Monitor and test security to identify weaknesses and implement controls.
	DSS06 Manage Business Process Controls	Design and implement business process controls to ensure that information meets defined control requirements.
Monitor, Evaluate and Assess (MEA)	MEA01 Monitor, Evaluate and Assess Performance and Conformance	Compile business and IT objectives and monitor process performance. Provide timely reports of any findings.
	MEA02 Monitor, Evaluate and Assess the System of Internal Control	Implement standards of internal control assessments and monitor and evaluate performance to identify inefficiencies and weaknesses.
	MEA03 Monitor, Evaluate and Assess Compliance with External Requirements	Evaluate the compliance of IT processes with laws, regulations and contracts and obtain external assurance where appropriate.

(ISACA, 2012b)

APPENDIX B: THE BENEFITS AND LIMITATIONS OF REVIEWED CONTROL FRAMEWORKS

B.1: COBIT

B.1.1 Benefits of COBIT

Babb (2014), Anisingaraju (2013), Oliver and Lainhart (2012), Oliver and Lainhart (2011) and Rudman (2008b) identified the following benefits to adopting COBIT as an IT governance framework:

- COBIT improves business-IT alignment.
- The framework presents a comprehensive view of the enterprise and covers all related IT processes.
- The framework is adaptable and can be applied to any enterprise regardless of size and industry. It is, however, the responsibility of the user to select and apply only the applicable and relevant processes within each domain.
- COBIT integrates other internationally accepted control frameworks, models and standards into an inclusive governance and management framework. It serves as the principal framework to which other frameworks, that provide more technical and detailed guidance, are mapped to ensure a comprehensive approach.
- COBIT and the 2013 COSO Internal Control – Integrated Framework (COSO framework) are complimentary and compatible.
- The framework creates value and financial benefits by facilitating the effective, efficient and innovative use of IT resources and processes.
- COBIT promotes user satisfaction with IT services by supporting an increase in user contributions to the investment and use of IT.
- The framework improves compliance with local and international laws, regulations, standards and policies.

B.1.2 Limitations of COBIT

The following limitations, as identified by Anisingaraju (2013), Zhang and Le Fever (2013:393) and Rudman (2008b) need to be considered when implementing COBIT:

- Due to its generic structure and extensive content, the framework is not always easily understandable.

- Implementation of COBIT requires a detailed understanding of the framework in its entirety and is therefore resource intensive in terms of financial, time and human resources.
- The framework will have to be adapted to the enterprise's specific business requirements, organisational structure and operational processes. The framework lacks operable and practicable guidance on how to execute the adaptation.
- The framework is written at a high level and lacks technical and operational guidelines and detail.
- While all areas of IT governance and management are addressed, additional emphasis on certain significant considerations, such as IT security, is lacking.

B.2 ITIL

B.2.1 Benefits of ITIL

Arraj (2013), ITIL (2011), Sahibudin *et al.* (2008:749) and Fry (2005) identified the following benefits to the implementation of ITIL:

- ITIL facilitates business-IT alignment.
- Implementation of the ITIL processes facilitates a more detailed understanding of IT services. This in turn allows for more realistic and achievable cost/benefit analyses as well as more flexibility and adaptability within both enterprise and service delivery processes.
- The consistent approach to the provision of IT services improves customer satisfaction as expectations are set according to these predictable and consistent processes.
- Consistent processes allow for the development of appropriate performance measures that promotes continuous improvement.
- ITIL includes a well-defined set of terms that allows for the consistent and simplified use of terminology throughout the enterprise, improving communication between departments
- Costs are reduced due to a more efficient delivery of IT services, a reduction in duplicate work and more effective resource management.

B.2.2 Limitations of ITIL

According to Goosen (2012:24) and Fry (2005), the following limitations need to be considered when implementing ITIL:

- ITIL comprises a great level of detail that often leads to the production of unnecessarily complex process outlines.
- Implementation of the framework is often cost, time and resource intensive as it requires training for its users.
- Some processes are applied across department lines and this can create inter-departmental conflicts, especially in enterprises where performance in departments is measured independently.
- ITIL does not provide detailed instructions in the application of its processes.

B.3 ISO/IEC 27000-series

B.3.1 Benefits of the ISO/IEC 27000-series

Standards Consultants (2014), Mataracioglu and Ozkan (2011) and Henry-Stocker (2010) and outline the following benefits to the implementation of the ISO/IEC 27000-series:

- The adoption of the standards is a clear statement of commitment towards information security management and promotes stakeholder trust and assurance.
- The standards require constantly revising, updating and improving information security management policies and procedures in order to keep up with the changing security risk landscape.
- Costs are reduced due to an improvement in the efficiency of security risk management and through a reduction of incidents that cause loss of information, time and stakeholder confidence.
- Implementing the standards ensures that relevant laws, regulations and policies are adhered to.
- The standards provide specific detail on how processes and controls are to be implemented on an operational level.

B.3.2 Limitations of the ISO/IEC 27000-series

The following limitations, as identified by ISO 27001 Security (2014), Mataracioglu and Ozkan (2011) and Sahibudin *et al.* (2008:752) need to be considered when implementing the ISO/IEC 27000-series:

- The standards do not address cost management.
- The controls are independently implemented and the standards do not provide guidance on IT governance as a whole.
- ISO/IEC 27002, specifically, contains a considerable amount of risks, controls and related detail obstructing the manageable implementation of the standard.

APPENDIX C: RISK AND CONTROL MATRIX USING COBIT

In order to identify the risks relating to the deployment of mobile solutions and the relevant internal controls to mitigate the risks, the detail processes for each of the 37 COBIT processes were reviewed and summarised (ISACA, 2012b). The processes were considered for relevance in the deployment of mobile solutions and only relevant processes were documented in summarised form. These included an extensive number of COBIT processes as mobile solutions affect all operations of the enterprise. Through the application of each process to a mobile solution environment and the review of the detail of each of the 37 processes, the specific risks to the enterprise were identified and the impact of the risks was evaluated. The risks are formulated in generic terms in order to maintain the adaptability of the control framework and the risk to specific enterprise characteristics. Lastly, the internal controls that need to be implemented to mitigate the specific identified risks were formulated.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Evaluate, Direct, Monitor	EDM01	Evaluate, direct and monitor a system of mobile solution governance.	<ul style="list-style-type: none"> Mobile solutions are inadequately addressed in governance strategies and policies. Mobility strategies and policies are not comprehensive and effective. The appropriate board involvement and authority levels are not obtained. Mobile solution governance is not monitored for effectiveness and performance. 	High	<ul style="list-style-type: none"> Identify and evaluate internal and external factors that are influenced by mobile solutions and develop and implement a comprehensive strategy and related policies. Obtain input from all relevant stakeholders. Board should designate authority, responsibility and decision-making regarding investment in and use of mobile technology. Design a system to monitor and report on effectiveness of mobile solution governance.
	EDM02	Evaluate, direct and monitor the value contribution of an investment in and use of mobile solutions.	<ul style="list-style-type: none"> The cost of mobile investments and use exceeds its benefits. Ineffective systems of value-add evaluation. 	High	<ul style="list-style-type: none"> Compile comprehensive feasibility analyses, describing all costs and determining expected benefits. Develop a practical and effective system of mobile technology value measurement including reporting timelines and structures, as well as the collection of accurate and relevant data.
	EDM03	Evaluate, direct and monitor the enterprise's exposure to risks relating to mobile solution deployment.	<ul style="list-style-type: none"> Mobile solution risk exposure exceeds the enterprise's risk tolerance levels. All risks relating to the investment in and use of mobile technology are not identified and mitigated appropriately. The risk management process does not operate effectively. 	High	<ul style="list-style-type: none"> Develop and implement a mobile solution risk management system that: <ul style="list-style-type: none"> establishes enterprise risk tolerance levels; documents risk identification processes to ensure comprehensive risk analysis; addresses the management of changes in mobile solution risks; and assigns the responsibility for the identification and management of risks. Remain involved in the mobile application development market.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Evaluate, Direct, Monitor	EDM04	Evaluate, direct and monitor resources involved in the investment and use of mobile solutions.	<ul style="list-style-type: none"> Resources are not used efficiently in the investment in and use of mobile solutions. Misallocation and excessive use of resources are not identified. 	High	<ul style="list-style-type: none"> As part of the feasibility study, evaluate resources available against resources required for the optimum operation of mobile technology. Develop and implement a resources management policy that assures alignment of resource use and strategy, and monitors the usage of resources against budgets and identifies and reports inefficiencies.
	EDM05	Evaluate stakeholder reporting requirements, direct and monitor stakeholder communication. Stakeholders include internal stakeholders such as the board of directors, users, and IT staff.	<ul style="list-style-type: none"> Communication with all stakeholders involved in the investment in and use of mobile solutions is not sufficient, relevant and timely. 	High	<ul style="list-style-type: none"> All stakeholders should be identified and a communications policy implemented.
Align, Plan and Organise	APO01	Align mobile solution investments and use with enterprise objectives. Define and establish mobile data parameters.	<ul style="list-style-type: none"> Objectives are poorly formulated. Investment in mobile solutions are not aligned with enterprise objectives. Ownership of mobile solution policies and procedures are not designated. Intellectual property rights to data created on personal devices outside of office hours and the ownership and control of data on mobile devices is not established. Mobile solution policies are insufficient and become obsolete. Value is not created through mobile investments. 	High	<ul style="list-style-type: none"> Define enterprise and mobile solution objectives and ensure alignment with enterprise objectives. Establish a mobile solution strategy, policies and procedures to support alignment. Establish the roles and responsibilities of the mobile strategy, allocating authority and defining reporting lines. Establish access rights to mobile data and authority levels with regards to the data. Implement a system of continuous monitoring and improvement of the strategy and policies based on changes in the mobile technology. Review employee contracts to update data ownership agreements in a mobile environment. Control data on mobile devices through: <ul style="list-style-type: none"> the containerisation of data; managing data storage; and dual identities on mobile devices.
	APO02	Establish and communicate a mobile solution strategy	Refer APO01 and EDM05	High	Refer APO01 and EDM05

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Align, Plan and Organise	APO03	Determine mobile solution component requirements and define policies for implementing new infrastructure and components.	<ul style="list-style-type: none"> Mobile solution infrastructure and components are not sufficient for the achievement of the mobile solution strategy. New investments are not managed appropriately leading to excessive costs. Mobile solution components are not compatible and data formats are inconsistent. Opportunities to advance enterprise operations are missed. 	High	<ul style="list-style-type: none"> Determine the full extent of the mobile solution infrastructure to support the strategy including identifying allowable mobile device types, network requirements and required and allowable applications, identifying all uses for mobile solutions. Implement MDM and MIM systems to manage the components and their interoperability. Implement MEM systems to manage costs. Continuously update mobile technology evaluations and identify areas for improvement and innovation.
	APO04	Identify areas for innovation.	Refer APO03	High	Refer APO03
	APO05	Identify required investments and manage portfolio of investments based on resources, risk and benefits.	Refer EDM04, APO01 and APO03	Medium	Refer EDM04, APO01 and APO03
	APO06	Identify, manage and account for all costs related to the investment in and use of mobile solutions.	<ul style="list-style-type: none"> The costs related to the investment in infrastructure, hardware and software is excessive and exceeds budgets. Data and other transmission costs are excessive. Costs required to ensure security of devices and data is excessive. 	High	<ul style="list-style-type: none"> Implement MEM systems. Implement MDM, MAM and MIM systems in order to cost-effectively manage security of devices and data. Set a budget reflecting all the anticipated costs related to the investment in and use of mobile solutions and monitor and report on performance. Use a tiered approach to service delivery. Create user groups and provide only necessary services to each group. Use managed wireless products to reduce set-up and configuration costs. Use converged networks.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Align, Plan and Organise	APO07	Identify key IT staff, maintain necessary skills and competencies and evaluate performance.	<ul style="list-style-type: none"> IT support is insufficient. Staff knowledge and experience is insufficient. 	High	<ul style="list-style-type: none"> Provide sufficient training for IT support staff and application developers on the various mobile devices, platforms, and applications. Implement succession planning in the event of IT support staff changes. Evaluate IT staff performance regularly. IT staff responsible for application development should receive appropriate skills development in mobile operating system coding. Users should be trained in appropriate use of mobile solutions. Install over-the-air provisioning software. Define and limit the applications that can be downloaded and used. Apply application white- and blacklisting. Virtualisation technologies and VPN networks facilitate IT support. Automate guest connections. Automate authentication and on-boarding processes.
	APO08	Manage business-IT relationship.	<ul style="list-style-type: none"> Mobile solutions are not aligned to enterprise strategies. 	High	Refer APO01
	APO09	Manage IT service delivery.	<ul style="list-style-type: none"> IT services, both internal and external, do not meet user requirements. Services that are not required, are delivered. 	High	<ul style="list-style-type: none"> Identify all stakeholders and determine their requirements in terms of mobile solutions. Identify areas of external service provision, determine requirements and prepare service level agreements. Evaluate, monitor and report on service levels and performance.
	APO10	Manage external service providers.	Refer APO09	High	Refer APO09
	APO11	Manage the quality of mobile solution service delivery.	Refer APO09	High	Refer APO09
	APO12	Identify, manage and mitigate all mobile solutions risks .	Refer EDM03	High	<ul style="list-style-type: none"> Establish a risk management team, define risks and formulate internal controls to mitigate the risks related to investment in and use of mobile solutions. Implement enterprise mobile management systems.
	APO13	Develop, implement and maintain an information security management system.	Refer DSS05	High	Refer DSS05

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Build, Acquire and Implement	BAI01	Coordinate all mobile solution investments.	Refer EDM04	Medium	Refer EDM04
	BAI02	Analyse and define enterprise and user requirements for mobile devices, infrastructure, networks, software and data.	Refer APO09	High	Refer APO09
	BAI03	Establish and maintain mobile solutions that are aligned with business strategy.	Refer APO08 and APO01	High	Refer APO01
	BAI04	Assess current availability and future requirements for capacity.	<ul style="list-style-type: none"> The enterprise has insufficient resources to meet enterprise and user requirements in terms of mobile service delivery. 	Medium	Refer EDM04
	BAI05	Enable innovation within mobile solutions.	Refer BAI06	Medium	Refer BAI06
	BAI06	Manage changes and new innovation introduction.	<ul style="list-style-type: none"> Opportunities for innovation are not capitalised. Planned or emergency changes to mobile solutions are not effectively completed. 	High	<ul style="list-style-type: none"> Mobile strategy and policies need to facilitate the identification of new opportunities. Develop and implement change policies addressing roles, responsibilities and prioritisation. Develop and implement an incident management system. Define reporting and documentation requirements and procedures. Implement comprehensive testing of new technology.
	BAI07	Implementing new mobile solutions.	Refer BAI06	Medium	Refer BAI06
	BAI08	Manage information and knowledge regarding mobile solutions.	<ul style="list-style-type: none"> Mobile solution information is not communicated appropriately and to the relevant users. 	Low	Refer EDM05

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Build, Acquire and Implement	BAI09	Manage all mobile solution assets (including mobile devices, networks and infrastructure and data on mobile devices).	<ul style="list-style-type: none"> • Mobile assets are lost or stolen. • Mobile devices do not operate as intended due to inherent limitations. • Mobile software is not updated and do not operate as intended. • Wireless networks do not operate as intended due to unreliable connectivity and performance and bandwidth bottlenecks. • Software licenses are out-of-date and insufficient. 	High	<ul style="list-style-type: none"> • Implement physical security controls. • Address the mobile device requirements for allowable mobile devices in the mobile solution strategy. • Regularly update software. • Test mobile applications regularly. • Manage wireless networks performance: <ul style="list-style-type: none"> • Prioritise usage of networks and bandwidth through configuration of mobile devices. • Establish a systems management team to monitor the performance of networks and identify and address incidents. • Update and review software licensing regularly.
	BAI10	Define and maintain descriptions and key functionality of mobile devices and wireless networks.	<ul style="list-style-type: none"> • Mobile devices and networks are not configured appropriately and do not meet enterprise objectives or user requirements. 	High	<ul style="list-style-type: none"> • Include configuration specifications in the mobile solution policies. • Provide sufficient training for IT support staff on configuration.
Deliver, Service and Support	DSS01	Coordinate mobile solution activities.	Refer APO09	Medium	Refer APO09
	DSS02	Provide sufficient user support.	Refer APO07	High	Refer APO07
	DSS03	Identify and resolve incidents.	<ul style="list-style-type: none"> • Incidents are not identified timeously and are not resolved efficiently. 	High	Refer BAI06
	DSS04	Implement and manage business continuity plans.	<ul style="list-style-type: none"> • Significant loss of data or disruptions to operations are experienced. • Reputational damage is experienced. • Business continuity plans in a real-time mobile environment are inadequate. 	High	<ul style="list-style-type: none"> • Design and implement a comprehensive business continuity plan including redundancy controls specifically for the mobile environment.

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Deliver, Service and Support	DSS05	Implement and manage security controls to ensure the security of assets and integrity of data.	<ul style="list-style-type: none"> • Unauthorised physical access to mobile devices (loss or theft). • Unauthorised access to corporate information on the mobile device or during transmission. • Intentional security breaches via malware • Security is not sufficiently managed. • Out-dated software leads to security vulnerabilities. 	High	<ul style="list-style-type: none"> • Implement physical security such as GPS tracking and cable locks. • Train users on physical safeguards when using mobile devices. • Implement access, authentication and mitigating controls: <ul style="list-style-type: none"> • User authentication • Mutual authentication • Out of band authentication • One time password • Encryption • Digital signatures • Remote wipe • Remote lock • Data fading • Poison pill • Segregate corporate functionality on the mobile device • Use application wrapping. • Implement configuration controls: <ul style="list-style-type: none"> • Browser security • Auto-lock • Password requirements • Disabling auto-complete on passwords • Manage network connections by: <ul style="list-style-type: none"> • Disabling wireless networks • Changing network settings to undiscoverable • Using network filters • Monitor and log device activity and identify breaches and vulnerabilities. • Install anti-virus software.
	DSS06	Manage roles, responsibility, access privileges and levels of authority with regards to mobile data.	Refer APO01	High	Refer APO01

Domain	Relevant COBIT process	Detail processes' requirements	Risk(s) identified	Impact of the risk	Control(s) to mitigate the risk(s)
Monitor, Evaluate and Assess	MEA01	Monitor and address inefficiencies in mobile solutions performance.	Refer APO09	High	Refer APO09
	MEA02	Monitor and asses the system of internal control.	Refer EDM01	High	Refer EDM01
	MEA03	Monitor and evaluate mobile solution compliance to laws and regulations.	<ul style="list-style-type: none"> The enterprise is exposed to litigation due to contravention of laws and regulations. 	High	<ul style="list-style-type: none"> Identify all laws and regulations applicable to mobile data, the use of mobile solutions and employee privacy and ensure that all requirements are met.