THE GOVERNANCE OF SIGNIFICANT ENTERPRISE MOBILITY SECURITY RISKS

by

Johanna Catherina Brand

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: Mrs Wandi van Renen

December 2013

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, 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: December 2013

ABSTRACT

Enterprise mobility is emerging as a megatrend in the business world. Numerous risks originate from using mobile devices for business-related tasks and most of these risks pose a significant security threat to organisations' information. Organisations should therefore apply due care during the process of governing the significant enterprise mobility security risks to ensure an effective process to mitigate the impact of these risks.

Information technology (IT) governance frameworks, -models and -standards can provide guidance during this governance process to address enterprise mobility security risks on a strategic level. Due to the existence of the IT gap these risks are not effectively governed on an operational level as the IT governance frameworks, -models and -standards do not provide enough practical guidance to govern these risks on a technical, operational level.

This study provides organisations with practical, implementable guidance to apply during the process of governing these risks in order to address enterprise mobility security risks in an effective manner on both a strategic and an operational level.

The guidance given to organisations by the IT governance frameworks, -models and -standards can, however, lead to the governance process being inefficient and costly. This study therefore provides an efficient and cost-effective solution, in the form of a short list of best practices, for the governance of enterprise mobility security risks on both a strategic and an operational level.

OPSOMMING

Ondernemingsmobiliteit kom deesdae as ’n megatendens in die besigheidswêreld te voorskyn. Talle risiko's ontstaan as gevolg van die gebruik van mobiele toestelle vir sake-verwante take en meeste van hierdie risiko's hou 'n beduidende sekuriteitsbedreiging vir organisasies se inligting in. Organisasies moet dus tydens die risikobestuursproses van wesenlike mobiliteit sekuriteitsrisiko’s die nodige sorg toepas om ’n doeltreffende proses te verseker ten einde die impak van hierdie risiko’s te beperk.

Informasie tegnologie (IT)- risikobestuurraamwerke, -modelle en -standaarde kan op ’n strategiese vlak leiding gee tydens die risikobestuursproses waarin mobiliteit sekuriteitsrisiko’s aangespreek word. As gevolg van die IT-gaping wat bestaan, word hierdie risiko’s nie effektief op ’n operasionele vlak bestuur nie aangesien die IT-risikobestuurraamwerke, -modelle en -standaarde nie die nodige praktiese leiding gee om hierdie risiko’s op ’n tegniese, operasionele vlak te bestuur nie.

Om te verseker dat organisasies mobiliteit sekuriteitsrisiko’s op ’n effektiewe manier op beide ’n strategiese en operasionele vlak bestuur, verskaf hierdie studie praktiese, implementeerbare leiding aan organisasies wat tydens die bestuursproses van hierdie risiko’s toegepas kan word.

Die leiding aan organisasies, soos verskaf in die IT-risikobestuurraamwerke, -modelle en -standaarde, kan egter tot ’n ondoeltreffende en duur risikobestuursproses lei. Hierdie studie bied dus 'n doeltreffende, koste-effektiewe oplossing, in die vorm van 'n kort lys van beste praktyke, vir die bestuur van die mobiliteit sekuriteitsrisiko’s op beide 'n strategiese en 'n operasionele vlak.

TABLE OF CONTENTS

LIST OF FIGURES, TABLES AND APPENDIXES

List of figures

List of tables

List of appendixes

CHAPTER 1: INTRODUCTION

1.1 Background

According to statistics on mobile device sales, internet traffic and the increase in the number of developed and downloaded applications, there currently is an increased use of mobile devices (Deloitte, 2013; Van der Meulen, 2012). This increased use of mobile technology seems to have brought on the recent consumerisation of mobile technology (Rowsell-Jones, Jones & Basso, 2011), and this has resulted in enterprise mobility emerging as a megatrend (Pettey & Van der Meulen, 2012).

This significant trend towards mobility and mobile business will have an increasingly commanding influence on the business strategy and business imperatives of organisations in the near future. An organisation's business strategy should be dynamic and evolve over time and those charged with governance must also consider and include the effect that current market trends and the emergence of new technologies will have on their current business strategy (Azim & Hassan, 2013:142; Burkhart, Krumeich, Wertch & Loos, 2011). Failure to include significant market trends and new technologies in a timely manner as business drivers or business imperatives may have a detrimental effect on an organisation's competitive advantage, profitability and life span (Azim & Hassan, 2013:142).

The establishment of an information technology (IT) solution that is required to satisfy an organisation's enterprise mobility needs will give rise to numerous risks (Ghosh, Gayar & Rai, 2013:64; ISACA, 2010:5; Milligan & Hutcheson, 2007:189). Amongst these risks are myriad vulnerabilities threatening the security of corporate information, and these security risks originating from enterprise mobility seem to be an increasingly significant concern for organisations (Botha, Furnell & Clarke, 2009:131).

For organisations to successfully mitigate these security risks and the resulting impact on their organisation, these security risks should be governed. ISACA has (2010:6) issued a white paper that touches on a strategy to govern security risks relating to enterprise mobility by creating a "mobile device strategy". It cautions the

reader to consider “issues such as organizational culture, technology and governance when creating” this strategy (ISACA, 2010:6). IT governance control documents, as suggested by this white paper, can assist organisations to address the organisational culture and governance issues and this will assist organisations to govern enterprise mobility security risks on a strategic level. IT governance control documents include governance frameworks, standards and models.

However, enterprise mobility security risks should also be governed on an operational level to ensure effective governance of security risks resulting from the implementation, maintenance and use of mobile technology. Although IT governance control documents discusses the policy for and governance of mobile technology, it gives no practical guidance to assist organisations in effectively addressing the impact technology has on the process of governing enterprise mobility security risks on an operational level. Furthermore, only using IT governance control documents to govern IT risks could lead to a gap, called the IT gap, which may result in the misalignment of business and IT goals as the IT control documents do not address enterprise mobility security risks on an operational level.

To ensure the IT gap is addressed and enterprise mobility security risks are effectively governed, these risks should be identified and addressed on both a strategic and an operational level.

To effectively govern enterprise mobility security risks on a strategic level, IT governance control documents, such as IT governance frameworks, -models and -standards, which are most relevant in addressing security risks should be identified. These identified IT control documents should be combined as the combination can ensure a strong basis for the effective governance of risks (IT Governance Institute, 2008). From these identified IT governance control documents, the processes listed in each control document that are relevant in governing enterprise mobility security risks should be identified as not all processes will be applicable to enterprise mobility security risks. These identified processes and their related control techniques will be implemented by organisations to address enterprise mobility security risks on a strategic level.

The implementation of these processes on an individual basis could easily result in an inefficient and costly undertaking. Any overlapping or similar processes should therefore be combined in an effort to limit the number of processes to implement and to increase the efficiency and cost effectiveness of the governance process.

Governing enterprise mobility security risks on an operational level proves to be difficult due the existence of an IT gap.

The aim of this study is to provide an effective and efficient solution for organisations to govern enterprise mobility security risks on an operational and a strategic level. The answer will be structured in the form of a short list of implementable best practices that organisations can use to increase the efficiency and effectiveness of the governance process necessary to successfully mitigate enterprise mobility security risks on both a strategic and an operational level and also effectively address the IT gap that exist.

1.2 Research question and objective

The research is structured to answer the following question: How can an organisation effectively and efficiently govern significant security risks originating from enterprise mobility?

The objective of this study is to find a practical solution, in the form of a short list of implementable best practices, which will assist organisations in bridging the IT gap to effectively and efficiently govern enterprise mobility security risks on both a strategic *and* an operational level.

1.3 Research motivation

Enterprise mobility will lead to several information security risks. These risks should be governed on both a strategic and an operational level. Due to the emergence of an IT gap, governing IT risks on an operational level and aligning business and IT seems to be problematic for many organisations. Furthermore, the guidance provided by IT control documents to govern enterprise mobility security risks on a strategic level is extensive and usually lead to a costly process.

This study was undertaken to determine an effective solution for organisations to successfully govern significant security risks resulting from enterprise mobility on a strategic and an operational level. This study was undertaken to also attempt to improve the efficiency and cost effectiveness of the governance process by developing a short list of best practices that organisations can implement to mitigate identified enterprise mobility security risks.

1.4 Design and methodology

A non-empirical study was conducted by reviewing existing literature that relates to the research topic, covering aspects such as enterprise mobility, security risks resulting from enterprise mobility, IT governance principles, IT governance control documents, business/IT alignment and the IT gap, the governance of enterprise mobility security risks on an operational level, access paths, and IT architectural components.

From the literature review, the author was able to:

1. identify significant security risks originating from enterprise mobility;
2. review different IT governance control documents and assess their applicability for addressing enterprise mobility security risks;
3. select the IT governance control documents that seemed most relevant for assisting organisations during the process of governing enterprise mobility security risks;
4. identify only the IT governance processes listed in the selected IT governance control documents that are relevant in governing enterprise mobility security risks;
5. map the identified security risks against the relevant IT governance processes in a matrix to identify significant IT governance processes that organisations should implement to effectively govern enterprise mobility security risks on a strategic level;
6. use Goosen's developed framework (2012) to effectively address the IT gap and to govern enterprise mobility security risks on an operational level; and
7. develop a list of best practices to effectively and efficiently governing significant enterprise mobility security risks on a strategic level and an operational level.

1.5 Organisation of the research

In Chapter 2, the results of the literature review on the definition of enterprise mobility; the impact of enterprise mobility on organisations; and identified security risks that originate from enterprise mobility are presented. The positive contribution of IT governance control documents, principles and processes in governing these identified security risks, together with the weakness of IT governance control documents as stated in the reviewed literature, are also summarised in this chapter.

An overview of the most relevant IT governance control documents selected for this study, as well as the identification of processes listed in these identified IT control documents that are relevant to addressing enterprise mobility security risks will be provided in Chapter 3.

Chapter 4 maps the security risks identified in Chapter 2 to the identified processes in Chapter 3 to determine the most significant processes that should be implemented to effectively govern enterprise mobility security risks on a strategic level.

In Chapter 5 the author presents a discussion of business/IT alignment, the IT gap and the positive contribution of Goosen's developed framework in effectively governing enterprise mobility security risks on an operational level.

A list of implementable best practices is developed in chapter 6; these will assist organisations in effectively and efficiently governing enterprise mobility security risks on an operational and a strategic level.

The study is concluded in Chapter 7 with a summary of the results of this study, final conclusions drawn and a discussion of possible future research.

1.6 Limitations of the research

The limitations of this study include the following:

- This study did not research the effective and efficient governance of all risks resulting from enterprise mobility. Only the governance of significant security risks originating from enterprise mobility was researched.

- Only the high-level processes listed in COBIT 5 formed part of this study. The detailed processes as listed in *ISACA's COBIT 5: Enabling Processes* will not form part of this study.
- Apart from the five core publications, ITIL also consists of additional complementary publications to enhance the practices discussed in the core publications. However these complementary guides did not form part of the scope of this study.
- This research explored the effective governance of enterprise mobility security risks on an operational level by applying Goosen's developed framework, but did not include a detailed, technical study of the implementation of this developed framework. The IT solution established by organisations to satisfy their enterprise mobility needs will be unique for almost all organisations. This study discusses possible IT architectural components and access paths that may form part of the generic design of an established IT solution addressing enterprise mobility needs, but must not be seen as an exhaustive list of all possibilities. Organisations should apply the guidance given in this study to the IT architectural components and activated access paths that are applicable to their specific, unique situation.
- This study includes an example of how to apply the guidance, as discussed in the study, in effectively governing enterprise mobility security risks on an operational level with the use of Goosen's developed framework. This example contains limited implementation guidance and was included for the purposes of illustrating the practical application of the steps suggested in Goosen's developed framework. This example was not intended as a comprehensive undertaking to identify all of the security risks resulting from the access paths and IT architectural components contained within an organisation's established IT solution that are necessary to satisfy their enterprise mobility needs and requirements.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Enterprise mobility seems to be a popular topic due to the consumerisation of mobile technology, as well as the resulting risks it poses to organisations. The study reviewed literature on enterprise mobility in order to define it; understand its impact on the competitive business strategy and strategic objectives of an organisation; as well as the potential risks it poses to organisations.

Governing the resulting risks on a strategic level can be achieved by applying IT governance principles. IT governance is defined and IT governance principles and IT control documents are investigated further to assess their positive contribution to governing and mitigating risks, as well as its weakness: the inability to effectively mitigate risks on an operational level due to the emergence of the IT gap.

2.2 Enterprise mobility

2.2.1 Defining enterprise mobility

For the purpose of this study "mobility" was regarded as an interchangeable term for mobile business, enterprise mobility and mobile computing.

Gartner's IT Glossary (2013) describes mobile business as:

> *… new business models enabled by the extensive deployment of key mobile and wireless technologies and devices (for example, Bluetooth, e-purses, smartphones, UMTS and WAP), and by the inherent mobility of most people's work styles and lifestyles. The value proposition of m-business is that the user can benefit from information or services any time and in any place.*

Enterprise mobility has been defined by Ghoda (2009:249) as follows:

> *Enterprise mobility represents the ability of organizations to transform from a traditional organization to a virtual organization. Enterprise mobility enables globally distributed and diversified interorganization and intraorganization teams to access, collaborate on, and process information and execute different business processes utilizing wireless satellite networking-based information systems and services.*

Based on the definitions described above, as well as the review of other relevant literature, the term mobility or mobile computing is referring to a business model where mobile employees make use of mobile technology to perform business tasks (Cuddy, 2009:65; Gartner's IT Glossary, 2013; Ghoda, 2009:249; Welling, 1999:1).

2.2.2 Defining mobile device

ISACA (2012) notes that the term "mobile device" can include a wide range of devices that has the ability to be moved. This study, however, will focus on mobile devices used by mobile employees to perform business tasks. This study will therefor limit the definition of mobile devices, for the purpose of this study and in line with ISACA's view on what types of mobile devices is generally used by organisations for business tasks, to the following devices:

- traditional mobile phones;
- smartphones; and
- tablet personal computers with wireless connectivity.

(ISACA, 2012)

2.2.3 Business strategy

All organisations originate from a business idea that is then translated into a business plan. The business plan should be developed into a formal business model to capture the key components of the envisioned business plan.

Alt and Zimmerman (2001:7) suggested that all business models are designed around six generic components (mission, structure, processes, revenues, legal issues and technology). According to them, one of the "most critical elements" of a successful business model is the "Mission" (Alt & Zimmerman, 2001:7). The Mission of an organisation is where the organisation develops "high-level understanding of the overall vision, strategic goals and value propositioning" in order to direct management in their decision-making process (Alt & Zimmerman, 2001:7). The importance of setting and achieving the strategic goals or strategic objectives is also highlighted in the definition developed by Al-Debei and Avison (2008:7):

> *The business model is an abstract representation of an organization, be it conceptual, textual, and/or graphical, of all core interrelated architectural,*

> *cooperational, and financial arrangements designed and developed by an organization presently and in the future, as well as all core products and/or services the organization offers, or will offer, based on these arrangements that are needed to achieve its strategic goals and objectives.*

The strategic objectives of an organisation will provide direction to the organisation with regard to their strategic positioning within its specific environment and will be unique for all organisations depending on its specific industry, geographical location, company size, and client base of the organisation, amongst other factors.

By formulating a competitive business strategy and realising its strategic objectives a competitive advantage within the specific environment of an organisation can be achieved and maintained (Porter, 1998:17).

Porter's book on competitive advantage (1998:xxvi) lists four key factors that an organisation has to consider during the formulation of a suitable and implementable business strategy:

- company strengths and weaknesses;
- personal values of the key implementers of the chosen competitive business strategy;
- industry opportunities and threats; and
- broader societal expectations.

One of the factors listed above is "broader societal expectations". Broader societal expectations refer, amongst other things, to the impact of "government policy, social concerns and evolving mores" on a company (Porter, 1998:xxvi). The effect of evolving mores or evolving societal trends will therefore have a significant influence on the development of an organisation's business strategy and strategic objectives.

The formulation of the business strategy and strategic objectives is a continuous process and not an isolated exercise. Schweizer (2005:51) deduced that an organisation wishing to maintain the competitive advantage gained through the business strategy they initially developed requires having a dynamic business strategy or business model. The business model, business strategy and strategic objectives should evolve over time to also take into consideration and include the

effect of market changes within the particular industry, as well as the impact of the emergence of new technologies (Azim & Hassan, 2013:142; Burkhart *et al*., 2011; Alt & Zimmerman, 2001:8). According to Burkhart *et al*. (2011), the faster a company is able to react to these drivers of change, the more likely it is to gain and maintain competitive advantage. Delaying adjustments to the business strategy, to also include new technologies as drivers or business imperatives of the business strategy, may have a detrimental effect on an organisation's competitive advantage, profitability and life span (Azim & Hassan, 2013:142).

Furthermore, identifying business imperatives is crucial for realising strategic objectives, as the business imperatives are the crucial drivers or principles directing management's decision-making processes in order to achieve the organisation's strategic objectives (Goosen, 2012:18).

2.2.4 Enterprise mobility as a crucial business imperative

Organisations wishing to integrate enterprise mobility with their existing computing methods should understand the possible impact of this approach on their business model, business strategy and strategic objectives.

As mentioned in the previous section, business imperatives are important for achieving an organisation's strategic objectives. One such a "new technology" that may have an incremental effect on organisations, their business strategy, strategic objectives and, ultimately, their business imperatives, is mobile technology. Although this is not necessarily a new technology, the recent consumerisation of mobile technology makes it new and topical for organisations.

According to Deloitte (2013) and Van der Meulen (2012) there is currently an increased use of mobile technology globally. The following statistics on mobile device sales, internet traffic and applications for mobile devices corroborate this statement:

- The United Nations specialised agency for information and communication technologies, the International Telecommunication Union, estimated that mobile subscriptions will reach 6.8 billion globally by the end of 2013 (International Telecommunication Union, 2013a) while other researchers

expect mobile subscribers to exceed 7 billion by the end of 2013 (Portio Research, 2013). These figures are approaching the world population that is currently estimated to be somewhere between 7.1 and 7.2 billion by the end of 2013 (United States Census Bureau, 2013; Worldometers, 2013). These figures emphasise the pervasive penetration of mobile devices globally.

- Globally, mobile traffic represents more than 17% of all internet traffic (Global stats, 2013). It is estimated that mobile devices will overtake personal computers as the preferred web access device by 2013 (Meeker & Wu, 2013; Pettey & Van der Meulen, 2010). As of May 2012 India's mobile internet usage already surpassed desktop internet usage (Meeker & Wu, 2012).
- Apple's App Store was introduced in July 2008 with about eight hundred applications available for download (Apple, 2008). In June 2013, Apple indicated that more than nine hundred thousand applications were available in the App Store, including more than three hundred and fifty native iPad applications (Apple, 2013b). It took close to four years for the first twenty-five billion applications to be downloaded from the App Store. The twenty-fifth billionth app was downloaded from the App Store during March 2012 (Apple, 2012) and in the following fourteen months another twenty-five billion applications were downloaded, bringing the total of downloaded applications via the App Store to fifty billion by May 2013 (Apple, 2013a).
- Van der Meulen (2012) made the following predictions:
    - 821 million smart devices (smart phones and tablets) will be purchased during 2012;
    - 1.2 billion smart devices will be sold during 2013; and
    - tablets will be the key accelerator for mobility.
- The following predictions were made by Van der Meulen (2012):
    - businesses will purchase 13 million tablets during 2012;
    - businesses will purchase 53 million tablets during 2016; and
    - by 2016 40 percent of the workforce will be using mobile technology to perform work related tasks.
- In a recent survey by Symantec in which they contacted over six thousand organisations globally, it was clear that the adoption of mobility as part of an organisation's competitive strategy is becoming a reality. Almost three

quarters of the respondents indicated that they were discussing custom mobile applications since they considered the business benefits of mobile computing to increase efficiency, increase business agility and help in gaining a competitive advantage (Symantec, 2012).

Due to the recent consumerisation of mobile technology (Rowsell-Jones *et al.*, 2011), a "societal expectation" seemed to be created that, according to Porter (1998), should be considered during the formulation of a business strategy and strategic objectives. Statistics relating specifically to the use of mobile technology for business purposes shows its pervasive influence on organisations and business decisions and support the notion of the consumerisation of mobile technology. Gartner identified the current shift to enterprise mobility as a "megatrend" (cited in Pettey & Van der Meulen, 2012) and the statistics discussed above support this statement.

Enterprise mobility as a megatrend will have an increasingly commanding influence on the business model, business strategy, strategic objectives and business imperatives of organisations in the near future. Mobility is the driver for, amongst other benefits, directing business managers in making the right decisions to gain and maintain a competitive advantage in today's technologically driven business world. Many organisations are therefore starting to see enterprise mobility as a crucial driver or business imperative necessary to realise their envisioned business strategy.

2.2.5 Enterprise mobility risks

Enterprise mobility as a megatrend and a crucial business imperative will require organisations to implement an IT solution to satisfy their enterprise mobility needs in order to achieve their strategic objectives. However, numerous risks relating to enterprise mobility are listed in the literature. These include, amongst others,

- loss, theft or damage of mobile device;
- unauthorised access to sensitive data on the mobile device itself or on the organisation's internal network through lost or stolen mobile devices;
- unauthorised access by hackers leading to mobile device corruption, lost data and unauthorised access to sensitive information;
- data leakage through wireless sniffers;

- malware propagation and spyware attacks;
- phishing (scams using email or pop-up messages), pharming (malicious code installed on a mobile device by a hacker), vishing (or voice phishing) and smishing (scams making use of text messages) attacks;
- workers dependent on mobile devices unable to work in the event of broken, lost or stolen mobile device;
- data on mobile device not backed up regularly. In the event of a broken, lost or stolen mobile device, this information may be lost forever;
- high variability in the operating systems of mobile devices (the bring-your-own-device problem); and
- unrestricted access to applications that can be installed on the mobile device. Applications pose significant privacy risks for users and the organisation if they are not aware of how their personal data are used by applications that are installed on the mobile device.

(Ghosh, Gajar & Rai, 2013:64; ISACA, 2010:5; Milligan & Hutcheson, 2007:189)

The above-mentioned risks indicate that enterprise mobility has a magnitude of risks to address. Most of these risks relate to security threats to corporate information. Security is therefore one of the most significant concerns with enterprise mobility (Botha *et al.*, 2009:131) that should be addressed by organisations.

2.2.6 Identifying significant security risks relating to enterprise mobility

Mobile technology, along with other information technology, will be implemented to satisfy an organisation's enterprise mobility needs. As mobile technology falls within the wider reach of information technology (Cukier, Shortt & Devine, 2002:143), the principles of IT security risks will thus also apply to mobile technology security risks.

IT security risk is defined as the risk relating to the loss of confidentiality, integrity and availability of information or IT resources (Ross, 2011). These three general security benchmarks are defined as follows:

- **Confidentiality** is concerned where access to protected information is only made available or disclosed to authorised individuals, entities, systems or processes.

- **Availability** refers to timely and reliable access to and use of information, software and hardware upon demand by an authorised user.
- **Integrity** concerns ensuring that information is only created, modified or destroyed by authorised users in authorised ways to protect the accuracy, completeness, non-repudiation and authenticity of the information.

(ISO/IEC, 2012; Ross, 2011; Zissis & Lekkas, 2012:586)

Security risks resulting from enterprise mobility causing threats to the confidentiality, integrity and availability of corporate information have been identified by various authors. A matrix table was compiled summarising the security risks and causes thereof from each source reviewed for this study, limited to security risks most frequently identified in literature reviewed. Table 2.1 summarises the most recurring security risks as identified by the various authors as well as the causes thereof. It also indicates the impact of the identified risks on the security benchmarks (confidentiality, availability and integrity).

Table 2.1: Identified security risks originating from enterprise mobility

Risks and causes of these risks	Authors								Threat to:		
	ISACA 2010	Ghosh *et al.* 2013	Milligan & Hucheson 2007	ISACA 2012	Khokhar 2006	Miller 2004	Souppaya & Scarfone 2013	OWASP 2011	Confidentiality	Availability	Integrity
Risk 1: Unavailable mobile device or unavailable resources on a mobile device											
Lost, stolen or damaged device	x	x	x	x		x	x	x	#	#	#
Trojans and viruses			x		x					#	
Smsing attacks			x							#	
Malware propagation	x			x						#	
Spam		x	x		x					#	
Risk 2: Data loss or data corruption											
Lost stolen or damaged device	x	x	x	x		x	x	x		#	#
Trojans and viruses			x		x					#	
Smsing attacks			x							#	
Malware propagation	x			x						#	
Malicious hackers	x	x	x		x		x	x		#	#
Risk 3: Unauthorised access to sensitive and confidential information											
Lost or stolen device	x	x	x	x		x	x	x	#	#	#
Data or call interception	x	x	x	x	x	x	x	x	#		#
Wireless sniffers	x			x					#		
Phishing attacks		x		x			x		#		
Spyware attacks	x			x					#		
Malicious hackers	x	x	x		x		x	x	#	#	#
Untrustworthy applications				x			x		#		
Risk 4: Insufficient security management											
Unsupported operating systems	x		x						#	#	#
Operating system limitations			x							#	#
Untrained or uninformed users			x						#		#

(Ghosh *et al.*, 2013:64; ISACA, 2010:5; ISACA, 2012; Khokhar, 2006; Miller, 2004; Milligan & Hutcheson, 2007:189; OWASP, 2011; Souppaya & Scarfone, 2013)

Key

x	The author listed the occurrence as an incident that can lead to an enterprise mobility security risk
#	The occurrence is a threat to the security benchmark

Ghosh *et al.* (2013:64), ISACA (2010:5), ISACA (2012), Khokhar (2006), Miller (2004), Milligan and Hutcheson (2007:189), OWASP (2011) and Souppaya and Scarfone (2013) described the most recurring security risks and the impact of these risks as follows:

Risk 1: Unavailable mobile device or unavailable resources on a mobile device

The use of mobile devices is an integral part of the IT solution facilitating the establishment of enterprise mobility. Due to the mobile nature of these devices, they can be easily lost, stolen or damaged. A mobile device's software or operating system can be corrupted by Trojans, viruses, smsing attacks and malware propagation, rendering the mobile device unavailable for functional use by employees. Spam can lead to resources on the mobile device being wasted, causing the device to become temporarily unavailable. The following may result in the unavailability of mobile devices or unavailable resources on a mobile device:

- A lost, stolen, damaged or corrupted mobile device can cause information stored on the device to be permanently lost (unavailable) if employees failed to follow sufficient back-up procedures for corporate information stored on the mobile device itself.
- If an employee uses a mobile device to access information on the corporate network of the organisation, this information may become inaccessible if the mobile device is lost, stolen, damaged or corrupted and can therefore not be used to access this information.
- A lost, stolen, damaged or corrupted mobile device can prevent employees from performing work-related tasks if they are dependent on software or applications installed on their mobile devices.
- Resources on a mobile device, such as bandwidth and memory space, are crucial for employees to perform work-related tasks. Unsolicited messages and e-mails received from known or unknown sources (spam and smsing) can cause wastage of these resources. This can lead to the user of the mobile device being denied timely and reliable access to the software, applications or information that is necessary for performing work-related tasks on the device itself or on the corporate network.

Risk 2: Data loss or data corruption

Mobile devices can easily be lost, stolen or damaged, resulting in data loss. Malware propagation, smsing attacks, malicious hackers, Trojans and viruses can lead to the corruption of data stored on the mobile device. The following may result in data loss or data corruption:

- Failure by employees to follow sufficient back-up procedures may lead to data stored on their mobile device becoming permanently lost or unavailable as a result of the lost, stolen or damaged mobile device, or the data on the device becoming corrupt.
- Corruption of the data on the mobile device may cause problems with accuracy, completeness, non-repudiation and authenticity.

Risk 3: Unauthorised access to sensitive and confidential information

Unauthorised access to sensitive and confidential information can be the result of a mobile device with unsecured data storage being lost or stolen, data or call interception (vishing or man-in-the-middle attacks), wireless sniffers, phishing attacks, spyware attacks, malicious hackers or untrustworthy applications installed on the mobile device. The abovementioned occurrences can lead to the following threats to security:

- Unauthorised access can be gained to information stored on the mobile device itself. Furthermore, it can lead to unauthorised access to information on the internal network if the compromised device allows easy access to the corporate network. This disclosure of sensitive or confidential information may cause damage to the organisation, its customers, its employees, or its reputation, and may result in possible legal action.
- Applications pose significant privacy and confidentiality risks if mobile device users are not aware of how personal or corporate data stored on the device is used by the installed applications. This can result in unauthorised exposure of sensitive or confidential information, as discussed above.
- Unauthorised access can be gained to:
    - information during the transmission of information through unsecured or compromised communication channels;

- information stored on the mobile device itself; or
- information stored on the organisation's internal network, if easy access to the corporate network is gained through the mobile device.

Unauthorised access may lead to the unauthorised creation, modification and destruction of information, causing problems with integrity due to the possible unauthorised creation, modification or destruction of the information.

Risk 4: Insufficient security management

There is high variability amongst the operating systems for mobile devices available for use by employees (the bring-your-own-device problem). Each operating system has its own unique characteristics and implementable security measures (Wagner, 2008:10). This high variability in operating systems can result in insufficient security management due to IT departments and users of mobile devices not implementing adequate security measures:

- For IT departments to fully understand and therefore effectively implement the available security measures for all the possible operating systems can lead to exorbitant and unwanted IT costs. When organisations try to avoid these unwanted cost implications, IT personnel may be unable to fully support and effectively implement security measures for all possible operating systems. Such insufficient security management by IT departments for certain mobile devices may result in exposed, unsecured mobile devices creating an easy target for hackers; unauthorised access to sensitive or confidential information; or malware propagation, resulting in problems concerning confidentiality, integrity and availability (as discussed above in Risk 3).
- Enforcing strong passwords and encryption on certain mobile devices may be restricted or limited due to the variability of the security capabilities of the different operating system. This may lead to unauthorised access to, or the unauthorised creation, modification or destruction of information.
- Untrained mobile device users may inadvertently expose the organisation to unnecessary risks if they do not fully understand or comprehend the security threats arising from the extended features of their mobile devices, such as inadvertent data roaming, GPS tagging, or saving sensitive information (such as usernames and passwords) in a "secure" repository offered by the operating

system. This can lead to problems concerning confidentiality and integrity if the mobile device is hacked, lost, stolen, or information on the compromised device is intercepted.

Enterprise mobility will have an impact on the confidentiality, integrity and availability of information due to the resulting security risks identified above. Organisations should govern and manage these identified risks in order to limit or completely eliminate the possible impact. This process of governing and managing risks can be time consuming, costly and sometimes not even effective.

2.3 IT governance

2.3.1 The need for IT governance

Corporate governance pertains to a framework of rules and practices that assist a company's board of directors in directing, managing and controlling an entity in order to ensure ethical values, accountability, responsibility, fairness and transparency in the company's relationship with its stakeholders (Cuong, 2007:1; Institute of Directors Southern Africa , 2009; Naidoo, 2002:2).

IT governance, as an important subset discipline of corporate governance, has specifically been addressed in available authoritative literature on corporate governance, such as King III in South Africa, Basel II in Europe and the Sarbanes Oxley Act in the United States of America (Institute of Directors Southern Africa, 2009; Robinson, 2005:45; Robles, Choi, Cho, Lee & Kim, 2009:82) hinting to the increased importance of governing IT related risks. Given the increase in the use of IT in businesses, as well as the pervasive nature of the IT used, as discussed earlier, it is inevitable that risks will be encountered. These risks have to be managed and mitigated. According to the IT Governance Institute (2003) proper IT governance will assist organisations to mitigate and manage IT risks.

The IT Governance Institute (2012) defines risk management as one of the governance objectives. It

> …*entails recognising risk; assessing the impact and likelihood of that risk; and developing strategies, such as avoiding the risk, reducing the negative effect of the risk and/or transferring the risk, to manage the risk within the context of the enterprise's risk appetite* (IT Governance Institute, 2012).

A good understanding of what IT governance entails was therefore important in answering the research question of this study, as IT governance principles comprise a widely used mechanism for successfully governing significant risks that can be made applicable to security.

2.3.2 Defining IT governance

There are many definitions for the term “IT governance” (Institute of Directors Southern Africa , 2009; IT Governance Institute, 2003; Van Grembergen & De Haes, 2009:2; Weill & Woodham, 2002:1). Webb, Pollard and Ridley (2006:200) identified twelve definitions for this term during their review of existing literature and suggested the following definition to cover the “broad reach” of IT governance: “IT Governance is the strategic alignment of IT with the business such that maximum business value is achieved through the development and maintenance of effective IT control and accountability, performance management and risk management” (Webb, Pollard and Ridley, 2006:200).

This definition was based on the following five IT governance objectives that capture the broad reach of IT governance: strategic alignment; delivery of business value through IT; control and accountability; performance management; and risk management (Webb *et al.*, 2006:200).

These IT governance objectives are echoed by the more recent definition of IT governance as described in the IT Governance Institute’s latest release of COBIT, COBIT 5 (IT Governance Institute, 2012). The authors list the main objective of governance as value creation that can be “achieved when the three underlying objectives (benefits realisation, risk optimisation and resource optimisation) are balanced” (IT Governance Institute, 2012). Through the process of applying the principles and guidance given by widely adopted IT governance guidance, managing or governing IT risks will be one of the beneficial consequences.

2.3.3 IT governance principles and IT control documents

An abundance of IT best practices is available to assist business managers with the governance of IT. Practices range from broad and general control frameworks, such as COBIT 5, that denote *what* should be done, to more narrow and specific control -models and -standards that describe *how* it should be done.

According to the IT Governance Institute (2008) and Năstase, Năstase and Ionescu (2009:8) there is a multitude of benefits in using these IT control documents (control frameworks, -models and -standards). IT governance control documents are important to organisations as they provide, amongst other benefits, a benchmarked framework of generally accepted standards that assist business managers to effectively govern IT, which, in turn, will lead to increased business value through business/IT alignment and decreased IT and business risks. Using standardised best practices is also more cost-effective than standards developed in-house and, due to the continuous improvement and update of IT governance frameworks, -models and -standards, is gaining maturity and increased acceptance amongst peers (IT Governance Institute, 2008; Năstase *et al.*, 2009:8).

However, best practice IT control documents are not mutually exclusive. This is underlined by the available literature on combining, integrating or mapping different best practice documents together. Combining different documents can provide organisations with a strong basis for an IT governance strategy (IT Governance Institute, 2008).

The benefit of combining different IT control documents can, however, be reduced by the costly and unfocused adoption of these documents, rendering the process inefficient. To efficiently utilise guidance given in the different IT control documents, organisations should apply the guidance they give only where it is fundamental and would provide the most benefit within the organisation (Năstase *et al.*, 2009:8). Only the relevant control techniques applicable to organisations implementing enterprise mobility should be implemented.

The control documents listed below addressing IT governance and mobile security risk management were chosen for this study as they are widely adopted IT control documents specifically addressing IT governance and/or the management of security risks related to mobility by many organisations. Furthermore, these IT control documents are also updated regularly to include the most relevant, up-to-date IT governance principles and control techniques:

- COBIT 5;
- ITIL; and
- ISO/IEC 27000 series.

2.3.4 Weakness of IT governance control documents

ISACA's white paper (2010) indicated that the IT governance principles and control techniques discussed in IT governance control documents cannot, on their own, provide an effective, comprehensive solution to address and mitigate IT risks. This white paper cautions organisations to also consider aspects other than governance, and lists technology and the culture of an organisation specifically as issues to consider during the process of creating the organisation's mobile device security strategy (ISACA, 2010:6).

This collective approach to include aspects other than just IT governance control documents to manage IT risks is echoed by Rudman (2010:3253) who calls for a collective effort between business and IT managers to create a unified "risk management unit". Within this unified unit the policies and procedures of business managers, such as the IT governance principles and control techniques discussed in IT governance control documents, are successfully merged and aligned with the policies and procedures of IT managers such as IT principles and IT control techniques (Rudman, 2008:13; Rudman, 2010:3253).

However, attempting to align business and IT and successfully addressing risks on both the strategic and operational levels has proven to be a problem (Rudman, 2010:3253). Business managers do not understand technology and IT control techniques and IT managers do not understand the IT governance control documents (Rudman, 2008:12). This misalignment of business and IT is also referred to as the IT gap as there is a gap between what business managers expect from IT according to their IT governance control documents, and the reality of how IT and the IT control techniques are implemented by the IT managers (Goosen & Rudman, 2013:839).

These IT governance documents, principles and control techniques will address the security risks of enterprise mobility on a strategic level. The weakness of IT governance control documents lies in addressing the security risks of enterprise mobility on an operational level by effectively aligning business and IT and bridging the IT gap as IT governance frameworks, -models and -standards does not provide technical, implementable guidance on how to implement IT control techniques on an operational level.

2.4 Conclusion

Enterprise mobility is a megatrend. The effect of the consumerisation of mobile technology, and therefore the societal expectation with regard to the enterprise mobility of organisations, their business models, business strategy, strategic objectives, business imperatives and risk management is undeniable. These risks should be governed. The governance of these risks on a strategic level is discussed in Chapter 3 and the governance of these risks on an operational level is discussed in Chapter 5.

CHAPTER 3: IT GOVERNANCE CONTROL DOCUMENTS AND THEIR RELEVANCE IN THE GOVERNANCE OF IDENTIFIED ENTERPRISE MOBILITY SECURITY RISKS ON A STRATEGIC LEVEL

3.1 Introduction

As discussed in Chapter 2, IT governance control documents assist organisations to effectively manage IT risks on a strategic level by providing guidance in the form of implementable processes. Combining IT governance frameworks, -models and -standards can provide organisations with a strong basis for an effective IT governance strategy (IT Governance Institute, 2008), but can become costly if implemented in an unfocused, inefficient manner (Năstase *et al.*, 2009:8). Organisations should identify and apply only the processes that will be relevant and beneficial in their specific context.

The following widely adopted and recently updated IT control documents giving relevant guidance on IT governance principles and the management of enterprise mobility security risks were reviewed and assessed to be most relevant for this study in assisting organisations during the process of governing identified security risks originating from enterprise mobility on a strategic level:

- COBIT 5;
- ITIL; and
- the ISO/IEC 27000 series.

This chapter presents a discussion of the above-mentioned IT control documents and their specific relevance during the process of governing IT risks on a strategic level. The processes listed in each framework are reviewed and evaluated to assess their relevance in specifically addressing security risks originating from enterprise mobility. From this assessment the relevant processes listed in each IT control document that should be implemented to ensure the effective governance of enterprise mobility security risks on a strategic level, are identified.

3.2 COBIT 5

3.2.1 COBIT 5 overview

COBIT is a widely adopted best practice IT governance framework (Gerke & Ridley, 2006; Liu & Ridley, 2005; Năstase *et al.*, 2009:8; Ramos, 2006:58; Shivashankarappa, Smalov, Dharmalingam & Anbazhagan, 2012:144; Simonsson & Johnson, 2006:7) and some writers are of the opinion it is a *de facto* standard for IT governance (Robinson, 2005:48; Sallé, 2004; Soomro & Hesson, 2012:273). COBIT is applied by organisations to effectively govern IT in order to mitigate risks and achieve business value through IT (IT Governance Institute, 2003; Simonson & Johnson, 2006:2).

The latest edition, COBIT 5, was released in 2012 and consolidates several ISACA IT governance control documents (COBIT 4.1, Val IT and Risk IT) and other best practices, such as ITIL and TOGAF, to provide high-level guidance in the form of an overarching framework that enables organisations to govern and manage enterprise IT (IT Governance Institute, 2012).

Organisations can benefit from the adoption of COBIT 5 as it assists organisation to increase the trust in IT systems while still retaining the value obtained from these systems by maintaining the balance between the risks and benefits of IT and to increase the trust in, and value from, information systems (IT Governance Institute, 2012).

COBIT 5 is based on five key principles (IT Governance Institute, 2012):

> Principle 1: Meeting Stakeholder Needs
>
> Creating value for stakeholders, either financial benefit for commercial organisations; public service for government entities; or social benefits for non-profit organisations, is the reason for the existence of all organisations. Applying COBIT 5 can assist those charged with governance to translate stakeholders' needs into an organisation's actionable strategy. The goals cascade is based on four steps:
>
> - Step 1: Stakeholder Drivers Influence Stakeholder Needs

- Step 2: Stakeholder Needs Cascade to Enterprise Goals
- Step 3: Enterprise Goals Cascade to IT-related Goals
- Step 4: IT-related Goals Cascade to Enabler Goals

The concept of enabler goals is explained in detail under Principle 4, below.

Principle 2: Covering the Enterprise End to End

The governance and management of an organisation's information and related technology are addressed by COBIT 5. This enterprise-wide, end-to-end perspective is achieved by including "everything and everyone, internal and external, that are relevant to governance and management of enterprise information and related IT, including the activities and responsibilities of both the IT functions and non-IT business functions" (IT Governance Institute, 2012).

Principle 3: Applying a Single, Integrated Framework

COBIT 5 integrates and aligns, on a high level, with many other IT-related standards and best practices.

Principle 4: Enabling a Holistic Approach

The holistic approach defines seven categories of enablers that can assist an organisation to effectively and efficiently govern and manage enterprise IT.

According to the IT Governance Institute (2012),

> *enablers are organisational resources for governance, such as frameworks, principles, structures, processes and practices, through which action is directed and objectives can be attained. Enablers also include the enterprises' resources – e.g., service capabilities (IT infrastructure, applications, etc.), people and information.*

The seven categories of enablers are listed as:

1. Principles, Policies and Frameworks

   This enabler will provide the organisation's decision-makers with the necessary guidance for making the correct decisions to achieve the organisation's strategic objectives.
2. Processes

   A set of implementable practices and activities are outlined under this enabler that will contribute to the achievement of the business and IT objectives within the organisation's overall strategy.
3. Organisational Structures

   These structures will assign responsibility in key areas within the organisation.
4. Culture, Ethics and Behaviour

   This enabler will encourage good practices and ethical behaviour within the organisation.
5. Information

   Information is a significant part of any organisation and the quality and security of information used and produced are discussed under this enabler.
6. Services, Infrastructure and Applications

   Good governance practices for the IT resources that are necessary for the processing, storage and access of information are highlighted under this enabler.
7. People, Skills and Competencies

   The importance of employing qualified people with the necessary skills and competencies for each role within an organisation is discussed under this enabler.

Principle 5: Separating Governance from Management

The framework subdivides the practices, activities and organisational structures necessary to manage and govern the organisation's IT into two main areas, governance and management. The governance area consists of one domain called "Evaluate, direct and monitor". The management area is

divided into four domains of processes:

- Align, plan and organise;
- Build, acquire and implement;
- Deliver, service and support; and
- Monitor, evaluate and assess.

Processes are one of the enablers listed under Principle 4. Under this enabler, the framework describes a number of implementable governance and management practices that can be applied during the process of risk management in detail. Figure 3.1 illustrates the thirty-seven processes listed in COBIT 5, divided into five domains as described under Principle 5.

These processes were evaluated to identify the specific processes that are relevant in the process of governing enterprise mobility security risks, as not all processes are applicable to all organisations, mobile technology or security risks.

3.2.2 COBIT 5 processes addressing enterprise mobility security risks

The study has assessed all high-level processes listed in COBIT 5 and identified the following processes in each domain that are specifically relevant in addressing security risks in mobile devices:

- Domain: Evaluate, Direct and Monitor:
  - EDM01 Ensure governance framework setting and maintenance
  - EDM02 Ensure benefits delivery
  - EDM03 Ensure risk optimisation
  - EDM04 Ensure resource optimisation
  - EDM05 Ensure stakeholder transparency
- Domain: Align, Plan and Organise:
  - APO01 Manage the IT Management Framework
  - APO02 Manage Strategy
  - APO04 Manage innovation
  - APO05 Manage Portfolio
  - APO06 Manage Budget and Costs
  - APO07 Manage Human Resources
  - APO09 Manage Service Agreements

  - APO10 Manage Suppliers
  - APO12 Manage risk
  - APO13 Manage security
- Domain: Build, Acquire and Implement:
  - BAI01 Manage Programmes and Projects
  - BAI02 Manage Requirements Definition
  - BAI03 Manage Solutions Identification and Build
  - BAI04 Manage Availability and Capacity
  - BAI06 Manage Changes
  - BAI09 Manage Assets
  - BAI10 Manage Configuration
- Domain: Deliver, Service and Support:
  - DSS02 Manage Service Requests and Incidents
  - DSS03 Manage Problems
  - DSS04 Manage Continuity
  - DSS05 Manage Security Services
- Domain: Monitor, Evaluate and Assess:
  - MEA01 Monitor, Evaluate and Assess Performance and Conformance
  - MEA02 Monitor, Evaluate and Assess the System of Internal Control
  - MEA03 Monitor, Evaluate and Assess Compliance with External Requirements

(ISACA, 2012; IT Governance Institute, 2012)

The identified processes are described in Appendix A.

3.3 The Information Technology Infrastructure Library (ITIL)

3.3.1 ITIL overview

ITIL provides guidance for the management of IT services in the form of best practices and is widely adopted by organisations (England, 2011; Hornbill Systems, 2009; Lucio-Nieto, Colomo-Palacios, Soto-Acosta, Popa & Amescua-Seco, 2012:592; Pastuszak, Czarnecki & Orlowski, 2012:1431). ITIL 2011 is the latest edition. This edition addresses each stage of the service life cycle and the set of key processes and functions required during that specific stage. The five core

publications, each of which addresses one of the five stages in the service lifecycle, are summarised in Table 3.1.

Table 3.1: ITIL core publications

ITIL service lifecycle stage	Description
Service Strategy (SS)	This publication assists business managers to develop a long-term strategy for IT systems that will achieve alignment between the business and IT strategy.
Service Design (SD)	This publication gives direction on the design and development of IT services, their architectures, processes, and other aspects of the service management effort in order to increase business value by aligning to the business strategy. This guidance is applicable to new services and also to any modifications and improvements to existing IT services.
Service Transition (ST)	This publication provides guidance on managing and controlling the transition of new and modified IT services required by an organisation into the live IT operational environment in order to provide for innovation and added value whilst still controlling the risks of failure, error and disruption.
Service Operation (SO)	Once transitioned, this publication directs business managers, with the help of best practices, in delivering and supporting the day-to-day operation of IT services, including the applications, technology and infrastructure, to ensure value is delivered to the organisation and its end-users while also meeting the strategic objectives of the organisation.
Continual Service Improvement management (CSI)	This publication is concerned with measuring IT service levels and determining and executing improvements to the IT services on a continuing basis to create and maintain value for end-users through better design, transition and operation of services to better support the business processes.

(Arraj, 2010; Cartlidge, Hanna, Rudd, Macfarlane, Windebank & Rance, 2007; Itinfo, s.a.; Kneller, 2010)

A total of twenty-six processes are listed in ITIL. The twenty-six processes were evaluated to identify the specific processes that are relevant in the process of governing enterprise mobility security risks, as not all processes are applicable to all organisations, mobile technology or security risks.

3.3.2 ITIL processes addressing enterprise mobility security risks

The study has assessed all high-level processes per life cycle stage listed in ITIL 2011 and identified the following processes that are specifically relevant in addressing security risks in mobile devices:

- ITIL Service Strategy
    - Strategy Management for IT Services
    - Service Portfolio Management
    - Financial Management for IT Services
    - Demand Management
    - Business Relationship Management
- ITIL Service Design
    - Service Catalogue Management
    - Service-level Management
    - Supplier Management
    - Capacity Management
    - Availability Management
    - IT Service Continuity Management
    - Information Security Management
    - Design Coordination
- ITIL Service Transition
    - Project Management (Transition Planning and Support)
    - Change Management
    - Service Asset and Configuration Management
    - Release and Deployment Management
    - Knowledge Management
    - Service Validation and Testing
    - Change Evaluation
- ITIL Service Operation
    - Event Management
    - Incident Management
    - Problem Management
    - Request Fulfilment
    - Access Management

- Continual Service Improvement
    - Seven-step improvement

(Cartlidge *et al.*, 2007)

The identified processes are described in more detail in Appendix B.

3.4 ISO/IEC 27000 series

3.4.1 ISO/IEC 27000 series overview

The ISO/IEC 27000-series is published by the International Organization for Standardization (ISO) in partnership with the International Electrotechnical Commission (IEC). It provides organisations with internationally recognised best practice recommendations on information security management systems.

This series consist of more than twenty published standards, with several more still under development. As the focus of this study is on implementable best practices for the governance of enterprise mobility security risks, only the four standards mentioned below were selected as these standards provide guidance for “initiating, implementing, maintaining, and improving” information security management systems (ISO27001 Security;2013). The focus of these standards are on operational risk, application security, computing platform security, network security and physical security (Nicho, Fakhry & Haiber, 2011:57), which make it applicable to this study focused on security risks. The following four standards in this series will be investigated:

- **ISO/IEC 27000** gives an overview of the ISO/IEC 27000-series addressing information security management systems and it also explains relevant terms and definitions.
- **ISO/IEC 27001** explains how to apply the processes listed in ISO/IEC 27002.
- **ISO/IEC 27002** contains an implementable list of recommended best practices for the management of information security based on the control objectives discussed in ISO/IEC 27001.

- **ISO/IEC 27014** focuses specifically on information security and discusses best practices for the governance thereof.

(ISO27001 Security, 2013; International Telecommunication Union, 2013b)

The high-level processes listed in ISO/IEC 27002 and ISO/IEC 27014 are evaluated in conjunction with applicable information pertaining to these processes as discussed in ISO/IEC 27000 and ISO/IEC 27001.

3.4.2 ISO/IEC 27000 series processes addressing enterprise mobility security risks

The study has assessed all high-level processes listed in ISO/IEC 27002 and ISO/IEC 27014 (ISO27001 Security, 2013; International Telecommunication Union, 2013b) and identified processes that are specifically relevant in the process of governing enterprise mobility security risks, as not all processes are applicable to all organisations, mobile technology or security risks. ISO/IEC 27002's relevant processes are listed in Table 3.2.

Table 3.2: ISO/IEC 27002 processes for the governance of security risks relating to mobility

Domain	Process
Security policy	• Establish a security policy
Organisation of information security	• Establish an internal security organisation • Control external party use of the organisation's information
Asset management	• Establish responsibility for the organisation's mobile devices and other IT assets necessary to secure the organisation's information • Use an information classification system
Human resources security	• Emphasise security prior to employment • Emphasise security during employment • Emphasise security at termination of employment
Physical and environmental security	• Use secure areas to protect facilities • Protect the organisation's mobile devices and other IT resources

Domain	Process
Communications and operations management	• Establish procedures and responsibilities • Control third party service delivery • Carry out future system planning activities • Protect against malicious and mobile code • Establish back-up procedures • Protect computer and mobile networks • Control how media are handled • Protect exchange of information • Protect electronic commerce services • Monitor information processing facilities
Access control	• Control access to information • Manage user access rights • Encourage good access practices • Control access to network services • Control access to operating systems • Control access to applications and systems • Protect mobile and teleworking facilities
Information systems acquisition, development and maintenance	• Identify information system security requirements • Make sure applications process information correctly • Use cryptographic controls to protect the organisation's information • Protect and control the organisation's system files • Control development and support processes
Information security incident management	• Report information security events and weaknesses • Manage information security incidents and improvements
Business continuity management	• Use continuity management to protect the organisation's information
Compliance	• Comply with legal requirements • Perform security compliance reviews • Carry out controlled information system audits

(ISO27001 Security, 2013)

The processes listed in ISO/IEC 27014 that is relevant in the process of governing enterprise mobility security risks are listed in Table 3.3.

Table 3.3: ISO 27014 processes for the governance of security risks relating to mobility

Domain	Process
'Evaluate' is the governance process that considers the current and forecast achievement of security objectives based on current processes and planned changes, and determines where any adjustments are required to optimise the achievement of strategic objectives in future	a. Ensure that organisation initiatives take into account information security issues b. Ensure that information security adequately supports and sustains the business objectives c. Respond to information security performance result and prioritise and initiate required actions d. Submit new information security projects with significant impact to governing body
'Direct' is the governance process by which the governing body gives direction about the information security objectives and strategy that need to be implemented. Direction can include changes in resourcing levels, allocation of resources, prioritisation of activities, and approval of policies, material risk acceptance and risk management plans	a. Determine the organisation's risk appetite b. Align information security objectives with business objectives c. Promote a positive information security culture d. Develop, approve and implement information security strategy and policy e. Allocate adequate investment and resources
'Monitor' is the governance process that enables the governing body to assess the achievement of strategic objectives	a. Select appropriate performance metrics from a business perspective b. Assess the effectiveness of information security performance c. Consider the changing business, legal and regulatory environment and their potential impact on information risk and information security d. Ensure conformance with internal and external requirements
'Communicate' is the bidirectional governance process by which the governing body and stakeholders exchange information about information security appropriate to their specific needs	a. Report to external stakeholders that the organisation practices a level of information security commensurate with the nature of its business b. Notify executive management of the results of any external reviews that have identified information security issues, and request corrective actions. c. Recognise information concerning regulatory obligations, stakeholders' expectations, and business needs with regard to information security
'Assure' is the governance process by which the governing body commissions independent and objective audits, reviews or certifications. These will identify and validate the objectives and actions related to carrying out governance activities and conducting operations in order to attain the desired level of information security	Commission independent and objective opinions of how it is complying with its accountability for the desired level of information security

(International Telecommunication Union, 2013b)

3.5 Conclusion

This chapter identified the relevant processes listed in the selected IT control documents that will assist organisations to govern security risks resulting from enterprise mobility on a strategic level. Implementing these identified processes one by one will not be practical. It will be time consuming and inefficient. If organisations only implement the processes that are most significant or most relevant to their organisation, it will result in a more efficient process for governing security risks resulting from enterprise mobility.

CHAPTER 4: MAPPING OF THE IDENTIFIED RELEVANT IT GOVERNANCE PROCESSES AGAINST THE IDENTIFIED ENTERPRISE MOBILITY SECURITY RISKS

4.1 Introduction

IT governance control documents, such as governance frameworks, -models and -standards, assist organisations in managing IT risks effectively on a strategic level by providing guidance in the form of implementable processes designed to govern such risks. Combining best practice IT governance control documents can provide organisations with a strong basis for an effective IT governance strategy (IT Governance Institute, 2008), but can result in a costly and inefficient process (Năstase *et al.*, 2009:8). Organisations should identify and apply only those processes that will be relevant and beneficial in their specific situation with regard to existing enterprise mobility security risks and their risk appetite.

Organisations implementing an IT solution to facilitate the establishment of enterprise mobility have to effectively and efficiently manage the resulting security risks. Only the relevant processes addressing the identified security risks related to enterprise mobility should be implemented to prevent a costly and inefficient IT governance process.

4.2 Mapping of the identified security risks that result from enterprise mobility against the relevant COBIT 5 processes

In Table 4.1 the enterprise mobility security risks, as identified in Chapter 2, are mapped to the processes listed in COBIT 5 that are relevant in addressing these security risks. This matrix is used to assess which processes are most significant and should be implemented by organisations to effectively govern enterprise mobility security risks on a strategic level.

Table 4.1: Mapping security risks to COBIT 5 processes

COBIT 5 process	Risk 1	Risk 2	Risk 3	Risk 4
EDM01 Ensure governance framework setting and maintenance	x	x	x	x
EDM02 Ensure benefits delivery	x	x	x	x
EDM03 Ensure risk optimisation	x	x	x	x
EDM04 Ensure resource optimisation	x	x	x	x
EDM05 Ensure stakeholder transparency	x	x	x	x
APO01 Manage the IT Management Framework	x	x	x	x
APO02 Manage Strategy	x	x	x	x
APO04 Manage Innovation	x	x	x	x
APO05 Manage Portfolio				x
APO06 Manage Budget and Costs	x	x	x	x
APO07 Manage Human Resources	x	x	x	x
APO09 Manage Service Agreements	x	x	x	x
APO10 Manage Suppliers	x	x	x	x
APO12 Manage risk	x	x	x	x
APO13 Manage security	x	x	x	x
BAI01 Manage Programmes and Projects				x
BAI02 Manage Requirements Definition				x
BAI03 Manage Solutions Identification and Build	x	x	x	x
BAI04 Manage Availability and Capacity	x	x	x	x
BAI06 Manage Changes	x	x	x	x
BAI09 Manage Assets	x	x	x	x
BAI10 Manage Configuration	x	x	x	x
DSS02 Manage Service Requests and Incidents	x	x	x	x
DSS03 Manage Problems	x	x	x	x
DSS04 Manage Continuity	x	x	x	x
DSS05 Manage Security Services	x	x	x	x

COBIT 5 process	Risk 1	Risk 2	Risk 3	Risk 4
MEA01 Monitor, Evaluate and Assess Performance and Conformance	x	x	x	x
MEA02 Monitor, Evaluate and Assess the System of Internal Control	x	x	x	x
MEA03 Monitor, Evaluate and Assess Compliance with External Requirements	x	x	x	x

Key

Risk 1	Unavailable mobile device or unavailable resources on a mobile device
Risk 2	Data loss or data corruption
Risk 3	Unauthorised access to sensitive and confidential information
Risk 4	Insufficient security management
x	The process is applicable in governing the risk

All of these processes, except APO05, BAI01 and BAI02, address three or more of the identified enterprise mobility security risks and seem to be significant processes for the purpose of effectively governing the four risks. The three processes that are relevant in addressing one of the identified risks only have been reviewed and evaluated, and also seem to be significant processes. The three processes should therefore also be implemented during the process of governing enterprise mobility security risks.

4.3 Mapping of the identified security risks that result from enterprise mobility against the relevant ITIL processes

In Table 4.2 the enterprise mobility security risks, as identified in Chapter 2, are mapped to the processes listed in ITIL that is relevant in addressing these security risks, as identified in Chapter 3. This matrix is used to assess which processes is most significant and should be implemented by organisations to effectively govern enterprise mobility security risks on a strategic level.

Table 4.2: Mapping security risks to ITIL processes

ITIL process	Risk 1	Risk 2	Risk 3	Risk 4
Service Strategy				
Strategy Management for IT Services	x	x	x	x
Service Portfolio Management	x	x	x	x
Financial Management for IT Services	x	x	x	x
Demand Management	x	x		x
Business Relationship Management				x
Service Design				
Service Catalogue Management				x
Service-level Management	x	x	x	x
Supplier Management	x	x	x	x
Capacity Management	x	x		x
Availability Management	x	x		x
IT Service Continuity Management	x	x		x
Information Security Management	x	x	x	x
Design Coordination	x	x	x	x
Service Transition				
Project Management (Transition Planning and Support)	x	x	x	x
Change Management	x	x	x	x
Service Asset and Configuration Management	x	x	x	x
Release and Deployment Management	x	x	x	x
Knowledge Management	x	x	x	x
Service Validation and Testing	x	x	x	x
Change Evaluation	x	x	x	x
Service Operation				
Event Management	x	x	x	x
Incident Management	x	x	x	x
Problem Management	x	x	x	x

ITIL process	Risk 1	Risk 2	Risk 3	Risk 4
Service Operation (continued)				
Request Fulfilment	x	x	x	x
Access Management			x	x
Continual Service Improvement				
Seven-step improvement	x	x	x	x

Key

Risk 1	Unavailable mobile device or unavailable resources on a mobile device
Risk 2	Data loss or data corruption
Risk 3	Unauthorised access to sensitive and confidential information
Risk 4	Insufficient security management
x	The process is applicable in governing the risk

All of the processes, except Business Relationship Management, Service Catalogue Management and Access Management, address three or more of the identified enterprise mobility security risks and seem to be significant processes for the purpose of effectively governing the four risks. The three processes that are only relevant in addressing one or two of the identified risks have been reviewed and evaluated, and also seem to be significant processes. The three processes should therefore also be implemented during the process of governing the enterprise mobility security risks.

4.4 Mapping of the identified security risks that result from enterprise mobility against the relevant ISO/IEC 27002 processes

In table 4.3 the enterprise mobility security risks, as identified in Chapter 2, are mapped to the processes listed in ISO/IEC 27002 that is relevant in addressing these security risks, as identified in Chapter 3. This matrix is used to assess which processes are most significant and should be implemented by organisations to effectively govern enterprise mobility security risks on a strategic level.

Table 4.3: Mapping security risks to ISO/IEC 27002 processes

ISO27002 process	Risk 1	Risk 2	Risk 3	Risk 4
Establish a security policy	x	x	x	x
Establish an internal security organisation	x	x	x	x
Control external party use of the organisation's information	x	x	x	x
Establish responsibility for the organisation's mobile devices and other IT assets necessary to secure the organisation's information	x	x	x	x
Use an information classification system				x
Emphasise security prior to employment	x	x	x	x
Emphasise security during employment	x	x	x	x
Emphasise security at termination of employment	x	x	x	x
Use secure areas to protect facilities	x	x	x	x
Protect the organisation's mobile devices and other IT resources	x	x	x	x
Establish procedures and responsibilities	x	x	x	x
Control third party service delivery		x	x	x
Carry out future system planning activities	x	x	x	x
Protect against malicious and mobile code	x	x	x	x
Establish back-up procedures	x	x	x	x
Protect computer networks		x	x	x
Control how media are handled	x	x	x	x
Protect exchange of information		x	x	x
Protect electronic commerce services	x	x	x	x
Monitor information processing facilities	x	x	x	x
Control access to information	x	x	x	x
Manage user access rights	x	x	x	x
Encourage good access practices	x	x	x	x
Control access to network services		x	x	x
Control access to operating systems	x	x	x	x

ISO27002 process	Risk 1	Risk 2	Risk 3	Risk 4
Control access to applications and systems	x	x	x	x
Protect mobile and teleworking facilities	x	x	x	x
Identify information system security requirements	x	x	x	x
Make sure that applications process information correctly		x	x	x
Use cryptographic controls to protect the organisation's information	x	x	x	x
Protect and control the organisation's system files	x	x	x	x
Control development and support processes		x	x	x
Report information security events and weaknesses	x	x	x	x
Manage information security incidents and improvements	x	x	x	x
Use continuity management to protect the organisation's information	x	x	x	x
Comply with legal requirements	x	x	x	x
Perform security compliance reviews	x	x	x	x
Carry out controlled information system audits	x	x	x	x

Key

Risk 1	Unavailable mobile device or unavailable resources on a mobile device
Risk 2	Data loss or data corruption
Risk 3	Unauthorised access to sensitive and confidential information
Risk 4	Insufficient security management
x	The process is applicable in governing the risk

All of the processes, except "Use an information classification system" address three or more of the identified enterprise mobility security risks and seem to be significant processes for the purpose of effectively governing the four risks. The "Use an information classification system" process has been reviewed and evaluated, and seems to also be a significant process. This process should therefore also be implemented during the process of governing the enterprise mobility security risks.

4.5 Mapping of the identified security risks that result from enterprise mobility against the relevant ISO/IEC 27014 processes

In Table 4.4 the enterprise mobility security risks, as identified in Chapter 2, are mapped to the processes listed in ISO/IEC 27014 that are relevant in addressing these identified security risks, as identified in Chapter 3. This matrix is used to assess which processes are most significant and should be implemented by organisations to govern enterprise mobility security risks effectively on a strategic level.

Table 4.4: Mapping security risks to ISO/IEC 27014 processes

ISO27014 process	Risk 1	Risk 2	Risk 3	Risk 4
Ensure that business initiatives take into account information security issues	x	x	x	x
Ensure that information security adequately supports and sustains the business objectives	x	x	x	x
Respond to information security performance result and prioritise and initiate required actions	x	x	x	x
Submit new information security projects with significant impact to governing body				x
Determine the organisation's risk appetite	x	x	x	x
Align information security objectives with business objectives	x	x	x	x
Promote a positive information security culture	x	x	x	x
Develop, approve and implement information security strategy and policy	x	x	x	x
Allocate adequate investment and resources	x	x	x	x
Select appropriate performance metrics from a business perspective	x	x	x	x
Assess the effectiveness of information security performance	x	x	x	x
Consider the changing business, legal and regulatory environment and their potential impact on information risk and information security	x	x	x	x
Ensure conformance with internal and external requirements	x	x	x	x

ISO27014 process	Risk 1	Risk 2	Risk 3	Risk 4
Report to external stakeholders that the organisation practices a level of information security commensurate with the nature of its business				x
Notify executive management of the results of any external reviews that have identified information security issues, and request corrective actions	x	x	x	x
Recognise information concerning regulatory obligations, stakeholders' expectations, and business needs with regard to information security	x	x	x	x
Commission independent and objective opinions of how it is complying with its accountability for the desired level of information security	x	x	x	x

Key

Risk 1	Unavailable mobile device or unavailable resources on a mobile device
Risk 2	Data loss or data corruption
Risk 3	Unauthorised access to sensitive and confidential information
Risk 4	Insufficient security management
x	The process is applicable in governing the risk

All of the processes, except "Submit new information security projects with significant impact to governing body" and "Report to external stakeholders that the organisation practices a level of information security commensurate with the nature of its business" address three or more of the identified enterprise mobility security risks and seem to be significant processes for the purpose of effectively governing the four risks. The two processes that are only relevant in addressing one of the identified risks have been reviewed and evaluated, and also seem to be significant processes. The two processes should therefore be implemented during the process of governing the enterprise mobility security risks.

4.6 Conclusion

The relevant or fundamental processes identified in this chapter that are necessary to effectively govern security risks resulting from enterprise mobility on a strategic

level, comprise a lengthy list. A number of processes from the different IT control documents also seem to overlap. The length of the list and the overlapping processes make it inefficient to implement all the identified processes individually.

To arrive at an effective and efficient process to govern security risks relating to enterprise mobility on a strategic level, the study composed a list of high-level best practices that an organisation should implement to effectively govern these risks. This is presented in Chapter 6. By combining any overlapping processes into one best practice, the best practices were kept to a minimum and are concise.

CHAPTER 5: A PROCESS TO EFFECTIVELY AND EFFICIENTLY GOVERN ENTERPRISE MOBILITY SECURITY RISKS ON AN OPERATIONAL LEVEL

5.1 Introduction

The governance of security risks with the assistance of IT governance control documents giving guidance in the form of IT governance principles and processes was discussed in Chapters 3 and 4. However, these chapters addressed the effective and efficient governance of security risks on a strategic level only. Governing risks on a strategic level is not sufficient and will result in risks being managed ineffectively because of the weakness of IT governance control documents, as discussed in Chapter 2.

The weakness of IT governance control documents is that it cannot address security risks that result from enterprise mobility on a technical or operational level due to the lack of technical, implementable guidance in these documents. This weakness will result in the misalignment of business and IT and the emergence of an IT gap leading to IT risks being managed ineffectively.

5.2 Business/IT alignment and the IT gap

Business/IT alignment has been researched extensively over the years. Chan and Reich (2007:297) conducted a study on business/IT alignment research to summarise what has been learned and what is still being disputed. According to their study there are different models and measures for business/IT alignment, but the most dominant model for it was suggested by Sauer and Yetton (1997:7) who argue that the "basic principle is that IT should be managed in a way that mirrors management of the business". This principle is supported by ISACA (2012) who defines alignment, in COBIT 5, as the state where the organisation's IT solutions and services are governed and managed in such a way that it supports the overall objectives and strategies of that organisation. Business/IT alignment is one of the principal objectives of IT governance.

Even after the extensive research conducted on this topic since the late 1970s (Luftman & Brier, 1999:110), achieving successful business/IT alignment remains a

major concern of many business managers (Luftman & Ben-Zvi, 2010a:205; Luftman & Ben-Zvi, 2010b:265; Luftman & Ben-Zvi, 2011:205). It has been one of the top three concerns since 2003 (Gerow, 2013:36; Luftman & Ben-Zvi, 2010a:205) and amongst the top concerns for more than twenty years (Gerow, 2013:36; Luftman & Ben-Zvi, 2010b:265). This misalignment concern of business managers will become even more critical in the coming years due to accelerating IT advances and recent consumerisation of IT that escalated the rate of development of new IT-based solutions within organisations (IBM, 2012).

Misalignment is the gap that can emerge between what business managers require and expect of the IT solutions and what the IT solution, as provided by the IT personnel, actually delivers. This gap usually arises due to:

- business managers not understanding IT;
- IT managers not understanding business; and
- ineffective communication between business people and technical people.

(Chen, 2010:10; Luftman, Papp & Brier, 1999:16; Štemberger, Manfreda & Kovačič, 2011:428)

This gap between strategic business objectives and IT objectives, as illustrated in Figure 5.1, is a risk organisations have to address. According to Elmorshidy (2013:819), the basic foundation of any business strategy should be to align IT with business objectives in order to achieve the common objectives of the organisation as a whole. Other authors also suggest that organisations can only benefit from IT solutions if the IT strategies and IT resources are aligned to the business strategy (Kearns & Sabherwal, 2007:628).

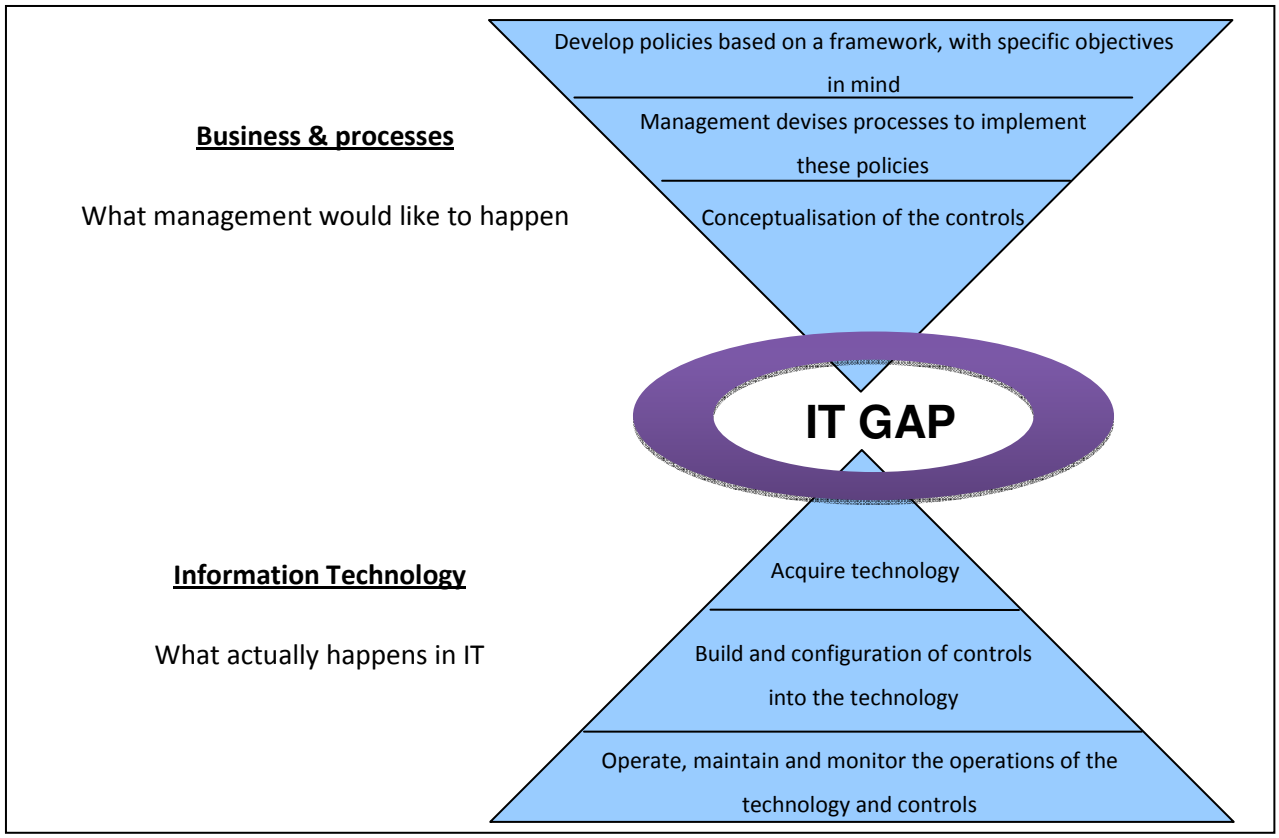

Figure 5.1: The IT gap

Source: Kruger and Rudman, 2013

If business and IT is not aligned, it can have several undesired consequences for organisations. Literature listed the following risks as consequences of misalignment:

- organisations do not meet their strategic business objectives due to ineffective IT solutions;
- IT resources are used ineffectively, leading to exorbitantly high IT costs;
- expensive IT systems that do not provide adequate return on investment;
- IT development is seen as a pure cost driver;
- laws and regulations can be breached leading to legal action; and
- the success and failure of IT strategies cannot be evaluated due to unrealistic goals set by business managers that cannot be met by IT departments. The impact and value of IT is therefore unclear and underestimated by business managers.

(Goosen, 2012:16; Sidhu, 2013:21; Trendowicz, Heidrich & Shintani, 2011:142)

Bridging the IT gap, and therefore successfully achieving business/IT alignment and managing the consequences of misalignment, is therefore becoming more critical than ever (Sidhu, 2013:26).

Business managers approach the alignment process in terms of business principles and processes within the framework of IT governance. If this process is conducted appropriately, this will address the implementation and associated risks of IT on a strategic level.

IT managers approach the alignment process in terms of IT principles:

- IT processes to choose, develop or acquire the necessary technology;
- IT processes and methodologies to develop and configure control techniques to address IT related risks;
- the processes and methodologies during the operation, maintenance and monitoring of the IT operations; and
- the processes and methodologies during the operation, maintenance and monitoring of the implemented controls.

(Kruger & Rudman, 2013)

If this process is conducted appropriately, this will address the implementation and associated risks of IT on an operational level.

To align business and IT, bridge the IT gap, and effectively manage security risks originating from enterprise mobility on an operational level, it is important to have an implementable, understandable, well-communicated process, structure or plan.

5.3 A plan to effectively address enterprise mobility security risks on an operational level

An implementable, understandable, well-communicated process, structure or plan may assist organisations to minimise the effect of the misunderstanding and miscommunication between business managers and IT managers. It may also assist organisations to maximise business/IT alignment and effective risk management. While IT governance principles and processes address risk management on a strategic level, these principles and processes provide limited practical guidance for addressing risks on an operational level. To address risks on an operational level,

the technical components within the IT solution should be better understood by business managers in order to communicate, in an effective way, with IT managers to ensure that they understand and address risks arising from the operational level of the IT solution (Sidhu, 2013:25).

Goosen (2012:31) discussed the implementation of an *integrated framework* to bridge the IT gap and align business and IT. This integrated framework includes guidance from a strategic as well as from an operational level. Goosen (2012:34) provided implementation guidance in the form of seven steps divided into three steps for the strategic level and four steps for the operational level.

The three steps (determine business imperatives; evaluate the risks of the identified business imperatives and identify relevant COBIT processes that will address these risks; and link relevant ITIL and ISO 27000 processes to the selected COBIT processes) to implement IT governance on a strategic level, as suggested by Goosen in this framework, have been applied in a similar fashion during this study to address risks on a strategic level, as was covered in Chapter 3 and Chapter 4.

The current chapter discusses the governance of enterprise mobility security risks on an operational level by implementing the four steps suggested in the integrated framework by Goosen.

5.4 Integrated framework steps applicable to govern enterprise mobility security risks on an operational level

The steps suggested by Goosen for governing enterprise mobility-related risks on the operational level include the use of applicable control techniques of the relevant processes; access paths; IT architecture components that form these access paths; and relevant configuration controls.

5.4.1 Step 1: Implement the applicable control techniques of the relevant processes identified on a strategic level

The relevant processes that would address the significant security risks related to enterprise mobility, as identified in Chapter 2, should be physically implemented by implementing the controls and control techniques listed with each process.

5.4.2 Step 2: Determine the different access paths which are affected by the selected business imperatives

Boshoff (1990) formulated the concept of an access path and discussed the value of it within the process of aligning business and IT to bridge the gap between the strategic and operational levels.

Boshoff (1990) describes an access path as follows:

> *A user performs computerised activities by activating an access path. An access path is formed by the various IT components that need to be activated in order for a typical user (business, IT or otherwise) request (functionality, data or otherwise) to be executed, in order to access computer controlled resources.*

Enterprise mobility has been identified as a critical business imperative. Within the IT solution to address enterprise mobility, a user can activate a number of different access paths. ISACA (2012) lists the following possibilities for access paths within an IT solution for enterprise mobility:

- access from a mobile device to another device;
- access from a mobile device to a public cloud;
- access from a mobile device to a private cloud; or
- access from a mobile device to the corporate network.

5.4.3 Step 3: Identify the IT architecture components which form the relevant access paths

Within all identified or activated access paths, as identified in step 2, there is a multitude of possibilities for IT components and connections between the various IT components. The following types of hardware, software and other IT architecture components may be present within the design of an enterprise mobility network necessary to provide a generic solution to address the enterprise mobility needs of an organisation:

- mobile devices;
- mobile applications;
- middleware;

- security and management software;
- switches;
- routers;
- operating system(s) (OS);
- servers;
- firewalls;
- wireless networks;
- cellular networks;
- wired access points; and
- an internet connection.

(Goosen, 2012:29; ISACA, 2012; Wagner, 2008:10)

5.4.4 Step 4: Implement relevant configuration controls over each IT architectural component

Goosen (2012:28) identified the use of access paths and IT architectural components, together with their relevant configuration controls, as a mechanism to identify and mitigate IT risks on an operational level. As discussed by her, the IT architectural components within each possible access path within the design of the technology that is implemented, should be "identified, risk assessed and controlled, by implementing appropriate configuration controls" (Goosen, 2012:45). The configuration controls necessary to manage the risks of identified IT architectural components within an access path were defined as follows:

> *Computer hardware is **'built'** by assembling the various components, enabling them to accept an operating system, and to function in a computer. Computer software is also **'built'**, referring either to the process of creating and converting source code files into stand-alone software artefacts that can be run on a computer, or the result of doing so. This will include the compilation process, where source code files are converted into executable code.*
>
> ***'Set up'** or **'installation'** of a program (including drivers, plugins, etc.) refers to implementing the program on a computer system and ensuring the execution thereof.*

> *The term **'configuration'** refers to the configuration of files, or configuring the initial settings of some computer programs. User applications, server processes and operating system settings are normally configured items.*
>
> *A computer is **'operated'** by overseeing the smooth running of a computer/device and intervening in the process by stopping and restarting services or the whole computer.*
>
> ***'Maintenance'** ensures that software is upgraded and/or computers/devices are repaired so as to ensure the optimum performance and reliability of such devices* (Goosen, 2012:46).

Goosen (2012:47) concludes that implementing these configuration controls correctly will effectively address the IT risks surrounding access paths on an operational level.

As seen in this step, the more thorough the organisation is in listing all IT architectural components present within its design of the established enterprise mobility IT solution, as identified in step 3, the more effective this process will be in addressing security risks on an operational level.

5.4.5 Effective governance of enterprise mobility security risks on an operational level with the use of Goosen's integrated framework

These four steps, together with a basic understanding by business managers of the concepts of access paths, IT architectural components and configuration controls, will provide organisations with a possible solution to decrease the level of miscommunication and misunderstanding between business and IT managers. This will lead to the bridging of the IT gap and the effective governance of enterprise mobility security risks on an operational level.

5.5 Conclusion

In the process of implementing trending technologies such as enterprise mobility, a possible solution to ensure that business and IT is aligned, the IT gap is bridged and security risks are also effectively and efficiently addressed on an operational level, is to communicate technology needs (from the business side) and technology capabilities (from a technical side) on the level of access paths. Access paths, IT

architectural components and configuration controls provide a mechanism for assisting organisations to effectively address security risks resulting from the implemented enterprise mobility IT solution on an operational level.

If this process is implemented correctly, it will assist business and IT managers to effectively address risks by decreasing the level of miscommunication during the planning, implementation and operation of the IT solution for addressing the enterprise mobility needs of an organisation.

CHAPTER 6: LIST OF BEST PRACTICES TO EFFECTIVELY AND EFFICIENTLY GOVERN ENTERPRISE MOBILITY SECURITY RISKS

6.1 Introduction

The effective governance of enterprise mobility security risks on both a strategic and an operational level is investigated in previous chapters. Effective governance of identified enterprise mobility security risks on a strategic level can be achieved by combining and applying the IT governance principles and relevant processes, as indicated by relevant IT governance control documents. Any overlapping or similar processes from the different IT governance control documents listed in Chapter 4 are combined to improve the efficiency of this solution. Effective governance on an operational level can be achieved by applying the integrated framework developed by Goosen (2012:47).

This chapter establishes a list of high-level best practices to provide organisations with an effective and efficient solution to govern security risks that result from enterprise mobility on both a strategic and an operational level. This list of best practices with regards to governance on a strategic level is populated from the relevant processes identified in Chapter 4, and the steps discussed in Chapter 5 will be used as a basis for best practices necessary to govern enterprise mobility security risks on an operational level.

6.2 List of best practices to govern security risks originating from enterprise mobility on a strategic level

A list of best practices was populated by combining similar processes listed in the three IT governance control documents investigated for this study.

6.2.1 Best practice 1: Develop and manage an enterprise mobility security strategy

Organisations should design an enterprise mobility strategy to provide an overarching view of the initiatives and resources that are necessary in the process of migrating their current business and IT environment to the desired

environment, which will entail the establishment of an IT solution that will satisfy their enterprise mobility needs. Organisations should ensure that the IT strategy with regard to the establishment of an IT solution for enterprise mobility is aligned with the business strategy for enterprise mobility and that these strategies (business and IT) properly support and sustain the organisation's strategy and strategic objectives.

The developed enterprise mobility strategy should also include directions for how organisations should continually manage the initiatives and resources of the implemented enterprise mobility strategy.

6.2.2 Best practice 2: Develop an enterprise mobility security policy

Organisations should develop, communicate and implement an enterprise mobility security policy that would assist them in expressing the requirements for the effective governance of security risks related to enterprise mobility. This policy should give detailed guidance on how to implement the organisation's enterprise mobility strategy and assist organisations in achieving their strategic objectives. This policy should address issues such as:

- security risk management;
- architectural security management;
- incident management;
- project management;
- change management;
- back-up procedures, business continuity and disaster recovery;
- awareness and training;
- responsibility and authority; and
- privacy.

6.2.3 Best practice 3: Manage human resources

A structured approach with regard to human resources should be followed to ensure that:

- all employees are aware of the security threats originating from enterprise mobility;
- organisations provide a suitable level of education and training for their employees with regard to the security measures available to mitigate these security threats;
- the roles, responsibilities and accountability with regard to security, as described in the enterprise mobility security policy and in their job descriptions, are explicitly communicated to each employee; and
- personnel in the IT department maintain their skills and competencies at an appropriate level to enable them to effectively and efficiently address security risks originating from enterprise mobility.

6.2.4 Best practice 4: Be informed of the security requirements and ensure continued compliance with these requirements

Organisations should identify and document all information system security requirements and expectations and ensure continued compliance with these requirements. This could include:

- legal requirements;
- regulatory requirements;
- expectations of stakeholders;
- the requirements of the employees; and
- the organisation's needs with regard to security.

Organisations should also be mindful of any changes in these requirements and consider its potential impact on information security.

6.2.5 Best practice 5: Risk management

Organisations should assess and document their risk appetite thresholds and risk tolerance levels. Furthermore organisations should continuously identify

enterprise mobility security risks, evaluate the potential impact of these risks on the organisation, and respond to these threats by managing it, together with the potential impact, in an attempt to ensure that it does not exceed the acceptable risk appetite thresholds and risk tolerance levels. The management of these risks should be in accordance with the developed enterprise mobility security policy.

6.2.6 Best practice 6: Value, protect, track and manage assets

The budget, costs and benefits of assets necessary to establish and maintain enterprise mobility, as well as the necessary assets and resources necessary to secure the enterprise mobility IT solution within an organisation, should be managed. Investments in mobile technology, mobile devices and related IT and other resources and services should be made at costs that are reasonable when compared to their value contribution during the process of effectively and efficiently managing security risks originating from enterprise mobility.

Unauthorised access to critical hardware assets, sensitive information and other IT services and resources should be prevented by implementing and maintaining an enterprise-wide security architecture based on satisfying business objectives and protecting the most critical information assets. Protect the organisation's assets from damage, environment threats, loss or theft. Protect the organisation's assets by following proper disposal practices and procedures.

6.2.7 Best practice 7: Manage service level agreements and suppliers

Organisations should establish and document performance indicators for IT services and service levels, irrespective of whether these services are provided by their own IT department or by third parties. They should monitor and measure the delivery of IT services and service levels against these performance indicators in order to ensure alignment with the organisation's current needs, as well as their future needs and expectations for these IT services and service levels.

If third parties provide these services, the organisation should be scrupulous during the selection of suppliers to secure a supplier that can provide acceptable levels of performance and service delivery at a competitive price. The contracts negotiated with suppliers should document the expected level for the delivery of IT services, and organisations should monitor and measure their performance for effectiveness and compliance with the agreed terms and conditions.

6.2.8 Best practice 8: Design and implement proper change controls and project management practices and procedures

The need for new IT projects to:

- improve the process of managing security risks with regard to enterprise mobility;
- provide for future requirements of processing capacity and other IT resources; and
- avoid future problems with regard to possible system overloads

has to be identified and any new projects with a significant impact on the organisation have to be communicated to the governing body of the organisation.

All IT projects should be initiated, approved, planned, documented, managed, executed, tested and evaluated in accordance with the enterprise mobility security strategy and relevant policies. Implementing sound project management practices and procedures will reduce the risk of unexpected delays and exorbitant costs and will maximise the value delivery of all IT projects.

It is imperative to establish and document the operational requirements of the new IT systems during the planning stage by communicating with stakeholders, the governing body and end-users and to include these requirements in the design of the new IT projects.

A formal policy for the implementation and management of all required changes to existing or new IT projects, should be established. This policy

should include directions for the management and coordination of the configuration, implementation and testing of planned IT projects and emergency changes, such as the emergency addition, modification or removal of planned or existing IT components. Furthermore, it should provide guidance on prioritisation, authorisation, evaluation and reporting to ensure that authorised changes are accurately implemented in a timely manner, with minimal disruption and errors and maximum benefit.

6.2.9 Best practice 9: Ensure sufficient back-up procedures, business continuity and disaster recovery

The developed policies describing back-up procedures, business continuity and disaster recovery plans should be communicated to all employees. Employees should adhere strictly to these prescribed procedures to ensure that downtime, disruption and loss of critical information and other IT resources are kept to a minimum.

Scheduled back-ups of data and software should be performed on a regular basis. The integrity of data and software should be verified before and after back-ups. The ability to restore data and software from back-ups should also be ensured by developing procedures for data restoration and for testing these procedures on a regular basis.

In the event of major incidents, interruptions, disruption and system failures, plans should be in place to ensure:

- continued functioning of critical business operations on the minimum required service levels by means of sufficient flexibility and redundancy solutions for these critical operations;
- continued availability of critical information; and
- effective solutions to minimise the impact on the organisation and its business processes during such incidents.

The continuity and disaster recovery plans should be reviewed and updated on a regular basis to take into account changes in business and IT requirements. Employees should be trained on these plans and the effectiveness of the plans should be tested on a regular basis.

6.2.10 Best practice 10: Monitor, evaluate, assess and improve the mitigating controls implemented within the established enterprise mobility solution

Organisations should continuously monitor, evaluate, assess and improve the established enterprise mobility solution. Responsibility for conducting these functions should be assigned to specific individuals or departments.

Internal and external, independent information system audits should be conducted on a regular basis to:

- evaluate the effectiveness and efficiency of the risk management procedures implemented in these information systems;
- evaluated and assess the impact of all new IT projects and changes to ensure that the implementation thereof result in effective and efficient management of security risks;
- identify critical assets, IT operations and corporate information that should be managed specifically as they may result in serious security breaches;
- identify, evaluate and assess security threats, vulnerabilities and risks resulting from the identified critical assets, IT operations and corporate information; and
- evaluate and assess performance, conformance, the system of internal control and compliance with external and internal security requirements and regulations.

Security weaknesses and problems should be identified through this system of monitoring, evaluating and assessing to address and improve the risk management process for enterprise mobility security risks. Any changes in business requirements and identified incidents, events, problems, weaknesses or threats should also be noted and addressed.

6.2.11 Best practice 11: Report to stakeholders

Organisations should report results of their monitoring, evaluation, assessment and improvement actions to stakeholders in an accurate, effective and timely manner to ensure transparency.

Appendix C lists the best practices populated in this study, as discussed above, together with references to the relevant processes listed in the various IT governance control documents to provide organisations with more detailed assistance on how to practically implement each best practice.

6.3 Best practices to govern security risks originating from enterprise mobility on an operational level

The IT control documents do provide theoretical guidance on governing enterprise mobility security risks on an operational level. This guidance, in the form of implementable processes, is listed in Appendix D.

However, the weakness of the theoretical guidance provided by IT governance control documents is the resulting IT gap that will lead to enterprise mobility security risks being governed in an ineffective manner.

Goosen's developed integrated framework (2012) provides guidance to govern these risks in a practical manner that will, if implemented effectively, result in organisations bridging the IT gap and effectively governing enterprise mobility security risks on an operational level. She suggested four steps which have been used by this study as a basis for the formulation of four best practices providing guidance to effectively govern enterprise mobility security risks on an operational level.

6.3.1 Best practice 12: Implement the applicable control techniques

The actual controls of the relevant processes should be implemented during this step.

6.3.2 Best practice 13: Determine the different access paths

As per Chapter 5, section 5.4.2, ISACA identified four possible access paths within the established IT solution necessary to satisfy the organisation's enterprise mobility needs. However, each organisation will have a unique enterprise mobility solution. The organisation should identify all possible access paths within their specific established IT solution and manage the resulting risks of every identified or activated access path.

6.3.3 Best practice 14: Identify the IT architecture components which form the identified access paths

Chapter 5, section 5.4.3, includes a list of examples of IT architectural components that can possibly be included in forming an activated access path as identified by the organisation. This list should not be seen as an extensive list of all IT component types. In 2008, Pelino, Daley and Muhlhausen (cited in Wagner, 2008:10) noted that, when considering the possible adoption or implementation of trending technologies (such as enterprise mobility), the multitude of IT components and options available can lead to confusion and risks. Enterprise mobility network designs will be tailored to satisfy the unique requirements and situation of the specific organisation requiring an IT solution for their enterprise mobility needs. This uniquely tailored solution may exclude some of the listed components and include components not listed. Organisations should therefore invest time to ensure the enterprise mobility solution developed and implemented is:

- aligned with all of their business imperatives;
- thorough in its design to include a list of all IT components present within this solution; and
- will satisfy the needs of all the users of the enterprise mobility solution.

6.3.4 Best practice 15: Implement relevant configuration controls

Managing the risks of IT architectural components within the activated or identified access paths, as discussed in Chapter 5, section 5.4.4, can only be applied in an effective manner if:

- all of the possible access paths; and
- all of the IT architectural components within the design of the enterprise mobility solution have been identified and listed.

With the help of the configuration controls necessary for each IT architectural component identified, IT personnel can then assess what the possible risks are and how to effectively address these identified risks.

In Table 6.1, a short example illustrates how to practically implement this best practice. This example apply configuration controls to identify and effectively govern, on an operational level, security risks resulting from IT architectural components within the activated access paths of the established IT solution necessary to satisfy an organisation's enterprise mobility needs.

Table 6.1: An illustrative example of using configuration controls to identify security risks of IT architectural components that form part of activated access paths

Configuration control (Chapter 5, section 5.4.4)	IT architectural component (Chapter 5, section 5.4.3)		
	Applications (apps) on mobile device – developed in-house	**Applications (apps) on mobile device** – purchased from an app store	**Mobile device**
BUILD	✓ Apps will be developed in-house according to specifications and needs of the employees and organisation	**x** Purchased apps will not be developed in-house and will be used, without modifications, by employees	**x** The mobile device will be purchased, either by the organisation or by the employee (BYOD)
SETUP	✓ Apps should be installed on mobile devices	✓ Apps should be installed on mobile devices	**x** The OS will already be installed on the mobile device
CONFIGURE	✓ Security controls, such as access permission to information on the mobile device, etc. should be configured correctly to minimise unauthorised activity	✓ Security controls, such as access permission to information on the mobile device, etc. should be configured correctly to minimise unauthorised activity	✓ Configuring controls on the mobile device, such as pin code-enabled access control, remote SIM card lock capabilities, remote shutdown/wipe capabilities, and cell-based tracking and locating of the mobile device can enhance security features and lower security risks
MAINTAIN	✓ Apps should be updated regularly to include the evolving needs of the organisation and the users	✓ Apps usually require regular updates to fix bugs and improve usability	✓ Mobile devices are evolving over time to include the newest technology inventions and security features. To make use of such improvements and increased security capabilities, these devices should be updated regularly

Configuration control (Chapter 5, section 5.4.4)	IT architectural component (Chapter 5, section 5.4.3)		
	Applications (apps) on mobile device – developed in-house	**Applications (apps) on mobile device** – purchased from an app store	**Mobile device**
OPERATE	✓ Apps installed on the mobile device will be used by employees for business purposes	✓ Apps installed on the mobile device will be used by employees for personal and business purposes and can result in serious security threats	✓ Operating the mobile device without the necessary security features enabled and properly implemented can result in serious security threats

Key

x	The configuration control is not applicable.
✓	The configuration control is applicable and possible security risks, as a result of this configuration control, should be identified and governed.

6.4 Conclusion

The implementation of the 15 best practices listed in this chapter will result in an effective and efficient solution for governing enterprise mobility security risks.

CHAPTER 7: SUMMARY AND CONCLUSION

Various significant security risks originate from IT solutions that organisations have to establish in an effort to satisfy their enterprise mobility needs and requirements resulting from the societal expectations that emerge as a result of the recent consumerisation of mobile technology and mobile devices.

The purpose of this study was to identify significant security risks originating from enterprise mobility and to find a solution to effectively and efficiently govern these risks on a strategic and operational level in an attempt to minimise their impact on the availability, integrity and confidentiality of corporate information.

The use of a combination of IT governance control documents, principles and processes provide organisations with an effective solution to govern enterprise mobility security risks on a strategic level. This can, however, result in an inefficient and costly process. To increase the efficiency of this governance process, but still retain its effectiveness, a list of best practices has been developed by combining the processes from the selected relevant IT governance control documents relevant in the process of governing enterprise mobility security risks.

Due to the lack of practical guidance provided by the principles and processes listed in IT governance control documents, there is a lack of available guidance for organisations to govern enterprise mobility security risks on an operational level. Goosen's developed framework (2012) provides guidance on governing IT risks on an operational level.

In conclusion, implementing the developed best practices with proper care will result in an effective, efficient and cost effective solution that organisations can apply to govern the identified enterprise mobility security risks on a strategic and an operational level.

This study focused on the development of a list of best practices to assist organisations in governing enterprise mobility security risks effectively and efficiently on the strategic and the operational level. Areas for possible further research include:

- a case study on the implementation of these best practices by a South African company in an effort to evaluate and assess its usefulness and practicality;
- a more in-depth study of the security risks originating on the operational level as a result of activated access paths and IT architectural components; and
- assessing the effect of the newly enacted Protection of Personal Information (POPI) bill on the governance of enterprise mobility security risks.

LIST OF REFERENCES

Al-Debei, M.M. & Avison, D. 2008. Defining the business model in the new World of Digital, in *Proceedings of the Fourteenth Americas Conference on Information Systems (AMCIS)*. Toronto, ON: Canada, August 14-17, 2008, pp. 1-11.

Alt, R. & Zimmermann, H.D. 2001. Introduction to special section - Business models. *Electronic Markets*, 11(1), 3-9.

Apple. 2008. *iPhone App Store Downloads Top 10 Million in First Weekend* [Online]. Available: http://www.apple.com/pr/library/2008/07/14iPhone-App-Store-Downloads-Top-10-Million-in-First-Weekend.html [2013, August 1].

Apple. 2012. *Apple's App Store Downloads Top 25 Billion* [Online]. Available: http://www.apple.com/pr/library/2012/03/05Apples-App-Store-Downloads-Top-25-Billion.html [2013, August 1].

Apple. 2013a. *Apple's App Store Marks Historic 50 Billionth Download* [Online]. Available: http://www.apple.com/pr/library/2013/05/16Apples-App-Store-Marks-Historic-50-Billionth-Download.html [2013, August 1].

Apple. 2013b. *Apple Unveils iOS 7* [Online]. Available: http://www.apple.com/pr/library/2013/06/10Apple-Unveils-iOS-7.html [2013, August 1].

Arraj, V. 2010. *ITIL: The basics* [Online]. Available: http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf [2013, June 11].

Azim, R. & Hassan, A. 2013. Impact analysis of wireless and mobile technology on business management strategies. *Information and Knowledge Management,* 3(2), 141-150.

Boshoff, W.H. 1990. A path context model for computer security phenomena in potentially non-secure environments. Unpublished doctoral dissertation. Johannesburg: University of Johannesburg (previously: Rand Afrikaans University).

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

Burkhart, T., Krumeich, J., Werth, D., & Loos, P. 2011. Analyzing the business model concept – A comprehensive classification of literature. Unpublished paper delivered at the Thirty-Second International Conference on Information Systems. Shanghai, China. 5 December.

Cartlidge, A., Hanna, A., Rudd, C., Macfarlane, I., Windebank, J. & Rance, S. 2007. *An introductory overview of ITIL V3. The UK chapter of the itSMF* [Online]. Available: http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf [2013, June 25].

Chan, Y.E., & Reich, B.H. 2007. IT alignment: What have we learned? *Journal of Information Technology,* 22(4), 297-315.

Chen, L. 2010. Business–IT alignment maturity of companies in China. *Information & Management,* 47(1), 9-16.

Cuddy, C. 2009. Mobile computing. *Journal of Electronic Resources in Medical Libraries*, 6(1), 64-68.

Cukier, W., Shortt, D., & Devine, I. 2002. Gender and information technology: Implications of definitions. *ACM SIGCSE Bulletin*, *34*(4), 142-148.

Cuong, N.H. 2007. The need for legislation like Sarbanes-Oxley for IT governance: An Australian perspective. *Information Systems Control Journal*, 3, 1-5.

Deloitte. 2013. *Tech Trends 2013, Elements of postdigital* [Online]. Available: http://www.deloitte.com/view/en_ZA/za/services/consulting/technology/tech-trends-2013/index.htm [2013, May 21].

Elmorshidy, A. 2013. Aligning IT with business objectives: A critical survival and success factor in today's business. *Journal of Applied Business Research (JABR),* 29(3), 819-828.

England, R. 2011. *Review of recent ITIL studies* [Online]. Available: http://www.best-management-practice.com/gempdf/Review_ITIL_Studies_White_Paper_Nov11.pdf [2013, June 26].

Gartner's IT Glossary. 2013. [Online]. Available: http://www.gartner.com/it-glossary/m-business-mobile-business [2013, August 1].

Gerke, L. & Ridley, G. 2006. Towards an abbreviated COBIT framework for use in an Australian state public sector. Unpublished paper presented at the 17th Australasian Conference on Information Systems. 6-8 December. Adelaide, South Australia.

Gerow, J. 2013. Research-in-progress: Understanding the relationship between IT-business strategic alignment and firm performance, in *Proceedings of the Southern Association for Information Systems Conference.* Savannah: SAISC, pp. 36-40.

Ghoda, A. 2009. Mobile applications and Silverlight, in A. Ghoda, *Pro Silverlight for the Enterprise,* pp. 249-266, New York: Apress.

Ghosh, A., Gajar, P.K. & Rai, S. 2013. Bring your own device (BYOD): Security risks and mitigating strategies. *Journal of Global Research in Computer Science,* 4(4), 62-70.

Global Stats. 2013. [Online]. Available: http://gs.statcounter.com/#mobile_vs_desktop-ww-monthly-201207-201307 [2013, August 5].

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

Goosen, R. & Rudman, R. 2013. An integrated framework to implement IT governance principles at a strategic and operational level for medium- to large-sized South African businesses. *International Business & Economics Research Journal (IBER),* 12(7), 835-854.

Hornbill Systems. 2009. *ITIL: State of the Nation survey findings. A research report sponsored by Hornbill Systems* [Online]. Available: http://www.hornbill.com/campaigns/itil-state/_files/ITIL-State-of-the-Nation-Survey.pdf [2013, June 26].

IBM. 2012. *The business-IT gap: A key challenge* [Online]. Available: http://www.almaden.ibm.com/coevolution/pdf/mcdavid.pdf [2013, August 28].

Institute of Directors Southern Africa. 2009. *King Report on corporate governance for South Africa (King III)* [Online]. Available: http://www.iodsa.co.za [2013, June 12].

International Telecommunication Union. 2013a. *The world in 2013, ICT facts and figures* [Online]. Available: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf [2013, August 1].

International Telecommunication Union. 2013b. *Recommendation ITU-T X.1054 (2013) | ISO/IEC 27014:2013 Information technology - Security techniques - Governance of information security* [Online] Available: http://www.itu.int/rec/T-REC-X.1054-201209-I/en [2013, June 28].

ISACA. 2010. *White paper on Securing Mobile Devices* [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx [2013, May 16].

ISACA. 2012. *Securing Mobile Devices Using COBIT 5 for Information Security* [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices-Using-COBIT-5-for-Information-Security.aspx [2013, June 21].

ISO27001 Security. 2013. [Online]. Available: http://www.iso27001security.com/index.html [2013, June 26].

ISO/IEC. 2012. *ISO/IEC 27000:2012 Information technology – Security techniques – Information security management systems – Overview and vocabulary* [Online]. Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html [2013, June 27].

IT Governance Institute. 2003. *Board briefing on IT governance*, 2nd edition [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx [2013, June 12].

IT Governance Institute. 2008. *Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit* [Online]. Available: http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf [2013, June 12].

IT Governance Institute. 2012. *COBIT 5* [Online]. Available: http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx [2012, October 19].

Itinfo. s.a. *Information Technology Infrastructure Library (ITIL) Guide* [Online]. Available: http://www.itinfo.am/eng/information-technology-infrastructure-library-guide/ [2013, June 26].

Kearns, G.S. & Sabherwal, R. 2007. Antecedents and consequences of information systems planning integration. *IEEE Transactions on Engineering Management*, 54(4), 628-643.

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

Kneller, M. 2010. *Executive briefing: The benefits of ITIL* [Online]. Available: http://certifications.edu.in/wp-content/uploads/Benefits-of-ITIL.pdf [2013, June 11].

Kruger, W. & Rudman, R. 2013. Strategic alignment of application software packages and business processes using PRINCE2. *International Business & Economic Research Journal,* 12(10), 1239-1260.

Liu, Q. & Ridley, G. 2005. IT control in the Australian public sector: An international comparison. Unpublished paper delivered at the 13th European Conference of Information Systems, 26-28 May, Regensburg, Germany.

Lucio-Nieto, T., Colomo-Palacios, R., Soto-Acosta, P., Popa, S. & Amescua-Seco, A. 2012. Implementing an IT service information management framework: The case of COTEMAR. *International Journal of Information Management,* 32, 589-594.

Luftman, J. & Ben-Zvi, T. 2010a. Key issues for IT executives 2009: Difficult economy's impact on IT. *MIS Quarterly Executive,* 9(1), 203-213.

Luftman, J. & Ben-Zvi, T. 2010b. Key issues for IT executives 2010: Judicious IT investments continue post-recession. *MIS Quarterly Executive,* 9(4), 263-273.

Luftman, J., & Ben-Zvi, T. 2011. Key issues for IT executives 2011: Cautious optimism in uncertain economic times. *MIS Quarterly Executive*,10(4), 203-212.

Luftman, J., & Brier, T. 1999. Achieving and sustaining business-IT alignment. *California Management Review,* 42(1), 109-122.

Luftman, J., Papp, R., & Brier, T. 1999. Enablers and inhibitors of business-IT alignment. *Communications of the AIS,* 1(3), 1-30.

Meeker, M. & Wu, L. 2012. *2012 Internet Trends (Update)* [Online]. http://www.kpcb.com/insights/2012-internet-trends-update [2013, August 1].

Meeker, M. & Wu, L. 2013. *2013 Internet Trends* [Online]. http://www.kpcb.com/insights/2013-internet-trends [2013, August 1].

Miller, A. 2004. PDA security concerns. *Network Security*, 2004(7), 8-10.

Milligan, P.M. & Hutcheson, D. 2007. Business Risks and Security Assessment for Mobile Devices, in *Proceedings of the 8th WSEAS Int. Conference on Mathematics and Computers in Business and Economics.* Vancouver: World Scientific and Engineering Academy and Society, pp. 189-193.

Naidoo, R. 2002. *Corporate governance: an essential guide for South African companies*. Cape Town: Juta.

Năstase, P., Năstase, F. & Ionescu, C. 2009. Challenges generated by the implementation of the IT standards CobiT 4.1, ITIL v3 and ISO/IEC 27002 in enterprises. *Economic Computation & Economic Cybernetics Studies & Research*, 43(3), 5-20.

Nicho, M., Fakhry, H. & Haiber, C. 2011. An integrated security governance framework for effective PCI DSS implementation. *International Journal of Information Security and Privacy (IJISP),* 5(3), 50-67.

OWASP. 2011. *OWASP Top 10 Mobile Risks* [Online]. Available: https://www.owasp.org/index.php/Mobile#tab=Top_Ten_Mobile_Risks [2013, May 21].

Pastuszak, J., Czarnecki, A. & Orłowski, C. 2012. Ontologically aided rule model for the implementation of ITIL processes, in M. Graña, C. Toro, J. Posada, R.J. Howlett & L.C, Jain (eds.). *Advances in knowledge-based and intelligent information and engineering systems,* pp. 1428-1438. Poland: IOS Press.

Pettey, C. & Van der Meulen, R. 2010. *Gartner Highlights Key Predictions for IT Organizations and Users in 2010 and Beyond* [Online]. Available: http://www.gartner.com/newsroom/id/1278413 [2013, August 1].

Pettey, C. & Van der Meulen, R. 2012. *Gartner Says the Personal Cloud Will Replace the Personal Computer as the Center of Users' Digital Lives by 2014* [Online]. Available: http://www.gartner.com/newsroom/id/1947315 [2013, May 21].

Porter, M.E. 1998. *Competitive strategy: Techniques for analyzing industries and competitors*. New York: Free press.

Portio Research. 2013. *Portio Research Mobile Factbook 2013* [Online]. Available: http://www.portioresearch.com/media/3986/Portio%20Research%20Mobile%20Factbook%202013.pdf [2013, August 1].

Ramos, M.J. 2006. *How to comply with Sarbanes-Oxley section 404: Assessing the effectiveness of Internal Control*. 2nd edition. Hoboken, NJ: Wiley.

Robinson, N. 2005. IT excellence starts with governance. *Journal of Investment Compliance,* 6(3), 45-49.

Robles, R.J., Choi, M., Cho, S., Lee, Y. & Kim, T. 2009. SOX and its effects on IT security governance. *International Journal of Smart Home*, 3(1), 81-87.

Ross, R.S. 2011. *NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View* [Online]. Available: http://www.nist.gov/manuscript-publication-search.cfm?pub_id=908030 [2013, June 26].

Rowsell-Jones, A., Jones, N. & Basso, M. 2011. *Executive Summary: Capturing Business Value From Mass-Market Mobile Technologies* [Online]. Available: http://www.gartner.com/id=1779628 [2013, August 1].

Rudman, R.J. 2008. IT governance: A new era. *Accountancy SA,* March, 12-14.

Rudman, R.J. 2010. Framework to identify and manage risks in web 2.0 applications. *African Journal of Business Management,* 4(13), 3251-3264.

Sallé, M. 2004. *IT Service Management and IT Governance: Review, comparative analysis and their impact on utility computing* [Online]. Available: https://www.hpl.hp.com/techreports/2004/HPL-2004-98.pdf [2013, June 11].

Sauer, C. & Yetton, P.W. 1997. The right stuff – An introduction to new thinking about management, in C. Sauer & P.W. Yetton (eds.), *Steps to the future: Fresh thinking on the management of IT-based organizational transformation*, pp. 1-21. San Francisco: Jossey-Bass.

Schweizer, L. 2005. Concept and evolution of business models. *Journal of General Management*, *31*(2), 37-56.

Shivashankarappa, A.N., Smalov, L., Dharmalingam, R. & Anbazhagan, N. 2012. Implementing IT governance using COBIT: A case study focusing on critical success factors, in *World Congress on Internet Security 2012 (WorldCIS-2012).* Guelph: IEEE. pp. 144-149.

Sidhu, B.S. 2013. Demystifying business IT alignment. *International Journal of Science & Technology*, 3(1), 20-26.

Simonsson, M. & Johnson, P. 2006. Assessment of IT governance - A prioritization of Cobit, in *Proceedings of the Conference on Systems Engineering Research*. Los Angeles: INCOSE. pp. 1-10.

Soomro, T.R. & Hesson, M. 2012. Supporting best practices and standards for Information Technology infrastructure library. *Journal of Computer Science*, 8(2), 272-276.

Souppaya, M. & Scarfone, K. 2013. *NIST Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise* [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf [2013, Aug 6].

Štemberger, M.I., Manfreda, A. & Kovačič, A. 2011. Achieving top management support with business knowledge and role of IT/IS personnel. *International Journal of Information Management,* 31(5), 428-436.

Symantec. 2012. *2012 State of Mobility Survey* [Online]. Available: http://www.symantec.com/en/za/content/en/us/about/media/pdfs/b-state_of_mobility_survey_2012.en-us.pdf [2013, August 5].

Trendowicz, A., Heidrich, J. & Shintani, K. 2011. Aligning software projects with business objectives, in *Software Measurement, 2011 Joint Conference of the 21st International Workshop on Software Measurement and the 6th International Conference on Software Process and Product Measurement (IWSM-MENSURA)*. Nara, Japan: IEEE. pp 142-150.

United States Census Bureau. 2013. [Online]. Available: http://www.census.gov/popclock/ [2013, August 5].

Van der Meulen, R. 2012. *Gartner Says 821 Million Smart Devices Will Be Purchased Worldwide in 2012; Sales to Rise to 1.2 Billion in 2013* [Online]. Available: http://www.gartner.com/newsroom/id/2227215 [2013, May 21].

Van Grembergen, W. & De Haes, S. 2009. *Enterprise governance of information technology: Achieving strategic alignment and value.* New York, NY: Springer.

Wagner, E.D. 2008. Realizing the promises of mobile learning. *Journal of Computing in Higher Education,* 20(2), 4-14.

Webb, P., Pollard, C. & Ridley, G. 2006. Attempting to define IT governance: Wisdom or folly?, in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS).* Kauia, Hawaii: IEEE. pp. 194-204.

Weill, P. & Woodham, R. 2002. *Don't just lead, govern: Implementing effective IT governance (MIT Sloan School of Management Working Paper 4237-02)* [Online]. Available: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=317319 [2013, June 26].

Welling, G.S. 1999. Designing adaptive environment-aware applications for mobile computing. Unpublished doctoral dissertation. Rutgers, The State University of New Jersey.

Worldometers. 2013. [Online]. Available: http://www.worldometers.info/world-population/#pastfuture [2013, August 5].

Zissis, D. & Lekkas, D. 2012. Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592.

Appendix A: COBIT 5 processes for the governance of security risks relating to enterprise mobility

COBIT 5 domain	COBIT 5 process	Description
Evaluate, direct and monitor (EDM)	EDM01 Ensure governance framework setting and maintenance	Develop overarching IT governance structures, principles, processes and practices in line with the business strategy; assign responsibility and authority; and apply them to mobile devices and their security.
	EDM02 Ensure benefits delivery	Apply cost-benefit analysis to the risk-weighted options for mobile device security governance.
	EDM03 Ensure risk optimisation	Ensure that the organisation's risk appetite and tolerance are understood, articulated and communicated, and that risk to organisation value related to the use of IT is identified and managed.
	EDM04 Ensure resource optimisation	Ensure that adequate and sufficient IT-related capabilities (people, process and technology) are available to support business objectives effectively at optimal cost.
	EDM05 Ensure stakeholder transparency	Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions.
Align, plan and organise (APO)	APO01 Manage the IT Management Framework	Clarify and maintain the governance of enterprise IT mission and vision. Implement and maintain mechanisms and authorities to manage information and the use of IT in the organisation in support of governance objectives in line with guiding principles and policies.
	APO02 Manage Strategy	Provide a holistic view of the current business and IT environment, the future direction, and the initiatives required to migrate to the desired future environment. Leverage enterprise architecture building blocks and components, including externally provided services and related capabilities to enable nimble, reliable and efficient response to strategic objectives.

COBIT 5 domain	COBIT 5 process	Description
Align, plan and organise (APO)	APO04 Manage innovation	Maintain awareness of information technology and related service trends; identify innovation opportunities; and plan how to benefit from innovation in relation to business needs. Analyse what opportunities for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.
	APO05 Manage Portfolio	Determine the availability and sources of funds for investment in mobile technology and its security measures.
	APO06 Manage Budget and Costs	Manage the IT-related financial activities in the business and IT functions, covering budget, cost and benefit management, and prioritisation of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the organisation. Consult stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed.
	APO07 Manage Human Resources	Maintain the skills and competencies of personnel.
	APO09 Manage Service Agreements	Align IT-enabled services and service levels with business needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of IT services, service levels and performance indicators.
	APO10 Manage Suppliers	Manage IT-related services provided by all types of suppliers to meet business requirements, including the selection of suppliers, management of relationships, management of contracts, and reviewing and monitoring of supplier performance for effectiveness and compliance.
	APO12 Manage risk	Continually identify, assess and reduce IT-related risk within levels of tolerance set by the organisation's executive management team.

COBIT 5 domain	COBIT 5 process	Description
Align, plan and organise (APO)	APO13 Manage security	Define, operate and monitor a system for information security management.
Build, acquire and implement (BAI)	BAI01 Manage Programmes and Projects	Manage programme and project risk relating to mobile device related projects.
	BAI02 Manage Requirements Definition	Identify solutions and analyse requirements before acquisition or creation to ensure that they are in line with business strategic requirements covering business processes, applications, information/data, infrastructure and services. Co-ordinate with affected stakeholders the review of feasible options including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.
	BAI03 Manage Solutions Identification and Build	Establish and maintain identified solutions in line with business requirements covering design, development, procurement/sourcing and partnering with suppliers/vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.
	BAI04 Manage Availability and Capacity	Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.
	BAI06 Manage Changes	Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.

COBIT 5 domain	COBIT 5 process	Description
Build, acquire and implement (BAI)	BAI09 Manage Assets	Manage IT assets, such as mobile devices, through their life cycle to make sure that their use delivers value and the necessary security measures at optimal cost, they remain operational (fit for purpose), they are accounted for and physically protected, and those assets that are critical to support service capability are reliable and available.
	BAI10 Manage Configuration	Define and maintain descriptions and relationships between key resources and capabilities required to deliver IT-enabled services, including collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.
Deliver, service and support (DSS)	DSS02 Manage Service Requests and Incidents	Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.
	DSS03 Manage Problems	Identify and classify problems and their root causes and provide timely resolution to prevent recurring incidents. Provide recommendations for improvements.
	DSS04 Manage Continuity	Establish and maintain a plan to enable the business and IT to respond to incidents and disruptions in order to continue operation of critical business processes and required IT services and maintain availability of information at a level acceptable to the organisation.
	DSS05 Manage Security Services	Protect organisation information to maintain the level of information security risk acceptable to the organisation in accordance with the security policy. Establish and maintain information security roles and access privileges and perform security monitoring.

COBIT 5 domain	COBIT 5 process	Description
Monitor, evaluate and assess (MEA)	MEA01 Monitor, Evaluate and Assess Performance and Conformance	Collect, validate and evaluate business, IT and process goals and metrics. Monitor that processes are performing against agreed-on performance and conformance goals and metrics and provide reporting that is systematic and timely.
	MEA02 Monitor, Evaluate and Assess the System of Internal Control	Continuously monitor and evaluate the control and security environment, including self-assessments and independent assurance reviews. Enable management to identify control and security deficiencies and inefficiencies and to initiate improvement actions. Plan, organise and maintain standards for internal control and security assessments.
	MEA03 Monitor, Evaluate and Assess Compliance with External Requirements	Evaluate that IT processes and IT-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with, and integrate IT compliance with overall enterprise compliance.

(ISACA, 2012; IT Governance Institute, 2012)

Appendix B: ITIL processes for the governance of security risks relating to enterprise mobility

ITIL 2011 Service Life-cycle Stage	ITIL 2011 process	Process objective
ITIL Service Strategy	Strategy Management for IT Services	To assess the service provider's offerings, capabilities, competitors, as well as current and potential market spaces in order to develop a strategy to serve customers. Once the strategy has been defined, Strategy Management for IT Services is also responsible for ensuring the implementation of the strategy.
	Service Portfolio Management	To manage the service portfolio. Service Portfolio Management ensures that the service provider has the right mix of services to meet required business outcomes at an appropriate level of investment.
	Financial Management for IT Services	To manage the service provider's budgeting, accounting and charging requirements.
	Demand Management	To understand, anticipate and influence customer demand for services. Demand Management works with Capacity Management to ensure that the service provider has sufficient capacity to meet the required demand.
	Business Relationship Management	To maintain a positive relationship with customers. Business Relationship Management identifies the needs of existing and potential customers and ensures that appropriate services are developed to meet those needs.
ITIL Service Design	Service Catalogue Management	To ensure that a Service Catalogue is produced and maintained, containing accurate information on all operational services and those being prepared to be run operationally. Service Catalogue Management provides vital information for all other Service Management processes: Service details, current status and the services' interdependencies.

ITIL 2011 Service Lifecycle Stage	ITIL 2011 process	Process objective
ITIL Service Design	Service Level Management	To negotiate Service Level Agreements with the customers and to design services in accordance with the agreed service level targets. Service Level Management is also responsible for ensuring that all Operational Level Agreements and Underpinning Contracts are appropriate, and to monitor and report on service levels.
	Supplier Management	To ensure that all contracts with suppliers support the needs of the organisation, and that all suppliers meet their contractual commitments.
	Capacity Management	To ensure that the capacity of IT services and the IT infrastructure is able to deliver the agreed service level targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT service, and plans for short, medium and long term business requirements.
	Availability Management	To define, analyse, plan, measure and improve all aspects of the availability of IT services. Availability Management is responsible for ensuring that all IT infrastructure, processes, tools, roles, etc. are appropriate for the agreed availability targets.
	IT Service Continuity Management	To manage risks that could seriously impact IT services. ITSCM ensures that the IT service provider can always provide minimum agreed Service Levels, by reducing the risk from disaster events to an acceptable level and planning for the recovery of IT services. ITSCM should be designed to support Business Continuity Management.
	Information Security Management	To ensure the confidentiality, integrity and availability of an organisation's information, data and IT services. Information Security Management usually forms part of an organisational approach to security management which has a wider scope than the IT Service Provider.

ITIL 2011 Service Lifecycle Stage	ITIL 2011 process	Process objective
ITIL Service Design	Design Coordination	To coordinate all service design activities, processes and resources. Design coordination ensures the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information and metrics.
ITIL Service Transition	Project Management (Transition Planning and Support)	To plan and coordinate the resources to deploy a major release within the predicted cost, time and quality estimates.
	Change Management	To control the life cycle of all changes. The primary objective of change management is to enable beneficial changes to be made, with minimum disruption to IT services.
	Service Asset and Configuration Management	To maintain information about configuration items required to deliver an IT service, including their relationships.
	Release and Deployment Management	To plan, schedule and control the movement of releases to test and lived environments. The primary goal of Release Management is to ensure that the integrity of the lived environment is protected and that the correct components are released.
	Knowledge Management	To gather, analyse, store and share knowledge and information within an organisation. The primary purpose of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge.
	Service Validation and Testing	To ensure that deployed releases and the resulting services meet customer expectations, and to verify that IT operations are able to support the new service.
	Change Evaluation	To assess major changes, like the introduction of a new service or a substantial change to an existing service, before those changes are allowed to proceed to the next phase in their life cycle.

ITIL 2011 Service Lifecycle Stage	ITIL 2011 process	Process objective
ITIL Service Operation	Event Management	To make sure configuration items and services are constantly monitored, and to filter and categorise events in order to decide on appropriate actions.
	Incident Management	To manage the life cycle of all incidents. The primary objective of Incident Management is to return the IT service to users as quickly as possible.
	Problem Management	To manage the life cycle of all problems. The primary objectives of Problem Management are to prevent incidents from happening, and to minimise the impact of incidents that cannot be prevented. Proactive Problem Management analyses incident records, and utilise data collected by other IT service management processes to identify trends or significant problems.
	Request Fulfilment	To fulfil service requests, which in most cases are minor (standard) changes (e.g. requests to change a password) or requests for information.
	Access Management	To grant authorised users the right to use a service, while preventing access to non-authorised users. The Access Management processes essentially execute policies defined in Information Security Management. Access Management is sometimes also referred to as Rights Management or Identity Management.
Continual Service Improvement	Seven-step improvement	Improvement initiatives typically follow a seven-step process: 1. Identify the strategy for improvement 2. Define what will be measured 3. Gather the data 4. Process the data 5. Analyse the information and data 6. Present and use the information 7. Implement improvement

(Cartlidge *et al.*, 2007)

Appendix C: Best practices mapped with detailed processes (strategic level)

Best practice 1: Develop and manage an enterprise mobility security strategy

IT Control document	Relevant processes
COBIT 5	• APO02 Manage Strategy
ITIL	All processes listed in ITIL's *Service Strategy* publication: • Strategy Management for IT Services • Service Portfolio Management • Financial Management for IT Services • Demand Management • Business Relationship Management
ISO27014	• Ensure that business initiatives take into account information security issues • Ensure that information security adequately supports and sustains the business objectives • Align information security objectives with business objectives

(Cartlidge *et al.*, 2007; IT Governance Institute, 2012; International Telecommunication Union, 2013b)

Best practice 2: Develop an enterprise mobility security policy

IT control document	Relevant processes
COBIT 5	• EDM01 Ensure governance framework setting and maintenance • APO001 Manage the IT Management Framework
ISO27002	• Establish a security policy
ISO27014	• Develop, approve and implement information security strategy and policy

(IT Governance Institute, 2012; International Telecommunication Union, 2013b; ISO27001 Security, 2013)

Best practice 3: Manage human resources

IT control document	Relevant processes
COBIT 5	• APO07 Manage Human Resources
ISO27002	• Emphasise security prior to employment • Emphasise security during employment • Emphasise security at termination of employment • Encourage good access practices • Establish an internal security organisation • Establish responsibility for the organisation's mobile devices and other IT assets necessary to secure the organisation's information • Establish procedures and responsibilities
ISO27014	• Promote a positive information security culture

(IT Governance Institute, 2012; International Telecommunication Union, 2013b; ISO27001 Security, 2013)

Best practice 4: Be conscious and informed of the security requirements and ensure continued compliance with these requirements

IT control document	Relevant processes
COBIT 5	• BAI02 Manage Requirements Definition
ISO27002	• Identify information system security requirements • Comply with legal requirements with regards to confidentiality of information
ISO27014	• Consider the changing business, legal and regulatory environment and their potential impact on information risk and information security • Recognise information concerning regulatory obligations, stakeholders' expectations and business needs with regard to information security

(IT Governance Institute, 2012; International Telecommunication Union, 2013b; ISO27001 Security, 2013)

Best practice 5: Risk management

IT control document	Relevant processes
COBIT 5	• EDM03 Ensure Risk Optimisation • APO12 Manage Risk
ISO27002	• Use an information classification system
ISO27014	• Determine the organisation's risk appetite

(IT Governance Institute, 2012; International Telecommunication Union, 2013b; ISO27001 Security, 2013)

Best practice 6: Value, protect, track and manage assets

IT control document	Relevant processes
COBIT 5	• EDM02 Ensure benefits delivery • EDM03 Ensure risk optimisation • EDM04 Ensure resource optimisation • APO05 Manage Portfolio • APO06 Manage Budget and Costs • BAI09 Manage Assets
ITIL	• Service Portfolio Management • Financial Management for IT Services • Capacity management
ISO27002	• Use secure areas to protect facilities • Protect the organisation's mobile devices and other IT resources
ISO27014	• Allocate adequate investment and resources

(Cartlidge *et al.*, 2007; IT Governance Institute, 2012; International Telecommunication Union, 2013b; ISO27001 Security, 2013)

Best practice 7: Manage service level agreements and suppliers

IT control document	Relevant processes
COBIT 5	• APO09 Manage Service Agreements • APO10 Manage Suppliers
ITIL	• Service Catalogue Management • Service Level Management • Supplier Management

(Cartlidge *et al.*, 2007; IT Governance Institute, 2012)

Best practice 8: Design and implement proper change controls and project management practices and procedures

IT control document	Relevant processes
COBIT 5	• BAI01 Manage Programmes and Projects • BAI03 Manage Solutions Identification and Build • BAI06 Manage Changes
ITIL	All processes listed in ITIL's *Service Transition* publication: • Project Management (Transition Planning and Support) • Change Management • Service Asset and Configuration Management • Release and Deployment Management • Knowledge Management • Service Validation and Testing • Change Evaluation
ISO27002	• Carry out future system planning activities • Control development and support processes
ISO27014	• Submit new information security projects with significant impact to governing body

(Cartlidge *et al.*, 2007; IT Governance Institute, 2012; International Telecommunication Union, 2013b; ISO27001 Security, 2013)

Best practice 9: Ensure sufficient back-up procedures, business continuity and disaster recovery

IT control document	Relevant processes
COBIT 5	• BAI04 Manage Availability and Capacity • DSS04 Manage Continuity
ITIL	• IT Service Continuity Management
ISO27002	• Establish back-up procedures • Use continuity management to protect the organisation's information

(Cartlidge *et al.*, 2007; IT Governance Institute, 2012; ISO27001 Security, 2013)

Best practice 10: Monitor, evaluate, assess and improve the mitigating controls implemented within the established enterprise mobility solution

IT control document	Relevant processes
COBIT 5	• DSS02 Manage Service Requests and Incidents • DSS03 Manage Problems • DSS05 Manage Security Services • MEA01 Monitor, Evaluate and Assess Performance and Conformance • MEA02 Monitor, Evaluate and Assess the System of Internal Control • MEA03 Monitor, Evaluate and Assess Compliance with External Requirements
ITIL	• Change Evaluation • Event Management • Incident Management • Problem Management • Continual Service Improvement
ISO27002	• Monitor information processing facilities • Manage user access rights • Report information security events and weaknesses • Manage information security incidents and improvements • Perform security compliance reviews • Carry out controlled information system audits
ISO27014	• Respond to information security performance result and prioritise and initiate required actions • Select appropriate performance metrics from a business perspective • Assess the effectiveness of information security performance • Ensure conformance with internal and external requirements • Notify executive management of the results of any external reviews that have identified information security issues, and request corrective actions • Commission independent and objective opinions of how it is complying with its accountability for the desired level of information security

(Cartlidge *et al.*, 2007; IT Governance Institute, 2012; International Telecommunication Union, 2013b; ISO27001 Security, 2013)

Best practice 11: Report to stakeholders

IT control document	Relevant processes
COBIT 5	• EDM05 Ensure stakeholder transparency
ISO27014	• Report to external stakeholders that the organisation practices a level of information security commensurate with the nature of its business

(IT Governance Institute, 2012; International Telecommunication Union, 2013b)

Appendix D: Detailed processes providing guidance in governance of security risks on an operational level

Appendix D lists the implementable processes (according to the IT governance control documents discussed in Chapter 3) that are relevant and will provide assistance to organisations in governing enterprise mobility security risks on an operational level.

IT control document	Relevant processes addressing security risks on an operational level
COBIT 5	• APO13 Manage security • BAI10 Manage Configuration • DSS02 Manage Service Requests and Incidents
ITIL	• Information Security Management • Design Coordination • Service Asset and Configuration Management • Release and Deployment Management • Knowledge Management • Service Validation and Testing • Request Fulfilment • Access Management
ISO27002	• Control external party use of the organisation's information • Control third party service delivery • Protect against malicious and mobile code • Protect computer networks • Control how media are handled • Protect exchange of information • Protect electronic commerce services • Control access to information • Manage user access rights • Control access to network services • Control access to operating systems • Control access to applications and systems • Protect mobile and teleworking facilities • Make sure applications process information correctly • Use cryptographic controls to protect the organisation's information • Protect and control the organisation's system files

(Cartlidge *et al.*, 2007; IT Governance Institute, 2012; International Telecommunication Union, 2013b; ISO27001 Security, 2013)