

Proposed Practices To Mitigate Significant Mobility Security Risks

Johanna Catherina Brand, Stellenbosch University, South Africa
Wandi Kruger-Van Renen, Stellenbosch University, South Africa
Riaan Rudman, Stellenbosch University, South Africa

ABSTRACT

Enterprise mobility is emerging as a fast-growing trend worldwide. Numerous risks originate from using mobile devices for business-related tasks and most of these risks pose a significant security threat to organisations' information. Information Technology (IT) governance frameworks can provide guidance in managing these risks at a strategic level, but these frameworks do not effectively govern on a technical operational level. Implementation of these frameworks may also be inefficient, as they are generic and do not necessarily cover all the risks relating to a specific technology. This study provides organisations with guidance on how to govern these enterprise mobility security risks in an effective manner at both a strategic and an operational level. Using three IT governance frameworks, this study identified 12 practices that companies can employ to mitigate significant mobility security risks.

Keywords: COBIT; ITIL; ISO; IT Governance; Mobility; Mobility Risks

1 INTRODUCTION

1.1 Background

In recent years, there has been a global increased use of mobile devices, mobile business and workforce mobility (Deloitte, 2013; Van der Meulen, 2012). This increased use of mobile technology was brought on by the recent consumerisation of mobile technology (Rowell-Jones, Jones, & Basso, 2011) and has had an influence on the business strategies of many organisations. Those charged with governance must consider the effect that this trend and the emergence of new technologies, many of which use wi-fi or 4G technology, has on their current business strategy (Burkhart, Krumeich, Werth, & Loos, 2011) and Information Technology (IT) controls. Failure to take the effect into consideration in a timely manner may have a detrimental effect on an organisation's competitive advantage, profitability and life span (Azim & Hassan, 2013). The establishment of an IT solution that satisfies an organisation's enterprise mobility needs will give rise to numerous risks (Ghosh, Gajar, & Rai, 2013; ISACA, 2010; Milligan & Hutcheson, 2007). Among these risks are various vulnerabilities that threaten the security of corporate information (Botha, Furnell, & Clarke, 2009). For organisations to successfully mitigate these security risks and the resulting impact on their organisation, these security risks should be governed. ISACA (2010) issued a white paper that proposes 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 organisational culture, technology and governance when creating this strategy (ISACA, 2010); hence only governing enterprise mobility security risks at a strategic level. It does not address an enterprise's mobility security risks at an operational level in terms of the implementation, maintenance and use of mobile technology. Other IT governance frameworks provide very little guidance to assist organisations in effectively addressing the impact of mobile technology on the process of governing enterprise mobility security risks. To ensure effective overall governance, these risks should be identified and addressed on both a strategic and an operational level. Governing enterprise mobility security risks on an operational and strategic level proves to be difficult due the existence of an IT gap. The aim of this study was to develop practices for organisations to use to govern enterprise mobility security risks. The study answers the following question: *How can an organisation effectively and efficiently govern significant security risks originating from enterprise mobility?*

Section 2 defines enterprise mobility and motivates why a need exists to govern mobility security risks. The importance of IT governance together with the weakness of IT governance frameworks is also discussed. Section 2 concludes with an overview of relevant IT governance frameworks. Section 3 discusses the security risks relating to mobile technologies. Using the security risks identified in Section 3, the processes of the IT governance frameworks that are applicable to mobility security risks are identified in Section 4. Thereafter, a list of practices that will assist organisations in effectively and efficiently governing enterprise mobility security risks is outlined. The study is concluded in Section 5.

1.2 Research Methodology

A non-empirical study was conducted by reviewing the existing literature. The historical analysis conducted during the literature review (refer to steps 1–3) followed a concept-centric approach, as suggested by Webster and Watson (2002), and a four-stage approach, as suggested by Sylvester, Tate and Johnstone (2011). Each stage was carried out iteratively and incrementally. Initially, a broad range of selection criteria was deliberately chosen, and the selection and number of articles included in this study varied as the author moved through the process. The timeline distribution of the final selection of articles is between 1990 and 2013.

1. The searching stage: Search terms included ‘enterprise mobility’, ‘security risks resulting from enterprise mobility’, ‘IT governance principles’, ‘IT governance control frameworks’, ‘business/IT alignment and IT gap’, ‘the governance of enterprise mobility security risks’, ‘access paths’ and ‘IT architectural components’. Interloan services, library books, online bibliographic databases and professional subscriptions (for example *IEEE*, *Science Direct* and *Ebsco Host*) were used to conduct the literature study. No screening of the articles for reputation of journal, quality of methods, academic focus or any other criteria took place. The only requirement was that the articles fall broadly within the scope of the study. This process provided a set of 253 possible items.
This stage gave the author an idea of the diversity and scope of the topic. The scope was then adjusted to include seminal articles. The following questions were taken into consideration during the selection of seminal articles: *Does it make a substantial scholarly contribution? Has the specific article been cited sufficiently and often enough to be regarded as a guiding influence?* The specific articles chosen for this study were monitored for objectivity and appropriate distribution across the timeline.
2. Article selection: This entailed refining the original selection of items according to recurring themes. For the purpose of this study, the recurring themes included ‘security risks resulting from enterprise mobility’, ‘business/IT alignment and IT gap’, ‘the governance of enterprise mobility security risks’ and ‘access paths’. This process was followed by a more detailed reading of the abstracts, introductions and conclusions of the articles. The result of this stage was that the original selection of items was reduced to 92 items. The outcomes of this stage helped the author to establish the conceptual, theoretical and methodological concerns with regard to the study.
3. Appraisal stage: A detailed reading of each article took place during the appraisal stage. The different themes were compiled into thematic context by making notes on the articles. This stage concluded with the identification of the main concepts and aspects that should be considered and addressed with regard to the governance of security risks resulting from enterprise mobility.
4. Data-analysis stage: In the data-analysis stage, the author followed activities such as combining, integrating, modifying, rearranging, composing and generalising concepts that were identified during the appraisal stage to ensure that a theme runs through the study, which assisted in preparing practices to govern mobility security risks.

From the literature review, the author was able to do the following:

- Obtain an understanding of the technology driving a mobile solution, as well as the components that make up the technology. Only the IT architectural components and access paths that may form part of the generic design of an established IT solution addressing enterprise mobility needs were considered and it therefore cannot be seen as an exhaustive list of all possibilities.
- Identify significant security risks originating from enterprise mobility.

- Review different IT governance frameworks to firstly assess which IT governance frameworks address enterprise mobility security risks and to secondly identify the processes listed in these IT governance frameworks that appear to be most relevant for assisting organisations during the process of governing enterprise mobility security risks. The study assessed all high-level processes listed in COBIT 5, as well as the 26 processes contained in ITIL. The processes listed in ISO/IEC 27002 and ISO/IEC 27014 were evaluated in conjunction with applicable information pertaining to these processes, as discussed in ISO/IEC 27000 and ISO/IEC 27001. These frameworks were selected because they are widely adopted and have recently been updated. Only the IT governance processes that are applicable to enterprise mobility security risks were considered. Moreover, this study considered the governance of significant security risks originating from enterprise mobility and therefore only the high-level processes listed in the IT governance frameworks were considered. Although each IT governance framework has complementary publications to assist in, for example, implementation or specific use thereof, these guidelines and complementary guides did not form part of the scope of this study.
- Map the security risks identified from the literature against the relevant, significant IT governance processes that organisations should implement to effectively govern enterprise mobility security risks.
- Consolidate any overlapping or processes that are similar from the IT governance frameworks listed in Step 4 in order to develop a list of practices to govern significant enterprise mobility security risks. This was done because the IT Governance Institute (2008) argues that the IT control processes from various IT governance frameworks should be combined to ensure a strong basis for the effective governance of risks.

2 LITERATURE REVIEW

2.1 Enterprise Mobility

Gartner (2013) describes ‘mobile business’ in its IT glossary as follows:

New business models enabled by the extensive deployment of key mobile and wireless technologies and devices, 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.

Ghoda (2009) defines ‘enterprise mobility’ 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.

In the literature, the term ‘mobility’ is used interchangeably to refer to ‘mobile business’, ‘enterprise mobility’ and ‘mobile computing’. In principle, the term ‘mobility or ‘mobile computing’ refers to a business model where employees make use of mobile technology to perform business tasks (Cuddy, 2009; Gartner’s IT Glossary, 2013; Ghoda, 2009; Welling, 1999). It is important to be able to link the mobile device to performing business tasks. ISACA (2012) notes that the term ‘mobile device’ can include a wide range of devices that have the ability to be moved. Examples include traditional mobile phones, smartphones and tablet personal computers with wireless connectivity.

2.2 Components Underlying Mobile Technologies

In order to understand the technology underlying mobile technologies, it is necessary to consider the access paths, IT architecture components and relevant configuration controls in generic mobile technology. An access path is described by Boshoff (1990) 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.

Within a generic mobile IT solution, a user can activate a number of different access paths. ISACA (2012) lists four possible access paths, namely access from a mobile device to another device, a public or private cloud or the corporate network. Within these access paths, there is a multitude of possibilities for IT components and connections. The following types of hardware, software and other IT architecture components may be present:

- Mobile devices
- Mobile applications
- Middleware
- Security and management software
- Switches
- Routers
- Operating system(s)
- Servers
- Firewalls
- Wireless networks
- Cellular networks
- Wired access points
- Internet connection

2.3 Extent Of Enterprise Mobility

Although mobile technology is not necessarily a new technology, the recent consumerisation of mobile technologies fuelled global growth in the use of mobile technology (Deloitte, 2013; Van der Meulen, 2012). The following statistics on mobile device sales, internet traffic and applications for mobile devices support these findings:

- The United Nations estimated that by the end of 2013, mobile subscriptions will amount to 6.8 billion subscribers globally (International Telecommunication Union, 2013), while other researchers estimated it to exceed 7 billion (Portio Research, 2013). This is in comparison with the world population, which was estimated at between 7.1 and 7.2 billion at the time (United States Census Bureau, 2013; Worldometers, 2013). These figures emphasise the 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 (Meeker & Wu, 2013).
- Apple's App Store was introduced in July 2008 with approximately 800 applications available for download (Apple, 2008). By June 2013, Apple indicated that more than 900 000 applications were available in the App Store (Apple, 2013b). The total number of downloaded applications via the App Store since its inception amounted to 50 billion by May 2013 (Apple, 2013a).
- Van der Meulen (2012) predicted that:
 - 1.2 billion smart devices will be sold during 2013;
 - businesses will purchase 53 million tablets during 2016; and
 - by 2016, 40% of the workforce will be using mobile technology to perform work-related tasks.
- In a survey by Symantec (2012) in which they contacted over 6 000 organisations globally, it was clear that the adoption of mobility (as part of an organisation's competitive strategy) has been realised. Almost three-quarters of the respondents indicated that they were discussing custom mobile applications, as they considered the business benefits of mobile computing as an increase in efficiency, an increase in business agility and aiding in gaining a competitive advantage.

The statistics relating specifically to the use of mobile technology above, whether it be for private or business use, show its pervasive influence on organisations and business decisions and will therefore influence the business model, business strategy, strategic objectives and business imperatives of organisations in the near future. In light of the impact of this, this new technology must be governed in order to mitigate potential risks.

2.4 IT Governance

2.4.1 The Need For IT Governance

Given the increase in the use of IT in businesses, as well as the pervasive nature of the IT used, it is inevitable that risks will be encountered. These risks must be managed. IT governance, as an important subset discipline of corporate governance, has specifically been addressed in authoritative literature on corporate governance, such as King III (Institute of Directors, 2009) in South Africa, Basel II in Europe and the Sarbanes Oxley Act in the United States of America, indicating the increased importance of governing IT-related risks. There are many definitions for the term 'IT governance'. Webb, Pollard and Ridley (2006) identified 12 definitions for this term during their review of existing literature and suggested the following definition: "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". This definition was based on five IT governance objectives that capture the broad reach of IT governance: (i) strategic alignment; (ii) delivery of business value through IT; (iii) control and accountability; (iv) performance management; and (v) risk management. 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 5.

2.4.2 IT Governance Principles And Frameworks

An abundance of IT governance frameworks is available to assist business managers with the governance of IT. Practices range from control frameworks that denote *what* should be done to more narrow and specific control models and standards that describe *how* it should be done. There are various benefits in using IT governance frameworks, models and standards (commonly referred to as governance frameworks). They provide a benchmarked 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. Relying on governance frameworks are also more cost-effective than in-house-developed risk matrices and, due to the continuous improvement and updating of IT governance frameworks, they are gaining maturity and increased acceptance among peers (IT Governance Institute, 2008; Năstase, Năstase, & Ionescu, 2009). However, IT governance frameworks are not mutually exclusive and combining, integrating or mapping different frameworks together can provide organisations with a strong basis for an IT governance strategy (IT Governance Institute, 2008). The benefits of combining different IT governance frameworks are reduced costs and reduced risk of unfocused adoption of these frameworks, hence reducing inefficiencies. It can provide organisations with a strong basis for an effective IT governance strategy, but can become costly if implemented in an unfocused, inefficient manner (Năstase *et al.*, 2009); therefore, it is recommended that organisations identify and apply only the processes that will be relevant in their specific context.

ISACA's white paper (2010) indicated that the IT governance principles and control techniques discussed in IT governance frameworks cannot, on their own, provide an effective, comprehensive solution to address and mitigate IT risks. To manage IT risks, Rudman (2010) suggests a collective effort between business and IT managers. Within this unified unit, the policies and procedures of business managers, such as the IT governance principles and control techniques discussed in IT governance frameworks, are successfully merged and aligned with the policies and procedures of IT managers, such as IT principles and IT control techniques. However, attempting to align business and IT and successfully addressing risks on both the strategic and operational levels have proven to be problematic. Business managers do not understand technology and IT control techniques and IT managers do not understand the IT governance frameworks. This misalignment of business and IT is also referred to as the IT gap. These IT governance frameworks will address the security risks of enterprise mobility on a strategic level. The weakness of IT governance frameworks lies in the fact that it does not address the security risks on an operational level. It does not provide technical, implementable guidance on how to implement IT control techniques on an operational level. 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. Achieving successful business/IT alignment remains a major concern of many businesses (Luftman & Ben-Zvi, 2011). This concern will become even more critical in the coming years due to accelerating IT advances and recent consumerisation of IT, which 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 solutions, as provided by the IT personnel, actually deliver. This gap usually arises due to:

- Business managers not understanding IT;
- IT managers not understanding business;
- Ineffective communication between business people and technical people (Brier, 1999; Chen, 2010; Luftman, Papp & Štemberger, Manfreda & Kovačič, 2011)

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 the following 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;
- 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 on an operational level, it is important to have an implementable, understandable, well-communicated process, structure or plan. It may assist organisations in minimising the effect of the misunderstanding and miscommunication between business managers and IT managers. It may also assist organisations in maximising business/IT alignment and effective risk management. 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 (Sidhu, 2013).

2.5 IT Governance Frameworks

Three frameworks giving relevant guidance on IT governance principles and the management of enterprise mobility security risks were considered.

2.5.1 Control Objectives For Information And Related Technology

Control Objectives for Information and related Technology (COBIT) is a best practice IT governance framework used by organisations to effectively govern IT in order to mitigate risks and achieve business value through IT (IT Governance Institute, 2003). The latest edition, COBIT 5, was released in 2012 and consolidates, inter alia, COBIT 4.1, Val IT and Risk IT, as well as other best practices to provide high-level guidance in the form of an overarching framework that enables organisations to govern and manage enterprise IT. COBIT 5 is based on five key principles focused on meeting stakeholder needs by creating value while covering the governance and management of an organisation's information and related technology, including the activities and responsibilities of both the IT functions and the non-IT business functions. It forms a single, integrated framework that integrates and aligns, on a high level, with many other IT-related standards and best practices, enabling a holistic approach. 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 the following four further domains of processes:

- Align, plan and organise: This process consists of the management of the IT framework, strategy, budgets and costs, human resources, service agreements, suppliers, risk and security.
- Build, acquire and implement: This includes the management of projects, defining the requirements for the project, managing any changes made as well as managing the configuration thereof.
- Deliver, service and support: This process entails dealing with service requests, any problems that might exist and the continuity of the project.
- Monitor, evaluate and assess: This entails the performance of the project, the system of internal control and compliance with external requirements (IT Governance Institute, 2012).

2.5.2 *The Information Technology Infrastructure Library*

The Information Technology Infrastructure Library (ITIL) provides guidance for the management of IT services. ITIL 2011, the latest edition, addresses each stage of the service lifecycle and the set of key processes and functions required during that specific stage.

- 1) Service strategy: This assists in developing a long-term strategy that will achieve alignment between the business and IT strategy.
- 2) Service design: This gives direction on the design and development of IT services, their architectures and processes, and other aspects of the service-management effort in order to increase business value. It applies to new services as well as modifications and existing IT services.
- 3) Service transition: This provides guidance on managing and controlling the transition of new and modified IT services in order to added value while still controlling the risks of failure, error and disruption.
- 4) Service operation: This directs business managers in delivering and supporting the day-to-day operation of IT services to ensure that value is delivered while also meeting the strategic objectives of the organisation.
- 5) Continual service-improvement management: This measures IT service levels and determines and executes improvements to create value through better design, transition and operation of services.

2.5.3 *ISO/IEC 27000 Series*

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 best practice recommendations on information security management systems. This series consists of more than 20 published standards, with several more still under development. As the focus of this study is on implementable 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 is on operational risk, application security, computing platform security, network security and physical security. The following four standards in this series were investigated:

- ISO/IEC 27000 gives an overview of the ISO/IEC 27000 series, addressing information security management systems and explaining 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.

3 IDENTIFYING SIGNIFICANT RISKS RELATING TO ENTERPRISE MOBILITY



3.1 Security Risks Relating To Enterprise Mobility

Numerous risks relating to enterprise mobility are listed in the literature, among others in Ghosh *et al.* (2013), ISACA (2010) and Milligan and Hutcheson (2007). Most of these risks relate to security threats to corporate

information. Security is considered one of the most significant concerns with enterprise mobility (Botha *et al.*, 2009). Security risks are defined as the risk relating to the loss of:

- Confidentiality: is concerned where access to protected information is only made available or disclosed to authorised individuals, entities, systems or processes;
- 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; and
- Availability: refers to timely and reliable access to and use of information, software and hardware upon demand by an authorised user of information or IT resources (ISO/IEC, 2012; Zissis & Lekkas, 2012; Ross, 2011). The security risks originating from enterprise mobility that threatens corporate information have been summarised in Table 1.

Table 1: Security Risks Originating From Enterprise Mobility

Risks And Causes Of These Risks	Authors								Threat to:		
	ISACA 2010	Ghosh <i>et al.</i> 2013	Milligan & Hucheson 2007	ISACA 2012	Khokhar 2006	Miller 2004	Souppaya & Scarfone 2013	OWASP 2011	Confidentiality	Availability	Integrity
Unavailable mobile device or unavailable resources on a mobile device											
Lost, stolen or damaged device											
Trojans and viruses											
Smsing attacks											
Malware propagation											
Spam											
Data loss or data corruption											
Lost, stolen or damaged device											
Trojans and viruses											
Smsing attacks											
Malware propagation											
Malicious hackers											
Unauthorised access to sensitive and confidential information											
Lost or stolen device											
Data or call interception											
Wireless sniffers											
Phishing and similar attacks											
Spyware attacks											
Malicious hackers											
Untrustworthy applications											
Insufficient security management											
Unsupported operating systems											
Operating system limitations											
Untrained or uninformed users											
	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.										

Miller (2004), Khokhar (2006), Milligan and Hucheson (2007), ISACA (2010, p. 5), OWASP (2011), ISACA (2012), Ghosh *et al.* (2013) and Souppaya and Scarfone (2013) highlighted the following recurring security risks:

- 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 enterprise mobility. Due to the mobile nature of these devices, they can easily be lost, stolen or damaged. Similarly, due to the connective nature of these mobile

devices, their software or operating system can be corrupted by, for example Trojans, viruses, smsing (text messages scams) attacks (text message scams) and malware propagation, rendering the mobile device unavailable for functional use by employees. Spam can lead to resources on the mobile device being wasted.

- 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.
- 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 voice phishing or man-in-the-middle attacks), wireless sniffers, phishing (scams using email or pop-up messages) attacks, spyware attacks, malicious hackers or untrustworthy applications installed on 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 are many different operating systems for mobile devices used by employees (the bring-your-own-device problem). Each operating system has unique characteristics and implementable security measures (Wagner, 2008). This wide variety of operating systems can result in insufficient security management due to IT departments and users of mobile devices not implementing adequate security measures.

3.2 Other Risks Relating To Enterprise Mobility

Various other risks that do not relate to security have been identified by inter alia Milligan and Hutcheson (2007), ISACA (2010) and Ghosh *et al.* (2013). These include:

- Workers dependent on mobile devices unable to work in the event of broken, lost or stolen mobile devices;
- Data on mobile devices not backed up regularly. In the event of a broken, lost or stolen mobile device, this information may be lost forever; and
- High variability in the operating systems of mobile devices (the bring-your-own-device problem).

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 ineffective.

4 MAPPING ENTERPRISE MOBILITY SECURITY RISKS AGAINST RELEVANT IT GOVERNANCE FRAMEWORK PROCESSES

The enterprise mobility security risks, as identified in Section 3.1, were mapped to the processes listed in the IT governance frameworks (COBIT 5, ITIL, ISO/IEC 27002 and ISO/IEC 27014) that are relevant to addressing these security risks. This matrix, contained in Appendix A, was used to assess which processes are most significant and should be implemented by organisations to effectively govern enterprise mobility security risks.

All the processes of the IT governance frameworks, except for those listed below, were found to address three or more of the enterprise mobility security risks identified in Section 3.1 and appear to be significant processes for the purpose of effectively governing the four risks.

- COBIT 5: *APO05 Manage Portfolio, BAI01 Manage Programmes and Projects* and *BAI02 Manage Requirements Definition*
- ITIL: *Business Relationship Management, Service Catalogue Management* and *Access Management*
- ISO/IEC 27002: *Use an information classification system*

- ISO/IEC 27014: *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.*

The exception processes identified above that address fewer than three of the risks have been reviewed and evaluated, and also appear to be significant processes. These processes should also be implemented during the process of governing enterprise mobility security risks.

The processes identified in this section that are necessary to effectively govern security risks resulting from enterprise mobility comprise a lengthy list. A number of processes from the different IT governance frameworks also appear to overlap. The number of processes and the overlapping processes make it inefficient to implement all these processes individually. In order to effectively and efficiently govern security risks relating to enterprise mobility, a list of high-level practices is needed. By combining any overlapping processes into one practice, the practices were kept to a minimum and are concise. These proposed practices (PP) (referred to as ‘*practices*’ henceforth) are presented in sections 5.1 to 5.12. Appendix A lists the practices identified, together with references to the relevant processes listed in the various IT governance frameworks. Should more detail relating to each practice or detailed assistance on how to practically implement each of the practices be required, the applicable IT governance framework can be reviewed.

4.1 Develop And Manage An Enterprise Mobility Security Strategy (PP1)

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 properly support and sustain the organisation’s strategy and strategic objectives.

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

4.2 Develop An Enterprise Mobility Security Policy (PP2)

Organisations should develop, communicate and implement an enterprise mobility security policy that will 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 the following:

- 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
- Privacy

4.3 Manage Human Resources (PP3)

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.

4.4 Be Informed Of The Security Requirements And Ensure Continued Compliance With These Requirements (PP4)

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

- Legal requirements
- Regulatory requirements
- Expectations of stakeholders
- Requirements of the employees
- The organisation's needs with regard to security.

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

4.5 Manage Risks (PP5)

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 them, together with the potential impact, in an attempt to ensure that the risks do 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.

4.6 Value, Protect, Track And Manage Assets (Pp6)

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, 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 and protect the organisation's assets by following proper disposal practices and procedures.

4.7 Manage Service Level Agreements And Suppliers (PP7)

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.

4.8 Design And Implement Proper Change Controls And Project-Management Practices And Procedures (PP8)

The need for new IT projects to have 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. They are identified as follows:

- 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

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.

4.9 Ensure Sufficient Back-Up Procedures, Business Continuity And Disaster Recovery (PP9)

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:

- The continued functioning of critical business operations on the minimum required service levels by means of sufficient flexibility and redundancy solutions for these critical operations;
- The 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.

4.10 Monitor, Evaluate, Assess And Improve The Mitigating Controls Implemented Within The Established Enterprise Mobility Solution (PP10)

Organisations should continuously monitor, evaluate, assess and improve the established enterprise mobility solution. The 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;
- Assess The Impact Of All New It Projects And Changes To Ensure That The Implementation Thereof Results In The Effective And Efficient Management Of Security Risks;
- Identify Critical Assets, It Operations And Corporate Information That Should Be Managed To Mitigate The Risk Of 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.

4.11 Report To Stakeholders (PP11)

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

4.12 Implement The Applicable Control Techniques Placing Reliance On Configuration Controls (PP12)

In order to mitigate the risks relating to mobile technologies, it is necessary to consider the access paths, IT architecture components and relevant configuration controls underlying an IT solution. 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 its IT solution and manage the resulting risks of all activated access paths. The IT architecture components that form the access paths need to be evaluated. IT should be required to identify and document all the potential access paths relating to a mobile solution. Organisations should therefore invest time to ensure that the enterprise mobility solution developed and implemented is:

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

Managing the risks of IT architectural components within the activated access paths can be achieved with the help of the configuration controls necessary for each IT architectural component. IT personnel can then assess what the possible risks are and how to effectively address these identified risks.

The IT architectural components within each access path should be controlled by means of the amending of the configuration controls necessary to take the risks into account:

- 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 to 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, plug-ins, 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 the configuration of 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 device and intervening in the process by stopping and restarting services or the device.
- ‘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).

During the process of implementing technologies such as enterprise mobility, it is important to ensure that a possible solution results in business and IT alignment and the reduction of the IT gap, and that it addresses security risks effectively and efficiently on an operational level. It is necessary that all affected parties understand the technology needs (from the business side) and technology capabilities (from a technical side) for each IT architectural component in the 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.

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 of an organisation.

5 CONCLUSION

Various significant security risks originate from IT solutions that organisations must implement in an effort to satisfy their enterprise mobility needs and requirements resulting from societal expectations due to 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 recommend practices that mitigate mobile security risks, and thereby develop a list of practices to assist organisations in governing enterprise mobility security risks effectively and efficiently on the strategic and the operational level.

The use of a combination of IT governance control frameworks, principles and processes provide organisations with an effective solution to govern enterprise mobility security risks. This can, however, result in an inefficient and costly process. To increase the efficiency of this governance process, a list of 12 practices has been developed by combining the processes from the selected IT governance frameworks relevant to the process of governing enterprise mobility security risks. In order to address mobility security risks, the following practices must be observed:

1. Develop and manage an enterprise mobility security strategy
2. Develop an enterprise mobility security policy
3. Manage human resources
4. Be informed of the security requirements and ensure continued compliance with these requirements
5. Manage risks
6. Value, protect, track and manage assets
7. Manage service level agreements and suppliers
8. Design and implement proper change controls and project-management practices and procedures
9. Ensure sufficient back-up procedures, business continuity and disaster recovery
10. Monitor, evaluate and improve the mitigating controls implemented within the established enterprise mobility solution
11. Report to stakeholders
12. Implement the applicable control techniques placing reliance on configuration controls

AUTHOR INFORMATION

Mrs Johanna Catherina Brand

Having previously lectured financial accounting and worked as an external audit manager, Mrs Brand decided to focus on gaining international experience by pursuing further studies in business and financial management in the USA. E-mail: KarlienBrand@gmail.com

Mrs Wandi Kruger-Van Renen*

Mrs Kruger-Van Renen is currently a lecturer in financial accounting, with previous experience lecturing information systems. After spending a few years working as an external auditor, she pursued a career at Stellenbosch University. Her interests lie in accounting education and teacher's education. E-mail: WandivanRenen@sun.ac.za (contact author)

Mr Riaan Rudman

Mr Rudman is a Senior Lecturer at Stellenbosch University. He lectures at an under- and post-graduate level. He specialised in financial institutions before joining academia. His areas of interest lie in business management and acceptable corporate behaviour in an electronic environment and new technologies. E-mail: RJRudman@sun.ac.za

REFERENCES

1. Apple. (2008). *iPhone App Store Downloads Top 10 Million in First Weekend* Retrieved from <http://www.apple.com/pr/library/2008/07/14iPhone-App-Store-Downloads-Top-10-Million-in-First-Weekend.html>.
2. Apple. (2013a). *Apple's App Store Marks Historic 50 Billionth Download* Retrieved from <http://www.apple.com/pr/library/2013/05/16Apples-App-Store-Marks-Historic-50-Billionth-Download.html>.
3. Apple. (2013b). *Apple Unveils iOS 7* Retrieved from <http://www.apple.com/pr/library/2013/06/10Apple-Unveils-iOS-7.html>.
4. Azim, R. & Hassan, A. (2013). Impact analysis of wireless and mobile technology on business management strategies. *Information and Knowledge Management*, 3(2), 141-150.
5. Boshoff, W.H. (1990). A path context model for computer security phenomena in potentially non-secure environments. Unpublished doctoral dissertation. Johannesburg: University of Johannesburg.
6. Botha, R.A., Furnell, S.M. & Clarke, N.L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security*, 28(3), 130-137.
7. 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.
8. Chen, L. (2010). Business-IT alignment maturity of companies in China. *Information & Management*, 47(1), 9-16.
9. Cuddy, C. (2009). Mobile computing. *Journal of Electronic Resources in Medical Libraries*, 6(1), 64-68.

10. Deloitte. (2013). *Tech Trends 2013, Elements of postdigital* Retrieved from http://www.deloitte.com/view/en_ZA/za/services/consulting/technology/tech-trends-2013/index.htm.
11. *Gartner's IT Glossary*. (2013). Retrieved from <http://www.gartner.com/it-glossary/m-business-mobile-business>.
12. Ghoda, A. (2009). Mobile applications and Silverlight, in A. Ghoda, *Pro Silverlight for the Enterprise*, pp. 249-266, New York: Apress.
13. 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.
14. Global Stats. (2013). Retrieved from http://gs.statcounter.com/#mobile_vs_desktop-ww-monthly-201207-201307.
15. 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.
16. IBM. (2012). *The business-IT gap: A key challenge* Retrieved from <http://www.almaden.ibm.com/coevolution/pdf/mcdauid.pdf>.
17. Institute of Directors Southern Africa. (2009). *King Report on corporate governance for South Africa (King III)* Retrieved from <http://www.iodsa.co.za>.
18. International Telecommunication Union. (2013). *The world in 2013, ICT facts and figures* Retrieved from <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf>.
19. ISACA. (2010). *White paper on Securing Mobile Devices* Retrieved from <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx>.
20. ISACA. (2012). *Securing Mobile Devices Using COBIT 5 for Information Security* Retrieved from <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices-Using-COBIT-5-for-Information-Security.aspx>.
21. ISO27001 Security. (2013). Retrieved from <http://www.iso27001security.com/index.html>.
22. ISO/IEC. (2012). *ISO/IEC 27000:2012 Information technology – Security techniques – Information security management systems – Overview and vocabulary* Retrieved from <http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html>.
23. IT Governance Institute. (2003). *Board briefing on IT governance*, 2nd edition Retrieved from <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx>.
24. IT Governance Institute. (2008). *Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit* Retrieved from <http://www.isaca.org/Knowledge-Center/Research/Documents/Aligning-COBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf>.
25. IT Governance Institute. (2012). *COBIT 5* Retrieved from <http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx>.
26. Khokhar, R. (2006). Smartphones – A call for better safety on the move. *Network Security*, 2006(4), 6-7.
27. 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.
28. 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.
29. Luftman, J., Papp, R., & Brier, T. (1999). Enablers and inhibitors of business-IT alignment. *Communications of the AIS*, 1(3), 1-30.
30. Meeker, M. & Wu, L. (2013). *2013 Internet Trends* [Online]. <http://www.kpcb.com/insights/2013-internet-trends>.
31. Miller, A. (2004). PDA security concerns. *Network Security*, 2004(7), 8-10.
32. 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.
33. 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.

34. OWASP. (2011). *OWASP Top 10 Mobile Risks* Retrieved from https://www.owasp.org/index.php/Mobile#tab=Top_Ten_Mobile_Risks.
35. Portio Research. (2013). *Portio Research Mobile Factbook 2013* Retrieved from <http://www.portioresearch.com/media/3986/Portio%20Research%20Mobile%20Factbook%202013.pdf>.
36. Ross, R.S. (2011). *NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View* Retrieved from http://www.nist.gov/manuscript-publication-search.cfm?pub_id=908030.
37. Rowsell-Jones, A., Jones, N. & Basso, M. (2011). *Executive Summary: Capturing Business Value From Mass-Market Mobile Technologies* Retrieved from <http://www.gartner.com/id=1779628>.
38. Rudman, R.J. (2010). Framework to identify and manage risks in web 2.0 applications. *African Journal of Business Management*, 4(13), 3251-3264.
39. Sidhu, B.S. (2013). Demystifying business IT alignment. *International Journal of Science & Technology*, 3(1), 20-26.
40. Souppaya, M. & Scarfone, K. (2013). *NIST Special Publication 800-124 Revision 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise* Retrieved from <http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>.
41. 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.
42. Sylvester, A., Tate, M. & Johnstone, D. (2011). Beyond synthesis: Re-presenting heterogeneous research literature. *Behaviour & Information Technology*. DOI: 10.1080/0144929X.2011.624633.
43. Symantec. (2012). *2012 State of Mobility Survey* Retrieved from http://www.symantec.com/en/za/content/en/us/about/media/pdfs/b-state_of_mobility_survey_2012.en-us.pdf.
44. United States Census Bureau. (2013). Retrieved from <http://www.census.gov/popclock/>.
45. 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* Retrieved from <http://www.gartner.com/newsroom/id/2227215>.
46. Wagner, E.D. (2008). Realizing the promises of mobile learning. *Journal of Computing in Higher Education*, 20(2), 4-14.
47. 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.
48. Welling, G.S. (1999). Designing adaptive environment-aware applications for mobile computing. Unpublished doctoral dissertation. Rutgers, The State University of New Jersey.
49. Webster, J. & Watson, R.T. (2002). *Analyzing the past to prepare for the future: Writing a literature review*. *MIS Quarterly*, 26(2), xiii-xxiii.
50. Worldometers. (2013). Retrieved from <http://www.worldometers.info/world-population/#pastfuture>.
51. Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, 28(3), 583-592.

APPENDIX A

The enterprise mobility security risks (R1 – R4), as identified in Section 3.1, are mapped to the processes listed in the IT governance frameworks 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. In light of the high-level of overlap, the processes were also consolidated into 12 proposed practises (PP1- PP12) as presented in Table A.1 to A.4. The shaded blocks denoted the applicable process relating to the risk and proposed practise.

Table A.1: Mapping Security Risks To COBIT 5

R1	R2	R3	R4	COBIT 5 process	pp1	pp2	pp3	pp4	pp5	pp6	pp7	pp8	pp9	pp10	pp11	pp12
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												
Align, Plan And Organise																
				APO01 Manage the IT Management Framework												
				APO02 Manage Strategy												
				APO03 Manage Enterprise Architecture												
				APO04 Manage Innovation												
				APO05 Manage Portfolio												
				APO06 Manage Budget and Costs												
				APO07 Manage Human Resources												
				APO08 Manage Relationships												
				APO09 Manage Service Agreements												
				APO10 Manage Suppliers												
				APO11 Manage Quality												
				APO12 Manage risk												
				APO13 Manage security												
Build, Acquire And Implement																
				BAI01 Manage Programmes and Projects												
				BAI02 Manage Requirements Definition												
				BAI03 Manage Solutions Identification and Build												
				BAI04 Manage Availability and Capacity												
				BAI05 Manage Organisational Change Enablement												
				BAI06 Manage Changes												
				BAI07 Manage Change Acceptance and Transitioning												
				BAI08 Manage Knowledge												
				BAI09 Manage Assets												
				BAI10 Manage Configuration												
Deliver, Service And Support																
				DSS01 Manage Operations												
				DSS02 Manage Service Requests and Incidents												
				DSS03 Manage Problems												
				DSS04 Manage Continuity												
				DSS05 Manage Security Services												
				DSS06 Manage Business Process Controls												
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												

Table A.2: Mapping Security Risks To ITIL

R1	R2	R3	R4	ITIL process	PP1	PP2	PP3	PP4	PP5	PP6	PP7	PP8	PP9	PP10	PP11	PP12
Service Strategy				Strategy Management for IT Services												
				Service Portfolio Management												
				Financial Management for IT Services												
				Demand Management												
				Business Relationship Management												
Service Design				Service Catalogue Management												
				Service-level Management												
				Supplier Management												
				Capacity Management												
				Availability Management												
				IT Service Continuity Management												
				Information Security Management												
				Design Coordination												
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												
				Event Management												
				Incident Management												
				Problem Management												
				Request Fulfilment												
				Access Management												
Continual Service Improvement				Seven-step improvement												

Table A.3: Mapping Security Risks To ISO/IEC 27002

R1	R2	R3	R4	ISO27002 process	PP1	PP2	PP3	PP4	PP5	PP6	PP7	PP8	PP9	PP10	PP11	PP12
				Establish a security policy												
				Establish an internal security organisation												
				Control external party use of the organisation's information												
				Establish responsibility for the organisation's mobile devices and other IT assets necessary to secure the organisation's information												
				Use an information classification system												
				Emphasise security prior to employment												
				Emphasise security during employment												
				Emphasise security at termination of employment												
				Use secure areas to protect facilities												
				Protect the organisation's mobile devices and other IT resources												
				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 networks												
				Control how media are handled												
				Protect exchange of information												
				Protect electronic commerce services												
				Monitor information processing facilities												
				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												
				Identify information system security requirements												
				Make sure that 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												
				Report information security events and weaknesses												
				Manage information security incidents and improvements												
				Use continuity management to protect the organisation's information												
				Comply with legal requirements												
				Perform security compliance reviews												
				Carry out controlled information system audits												

Table A.4: Mapping Security Risks To ISO/IEC 27014 Processes

R1	R2	R3	R4	ISO27014 process	PP1	PP2	PP3	PP4	PP5	PP6	PP7	PP8	PP9	PP10	PP11	PP12
				Ensure that business initiatives take into account information security issues												
				Ensure that information security adequately supports and sustains the business objectives												
				Respond to information security performance result and prioritise and initiate required actions												
				Submit new information security projects with significant impact to governing body												
				Determine the organisation's risk appetite												
				Align information security objectives with business objectives												
				Promote a positive information security culture												
				Develop, approve and implement information security strategy and policy												
				Allocate adequate investment and resources												
				Select appropriate performance metrics from a business perspective												
				Assess the effectiveness of information security performance												
				Consider the changing business, legal and regulatory environment and their potential impact on information risk and information security												
				Ensure conformance with internal and external requirements												
				Report to external stakeholders that the organisation practices a level of information security commensurate with the nature of its business												
				Notify executive management of the results of any external reviews that have identified information security issues, and request corrective actions												
				Recognise information concerning regulatory obligations, stakeholders' expectations, and business needs with regard to information security												
				Commission independent and objective opinions of how it is complying with its accountability for the desired level of information security												

NOTES