Mobile Technology Risk Management

Lize-Marie Sahd, Stellenbosch University, South Africa
Riaan Rudman, Stellenbosch University, South Africa

ABSTRACT

Mobile technology is fast becoming an indispensable part of consumers' lives and an essential business tool in improving productivity, streamlining business processes and remaining competitive. The mobile revolution is transforming business operations, but the pervasive nature of mobile technology also introduces new and significant risks into all areas of the businesses. In most businesses, however, the governance of mobile technology and its related risks is often disjointed and implemented in an ad hoc manner, resulting in all risks not being addressed. This lack of appropriate governance policies and procedures is a direct consequence of a lack of understanding of the technology and the speed at which new technologies are developed and adopted. If the risks are not addressed in a comprehensive manner, it could have severe consequences for a business. The objective of this research is to address this problem by using an appropriate control framework, Control Objectives for Information Technology (COBIT), to identify a comprehensive set of internal controls to address mobile technology risks at a governance, management and operational level. The research proposes a comprehensive set of internal controls which can be used by those charged with governance to manage each significant risk arising from the implementation of mobile technology.

Keywords: Mobility; Mobile Technology; Risk Management; IT Governance; COBIT

1. INTRODUCTION AND METHODOLOGY

1.1 Background and Research Objective

Innovation and the rapid rate of adoption of mobile technology is driving a transformation in business models, referred to by IFS (2013) as the mobile revolution. Enterprises are increasingly compelled by employees, clients and business partners to adopt mobile technology as a means to access data and functionality from any location. As a result of this consumer-driven nature of the revolution and the rate of mobile technology innovation, the governance of mobile technology has been implemented as an *ad-hoc* reactive process to mitigate risks as they occur, as opposed to a proactive strategy appropriately aligning and governing the entire technology. As a result, all risks are not appropriately mitigated. The objective of this research is to develop a comprehensive set of control techniques necessary to address all significant risks that mobile technology exposes the business to. The purpose of the research is the design of key control techniques to address the significant risks relating to the deployment of mobile technology, and not to list all possible control techniques.

1.2 Research Design

A qualitative study was performed and the following methodology was employed to address the research objective. A non-empirical study was conducted in order to obtain an understanding of mobility as a trend, the core components of the technology, the risks introduced by mobile technology, as well as corporate and IT governance and its impact on business. The study included a review of papers published in accredited research journals, popular articles, whitepapers and websites. In order to add scientific rigour to a literature review and obtain a strong theoretical basis for the research, a four stage approach is suggested by Sylvester, Tate and Johnstone (2010). The four stages include the searching, mapping, appraisal and synthesis of literature. A wide selection of articles and readings was selected in the beginning stages to enable a comprehensive understanding of the underlying literature, and the selection was narrowed down to more specific areas in the latter stages. This process resulted in the original search result from 268 articles narrowed down to 132 relevant articles, which were read in depth.

Based on a review of various control frameworks and standards addressing IT governance (including IT Information Library (ITIL) and ISO/IEC 27002), an appropriate control framework to identify the risks applicable to mobile technology was selected after having considered the scope of each framework. Control Objectives for Information and related Technology (COBIT) was selected because of the potential low implementation cost, and the fact that it is openly available. Moreover, it is widely accepted and internationally recognised by various organisations. It covers a wide range of IT processes which ensures easy alignment with other international frameworks and standards, thereby ensuring sound controls and regulatory compliance.

The technology was mapped against the COBIT framework and its related processes and control objectives. These objectives were used to identify relevant risks associated with the changes in business operations due to the impact of mobility. The impact of each risk was evaluated. COBIT's processes were used in conjunction with the significant risks to identify internal controls measures. The mapping is available on request. Once the internal controls were identified, a further review of literature was performed in order to expand the detail of the controls and to identify practical controls.

This methodology provided the foundation for the identification of significant risks related to the implementation of mobile solutions and the formulation of relevant controls that will mitigate enterprises' exposure to these risks.

1.3 Organisational Structure of Research

This research is presented in five sections. Section 2 contains the initial literature review and investigates the theoretical concepts underlying the research. Section 3 reviews the significant risks relating to the deployment of mobile technology, while section 4 presents the findings of a risk-control matrix that serves as a quick-reference guide to the key controls that need to be implemented to address the significant risks relating to mobile technology. Section 4 also outlines the detailed internal controls to mitigate the significant risks. Section 5 summarises the key findings of the research and concludes with the identification of potential areas for future research.

2. LITERATURE REVIEW

2.1 Mobility Research

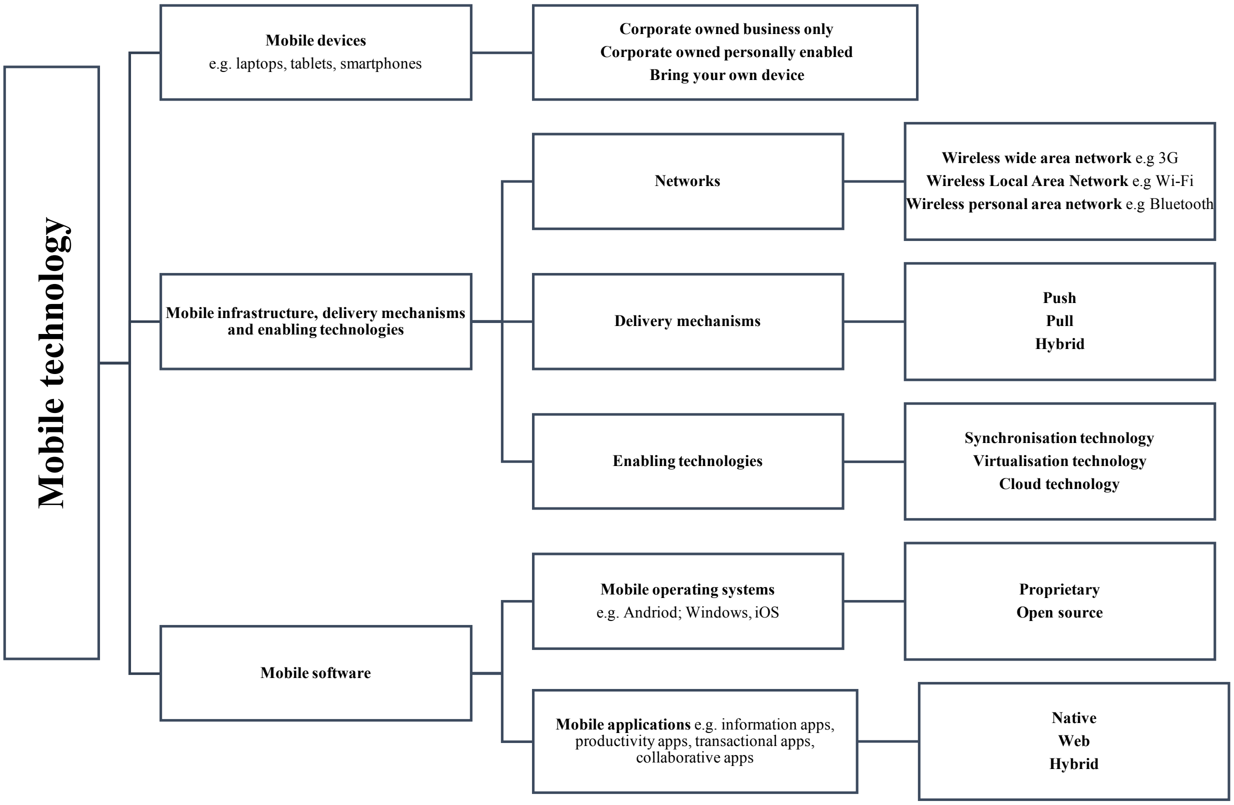
A review of existing literature is critical in forming a comprehensive understanding of the scope of the field. It establishes the foundation from which new knowledge can be generated by identifying a gap in current knowledge (Sylvester, *et al.*, 2010; Webster & Watson, 2002). A review of current literature confirmed that extensive research has been conducted on the risks that mobile technology exposes businesses to. Notable research reviewed in this regard includes Cisco & Citrix (2014), Akella, Brown, Gilbert & Wong (2012), Wright, Mooney & Parham (2011) and Unhelkar & Murugesan (2010). Research addressing the mitigation of the risks were, however, found to be either generic or tend to only address the most obvious risks such as security risks. Examples include GAO (2012) and Sathyan & Sadasivan (2010). A gap in research was recognised that identifies the detailed controls that address each of the significant risks arising from mobile technology in a comprehensive manner. In order to address this gap in research, it is necessary to first understand the nature and unique characteristics of mobile technology.

2.2 Mobility and Mobile Technology

Mobility refers to the ability of users, including employees, clients and business partners to access information and functionality outside of an organisations physical infrastructure (Wilkins, 2014). While mobile technology renders various significant benefits, its most fundamental impact is the initiation of ubiquity (Walters, 2012). This creates the opportunity to transform traditional structures and business processes into virtual structures and pervasive functionality. This core advantage, combined with the consumer-driven nature of mobile technology, has led to the emergence of the mobile enterprise (Ghoda, 2009). The mobile enterprise does not merely deploy mobile technology on an *ad hoc* basis to simplify or streamline operations. It transforms its entire operations and recognises mobile technology as a primary driver of business strategy, communication and operational processes (Basole, 2007). The scope of this research covers both enterprises that deploy mobile solutions on an *ad hoc* basis to primarily increase productivity and improve communication as well as the mobile enterprise that uses the technology to enhance quality of information, improve competitive advantage and modify business processes.

Mobile technology can be categorised into three core components: mobile devices, mobility infrastructure (networks, delivery mechanisms and enabling technologies) and mobile software (Deepak & Pradeep, 2012; Sathyan, Anoop, Narayan & Vallathai, 2012; Fling, 2009; Basole, 2008). Figure 1 shows the principal components that form the core elements of mobile solutions and refers to common examples of the components.

Figure 1. The core components of mobile solutions


Mobile technology
Mobile devices
e.g. laptops, tablets, smartphones
Corporate owned business only
Corporate owned personally enabled
Bring your own device
Mobile infrastructure, delivery mechanisms and enabling technologies
Networks
Wireless wide area network e.g 3G
Wireless Local Area Network e.g Wi-Fi
Wireless personal area network e.g Bluetooth
Delivery mechanisms
Push
Pull
Hybrid
Enabling technologies
Synchronisation technology
Virtualisation technology
Cloud technology
Mobile software
Mobile operating systems
e.g. Andriod; Windows, iOS
Proprietary
Open source
Mobile applications e.g. information apps, productivity apps, transactional apps, collaborative apps
Native
Web
Hybrid

Mobile devices are compact computing devices with both storage and communication capabilities that can access data and functionality from any location. In terms of device deployment in enterprises, devices used for corporate functionality are owned by either the company or the user. The bring-your-own-device (BYOD) model, where employees use personal mobile devices for both corporate and personal purposes, is becoming the more prevalent deployment model.

Wireless networks form the core component of **mobility infrastructure** as it facilitates location-independence. Wireless networks are generally categorised according to area of coverage and include wireless wide area networks that use cellular technology; wireless local area networks that connect to wired routers and switches; and wireless personal area networks such as Bluetooth connections (Verizon, 2012). Data **delivery mechanisms** transmit information on the wireless networks and function as push mechanisms that broadcast data to multiple users or pull mechanisms that transmit data on a request basis to a single user (Arokiamary, 2008). In terms of delivering the full benefits of mobile solutions, the following **enabling technologies** form part of the mobility infrastructure that supports mobility: synchronisation technologies ensure that all devices are updated with new information in order to eliminate duplicate work and ensure that all no information is lost; virtualisation technologies overcome physical IT resource restrictions by abstracting resources such as servers, networks, applications and storage space; and cloud technologies support mobile functionality by addressing the inherent limitations of storage capacity.

Mobile software includes mobile operating systems and mobile applications. Mobile operating systems are either proprietary systems that are developed and owned by the developing company or open source systems that make their source code available to the public in order to develop their own applications (Juniper, 2009). Mobile applications are developed as either native or web applications. Native applications reside locally on the mobile device and are developed specifically for that mobile platform. The application has full access to all device features and provide the best user experience. Web applications are basically websites delivered to the mobile device via internet connections (IBM, 2012).

2.3 Corporate governance and the governance of mobility

In order to comprehensively design internal controls that will address the risks related to the mobile technology components, the core elements of corporate and IT governance first needs to be investigated.

2.3.1 Corporate and IT Governance

Corporate governance consists of the policies and procedures according to which the board directs and controls an enterprise in order to meet its strategic objectives. An effective structure of governance incorporates responsibility, accountability, fairness and transparency into these policies and procedures (IODSA, 2009). Corporate governance systems need to keep evolving according to changes in business environments. The King Code for Governance in South Africa (King III) recognises IT developments as initiating fundamental business transformations and it has gained prominence in a South African context. Due to the pervasive nature of IT, good governance cannot be achieved without appropriately governing IT. The objectives of IT governance is alignment between IT and business strategies, value delivery, risk management, resource optimisation, assignment of accountability and responsibility as well as performance monitoring (SAICA, 2010; Webb, Pollard & Ridley, 2006; ITGI, 2003). Enterprises deploying mobile solutions need to consider the effect that mobile technology will have on the achievement of their IT governance objectives. A specifically challenging area in the governance of mobile technology is IT risk management as the technology is pervasive and introduces new risks in all business processes.

2.3.2 Control frameworks

In the development of a control structure to manage mobile technology risks, control frameworks provide a comprehensive and structured approach to governing IT systems and managing risks (Rudman, 2010). Nicho and Fahkry (2011) identified Control Objectives for Information and Related Technology (COBIT), IT Information Library (ITIL) and ISO/IEC 27002 as relevant frameworks for the governance of IT. An initial review of the scope and content of the frameworks identified that each framework deliver unique benefits and address specific areas of governance: COBIT is a generic yet comprehensive IT governance framework; ITIL addresses the best practices for the management of IT services; and the ISO 27000-series specifically addresses the management of IT security (ISO-security, 2014; ISACA, 2012, ITIL, 2011).

2.3.3 COBIT

From the review, COBIT was identified as the most relevant to this research. The focus of ITIL and the ISO-series was considered too narrow, whereas COBIT addresses the entire IT function and all areas of the enterprises affected by the use of IT. The core framework of COBIT includes five domains consisting of a number of processes (ISACA, 2012):

- **Evaluate, direct and monitor (5 processes):** the implementation and maintenance of a governance framework in order to meet IT governance objectives.
- **Align, plan and organise (13 processes):** the implementation of an IT strategy and the management of resources, stakeholders, IT output and risks.
- **Build, acquire and implement (10 processes):** the management of requirements, review of feasibility, and management of the full lifecycle of the IT on an operational level.
- **Delivery, service and support (6 processes):** the management of operations and incident management.
- **Monitor, evaluate and assess (3 processes):** the implementation of a system of performance management, internal control and compliance.

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

3. SIGNIFICANT RISKS ARISING FROM MOBILE TECHNOLOGY

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

The processes of COBIT were reviewed and benchmarked against a mobile environment in order to identify significant risks. The risks were categorised in two levels: strategic risks arising from a lack of governance and operational risks arising from the technology itself.

3.1 Strategic Risks

A critical area of mobile technology governance failures is a lack of board-level involvement and structured governance in the development of strategies and processes to mitigate the significant risks. A lack of clear strategies will lead to misaligned IT investments, excessive costs, ineffective resource allocation and unidentified risks. These risks could potentially have destructive consequences in all business operations.

3.2 Operational Risks

Risks identified at an operational level can be grouped into two classifications: risks that affect the users and the mobile technology's ability to function as intended and risks that affect the enterprise strategies and objectives.
Risks that affect the users and technology:

- **Interoperability:** In a mobile business environment users use diverse and varying versions of mobile devices as well as different wireless connections creating a heterogeneous landscape of devices, networks, operating systems and applications. This creates a complex environment of incompatible mobile technology components that have difficulty interoperating in terms of data exchange, communication, collaboration and storage (Bentley, 2013).
- **User experience:** Mobile technology's ability to deliver the benefits of improved productivity, communication and processes is dependent on the user's satisfaction with the device, speed and availability of connectivity, as well as the mobile software. Mobile devices and the related software are, however, often corporately prescribed and connectivity is often unreliable. In addition, mobile devices contain inherent limitations such as screen and keyboard size, limited memory space and battery life as well as slow processor speed (Unhelkar & Murugesan, 2010; Gansemer, Groner & Maus, 2007).
- **Connectivity:** The inherent design characteristics of a wireless network do not support reliable service delivery as wireless networks were initially designed as *ad hoc* connections and not primary operational networks. The fragmented evolution of current wireless network systems has created intricate and complex systems that are difficult to maintain (CDW, 2012; Gartner, 2012a). Further complications to reliable service delivery include increased communication traffic, data-rich applications, bandwidth bottlenecks, signal disturbances in cellular technologies and coverage dead zones (Cisco & Citrix, 2014; CDW, 2012; Deepak & Pradeep, 2012).
- **IT support:** Technical support in a mobile environment is often insufficient and challenging because of the many device types, related versions of operating systems and applications, the mobility of the user and device as well as user expectations of instant and real-time support (Cisco & Citrix, 2014).

Risks that affect the enterprise strategies and objectives:

- **Continuity:** The main threats to business continuity in a mobile environment arise from the nature of the technology. Mobile devices are vulnerable to loss or theft and corporate information may be lost, while unreliable wireless connectivity may disrupt critical business processes. In addition the enterprise may experience disruption of services or reputational damage due to security breaches and cyber-attacks (Sybase, 2011).
- **Security:** Mobile technology has not changed IT security risks, but new threats are introduced into the system because of the nature of the technology (Sterk & Spruijt, 2013). Mobile devices are more susceptible to theft or loss and wireless networks are more vulnerable to malicious attack and interception. Employees may use non-approved third party infrastructure and networks to connect to corporate systems. Employees also often use one device for personal and corporate purposes. This exposes corporate data as seemingly authorised users may obtain access to unauthorised data and sensitive data may easily be shared and uploaded to the web and cloud storage (Sybase, 2011; Wright *et al.*, 2011; Unhelkar & Murugesan, 2010). Another significant area of exposure is the increase in malicious and intentional security breaches. Mobile technology is exposed to standard attacks such as phishing, spam, viruses, Trojan horses and malware but are more exposed due to the nature of the technology. Wireless networks are vulnerable and is exposed to Wi-Fi sniffing, Bluetooth based attacks, automatic connectivity to unsecure networks, and unauthorised device tracking. Mobile devices are attacked through device cloning, keystroke logging and jailbreak software. Mobile software creates vulnerability through malicious applications that harvest data or that host remote command functionalities (GAO, 2012; Ernst & Young, 2012; Wright *et al.*, 2011; Sathyan & Sadasivan, 2010).
- **Cost:** The deployment of mobile technology has significant cost implications in terms of investment in devices; the development, acquisition and maintenance of software; the cost of enabling technologies such as virtualisation; and bandwidth cost. In addition, enterprises require investments in the establishment of new infrastructure and upgrading existing infrastructure as well as security management software such as authentication and encryption software (Cisco IBSG, 2012; Akella *et al.*, 2012; Gartner, 2012a). The number and wide variety of devices which now require support also has cost implications.
- **Data ownership:** In a mobile environment it becomes challenging to control data that can be easily accessed and shared on devices that are not owned or controlled by the enterprise. Intellectual property rights may also become uncertain in an environment where content is created on personally-owned devices outside of office hours (Madgwicks, 2012).

In addition to the significant risks that affect the user and the enterprise strategies, enterprises need to be aware of other risks that are not as significant but still affect enterprise operations. Software licensing may create exposure for enterprises where license terms apply only to corporate owned or leased devices and may not cover the use by employees of applications across multiple mobile devices. In environments where personal devices are used for corporate operations, enterprises may face litigation risk with regards to access to employees' private information. In addition, enterprises need to consider all relevant regulations in terms of data safeguarding, storage, structuring and extraction contained in acts such as the Sarbanes-Oxley Act of 2002.

Mobile technology components give rise to additional risks that expose the business. New controls and methods of regulating mobile activity will need to be adopted or existing controls will need to be modified in order for these new technologies to operate effectively and accurately.

4. CONTROLS IN A MOBILE ENVIRONMENT

Despite the significant risks introduced by mobile solutions, appropriate controls are often not planned and implemented appropriately (Sybase, 2011). The implementation of controls is complicated by the heterogeneous mobile technology landscape. Enterprises also perceive the adoption of a comprehensive mobility strategy to be too costly, complicated and challenging.

In order to ensure that a comprehensive control framework is developed, the risks identified from the processes of COBIT were used to identify generic control themes, followed by a further review of literature to identify detailed and practically implementable internal controls that can lower the threat to an acceptable level. From the initial generic control themes, it was found that enterprises need to implement sufficient and appropriate controls on three levels: governance, management and operational level. Table 1 summarises the specific control techniques that can be employed to mitigate each significant risk identified. The rows of Table 1 identify the internal control techniques and link these controls to the specific risks they address as denoted by the shaded block. These control techniques are discussed in detail in sections 4.1 to 4.3. The columns of Table 1 contain the significant risks, as identified in section 2.

Table 1. A risk-control matrix: linking the significant mobile solution risks to the relevant mitigating internal controls

Panel A

			Gover-nance	**Interoper-ability**		**User**	**Continuity**		**Connectivity**	
			Inadequate governance	**Hardware & software non-compatibility**	**Differences in data formats**	**Inherent device limitations**	**Significant loss or disruption**	**Inadequate business continuity plans**	**Unreliable connectivity & performance**	**Bandwidth bottlenecks**
Governance		Develop and implement governance system	▨	▨	▨	▨	▨	▨	▨	▨
		Develop and implement a mobile strategy	▨	▨	▨	▨	▨	▨	▨	▨
		Develop and implement mobile solution policies	▨	▨	▨	▨	▨	▨	▨	▨
		Training	▨	▨	▨	▨	▨		▨	▨
Management systems		Mobile device management systems	▨	▨			▨	▨		
		Mobile application management systems	▨	▨	▨					
		Mobile information management systems	▨		▨					
		Mobile expense management systems	▨							
Operational control techniques:	**Mobile device controls**	User authentication								
		Remote wipe					▨			
		Remote lock								
		Configuration controls: browser security, enabling auto-lock, password requirements, disabling auto-complete	▨				▨			
		Dual identify								
		Physical security					▨			
		Tiered approach to service delivery								▨
		Device activity monitoring and logging								
	Communication controls	Use managed wireless products							▨	
		Prioritise usage through configuration							▨	▨
		Manage guest connections								
		Mutual authentication								
		Digital signatures								
		Encryption and Secure Socket Layer								
		Virtual Private Networks		▨	▨		▨			
		Disable wireless networks								
		Wireless network settings undiscoverable								
		Network filters								
		Establish systems management team					▨		▨	▨
		Automate authentication and on-boarding								
		Use converged networks							▨	▨

(Table 1, Panel A continues on next page)

Table 1, Panel A continued

			Gover-nance	Interoper-ability		User	Continuity		Connectivity	
			Inadequate governance	**Hardware & software non-compatibility**	**Differences in data formats**	**Inherent device limitations**	**Significant loss or disruption**	**Inadequate business continuity plans**	**Unreliable connectivity & performance**	**Bandwidth bottlenecks**
Operational control techniques	**Application/ software controls**	Application management		▨	▨					
		Over the air provisioning								
		Application blacklisting and whitelisting		▨	▨					
		Installation management								
		Regular software updates								
		Review and update of software licensing								
		Virtualisation technologies								
		Testing applications		▨			▨			
		Segregating corporate functionality								
		One time passwords								
		Out-of-band authentication								
		Application wrapping								
		Sandboxing								
		Anti-virus software								
	Data controls	Data fading								
		Poison pill					▨			
		Managing data storage						▨		
		Containerisation of data					▨			
		Legal advice on employee contracts								

Panel B:

		Security					Data Ownership		Cost			IT support	
		Device loss or theft	**Unauthorised access**	**Intentional security breaches**	**Insufficient management**	**Out-dated software**	**Possession & control of data**	**Intellectual property rights**	**Device, software and infrastructure costs**	**Transmission costs**	**Security costs**	**Insufficient support**	**External service providers**
Governance	Develop and implement governance system	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	Develop and implement a mobile strategy	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	Develop and implement mobile solution policies	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	Training	▨	▨	▨	▨	▨	▨		▨	▨	▨	▨	
Management systems	Mobile device management systems	▨	▨	▨	▨	▨					▨	▨	
	Mobile application management systems		▨	▨	▨		▨				▨	▨	
	Mobile information management systems		▨	▨	▨		▨				▨	▨	
	Mobile expense management systems								▨	▨		▨	

Table 1, Panel B continued

			Security					Data Ownership		Cost			IT support	
			Device loss or theft	Unauthorised access	Intentional security breaches	Insufficient management	Out-dated software	Possession & control of data	Intellectual property rights	Device, software and infrastructure costs	Transmission costs	Security costs	Insufficient support	External service providers
Operational control techniques:	Mobile device controls	User authentication	▨	▨	▨		▨							
		Remote wipe	▨	▨	▨		▨							
		Remote lock	▨	▨	▨									
		Configuration controls: browser security, enabling auto-lock, password requirements, disabling auto-complete	▨	▨	▨			▨				▨		
		Dual identify		▨		▨		▨	▨				▨	
		Physical security	▨	▨										
		Tiered approach to service delivery								▨	▨		▨	
		Device activity monitoring and logging		▨	▨	▨					▨		▨	
	Communication controls	Use managed wireless products								▨	▨		▨	
		Prioritise usage through configuration									▨			
		Manage guest connections								▨	▨		▨	
		Mutual authentication		▨	▨									
		Digital signatures		▨	▨									
		Encryption and Secure Socket Layer		▨	▨									
		Virtual Private Networks		▨	▨							▨	▨	
		Disable wireless networks		▨	▨						▨			
		Wireless network settings undiscoverable		▨	▨						▨			
		Network filters		▨	▨	▨								
		Establish systems management team				▨					▨		▨	
		Automate authentication and on-boarding		▨									▨	
		Use converged networks								▨	▨		▨	

(Table 1, Panel B continued)

Table 1, Panel B continued

			Security					Data Ownership		Cost			IT support	
			Device loss or theft	Unauthorised access	Intentional security breaches	Insufficient management	Out-dated software	Possession & control of data	Intellectual property rights	Device, software and infrastructure costs	Transmission costs	Security costs	Insufficient support	External service providers
Operational control techniques	Application/ software controls	Application management											▨	
		Over the air provisioning					▨					▨	▨	
		Application blacklisting and whitelisting		▨	▨	▨							▨	
		Installation management	▨	▨				▨						
		Regular software updates					▨					▨		
		Review and update of software licensing					▨			▨				
		Virtualisation technologies		▨		▨		▨					▨	
		Testing applications				▨								
		Segregating corporate functionality		▨		▨			▨				▨	
		One time passwords	▨	▨										
		Out-of-band authentication		▨	▨									
		Application wrapping		▨		▨			▨				▨	
		Sandboxing		▨	▨			▨						
		Anti-virus software		▨	▨		▨							
	Data controls	Data fading		▨				▨						
		Poison pill	▨	▨	▨			▨						
		Managing data storage		▨				▨					▨	
		Containerisation of data	▨	▨				▨	▨				▨	
		Legal advice on employee contracts							▨					

The table assists enterprises in developing a comprehensive risk management strategy by optimising the implementation of internal controls to specifically target the significant risks relevant to their business operations. Following a structured approach in terms of the formulation of governance, management and operational controls will ensure that enterprise exposure is limited and the full benefits of mobile solutions can be extracted.

4.1 Mobile Solution Governance

In order to effectively govern mobile technology, enterprises need to identify all internal and external processes and resources influenced, define their mobile objectives and formulate mobile solution strategies and policies to support the objectives (Oracle, 2014). The mobile strategy needs to take into consideration all stakeholder requirements and expectations and facilitate the identification of new opportunities to advance business requirements (Akella *et al.*, 2012). Common oversights in the development of mobile strategies include focusing on only one mobility risk without understanding the overall effect of the risk (Gartner, 2012a). Another pitfall is the development of multiple mobile policies. It is important to have a single primary policy from which sub-policies are developed, ensuring consistency in the governance of all technology components (Cisco IBSG, 2012; Sybase, 2011).

According to ISACA (2010), the characteristics of effective, executable mobile strategies and policies are: simplicity and ease of implementation; flexibility in order to adapt to changes in stakeholder requirements; auditability; and reliability under abnormal circumstances. Other considerations that enterprises need to take into account when developing a mobile strategy and related policies include (Oracle, 2014; Gartner, 2012a; Ernst & Young, 2012; Wright *et al*., 2011; ISACA, 2010):

- Specifying requirements such as outsourcing or the in-house development and maintenance of mobile technology; feasibility analyses per enterprise division; determining the resources necessary to migrate existing systems onto mobile systems; and allocating specific responsibilities and decision-making authorities.
- Constantly monitoring and updating policies through performance measures for both outsourced and in-house services, compiling and reviewing external service level agreements and evaluating internal IT staff performance regularly; the continuous monitoring of new and emerging threats in mobile platforms; maintaining and updating existing strategies or developing new strategies to adapt to new mobile technology.
- Identifying all technology components in use by taking the full device life cycle into account; defining approved devices and applications and determining the configuration specifications; identifying and classifying both authorised or unauthorised uses of mobile technology; and specifying the storage and transmission procedures for enterprise information.

Deploying mobile policies should include sufficient training: application developers need to be trained in platform-specific coding and IT staff need regular refresher courses on new software and security risks. Users should be the trained in the proper use of mobile devices including awareness of security threats, regular updates of software and awareness of the appropriate channels for reporting problems and requesting IT support (Ernst & Young, 2012; GAO, 2012; Wright *et al*., 2011).

4.2 Mobile Solution Management Systems

Enterprise mobility management (EMM) systems are software solutions that assist the enterprise in effectively managing mobile solutions and are supported by the following support systems (Garcia, 2013; Sophos, 2013; Sterk & Spruijt, 2013; CDW, 2012):

- **Mobile Device Management (MDM):** MDM solutions are management and configuration tools that manage and administrate mobile devices by monitoring device statuses and controlling functionality remotely. Most MDM solutions operate on diverse mobile devices and related operating systems and features of MDM solutions include policy enforcement, asset management, administration and reporting, help-desk tools, and the facilitation of software updates, data back-up and application installation. MDM solutions do contain inherent limitations as enforceable capabilities are determined by device operating systems.
- **Mobile Application Management (MAM):** MAM tools are software systems that manage enterprise software on mobile devices and enable the secure provisioning of native applications. MAM systems facilitate enterprise software delivery, application configuration, application maintenance, usage tracking and policy enforcement. MAM solutions' effectiveness is limited, however, as it cannot manage mobile applications from public application stores.
- **Mobile information management (MIM):** MIM focuses on the management and administration of data. Off-the-shelf MIM system solutions have limited functionality in a diverse mobile landscape due to the closed architecture of mobile operating systems.
- **Mobile Expense Management (MEM):** MEM solutions monitor and manage mobile data usage and trends.

4.3 Mobile Solution Operational Control Techniques

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

4.3.1 Mobile Device Controls

Mobile devices will either be the property of the employee or the enterprise and in both instances sufficient security controls are critical. Device controls include the use of (Sterk & Spruijt, 2013; Akella *et al.,* 2012; Cisco IBSG, 2012; GAO, 2012; Sybase, 2011; Wright *et al*., 2011):

- **Configuration controls:** Configuring password settings to require complex passwords and browser security settings to enable the auto-lock function after a predetermined period of time and require a password to regain access. Disabling the autocomplete functions that recollect usernames and passwords.
- **User authentication:** Requesting password login to access enterprise applications.
- **Remote lock:** Remote disabling of the device, rendering it inoperable.
- **Remote wipe:** Deleting device content and deactivating device functionality.
- **Data control:** Deleting data or blocking access to corporate e-mail when the user is not connected to the network for a certain time.
- **Dual identity:** Enabling of two instances of the same operating system on one mobile device. One instance is enabled for corporate data and functionality and one for personal data and functionality.
- **Tiered administration:** Defining user groups and providing only the necessary functionality to each group.
- **Physical security:** Using cable locks and device tracking using GPS coordinates.

4.3.2 Communication Controls

Depending on existing enterprise infrastructure, enterprises deploying mobile solutions will either build new or upgrade existing wireless mobile networks and will need to consider:

- **Establishing requirements:** Consulting all stakeholders to determine coverage, security level and availability requirements.
- **Managed wireless products:** Employing wireless controller technology that considers the network as a single component. This simplifies the management and configuration process as each wireless access point is not managed and configured separately.
- **Prioritised usage:** Ensuring that critical corporate applications are prioritised through configuration management and firewalls.
- **Develop a guest policy:** Including a guest policy that provides guest connections to the enterprise network through the use of automated guest provisioning systems. This will ensure that valuable IT department time is not spent connecting guests.

A significant challenge for enterprises using wireless networks is the development of secure networks and the maintenance of data integrity during transmission. Data integrity can be controlled using the following techniques (GAO, 2012; Cisco IBSG, 2012; Wright *et al*., 2011; Sathyan & Sadasivan, 2010):

- **Mutual authentication:** An authentication process where the communicating parties authenticate each other before any transaction is concluded.
- **Digital signature:** Validates the authenticity of information by confirming that messages were created by a known sender and that it was not altered during transmission.
- **Encryption:** Secures sensitive information during transmission. Enterprises need to assess the options available in terms of encryption on its various supported devices.
- **Secure Socket Layer:** A standard security technology for internet transmissions that ensures endpoint authentication and confidential transmissions through cryptography.
- **Disable wireless networks:** Disabling of Wi-Fi, Bluetooth and infrared when not in use.
- **Mobile VPN network:** Increase in the security of connections.
- **Settings:** Changing of settings of Bluetooth devices to non-discoverable to make them invisible to unauthenticated devices when not in use.

- **Network filters:** Monitoring the identity of users attempting access to the corporate network and blocking users that do not run the enterprise MDM software.

In terms of implementing controls addressing the administration, cost and support of wireless mobile networks, Gartner (2012b) advises that a system management team is established to monitor and support these complex communication systems. In addition, enterprises should consider automating the authentication and on-boarding process of employees and guests in order to self-register devices on secure wireless networks as well as VPNs in order to relieve the support duties of the IT department (Aruba Networks, 2012). The use of converged networks, especially networks that integrate cellular and Wi-Fi transmissions, will further reduce costs and will be able to handle an increase in mobile device connections.

4.3.3 Application and Other Software Controls

Mobile platforms were not originally developed for corporate use (Ernst & Young, 2012) but corporate functionalities have systematically been integrated on personal devices and, therefore, need to be administrated and managed through (Garcia, 2013; Sterk & Spruijt, 2013; Sophos, 2013; Akella *et al.,* 2012; Madgwicks, 2012; Wright *et al*., 2011; Sybase, 2011; Sathyan & Sadasivan, 2010):

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

Virtualisation technologies allow for the efficient, secure and managed provisioning of corporate functionality on mobile devices. Two approaches can be considered. Desktop virtualisation occurs when you create a virtual desktop containing all authorised data and applications regardless of location or device. Data is transmitted directly from the corporate server to the device. IT supports and manages corporate software and applications centrally, while the user takes responsibility for device support (Cisco IBSG, 2012). Application virtualisation, on the other hand delivers the application to the user and not the device. This requires investment in virtualisation technologies such as server hosted virtual desktops (SHVD) (Gartner, 2012b).

Another significant area of control over corporate applications is the testing of the applications. The different categories of mobile applications expose both the device and enterprise to unique risks and they should, therefore, be tested for vulnerabilities and risks separately. Testing on native applications should be performed through the use of simulators contained within the software development kits as provided by the application developers. Web applications should be tested both as an anonymous user and as an authenticated user as web applications are accessible through the internet. Testers should also use traditional web browsers and standard application security assessment tool sets (Ernst & Young, 2012).

Protecting the security and integrity of corporate data is a priority for most enterprises, and this can be achieved through management of the applications that access, use, modify and store the data. MAM solutions are often used to facilitate these security controls by allowing the enterprise to monitor, administrate and control the functionalities of applications. The following are security controls that assist the enterprise in maintaining secure applications (Garcia, 2013; Sterk & Spruijt, 2013; Sophos, 2013; Sathyan & Sadasivan, 2010; Wright *et al*., 2011; Sybase, 2011):

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

4.3.4 Data Controls

Enterprise data is being accessed, modified, created and stored on both corporate and personal mobile devices and this influences the integrity of the data. Data can be safeguarded by (Garcia, 2013; Sterk & Spruijt, 2013; Cisco IBSG, 2012; Madgwicks, 2012; Wright *et al*., 2011; Sybase, 2011; Sathyan & Sadasivan, 2010):

- **Remote data wipe:** All corporate data can be removed remotely.
- **Data fading:** In cases where a device is not connected to the enterprise network, data is automatically removed after a specific lapse of time.
- **Poison pill:** A message is sent that destroys data on the device and renders the device useless.
- **Data encryption:** Certain data on the mobile device is encrypted and encryption/ decryption mechanisms are password protected.
- **Full disk encryption:** All data on the mobile device is encrypted.
- **Data storage:** Managing, encrypting and establishing access controls over stored and backed-up data.
- **Thin mobile client models:** Data is stored and managed centrally, limiting the data stored on each device.
- **Containerisation:** A security method provided by some MDM solutions that operates independently from the actual device by separating corporate and personal data and functionality on mobile devices. All information within the container is protected through user authentication and or encryption. The container is centrally managed allowing the enterprise to set all configurations. Information within the container can also be removed without affecting any other data in other containers.
- **Intellectual property protection:** Enterprises need to seek legal advice on existing employment contracts to ensure that intellectual property created by employees fall under corporate ownership regardless of location or device.

5. CONCLUSION

The deployment of mobile solutions introduces many new risks into business operations, but regardless of the significance of these risks, enterprises often follow a disjointed approach to the governance and management of the technology. The significant risks introduced into a business by mobile technology include: interoperability, inadequate user experience, a lack of continuous connectivity, insufficient IT support, impact on continuity of business, inadequate security, excessive costs and uncertainty around data ownership. The objective of the research was to use an appropriate control framework (COBIT) to identify internal controls to assist enterprises in managing these mobility risks in a structured manner. COBIT's detailed processes were used to summarise the significant risks arising from the introduction of mobile technology into a generic business. The processes were then used to design appropriate controls to mitigate these risks. Business that aim to comprehensively mitigate mobile technology risks need to follow a methodical approach incorporating mobile solution governance, mobile solution management systems, and operational control techniques. In terms of governance, the enterprise should develop and implement a customised and practicable mobile strategy as well as a set of comprehensive policies (with a focus on alignment) with best practices to ensure that the strategy is realised. All stakeholders must review sufficient training on the application and implementation of these strategies and policies. At a management level, the enterprise needs to implement management systems that run mainly automated controls that would assist in the control, administration and monitoring of mobile solutions. These should include manual or software systems that support the control of the components of mobile solutions and provide management with information on the use of the technology. In terms of operational controls, the enterprise should implement both automated and manual control techniques at a technology component level to detect and mitigate risk exposure at a mobile device, communication, application and data controls level. The risk-control matrix produced in this research can assists enterprises in implementing detailed controls that focus on their unique risk exposure and could be used as a starting point to mitigate these mobile technology risks to an acceptable level.

An area for future research is the application of this risk-control matrix to small and medium sized entities in the South African context to determine the practicality of its application.

AUTHOR BIOGRAPHIES

Mrs Lize-Marie Sahd is a lecturer at Stellenbosch University, South Africa and is a qualified CA(SA) with a Master's degree in computer auditing awarded *cum laude*. She lectures Financial Accounting at an under-graduate level. Her area of interest lies in advanced technologies and its impact on modern businesses from a governance and audit perspective. E-mail: LSahd@sun.ac.za (Corresponding author)

Mr Riaan Rudman is a Senior Lecturer at Stellenbosch University, South Africa. He lectures at an under- and post-graduate level. He spesialised 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

Akella, J., Brown, B., Gilbert, G. & Wong, L. (2012). Mobility disruption: A CIO perspective. Retrieved from: http://www.mckinsey.com/insights/business_technology mobility_disruption_a_cio_perspective.

Arokiamary, V.J. (2008). Mobile computing. Pune, India: Technical Publications.

Aruba Networks. (2012). Conquering today's bring-your-own-device challenges: A framework for successful BYOD challenges. Retrieved from: http://www. arubanetworks.com/pdf/technology/whitepapers/WP_BYOD.pdf.

Basole, R.C. (2007). The Emergence of the Mobile Enterprise: A Value-Driven Perspective. *Sixth International Conference on the Management of Mobile Business*. 9-7 July, 41. Toronto, Canada. Retrieved from: http://ieeexplore.ieee.org/stamp/stamp. jsp?tp=&arnumber=4278584.

Basole, R.C. (2008). Enterprise Mobility: Researching a new paradigm. *Information Systems Management,* 7:1-7.

Bentley. (2013). Interoperability Platform. Retrieved from: ftp://ftp2.bentley.com/dist/ collateral/Web/Platform/WP_Interop_Platform.pdf.

CDW. (2012). Wi-Fi: Far and Wide. Retrieved from: http://www.opus1.com/www/ whitepapers/WirelessInfrastructure2012.pdf.

Cisco IBSG. (2012). BYOD: A global perspective. Retrieved from: http://www. cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf.

Cisco and Citrix. (2014). Cisco and Citrix for Productive and Secure Enterprise Mobility. Retrieved from: http://www.cisco.com/c/dam/en/us/solutions/enterprise-networks/mobile-workspace-solution/citrix-cisco-mobility-wp.pdf.

Deepak, G. & Pradeep, B.S. (2012). Challenging issues and limitations of mobile computing. *International Journal of Computer Technology & Applications*, 3(1):177-181. Retrieved from: http://www.ijcta.com/documents/volumes/vol3issue1 /ijcta2012030132.pdf.

Ernst & Young. (2012). Mobile device security: Understanding vulnerabilities and managing risks. Retrieved from: http://www.ey.com/Publication/vwLUAssets/EY_ Mobile_security_devices/$FILE/EY_Mobile%20security%20devices.pdf.

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

Gansemer, S., Groner, U. & Maus, M. (2007). Data classification of mobile devices. *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*. 6-8 September, 699-703. Dortmund, Germany. Retrieved from: http://ieeexplore.ieee.org/stamp/stamp. jsp?tp=&arnumber=4488513.

GAO. (2012). Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. Retrieved from: http://www.gao.gov/assets/ 650/648519.pdf.

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

Gartner. (2012a). Bring Your Own Device: New Opportunities, New Challenges. Retrieved from: http://www.gartner.com/id=2125515.

Gartner. (2012b). Enterprise Mobility and Its Impact on IT. Retrieved from: http://www.gartner.com/id=1985016.

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

IBM. (2012). Native, Web or Hybrid mobile-app development. Retrieved from: www01.ibm.com/common/ssi/cgibin/ssialias?infotype=SA&subtype=WH&htmlfid= WSW14182USEN#loaded.

IFS. (2013). The business benefits of enterprise mobile solutions. Retrieved from: file:///C:/Users/lsahd/Downloads/White%20paper%20The%20business%20benefits%20of%20enterprise%20mobile%20solutions_004265%20(1).pdf.

Institute of Directors Southern Africa (IODSA). (2009). King Code of Governance for South Africa 2009. Retrieved from: http://african.ipapercms.dk/IOD/KINGIII/ kingiiireport/.

ISACA. (2010). Securing Mobile Devices. Retrieved from: http://www.isaca.org /knowledge-center/research/documents/securemobiledevices_whp_Eng_0710. pdf?id=.

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

ISO 27001 Security. 92014). Retrieved from: http://www.iso27001security.com/.

IT Governance Institute (ITGI). (2003). Board Briefing on IT Governance, 2nd Edition. Retrieved from: http://wikimp.mp.go.gov.br/twiki/pub/EstruturaOrganica/AreaMeio/ Superintendencias/SINFO/Estrategia/BibliotecaVirtual/MaterialExtra/26904_Board_Briefing_final.pdf.

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

Juniper. (2009). Open Source OS – The Future for Mobile? Retrieved from: http://www.juniperresearch.com/whitepaper/open-source-OS-the-future-for-mobile.

Madgwicks. (2012). Bring your own device. Retrieved from: http://madgwicks.com. au/files/file/PUBLIC/News/Whitepaper%20-%20BYOD%20%20September%2017% 202012.pdf.

Nicho, M. & Fahkry, H. (2011). An Integrated Security Governance Framework for Effective PCI DSS Implementation. *International Journal of Information Security and Privacy,* 5(3):50-67. Retrieved from: http://www.igi-global.com/article/integrated-security-governance-framework-effective/58982.

Oracle. (2014). The New Perimeter: Keeping Corporate Data Secure in the Mobility Era. Retrieved from: http://www.oracle.com/us/products/middleware/identity-management/mobile-security/transformation-perimeter-wp-2199245.pdf.

Rudman, R.J. (2010). Framework to identify and manage risks in Web 2.0 applications. *African Journal of Business Management,* 4(13):3251-3264. Retrieved from: http://www.academicjournals.org/article/article1380697598_Rudman.pdf.

SAICA. (2010). What is IT Governance?. Retrieved from: https://www.saica. co.za/Members/GovernIT/WhatisITGovernance/tabid/2270/language/en-ZA/Default.aspx.

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

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

Sophos. (2013). Sophos Mobile Control. Retrieved from: http://www.sophos.com/enus/medialibrary/PDFs/factsheets/sophosmobilecontroldsna.pdf?la=en.

Sterk, P. & Spruijt, R. (2013). Enterprise Mobility Management Smackdown. Retrieved from: http://www.pqr.com/enterprise-mobility-management-smackdown.

Sybase. (2011). Mobility Advantage: Why Secure your Mobile Devices? Retrieved from: www.sybase.co.za/files/White.../Sybase_Afaria_WhySecurity_wp.pdf.

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

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

Verizon. (2012). The Verizon Wireless 4G LTE Network: Transforming Business with Next-Generation Technology. Retrieved from: http://business.verizonwireless .com/content/dam/b2b/resources/LTE_FutureMobileTech_WP.pdf.

Walters, T. (2012). Understanding the "Mobile Shift": Obsession with the Mobile Channel Obscures the Shift to Ubiquitous Computing. Retrieved from: http://www.idgconnect.com/download/13186/understanding-mobile-shift-obsession-mobile-channel-obscures-shift-ubiquitous-computing?contact_id=512df0e2252e2e68 1a54a9ead26c1fa8&source=intl031513idgce&region=africa.

Webb, P., Pollard, C. & Ridley, G. (2006). Attempting to define IT Governance: Wisdom or Folly? *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*. 4-7 January,194a. Kauai, Hawaii. Retrieved from: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1579684.

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

Wilkins, B.R. (2014). Tips for Implementing Mobility Programs. @*ISACA*, 13. Retrieved from:http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Documents/2014/at-ISACA-Volume-13_nlt_Eng_0614.pdf.

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

NOTES