# SIGNIFICANT RISKS RELATING TO MOBILE TECHNOLOGY

**Lize-Marie Sahd**
*Stellenbosch University*
LSahd@sun.ac.za

Received: June 2015 Accepted: November 2015

## Abstract

The consumerisation of mobile technology is driving the large-scale adoption of mobile solutions in business models. Each component of mobile technology, however, introduces specific risks into the enterprise and those charged with governance are often unaware of all the risks they are exposed to. The research addresses this problem by using the processes of Control Objectives for Information and Related Technology (COBIT) to identify the significant risks introduced by mobile technology and linking these risks to the components of the technology. The resulting risk matrix determines an enterprise's risk exposure given its mobile technology component landscape and identifies the most effective technology to deploy given the enterprise risk tolerance levels. The matrix also promotes improved alignment through the development of IT governance systems that correlate with business strategies and by using the understanding of IT capabilities to drive business strategies.

### Keywords

Mobile technology, mobility, significant risks, IT governance, alignment, COBIT

---

**Ms L Sahd** is a lecturer in the School of Accountancy, Stellenbosch University, South Africa.

# 1. INTRODUCTION

## 1.1 Background and research objective

Mobile technology is not a new development. The unprecedented rate of innovation and the extent of its proliferation is, however, revolutionising the way business is conducted (Basole, 2007). While the number of mobile devices is growing at an extraordinary rate, the use of traditional mobile technologies such as laptops is decreasing steadily, while tablet and smartphone technologies are gaining significant market share. It is this change in the composition of the mobile device market that is driving the emergence of the mobile enterprise, where consumers, including employees, clients and business partners, are increasingly demanding ubiquitous access to information and corporate functionality from any location via personal mobile devices (Akella, Brown, Gilbert & Wong, 2012; Gartner, 2012a). Despite the benefits derived from the deployment of mobile technology, every area of the enterprise's operations is exposed to significant risks, and each component of the technology introduces unique risks into the business model. Due to the consumer-driven nature of mobile technology trends, the technology is often not properly aligned with business strategies, but is being implemented and controlled on an ad-hoc basis. This inadvertently causes enterprises to identify only the risks they are exposed to as they occur and result in losses and infringements. The full risk impact of mobile technology on the enterprise's operations is not understood and the purpose of this research is to use a structured approach to identify the significant risks that each component of mobile technology exposes the enterprise to. The research focuses on significant risk exposure and does not attempt to provide an exhaustive list of all risks that may arise from the adoption of mobile technology in business.

## 1.2 Research design and methodology

A qualitative study was performed and a review and summation of existing literature formed the foundation of the research. The following structured approach was followed:

1. A literature review was performed, taking into account all relevant subject matter. The theoretical concepts that were investigated include the definition of mobility; an understanding of the underlying components of mobile technology; and the theory of governance and control frameworks.
2. Through an initial review of the scope and content of selected control frameworks, Control Objectives for Information and Related Technology (COBIT) was identified as the most appropriate framework for the identification of risks relating to the use of mobile technology.
3. The detailed processes of COBIT were reviewed to identify the processes applicable to the management of mobile technology on a component level.
4. These processes were used to identify significant risks relating to the deployment of mobile technology. From the results of this process, a risk-component matrix was compiled, linking each mobile technology component to the significant risks it gives rise to.
5. A further review of literature was performed to define and explain the significant risks identified, and the risks were grouped into two levels: risks that arise from the inadequate governance of mobile technology and risks that arise on an operational level.

The research is presented in four sections. Section 2 contains the literature review and explores the theoretical concepts that provide the foundation for the research. It also summarises the key

components underlying mobile technology. Section 3 identifies and defines the significant risks related to the deployment of mobile solutions and includes a matrix that links the risks to the relevant mobile technology component. Section 4 summarises the key findings of the research and identifies potential areas for future research.

# 2. LITERATURE REVIEW

## 2.1 Historic review of prior research

Sylvester, Tate and Johnson (2010) and Webster and Watson (2002) determined that the review of historic literature forms the foundation for the creation of new knowledge by detecting the gap in current knowledge and differentiating the contribution of the research. A systematic review of existing literature established that current research emphasises three core themes:

(i) Quantitative research: The focus falls on the rate of adoption of mobile technologies internationally and trends in the use of emerging technologies;

(ii) Technical research: This area comprises extensive studies on the design, development and programming of the underlying components of mobile technology; and

(iii) Sponsored and peer-reviewed studies: These address generic mobile solution strategies, often addressing selected mobile technology risks.

The gap in current knowledge that was identified is the lack of a comprehensive list of significant risks relating to the deployment of mobile technology components.

## 2.2 Mobility and the mobile enterprise

In order to address the identified gap in knowledge, it is necessary first to understand the trend of mobility and its underlying technical components. This creates the basis for identifying risks specific to the technology and creating a link between the technology and the risks it gives rise to. Mobility is defined as the movement of an enterprise's information and technology beyond its physical capacity to facilitate employees' routine operations (Wilkins, 2014). For the purposes of this research, the terms 'mobility', 'mobile technology' and 'mobile solutions' are used interchangeably to represent the facilitation of mobile functionality within the enterprise. Mobile solutions have the potential to generate significant benefits if they are effectively and appropriately managed. The most significant benefits include: increased employee productivity, improved internal and external communication, enhanced quality of information, efficient business processes, costs reduction, improved competitive advantage, talent attraction and retention, stimulation of innovation as well as employee safety (Akella et al., 2012; Wright, Mooney & Parham, 2011; ISACA, 2010).

The mobile enterprise is an emerging organisational form that uses virtual structures and wireless network systems to transcend traditional organisational structures to enable ubiquitous operations and collaboration. A mobile enterprise does not simply deploy mobile technology for the convenient execution of basic activities, but transforms its entire strategy and operations (Ghoda, 2009). This research is relevant to both enterprises deploying ad hoc mobile solutions to derive isolated benefits in its daily operations as well as the mobile enterprise that extensively deploys mobile technology and has adopted a ubiquitous business model.

## 2.3 Mobile solution components

The benefits and functionality of mobile solutions are dependent on the components that constitute the technology. Studies by Deepak and Pradeep (2012), Sathyan, Anoop, Narayan and Vallathai (2012), Fling (2009) and Basole (2008) identified the essential layers of mobile solutions as the mobile device layer; the hardware and software infrastructure layer; and the mobile application layer.

### 2.3.1 Mobile device layer

A mobile device, for the purposes of this research, is defined as a compact and portable device with computing, storage and communication capabilities (Wilkins, 2014). Mobile devices can be deployed through one of three models. In a corporate-owned, business-only (COBO) model the enterprise issues a device that is owned by the enterprise and intended only for business use. In a company-owned, personally enabled (COPE) model the enterprise owns the device but personal use of the device is allowed in addition to corporate use. Bring your own device (BYOD) represents a model where the employee uses a personally selected and owned device to access corporate information and functionality (Blackberry, 2014).

### 2.3.2 Hardware and software infrastructure layer

Hardware and software infrastructure provide the structure for the facilitation of mobile functionality. This layer includes the mobile network, data delivery mechanisms and related enabling technologies.

Wireless networks constitute the core component of mobile infrastructure as they enable access to data and functionality from any location (Sathyan et al., 2012). Mobile networks can be categorised based on different characteristics, and for this research, area of coverage was selected as the most appropriate. Wireless wide area networks (WWAN) use cellular technologies to provide broadband data networks with broader coverage and range. WWANs include virtual private networks and use 2G, 3G and 4G standard technologies. Wireless local area networks (WLAN) facilitate connections through technologies such as Wi-Fi, where devices connect to wireless access points that are connected to local networks via wired connections. Wireless personal area networks (WPAN), such as Bluetooth connections, provide ad hoc network connections to devices at close range (Verizon, 2012; Fling, 2009).

Data delivery mechanisms ensure the transmission of data across wireless networks through the exchange of messages. Mobile applications often use broadcast data delivery connections where messages are simultaneously transmitted to multiple users, and these mechanisms can be grouped in the following categories (Arokiamary, 2008; Yunos, Gao & Shim, 2003):

- Push mechanisms: The server transmits information before the receipt of a request. The server initiates the transfer and perceives perpetual queries from users through their subscription and a single distribution addresses all queries in the broadcast.
- Pull mechanisms: The server locates and broadcasts information on receipt of a query.

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

- Synchronisation technologies: Synchronisation technology is a form of embedded middleware that supports the use of multiple devices by facilitating the updating of data between two or more devices, ensuring that the data sets are constantly identical. This is a practical technology used by employees who use more than one device for corporate functionality to eliminate duplicate work and outdated versions.
- Virtualisation technologies: Virtualisation technology delivers the benefits of mobile solutions through the abstraction of information technology (IT) resources such as servers, storage, networks and applications, and it bridges the physical limitations of the resources. A predominant virtualisation technology employed in a mobile environment is a server-hosted virtual desktop (SHVD). This separates the PC desktop from the physical device, stores it on a centralised server and allows for remote mobile access via a network. Another frequently applied form of virtualisation is application virtualisation. This virtualisation technique uses user-centric application delivery that delivers the application to the user, not the device.
- Cloud technologies: Cloud technologies support the growing use of mobile devices by overcoming their inherent limitations with regard to storage capacity and other functionalities. Cloud technology is a computing model that facilitates ubiquitous, flexible and on-demand access to off-site shared resources such as networks, servers, storage and applications delivered via internet technologies.

### 2.3.3 Mobile application layer

The application layer of mobile solutions includes mobile operating systems and mobile applications and provides the user with an interface to operate the mobile device (Sathyan et al., 2012). A mobile operating system is the principal software element on a processor-based mobile device and serves as the platform on which other programmes run. Mobile operating systems are either proprietary or open source. Proprietary operating systems are licensed systems that are developed, owned and regulated by the developing company. Users pay royalties for right of use, and the developing company provides support and updates. In open source operating systems, the source code is published and made available to members of the public to download and modify, allowing them to develop their own applications executable on the operating system (Fling, 2009; Juniper, 2009).

Mobile applications are relatively small, separable software units with limited functionality developed specifically to run on mobile devices. The development of mobile applications is classified into three categories (IBM, 2012; Fling, 2009):

- Native applications: Native applications have binary executable files that are downloaded directly onto the mobile device and reside locally on the device. These applications are developed and compiled specifically for one mobile platform and have full access to all device features and functionalities.
- Web applications: Web applications are essentially websites delivered to a mobile device over the internet. Because of the powerful browsers run by advanced mobile devices, these rich browser-based applications produce native-like functionalities but are not installed on the device.
- Hybrid applications: Hybrid applications are launched similarly to native applications and combine the capabilities of native applications that run on the mobile device, and multi-platform web technologies. Significant parts of the application are developed using web

technologies, but the applications retain access to the application programming interface (API) for some functionalities such as the device camera, the global positioning system and the list of contacts. APIs are sets of programming instructions, protocols, tools and routines used to develop applications by opening up a programme's internal functionality. In the mobile technology context APIs run on top of the mobile operating system and link the mobile application and the mobile operating system, thus allowing communication between the software.

## 2.4 Corporate governance and the governance of mobile technology

In order to comprehensively identify the risks relating to mobile technology the technology needs to be understood in the context of corporate and IT governance and it needs to be analysed against an appropriate control framework. Corporate governance comprises the policies, processes and systems according to which an enterprise is directed and controlled. The fundamental objective of corporate governance is the achievement of the long-term strategic objectives of the enterprise by taking into consideration the expectations of all stakeholders (Bai, Liu, Lu, Song & Zhang, 2003).

IT governance is the responsibility of the board of directors and is considered to be a subset discipline of corporate governance. IT governance is achieved through organisational structures, as well as a framework of best practices that encourages an established pattern of appropriate behaviour for both users and administrators in order to direct, manage, control and maintain IT investments (ITGI, 2003). IT governance aims to achieve strategic alignment, value delivery, risk management, the assignment of accountability as well as performance and resource management (IODSA, 2009; Hardy, 2006; ITGI, 2003). In order to meet these objectives, the enterprise needs to implement structures and mechanisms tailored to the specific technology deployed. IODSA (2009) refers to the use of control frameworks and guidelines as a governance tool to assist the board in systematically and adequately governing IT to meet stakeholder expectations.

The governance of IT requires those charged with governance to specifically tailor a governance system for IT assets, ensuring alignment with business strategies. In order to achieve business/IT alignment, IT investments and the delivery of IT services need to be driven by business strategies and business strategies need to be influenced by an understanding of IT capabilities and limitations. Those charged with governance can no longer steer a business successfully without a clear understanding of the technical IT implications of strategic decisions (Macehiter Ward-Dutton, 2005). The governance and alignment of mobility, as an IT asset, requires specific considerations due to specific characteristics of the technology. These include the rate at which the technology is advancing, the incremental risks related to mobile solutions and their technical design and functionality.

## 2.5 Control frameworks

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

### 2.5.1 Control frameworks reviewed

According to Nicho and Fahkry (2011), Control Objectives for Information and Related Technology (COBIT), IT Information Library (ITIL) and ISO/IEC 27002 are the most relevant and commonly adopted IT control frameworks and standards for the governance, management, maintenance and security of IT. According to their study, each framework or standard provides a different value to its users: COBIT is generally used as a benchmark framework and for audits, ITIL is used for the description and design of IT processes and ISO/IEC 27002 for security issues and the mitigation of specified risks. The King Code of Governance for South Africa (IODSA, 2009) also specifically makes reference to ISO/IEC 38500:2008: Corporate governance of information technology as a possible framework to employ in the governance of IT.

An initial review of the highlighted standards was performed in order to determine the most appropriate framework to identify risks relating to the deployment of mobile solutions. The core characteristics of each framework is summarised in TABLE 1 below:

**TABLE 1: The scope and lay-out of selected control frameworks and standards**

| | *COBIT* | *ITIL* | *ISO 27000 - series* | *ISO 38500* |
|---|---|---|---|---|
| Scope | Framework for the governance and management of the use of and investment in enterprise IT. | Framework containing best practices for IT service management and support processes. | Standards for the governance and management of IT security. | Advisory standard that provides broad guidance on IT governance. |
| Lay-out | Includes five domains, divided between the governance and management of IT<br>Each domain is broken down into detailed processes. | Comprises a series of eight books, five of which each cover a core stage of the IT service lifecycle. | Comprises 37 published and/or proposed standards that address information security management systems, best practices and controls. | Provides a model for governance through evaluation, direction and monitoring of a framework of six principles of good governance. |

*Source: ISO 27001 Security, 2014; ISACA, 2012; ITIL, 2011; ISO/IEC, 2008*

The four selected frameworks and standards were considered as potential bases from which risks arising from the deployment of mobile solutions will be identified. COBIT was selected as the most appropriate framework as it provides the most comprehensive approach to IT governance and addresses not only the IT function, but all areas in the enterprise affected by the investment in and use of IT solutions. ITIL and the ISO/IEC 27000-series are more detailed in terms of guidance and processes, but were considered to be too narrow for the purposes of identifying the significant risks relating to mobile solutions. ITIL focuses only on IT service delivery and the ISO/IEC 27000-series focuses only on IT security. ISO 38500 was considered to be too broad and generic in its scope.

### 2.5.2 COBIT

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

- Evaluate, direct and monitor (5 processes): the establishment of a governance framework and the monitoring of processes and systems.
- Align, plan and organise (13 processes): the development of an aligned IT strategy and an appropriate organisational and IT infrastructure to support this strategy, comprehensive risk assessment and resource management.
- Build, acquire and implement (10 processes): the development and implementation of IT solutions at an operational level, including the acquisition, installation, configuration and maintenance of IT assets and change management.
- Delivery, service and support (6 processes): the delivery of IT services and day-to-day operational and data management, security and continuity, and user support.
- Monitor, evaluate and assess (3 processes): the implementation of performance management and monitoring systems as well as structures of internal control, regulatory compliance and governance to ensure compliance with control objectives.

## 3. RISKS RELATED TO THE DEPLOYMENT OF MOBILE SOLUTIONS

Mobile technology is pervasive and influences the flow of information within the entire enterprise, modifies the business processes and affects employee practices (ISACA, 2010). As a result, risk is introduced into all aspects of the business. To ensure that significant risks are comprehensively identified, the details of each of the 37 COBIT processes were reviewed. Through the application of each process to a mobile solution environment the significant risks relating to mobile technology were identified. The detailed mapping is available from the author on request. Every component of mobile technology exposes the enterprise to specific significant risks and TABLE 2 creates a link between the components (as described in section 2) and the risks introduced by the technology. The table thereby enables enterprises to identify the significant risks their mobile investments are exposing them to, and allows enterprises to use the potential risk exposure of each component in relation to its risk tolerance strategy to drive future mobile technology investments.

Further consideration of the risks identified through the application of the COBIT processes established that the risks can be grouped in two levels: risks on a governance level and risks on an operational level. The identified risks can be categorised according to various characteristics, but for the purposes of this research the distinction between governance and operational risks is considered appropriate in order to improve IT governance and link the risks to mobile technology components on an operational level. A study of the literature was performed to formulate clear definitions of the selected risk categories and describe the vulnerabilities enterprises are exposed to.

**TABLE 2: Significant risks originating from mobile technology component**

| | | Governance | Inter-operability | | User | | Continuity | | Connectivity | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | Inadequate governance | Hardware and software non-compatibility | Differences in data formats | Inherent device limitations | User satisfaction and productivity | Significant loss or disruption | Inadequate business continuity plans | Unreliable connectivity and performance | Bandwidth bottlenecks |
| *Devices* | COBO | X | | | X | X | X | X | | |
| | COPE | X | | | X | X | X | X | | |
| | BYOD | X | X | | X | | X | X | | |
| *Networks* | WWAN | X | | | | X | X | X | X | X |
| | WLAN | X | | | | X | X | X | X | |
| | WPAN | X | | | | X | X | X | X | |
| *Delivery mechanisms* | Push | X | | X | | X | | | | |
| | Pull | X | | X | | | | | | X |
| *Enabling technologies* | Synchronisation | X | | | | | | | X | |
| | Virtualisation | X | X | | | | | | X | |
| | Cloud | X | X | X | | | | | X | |
| *Operating systems* | Proprietary | X | X | X | | | X | | | |
| | Open source | X | X | X | | | X | | | |
| *Applications* | Native | X | X | X | | | X | | | |
| | Web | X | | | | X | X | | | |
| | Hybrid | X | | | | X | | | | |

**TABLE 2: Significant risks originating from mobile technology component (continued)**

| | | Security | | | | | Data ownership | | | Cost | | IT support |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Device loss or theft | Unauthorised access | Intentional security breaches | Insufficient policy enforcement | Outdated software | Possession and control of data | Intellectual property rights | Device, software and infrastructure costs | Transmission costs | Security costs | Insufficient support |
| *Devices* | COBO | X | | X | X | | | | X | | | |
| | COPE | X | X | X | X | | X | X | X | | | |
| | BYOD | X | X | X | X | X | X | X | | | | X |
| *Networks* | WWAN | | | X | | | | | X | X | X | X |
| | WLAN | | | X | | | | | X | X | X | X |
| | WPAN | | | X | | | | | X | X | X | |
| *Delivery mechanisms* | Push | | | | | | | | X | | | |
| | Pull | | | | | | | | | | | X |
| *Enabling technologies* | Synchronisation | | X | | | X | | | | | | |
| | Virtualisation | | | | | | | | X | | | |
| | Cloud | | X | X | | | X | | | | | |
| *Operating systems* | Proprietary | | | X | X | X | | | X | | X | X |
| | Open source | | | X | X | X | | | | | X | |
| *Applications* | Native | | | X | X | X | | | X | | X | X |
| | Web | | | X | X | X | | | | | X | |
| | Hybrid | | | X | X | X | | | X | | X | |

## 3.1 Significant risks on a governance level

For many enterprises the deployment of mobile solutions is a reactive strategy to the consumerisation of mobile technology and is often not adequately governed to ensure that the IT governance objectives are met. A lack of appropriate, comprehensive mobile solution strategies exposes the enterprise in terms of all the IT governance objectives:

- Strategic alignment: Mobile solutions do not advance enterprise strategies and may become obsolete due to the rate of innovation.
- Value delivery: The cost of the technology exceeds its benefit and opportunities for innovation in enterprise operations are overlooked.
- Risk assessment: Risk exposure exceeds risk tolerance levels and all risks are not identified. This leads to insufficient controls and financial and other losses.
- Accountability: If ownership of mobile solution strategies and policies goes unassigned it leads to miscommunication, undetected inefficiencies and inadequate incident management. One of the key shortfalls of mobile solution strategies is board-level involvement.
- Performance management: Inadequate performance and insufficient change management policies are not addressed and improved.
- Resource management: Insufficient resources and ineffectively employed resources lead to excessive costs and opportunity costs.

The board of directors is charged with the implementation of IT governance systems. The IT team is, however, tasked with the implementation and execution of these governance systems on an operational level. This division of responsibilities gives rise to the IT gap. Those charged with governance often do not understand the underlying technology and its technical design, whereas those charged with the implementation of the technology do not understand the framework and strategic objectives within which IT needs to be governed. Risks arise on both sides of the IT gap: on a governance and operational level. From TABLE 2 it is clear that every component could potentially lead to significant governance risks if it is not aligned with business strategies and not appropriately governed through effective systems and processes. This emphasises the fact that the board needs to understand underlying technology in order to effectively govern it. Understanding the components of mobile technology is also essential in recognising and managing risks on an operational, technological level.

## 3.2 Significant risks on an operational level

Risks on an operational level can be grouped into two sub-categories: (i) risks that affect the users and the mobile technology's ability to function as intended, including interoperability, user experience, connectivity, and IT support, and (ii) risks that affect the enterprise strategies and objectives, including continuity, security, cost and data ownership.

### 3.2.1 Interoperability

Interoperability refers to the ability of multiple systems within an infrastructure with diverse components to exchange data and intercommunicate using the same communication protocol. Interoperability within a system is obstructed by three main features: (i) hardware and software differences preventing compatibility and machine-to-machine communication; (ii) differences in data formats and data storage methods; and (iii) complex relationships between mobile

components (Bentley, 2013; ETSI, 2008). Due to its nature, mobile solutions present challenges on all three levels. A mobile solution landscape is often a heterogeneous environment with diverse types and versions of mobile devices; software platforms and related programming languages; APIs and operating system architectures; and networking technologies. In addition, the structure and composition of a mobile system often includes islands of activity and functionality, which creates a complex system (ETSI, 2008).

### 3.2.2 User experience

User satisfaction with specific devices, operating systems, applications and connectivity dictate whether optimal functionality and productivity is possible. The performance requirements of the mobile user are productivity, convenience and personalised functionality. The user interface allows the mobile user to transact, communicate and locate information on a mobile device and dictates whether performance requirements are met (Gansemer, Groner & Maus, 2007). Mobile devices contain inherent limitations that restrict the realisation of user expectations in terms of performance:

- Visual output interface: Mobile devices have small screens, which inhibits optimal performance. Websites accessed via mobile devices are also often designed for desktop PCs.
- Input interface: Mobile devices have small keyboards or are reliant on haptic or touch input. Furthermore, business applications often require mouse input, a feature not common in mobile devices.
- Specifications: Mobile devices have a limited memory size, limited battery life and lower processor speeds than their desktop counterparts. These limitations are, however, increasingly addressed with the development of new devices (Gartner, 2012b; Sathyan et al., 2012; Unhelkar & Murugesan, 2010; Gansemer et al., 2007).

### 3.2.3 Connectivity

In the context of a mobile environment, connectivity refers to a user's ability to access data and functionality from any location. The inherent design of wireless networks, however, often creates a barrier to its performance, as wireless systems were traditionally not built for ubiquitous mobility or the delivery of critical IT services. They were initially intended to serve as temporary connectivity alternatives (Gartner, 2012a). In addition, the design of current wireless networks constitutes interconnected systems of physical and virtual servers, communication channels with mobile and fixed endpoints, as well as wired and wireless networks run by different organisations. The enterprise often does not own all of the components of its wireless system but still needs to ensure reliable service delivery and support (Gartner, 2012a). Infrastructure vendors have identified the challenges in building and maintaining wireless networks, but the solutions offered by these vendors often work in a siloed approach focusing on network policies and solutions per type of device. In a heterogeneous mobile environment, this provides a costly and complex solution to the problem (Aruba Networks, 2012).

The demands on wireless networks and bandwidth have increased with the growth in the number of connected devices, the prevalence of data-rich and real-time collaborative mobile applications as well as the increase in communication traffic (Cisco and Citrix, 2014; Gartner, 2012a). This creates bandwidth bottlenecks and unreliable networks. Other barriers to the delivery of reliable, high-performance connectivity include signal disturbances and interference, which

cause loss of connectivity and coverage dead zones (CDW, 2012; Sathyan et al., 2012; Deepak & Pradeep, 2012).

### 3.2.4 IT support

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

- the use of more than one device for both personal and corporate functionality;
- the use of various operating systems;
- the variety of mobile devices and related operational platforms;
- the frequency with which users upgrade or change devices;
- the users' expectations of instant service delivery; and
- the increase in required configuration, help-desk and network support (Cisco and Citrix, 2014; Aruba Networks, 2012).

In addition, mobile solution management is often outsourced to external service providers or vendors where the enterprise has insufficient internal resources or skills and the services are not aligned with the enterprise's specified requirements.

### 3.2.5 Continuity

Business continuity refers to the ability of an enterprise to continue its core business operations at an acceptable level during a time of interruption and disruption of services (ISO/IEC, 2012). Verizon (2008) identifies the six major IT threats to business continuity as hardware failure, software failure, security events, network transmission, change management error and human error. Three threats were considered relevant in a mobile environment:

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

Enterprise exposure to business continuity risk is further increased as traditional business continuity plans, involving off-site redundancy controls, are not appropriately revised to address the requirements of users and customers that expect real-time recovery and responses (Verizon, 2008).

### 3.2.6 Security

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

- Device loss or theft: Mobile devices are more susceptible to loss and theft than their desktop counterparts, and the security of data stored on the device is compromised. Device loss also leads to loss of critical data if it is not stored on corporate servers.
- Unauthorised data access and sharing: Where employees use one device for both personal and corporate use, seemingly authorised users may gain unauthorised access to data. Authorised users may also upload confidential data to cloud or website storage without enterprise knowledge or authorisation.
- Transmission of data: Mobile wireless networks are more vulnerable to malicious attack and interception than wired networks, and this affects both the confidentiality and integrity of data.
- Intentional security breaches: Much like desktop computers, mobile devices are exposed to malicious attacks such as viruses, malware, Trojan horses, malicious applications, spam, phishing, spoofing and worms. Mobile solutions, however, also introduce the following unique threats:
    - Device cloning: The electronic identity and information on a mobile device is cloned onto a second unofficial device.
    - Jailbreak software: Using specific coding, unauthorised access is gained to the device and all its content.
    - Keystroke logging: A type of malware is loaded onto the mobile device that records keystrokes to capture sensitive information.
    - Zero-day exploit: This attack takes advantage of security vulnerabilities on a mobile device before an update or patch is made available.
    - Bluetooth-based attacks: Bluebugging, bluejacking and blue snarling are examples of unauthorised access and the distribution of unsolicited messages using Bluetooth connections.
    - Wi-Fi sniffing: Data is intercepted while it is sent to or from a mobile device over a non-secure network.
    - Automatic connectivity: Mobile devices often have the capability to connect automatically to unknown Bluetooth devices in close vicinity or to unsecured Wi-Fi to create unsecure connections.
    - Man-in-the-middle attack: This attack intercepts and extracts information between two authorised users.
    - Eavesdropping: This is the process of intercepting voice transmissions or transactions and listening in without consent of the conversing parties.
    - Malicious applications: Applications on open platforms often have hidden functionality that harvest user data or act as hosting applications with administrative remote command execution capability.
    - Unauthorised location tracking: The positioning capabilities on mobile devices allow for the tracking of their location and content for malicious purposes.
- Gaps in security policy enforcement: The enforcement of security policies in a mobile environment is often inadequate, as mobile devices are often not present in order for security software to be loaded. The diverse landscape of mobile devices and operating systems and the rate of introduction of new devices create a challenge in their management. Furthermore, policy enforcement is complicated, as the applications used for the access, storage and

modification of business data have increased exponentially and each application includes its own distinct security protocols and data access capabilities.

- Outdated software: Old versions of mobile operating systems, plug-in software and application versions create a basic security risk on mobile devices. In BYOD environments, especially, it becomes impossible for enterprises to control whether users are running the latest versions of software and whether security patches and fixes are installed by the user (Blackberry, 2014; Akella et al., 2012; Ernst & Young, 2012; GAO, 2012; Sybase, 2011; Wright et al., 2011; Sathyan & Sadasivan, 2010; Unhelkar & Murugesan, 2010)

### 3.2.7 Cost

Deploying mobile solutions as part of an enterprise's operational activities may lead to significant cost implications for the enterprise:

- Device costs: In a COPE or COBO environment the enterprise carries the cost of investment in devices. In a BYOD environment the employee or user carries device cost, but other costs, identified below, are still influenced.
- Software costs: Software costs are increased by the cost of developing and maintaining applications, the cost of enabling mechanisms such as desktop virtualisation, and the cost of management software such as mobile device management systems.
- Connectivity costs: Bandwidth costs increase considerably in a mobile environment primarily due to an increase in network traffic. In addition, media rich applications and push delivery notifications cause further increases in connectivity costs.
- Infrastructure and operational costs: Mobile solutions require an investment in infrastructure modifications and upgrades as well as day-to-day costs to support and maintain operations. These costs include the cost of wireless networks, the expansion of data storage and transmission capacity, the management costs of devices and applications, IT support costs, and the cost of user self-support tools.
- Security costs: Mobile solutions introduce incremental security risks, and the costs to mitigate these risks include the costs of authentication and encryption software, content protection, containerisation of data as well as the resources employed in the management and monitoring of security risks. Security breaches also lead to costs such as data remediation and the possible loss of competitive advantage (Akella et al., 2012; Cisco IBSG, 2012; Gartner, 2012a; Sybase, 2011).

### 3.2.8 Data ownership

Data ownership refers to both the possession of and responsibility for data (Loshin, 2002). The responsibility for data assumes the control of data as an enterprise asset, and this includes the ability to access, modify, create, remove and sell data as well as the right to assign these abilities. Mobility creates uncertainty in both areas of data ownership, as corporate data is communicated, stored and accessed on devices not owned by the enterprise. The possession of the data is often not controlled, as data is easily and informally shared and used in a mobile environment. Rights to data use are also exercised without clear allocation of such rights (Oracle, 2014).

Intellectual property rights, similarly, have become unclear. Rights to content created on corporate devices are definite where employees create content on enterprise-owned devices. The enterprise had a valid claim to the content. The boundaries are, however, unclear in an

environment where content is created on personal devices outside of working hours (Madgwicks, 2012).

## 3.3 Less significant risks

In addition to the significant risks identified, enterprises need to be aware of other risks when mobile technology is deployed.

- Licensing: Software licensing may create exposure for enterprises where license terms apply only to corporate-owned or -leased devices and may not cover the use of applications across multiple mobile devices (Madgwicks, 2012).
- Litigation: Where personal mobile devices are used for corporate functionality, privacy and possible litigation risks exist with regard to corporate access to and control over employees' private information (Madgwicks, 2012). In addition, enterprises need to consider all relevant regulations in terms of data safeguarding, data storage, data structuring and data extraction contained in acts such as the Sarbanes-Oxley Act of 2002.
- Data retention: In mobile environments where corporate data is stored on personal or moving devices, enterprises may experience exposure in terms of regulations relating to the retention of corporate data (Madgwicks, 2012).

# 4. CONCLUSION

The consumerisation of mobile technology is driving the expansion of mobile solutions in business operations at an exponential rate. Due to the nature of mobile technology, significant new risks are being introduced into the business operations, and each component of the technology gives rise to specific risks. The objective of this research was to address this problem using a structured approach to identify the significant risks linked to each component of mobile technology. In order to achieve this, the research identified COBIT as the most appropriate control framework for the identification of significant risks in a mobile environment. The processes of COBIT were used to identify inadequate governance, interoperability, user experience, connectivity, IT support, continuity, security, cost and data ownership as the significant risks introduced by mobile technology. A study of literature defined each risk category and explained the specific vulnerabilities that enterprises are exposed to.

Each component of mobile technology implemented by an enterprise carries a particular risk profile, and the research focused on producing a matrix to identify mobile solution risks, given the specific mobility landscape of an enterprise. An area of future research is the application of the risk and component matrix to small and medium-sized entities to determine the practical results of its application. Another area of future research is the formulation of internal controls to address the significant risks identified.

## LIST OF REFERENCES

Akella, J., Brown, B., Gilbert, G. & Wong, L. (2012). *Mobility disruption: A CIO perspective.* Available: http://www.mckinsey.com/insights/business_technology/mobility_ disruption_a_cio_perspective. (Accessed 14 May 2013).

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

Aruba Networks. (2012). *Conquering today's bring-your-own-device challenges: A framework for successful BYOD challenges.* Available: http://www.arubanetworks.com/pdf/technology/whitepapers/WP_BYOD.pdf. (Accessed 26 February 2013).

Bai, C., Liu, Q., Lu, J., Song, F.M. & Zhang, J. (2003). Corporate governance and market valuation in China. *Journal of Comparative Economics, 32,* pp. 599-616.

Basole, R.C. (2007). *The Emergence of the Mobile Enterprise: A Value-Driven Perspective.* Sixth International Conference on the Management of Mobile Business, 9-7 July, Toronto, Canada. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber= 4278584. (Accessed 15 May 2013).

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

Bentley. (2013). *Interoperability Platform*. Available: ftp://ftp2.bentley.com/dist/collateral/Web/Platform/WP_Interop_Platform.pdf. (Accessed 22 July 2014).

Blackberry. (2014). *Making the case for COPE.* Available: http://us.blackberry.com/content/dam/blackBerry/pdf/business/english/Case-for-COPEWhitepaper.pdf. (Accessed 2 July 2014).

CDW. (2012). *Wi-Fi: Far and Wide.* Available: http://www.opus1.com/www/whitepapers/WirelessInfrastructure2012.pdf. (Accessed 8 May 2013).

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

Cisco and Citrix. (2014). *Cisco and Citrix for Productive and Secure Enterprise Mobility.* Available: http://www.cisco.com/c/dam/en/us/solutions/enterprisenetworks/mobile-workspace-solution/citrix-cisco-mobility-wp.pdf. (Accessed 2 July 2014).

Deepak, G. & Pradeep, B.S. (2012). Challenging issues and limitations of mobile computing. *International Journal of Computer Technology & Applications, 3(1)*, pp. 177-181.

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

ETSI. (2008). *Achieving Technical Interoperability – the ETSI approach.* Available: http://www.etsi.org/WebSite/document/whitepapers/IOP%20whitepaper%20Edition%203%20final.pdf. (Accessed 22 July 2014).

Fling, B. (2009). *Mobile design and development*. California: 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, Dortmund, Germany. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4488513. (Accessed 27 June 2014).

GAO. (2012). *Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged.* Available: http://www.gao.gov/assets/650/648519.pdf (Accessed 2 July 2014).

Gartner. (2012a). *Bring Your Own Device: New Opportunities, New Challenges.* Available: http://www.gartner.com/id=2125515. (Accessed 26 February 2013).

Gartner. (2012b). *Enterprise Mobility and Its Impact on IT.* Available: http://www.gartner.com/id=1985016. (Accessed 20 May 2013).

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

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

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

Institute of Directors Southern Africa (IODSA). (2009). *King Code of Governance for South Africa 2009.* Available: http://african.ipapercms.dk/IOD/KINGIII/kingiiireport/. (Accessed 7 July 2014).

ISACA. (2010). *Securing Mobile Devices.* Available: http://www.isaca.org/knowledgecenter/research/documents/securemobiledevices_whp_Eng_0710.pdf?id=. (Accessed 9 June 2014].

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

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

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

ISO 27001 Security. (2014). Available: http://www.iso27001security.com/. (Accessed 31 October 2014).

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

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

Juniper. (2009). *Open Source OS – The Future for Mobile?.* Available: http://www.juniperresearch.com/whitepaper/open-source-OS-the-future-for-mobile. (Accessed 17 July 2014).

Loshin, D. (2002). *Knowledge Integrity: Data Ownership.* Available: http://www.jbutler.biz/mis/Ownership.doc. (Accessed 4 August 2014).

Macehiter Ward-Dutton. (2005). *On IT-business alignment.* Available: http://www.mwdadvisors.com/asset/get_asset.php?id=1&file=alignment.pdf. (Accessed 18 June 2014).

Madgwicks. 2012. *Bring your own device.* Available: http://madgwicks.com.au/files/file/PUBLIC/News/Whitepaper%20%20BYOD%20%20September%2017%202012.pdf. (Accessed 26 February 2013).

Nicho, M. & Fahkry, H. (2011). An Integrated Security Governance Framework for Effective PCI DSS Implementation. *International Journal of Information Security and Privacy, 5(3),* pp. 50-67.

Oracle. (2014). *The New Perimeter: Keeping Corporate Data Secure in the Mobility Era.* Available: http://www.oracle.com/us/products/middleware/identity-management/ mobile-security/transformation-perimeter-wp-2199245.pdf. (Accessed 21 July 2014).

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

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

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

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

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

Verizon. (2008). *Business Continuity Management and the Extended Enterprise.* Available: http://www.verizonenterprise.com/resources/whitepapers/wp_ business-continuity-management-and-the-extended-enterprise_en_xg.pdf. (Accessed 12 August 2014).

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

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

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

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)*, pp. 12-21. Available: http://onlinelibrary.wiley.com/doi/10.1002/jcaf.20701/abstract. (Accessed 2 July 2014).

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