Journal of Economic and Financial Sciences
ISSN: (Online) 2312-2803, (Print) 1995-7076

Addressing the incremental risks associated with adopting Bring Your Own Device

Authors:
Lyle Weber[1]
Riaan J. Rudman[1]

Affiliation:
[1]School of Accountancy, Stellenbosch University, South Africa

Corresponding author:
Riaan Rudman,
rjrudman@sun.ac.za

Dates:
Received: 26 Apr. 2017
Accepted: 15 June 2017
Published: 16 Apr. 2018

How to cite this article:
Weber, L. & Rudman, R.J., 2018, 'Addressing the incremental risks associated with adopting Bring Your Own Device', *Journal of Economic and Financial Sciences* 11(1), a169. http://dx.doi.org/10.4102/jef.v11i1.169

Bring Your Own Device (BYOD) involves allowing employees to use their own mobile devices to access their organisations' networks. Many organisations are embracing this trend as a means to cut information technology (IT) expenditure, enhance employee satisfaction, etc. However, these and other benefits come at a cost in the form of exposing an organisation to new risks. The aim of this research was to assist organisations to identify the incremental risks they could potentially encounter if they implement a BYOD programme and how they can reduce the risks directly related to BYOD to an acceptable level. An extensive literature review was performed to identify the risks which arise as a result of the adoption of a BYOD programme. COBIT 5 was identified as the most appropriate framework which could be used to develop possible safeguards to mitigate the incremental risks associated with a BYOD programme to an acceptable level. Safeguards were developed to address the risks.

Introduction and research objective

What started several years ago with employees using their own personal computers to access their organisations' networks via dial-up and virtual private networks has changed dramatically in recent years. With the increased number of smartphones and tablet computers in the market place, more and more employees are using their personal mobile devices to connect to their organisations' networks. The concept where an employee uses his or her own personal mobile device to connect to the organisation's network is known as Bring Your Own Device (BYOD). It has been embraced by a large number of organisations of various sizes and in various sectors. Some employees use their mobile devices to perform basic tasks such as syncing their work emails and calendars with their mobile devices, whereas other employees use their mobile devices to perform specific work-related tasks such as compiling Excel spread sheets and accessing sensitive corporate data. This trend is driven by the number of mobile devices employees have access to. Gupta et al. (2013) indicated that global smartphone sales reached 225 million units in the second quarter of 2013. It is predicted that approximately 50% of all businesses will introduce a BYOD environment (Koh, Oh & Im 2014) and even though many organisations will not permit BYOD, employees will still use their own devices (Ogie 2016). Deloitte (2013) indicated that there are over 10 million active smartphones in South Africa. Although allowing employees to use their personal devices results in organisations deriving various benefits (such as cost savings and improved employee satisfaction, which result in increased productivity), it exposes an organisation to new risks. Failure by the organisation to implement sound internal controls and governance policies to address the risks could lead to the organisation suffering negative consequences. These consequences include, *inter alia,* significant financial losses as well as the leaking of sensitive client data into the public arena as a result of negligence or data theft. Sensitive data can also be leaked where malware infiltrates the network and corrupts the data or causes the information technology (IT) system to shut down.

The governance of the incremental risks related to BYOD should not only be of interest to those charged with governance of the organisation, but also to the external auditor. The auditor would need to understand which incremental risks have arisen as a result of the adoption of the BYOD programme because the control risk is no longer limited to the client's system, but each and every device connected to the network. An organisation that adopts or deploys a BYOD programme will be faced with increased incremental IT strategic and operational risks. These organisations will need to identify suitable internal controls in order to reduce the incremental risks to an acceptable level. The objective of this research is to develop a framework to identify and manage the incremental IT strategic and operational risks which arise when an organisation adopts a BYOD programme. The study will focus mainly on the incremental strategic risks and to a lesser extent on the incremental operational risks. This research will be of value to management, people

who are considering to adopt a BYOD programme, or are currently running a BYOD programme, as well as external auditors. It will assist in the understanding of the risk dynamics and how to mitigate the risks on devices not under the control of the organisation. The majority of the research conducted to date on BYOD programmes have investigated the benefits of adopting such programmes (Anderson 2014; Pelino 2012) and to a lesser extent the incremental risks associated with its implementation. Most of the research related to BYOD has been conducted by private organisations, such as IBM, Gartner, ISACA and Forrester. Prior academic research tends to focus on specific risks. Rose (2012) highlighted the security implications which arise as a result of BYOD. Markelj and Bernik (2012) indicated the threats that arise as a result of using mobile devices and the impact on corporate data security. Most of the research investigating the risks do so in an *ad hoc* manner, without relying on the available IT governance frameworks. A practical, integrated framework that will assist those charged with governance at the organisation to mitigate the risks associated with the adoption and deployment of a BYOD programme to an acceptable level has not yet been developed.

The research commences in the following section by describing the research methodology. The 'Literature review and findings' section contains an extensive literature review to identify the incremental IT strategic and operational risks which arise as a result of adopting a BYOD programme. It also presents the findings on the IT strategic and operational risks which arise when an organisation adopts a BYOD programme, as well as recommending mitigating controls. The 'Conclusion' section concludes the article.

Research methodology

As mentioned earlier, the aim of this research is to identify key internal controls and safeguards which an organisation can deploy by using the COBIT 5 framework as a basis to reduce the IT strategic and operational risks identified relating to BYOD to an acceptable level. The study is non-empirical in nature and the results drawn are from an extensive literature review that was performed on BYOD and the COBIT 5 framework. The following factors were considered whilst conducting the literature review:

- risks and concerns related to BYOD programmes
- compliance and legal considerations which arise as a result of BYOD
- the behaviour of employees whilst using their own devices
- implications of mobile devices being stolen or lost
- the control frameworks (including COBIT 5 framework).

In order to add scientific rigour to the literature review, a four-stage approach as suggested by Sylvester, Tate and Johnstone (2011) was followed. A wide range of articles and readings were selected at the beginning stages to enable a comprehensive understanding of the literature, and the selection was narrowed to more specific areas at a later stage in order to understand the concepts underlying BYOD, its underlying technologies, and to elaborate on the impact of BYOD on institutions locally and internationally. It will also be necessary in researching IT governance frameworks in order to select the most appropriate framework to be used as a benchmark. Following the literature review, the incremental IT strategic and operational risks were summarised in tabular format.

A control framework was used to identify controls because it provides structure to controls and ensures all applicable controls are identified. A control framework is a data structure that organises and categorises an organisation's internal controls, which are practices and procedures established to create business value and minimise risk (Rouse 2011). Some notable IT frameworks include Prince 2, Information Technology Infrastructure Library (ITIL) and COBIT 5. COBIT 5 was selected as the framework to identify appropriate safeguards to mitigate the risks. COBIT 5 is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. It provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT (ISACA 2012a). Stroud (2012) stated in a webinar conducted by ISACA that COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. The framework addresses both business and IT functional areas across an enterprise and considers the IT-related interests of internal and external stakeholders.

The processes underlying COBIT 5 were analysed (in the context of the literature review about BYOD performed) to determine which processes would be applicable to managing BYOD risks. The importance of each process was determined. Each applicable process was used to formulate appropriate controls that address the specific risk. COBIT 5 focuses on the following areas: governance and management. These two areas are divided into five domains. The evaluate, direct and monitor (EDM) domain addresses governance issues and provides organisations with guidance on how they should govern and manage their IT-enabled business investments. The management area contains four domains, which include the following:

- Align, plan and organise (APO): this provides guidance for planning and organising acquisitions which are made by the organisation.
- Build, acquire and implement (BAI): this provides guidance on the processes required to acquire and implement IT solutions.
- Deliver, service and support (DSS): this provides guidance for servicing and supporting IT solutions.
- Monitor, evaluate and assess (MEA): this provides directors with guidance on how they can monitor and evaluate the acquisition process and the internal controls which have been implemented. This will help ensure that acquisitions are properly managed and executed.

In order for an organisation to reduce identified risks to an acceptable level, it needs to implement internal controls.

Literature review and findings

Bring Your Own Device

Mobile devices (universal serial bus, tablet computers, laptops and smartphones) of all shapes and sizes have become a part of our daily lives. The concept of BYOD involves permitting an employee to connect his or her own personal mobile devices to the organisation's network and applications. The BYOD concept has been adopted by organisations, both governmental and non-governmental, of all sizes and across all industries (Burt 2011; Gatewood 2012; Willis 2013). Gupta et al. (2013) indicated that smartphone sales to end users have reached 225 million units in the second quarter of 2013 and Rohan (2013) stated that employees are using their personal mobile devices for official work purposes. If organisations do not support employees in their wish to use their own personal devices for work purposes, the employees may figure out ways to support their devices themselves. This will place sensitive corporate data at risk. It is therefore important that organisations enable employees to get their work done in the most appropriate manner without compromising the integrity of the data (Kanaracus 2012). Although it is not the purpose of this article to discuss the benefits associated with the adoption or deployment of a BYOD programme, a few benefits are listed. The benefits include, but are not limited to, the following:

- increase in productivity of employees (Anderson 2014; Pelino 2012)
- increased revenue (Pelino 2012)
- reduction in expenses for corporate-liable mobile device and data services (Pelino 2012).

Based on the above-mentioned benefits, it is understandable why many organisations would be inclined to opt for the adoption and deployment of BYOD programmes. It should however be noted that whilst the benefits are good, failure to consider the concerns and risks surrounding the adoption or deployment of a BYOD programme noted by industry experts could have dire consequences on the organisation. Several concerns and risks were identified during the extensive literature review, which arise as a result of an organisation deploying a BYOD programme. The concerns and risks identified have been classified as either strategic or operational in nature and have been discussed in sections 'Strategic incremental concerns and risks' and 'Operational concerns and risks'.

Strategic incremental concerns and risks

Malware

Malware enables hackers to steal passwords and in some cases even creates an opportunity for the hacker to take control of the organisations computer systems, including those that run smartphones and tablets (Staut 2012). With the BYOD concept being adopted on an increased basis by organisations across all business sectors, it comes as no surprise that many organisations are increasingly being affected by malware. This is because of the fact that there has been an increase in the amount of new malicious smartphone and tablet targeting software (Drew 2012; Kaspersky 2012; Lung Kao 2011; Ponemon Institute LLC 2012). The Ponemon Institute LLC (2012) indicated that traditional security solutions that most organisations employ, such as antivirus, firewalls and passwords, are not effective in stopping malicious or negligent employees of the organisation from deploying advanced malware into the organisation's computer systems. Users who access the Internet from their mobile devices are at constant risk of exposure to web-based threats, including data stealing malware. When a device downloads a new mobile application from any online application store, the software may contain malware that can steal or damage data on the device and, in some cases, even disable the mobile device itself (CISCO 2013). According to the CISCO survey results, 69% of BYOD users were using unapproved applications on their devices, which is difficult to detect (CISCO 2012). The recent increase in Android malware magnifies this problem (CISCO 2012). If an organisation fails to have proper internal controls in place to manage the risks associated with malware, the organisation could find itself being the target of some or other malicious malware attack which could have a disastrous impact on the organisation.

Data leakage

Each organisation has different types of data which they deal with on a daily basis. Some data types are more sensitive than others; for example, documents containing trade secrets or confidential client information would be more important than the organisations policy on whistle blowing. The risks associated with data leakage on mobile platforms have become a bigger problem than malware (Willis 2013). It is for this reason that organisations should be interested in safeguarding their data in order to prevent unauthorised individuals from gaining access to what could be seen as their most important asset. If an organisation has deployed a BYOD programme, there is a high probability that employees will sync their mobile devices with their home computers (Ogie 2016). This increases the risk of data leakage as the employee's home computer may already be infected with malware such as Trojan horses and spyware which would compromise the security of corporate data. If the employee's home computer has any unpatched vulnerabilities, this will grant cybercriminals the ability to gain access to the mobile data that has been backed up, stored or synced onto the employee's home computer (Kaspersky 2012).

Willis (2013) stated that most mobile devices are designed to share data via the cloud. Rouse (2010) indicated that cloud computing involves delivering hosted services over the Internet. Whilst Cloud-based sharing and storage of personal data is convenient, employees may forward sensitive documents and presentations relating to the organisation to their personal emails like Google Mail or file storage services like Dropbox so that they can access the information on their mobile device at a later stage.

This would create a 'shadow infrastructure' over which the organisation will have little to no control and will result in a direct increase in the risk of data leakage taking place (Anderson 2014; IBM 2011; Zahadat et al. 2015). The Ponemon Institute found the average organisational cost of a data breach increased to $7.2 million and cost companies an average of $214 per compromised record (IBM 2012). Failure on behalf of an organisation to safeguard their data through the implementation of proper internal controls could result in the organisation not only suffering legal action and huge financial losses, but depending on the extent of the breach, it could also cause irreparable damage on the organisation's ability to continue in the future.

Theft or loss of mobile devices

Mobile devices are popular amongst individuals of all ages. These devices are generally compact in nature, yet they have the ability to be used to perform tasks similar to most personal computers. It should come as no surprise that in a report prepared by IBM (2011) as well as research conducted by Markelj and Bernik (2012) that the most frequently seen mobile device security threats are the loss and the theft of these devices. The loss of a personal smartphone or tablet on which an employee has downloaded confidential data of the organisation creates an opportunity for a criminal to access the organisation's confidential information. This represents a serious security risk for the organisation (Kaspersky 2012). This is especially the case where the employee has not followed basic security practises such as locking the device with a strong password and encrypting sensitive data transmitted to and from the mobile device (Staut 2012). Mobile data-bearing devices that were lost or stolen may contain sensitive or confidential information (Drew 2012; Ponemon Institute LLC 2012). The data stored on the device may be compromised if access to the device or the data is not effectively controlled (Evangelista 2014). The risk of unauthorised access to the data is further increased as most organisations do not have the ability to remotely wipe a device if a smartphone is lost or stolen. Most employees do not know what to do if their device was lost or stolen (Rose 2012). It is for this reason that users of mobile devices need to take some form of precautionary measure to ensure that they too do not form part of the population of individuals who have lost their mobile device or have had it stolen from them.

Connectivity of the device (Bluetooth and Wi-Fi)

Mobile devices offer broad Internet and network connectivity through varying channels including, but not limited to, Bluetooth and Wi-Fi technology. Anderson (2014) stated that when an authenticated device has other devices tethered to it, it may be possible for non-authenticated devices and users to gain access to the corporate network by connecting through the authenticated device. The threat to the corporate network is further increased as Bluetooth and Wi-Fi technology can be easily exploited to infect a mobile device with malware or compromise transmitted data (IBM 2011). When a Bluetooth device is set on discoverable mode, it makes it very easy to scan for the device using a computer. Once the computer is connected to the device, it is able to download the private data located on the device (CISCO 2013). Users who make use of Bluetooth and Wi-Fi technology to connect to the Internet or to share information should be mindful that these channels may not be as safe as what they may have originally thought.

Web-based applications

Web-based applications are quite often designed by individuals who the owner of the mobile device may not know personally. Mobile device users normally download applications which are of interest to them onto their mobile devices. There are more than 700 000 apps in the Apple App Store and more than 700 000 apps in the Android Marketplace (Tibken 2012). When a device downloads a new mobile application from any online application store, the software may contain malware that can steal or damage data on the device and, in some cases, even disable the mobile device itself. It is not possible for application store owners to conduct in-depth code reviews of all applications (IBM 2011; 2012). Anderson (2014) indicated that individuals are more than likely to use their personal mobile devices to access both personal and business applications. An IBM survey conducted on several hundred of their employees revealed that many of their employees were completely unaware which popular apps were security risks (Rose 2012). The risks are further increased by the recent increase in Android malware (CISCO 2012). Web-based applications can therefore cause a substantial amount of damage to the organisations' IT infrastructure if the use of these applications is not properly controlled.

Compliance with laws and regulations governing the organisation

Complying with the laws and regulations governing the industry and geographical region in which an organisation locates should always be a priority for any organisation. Failure to adhere to laws and regulations affecting the organisation could result in the organisation being liable for large fines or penalties for breach of the relevant laws and regulations. McQuire (2012) indicated that organisations operating in highly regulated industries cannot afford any compromise to customer data records or the compliance requirements governing these industries. McQuire (2012) stated that in certain countries like Germany, the federal law concerning data protection stipulates that German company data must reside in Europe. *Protection of Personal Information Act* in South Africa and *Sarbanes-Oxley Act* when dealing with South African subsidiaries in a New York Stock Exchange-listed holding company have significant regulatory implications in this regard (Swanepoel 2015). Research conducted by Vodafone (2012) indicated that it is important that organisations ensure regulatory compliance, especially where employees are permitted to run corporate email on their devices, as this may be subject to some form of communication regulations. They also noted that it is more difficult to ensure compliance where the organisation does not own the device. Where an employee uses software

purchased for their personal mobile devices under 'personal use' licenses for business purposes, the organisation may not be complying with the rules governing the use of the software and may be liable for the additional costs (O'Brien 2013). There is a possibility that it will be more challenging for organisations to ensure that they are complying with the rules and regulations affecting them in the future. This is especially true with the constant technological advancements taking place and the manner in which data are shared and transferred from one device to another.

Obsolescence

New mobile devices are released into the market on a regular basis. The manufacturers of these devices have done a great job in convincing individuals to upgrade from their existing devices, even though the new devices may not offer much more than the user is currently receiving from their existing devices. Entner (2011) indicated that of the 14 countries which he investigated to determine handset replacement lifecycles, South Africans took 38.2 months before buying a new mobile telephone. The research indicated that the handset replacement lifecycle for South Africans in the previous year was 46.3 months. The most common practice with mobile phone companies is to have a new model or an updated model every year. Stylistic obsolescence is one of the driving phenomena that is occurring (particularly) in the mobile phone industry (Keeble 2013; Maycroft 2009). If employees continue to upgrade their devices on a regular basis, it will have a direct impact on the IT department. They may not be able to cope with the regular upgrades and they may not be able to identify the risks associated with all the new devices being deployed into the system.

Operational concerns and risks

The tasks performed by employees in IT departments at organisations have changed substantially over the past decade. In the past these employees were mainly responsible for configuring, installing, maintaining and operating the hardware and software used by employees at the organisation's offices. Many organisations deployed corporate-owned palmtop-computers and Blackberry or mobile devices to key individuals within the organisation during the early to mid-2000s. The configurations of these devices were generally straightforward. The devices were used primarily to send emails and retrieve key documents and presentations. With the deployment of these devices, it meant that the employees in the IT department needed to gain an understanding on how these devices function. In the past 2–3 years, with increased popularity of individuals wanting to use their own mobile devices to access sensitive information relating to the organisation, the role of IT employees has expanded yet again.

The security of mobile devices has become a top concern for many IT executives (IBM 2011). The concern is further increased as the number of mobile devices coming in the next few years will outstrip IT's ability to keep the enterprise secure (Klossner 2012). Kaspersky (2012) and Staut (2012) indicated that the average employee uses more than one mobile device to access the corporate network. Bring Your Own Device therefore brings IT and security departments the challenge of having to implement and manage mobile security across an almost limitless range of devices and operating systems.

Rose (2012) stated that IT departments now have the responsibility of managing and securing a wide range of mobile devices that could be used to access their organisations' corporate data. Rose further stated in the same article that research conducted by Forrester indicates that employees choose their own smartphones 70% of the time, with 48% of the devices picked without regard for IT support. Anderson (2014) stated that devices are evolving so rapidly that it is impractical to pre-approve each and every device brand and form factor. He also indicated that it was somewhat impractical to expect IT organisations to have the same level of support for each and every device that employees may bring to the workplace.

Employees' mobile devices which have not been configured and locked down by the company IT department create the opportunity for infiltration of malware, gaps in the firewall and exfiltration of sensitive data (Mansfield-Devine 2012). The risk is further increased as some corporations intentionally have open ports so that their employees can work in virtual environments. This is an opportunity for anyone on the Internet who wishes to access a corporation's information system in an unauthorised manner (Markelj & Bernik 2012). Bring Your Own Device has changed the manner in which IT departments now function. They are now required to have detailed knowledge of various mobile devices which employees could use to access the organisation's network.

Bring Your Own Device information technology strategic and operational risks and concerns

These key risk areas can be subdivided further. Table 1 lists the risks and concerns related to BYOD, which have been identified during the extensive literature review, as well as the sources used to identify the risks. The risks were identified performing a systematic literature review. The list of references is not exhaustive.

The risks identified in Table 1 need to be reduced to an acceptable level. This is best done by using an appropriate control framework to identify key controls which can be deployed.

Identification of applicable COBIT 5 processes which affect Bring Your Own Device programmes

Organisations can customise COBIT 5 to suit their own context. Table 2 lists the processes that are directly applicable to an organisation that has deployed a BYOD programme. It highlights the 37 COBIT 5 processes that are applicable to BYOD. The description column gives a detailed listing of what each process means. The definitions of the processes

TABLE 1: Detailed Bring Your Own Device risks and concerns.

Number	Summarised risk/concern	Description of risk/concern	Source
1. Malware			
1.1	Deployment of malware into an organisation's system.	There is a risk that employees may purposefully or negligently deploy malware into the organisation's computer system which may result in unauthorised access to sensitive information.	Ogie 2016; Ponemon Institute LLC 2012
1.2	Malicious software targets smartphones and tablets	There is a risk that new malicious software will target smartphones and tablets.	Drew 2012; IBM 2011; Kaspersky 2012; Ponemon Institute LLC 2012
1.3	Hackers' ability to control computer systems.	There is a risk that hackers will use malware to steal passwords of mobile device users and take control of the organisation's computer systems (including smartphones and tablets).	Staut 2012
1.4	Data stolen or damaged	There is a risk that data on the user's mobile device may be stolen or damaged by malicious malware.	CISCO 2013
1.5	Device disabled	There is a risk that malware may disable the users' mobile devices, resulting in the inability to perform tasks.	CISCO 2013
1.6	Use of unapproved applications.	There is a risk that users of mobile devices may be using unapproved applications on their devices, which may expose the organisation to malware attacks.	CISCO 2012
2. Data leakage			
2.1	Data leakage is a great problem.	There is a risk that data leakage problems may occur at the organisation.	Ogie 2016; Willis 2013
2.2	Employees sync mobile device with infected home computer.	There is a risk that employees will sync their mobile devices which they use to access the organisations network to their home computers, which may be infected with malware.	Kaspersky 2012
2.3	Unpatched vulnerabilities on home computer grant cybercriminals access to sensitive data.	There is a risk that unpatched vulnerabilities on the employees' home computer will grant cybercriminals the ability to gain access to the sensitive mobile data that have been backed up, stored or synced onto the employee's home computer.	Kaspersky 2012
2.4	Loss of control over data stored in the Cloud.	There is a risk that data shared and stored via a Cloud may result in the organisation having a shadow infrastructure where they have little to no control of the data.	Anderson 2014; IBM 2011
2.5	Unauthorised access to sensitive data.	There is a risk that data stored in the Cloud may be accessed by unauthorised individuals.	Anderson 2014; IBM 2011
2.6	Potential financial loss as a result of data breach.	There is a risk that a data breach could be financially costly for the organisation.	IBM 2012; Koczerginski 2015
3. Loss and theft			
3.1	Lost mobile devices create a security threat.	There is a risk that mobile devices which have been lost may contain confidential corporate information and this will create a serious security threat to the organisation.	Kaspersky 2012
3.2	Criminals may gain access to confidential information.	There is a risk that criminals may access confidential information relating to the organisation from a stolen smartphone or tablet.	Staut 2012
3.3	Information may not be password protected.	There is a risk that information on an employee's smartphone or tablet which has been lost or stolen may not be password protected and may result in unauthorised access to confidential information.	Ponemon Institute LLC 2012; Staut 2012
3.4	Data may not be encrypted.	There is a risk that the confidential corporate-related data transmitted to and from the employees' mobile device may not be encrypted and may therefore be accessed by unauthorised individuals.	Staut 2012
3.5	Mobile devices are easily stolen as a result of size.	There is a risk that mobile devices may be easily stolen as a result of these devices generally being small in size.	Markelj and Bernik 2012; Ogie 2016
3.6	Data on mobile device which has been lost or stolen may be compromised.	There is a risk that all of the data stored on a mobile device which has been lost or stolen may be accessed by unauthorised individuals if access to the mobile device or the data is not effectively controlled.	Evangelista 2014
3.7	Lost or stolen mobile devices may have personally identifying and confidential client information on it.	There is a risk that a lost or stolen mobile device may contain personally identifying or confidential client information on the device.	Drew 2012; Koczerginski 2015
3.8	Organisation cannot remotely wipe lost mobile device.	There is a risk that the organisation does not have the ability to remotely wipe a device if a smartphone is lost or stolen.	Rose 2012
3.9	Employees do not know what to do when their device is lost or stolen.	There is a risk that as a result of employees not knowing what to do if their device was lost or stolen that unauthorised individuals may gain access to sensitive corporate information.	Rose 2012
4. Connection			
4.1	Bluetooth device may be discoverable.	There is a risk that the Bluetooth on the mobile device on which sensitive corporate data are stored is set on discoverable mode which may grant unauthorised individuals access to the data.	CISCO 2013
4.2	Unauthorised data downloads.	There is a risk that an unauthorised individual may connect to the mobile device and download the private data from it.	CISCO 2013
4.3	Non-authenticated devices connecting to network.	There is a risk that non-authenticated devices may gain access to the organisation's network by connecting through an authenticated device.	Anderson 2014
4.4	Bluetooth and Wi-Fi technology are easily infected.	There is a risk that Bluetooth and Wi-Fi technology can be easily infected with malware which may result in the organisations' network also being infected.	IBM 2011
4.5	Data transmitted may be compromised.	There is a risk that the data transmitted via Bluetooth or Wi-Fi technology are compromised.	IBM 2011
5. Web-based applications			
5.1	Applications downloaded may steal or damage data.	There is a risk that applications downloaded may contain malware which may steal or damage company data stored on the mobile device.	IBM 2011, 2012
5.2	Unapproved applications may be stored on mobile devices.	There is a risk that unapproved applications on employee mobile devices may contain malware.	CISCO 2012
5.3	Unapproved applications may not be easily detectable	There is a risk that the unapproved applications may not be easily detectable and thus may result in malware entering the organisation's system undetected.	CISCO 2012
5.4	Employees unaware of risky applications.	There is a risk that employees are unaware of which popular applications are security risks, which may result in the employee downloading a malicious application that may infect the organisation's system.	Rose 2012

Table 1 continues on the next page →

TABLE 1 (Continues...): Detailed Bring Your Own Device risks and concerns.

Number	Summarised risk/concern	Description of risk/concern	Source
6. Compliance			
6.1	Organisation may not be complying with laws and regulations.	There is a risk that corporate data stored on the employees' mobile devices may be compromised, which could result in the organisation not complying with the laws and regulations affecting the industry in which the organisation operates.	McQuire 2012; Ogie 2016
6.2	Organisation may be unaware of specific geographical laws and regulations.	Certain geographical regions have unique laws and regulations such as the data protection laws in Europe which states that data must reside in Europe. The risk is that an employee may download sensitive corporate data onto their mobile device and leave Europe with the sensitive data on the device, resulting in the organisation not complying with the relevant laws and regulations.	McQuire 2012
6.3	Communication laws may be violated.	There is a risk that organisations may not comply with communication laws. This would arise where employees are not permitted to transfer corporate data to their personal devices.	Vodafone 2012
6.4	Organisations may not be able to ensure compliance on employee-owned devices.	There is a risk that the organisation may not be able to ensure regulatory compliance in instances where the organisation does not own the mobile device.	Vodafone 2012
6.5	Personal use software may be used for business purposes.	There is a risk that an employee may be using software on a mobile device designated under a personal use license for business purposes, resulting in the organisation contravening the terms of use of the software.	O'Brien 2013
6.6	Potential additional costs to be incurred by organisation.	There is a risk that the organisation may be liable for the additional costs where employees have breached software license agreements.	O'Brien 2013.
7. IT support			
7.1	IT may not be able to manage all mobile devices.	There is a risk that IT may not be able to manage the wide range of mobile devices which the employees of the organisation use to access sensitive corporate data.	Rose 2012
7.2	IT may not be able to secure all mobile devices.	There is a risk that IT may not be able to secure all of the mobile devices which the employees of the organisation use to access sensitive corporate data.	Klossner 2012; Rose 2012
7.3	IT may not be able to successfully implement mobile security.	There is a risk that IT and security departments may not be able to successfully implement mobile security as a result of the almost limitless range of devices and operating systems being used in the organisation.	Kaspersky 2012; Staut 2012
7.4	Employees may select a device without considering IT support.	Employees at the organisation may choose a mobile device without regard for IT support. The risk is that the IT department may not be able to assist employees when their devices are down and this will affect the employees' productivity and ability to complete their work-related tasks.	Rose 2012
7.5	Employees' mobile devices may not be configured or locked down.	There is a risk that employees' mobile devices that are not configured and locked down by the IT department will result in an infiltration of malware and an exfiltration of sensitive corporate data.	Mansfield-Devine 2012
7.6	IT may not pre-approve all mobile devices.	There is a risk that employees may use devices to access sensitive corporate data which has been determined by the IT department as devices which expose the organisation to security risks.	Anderson 2014
7.7	IT may not be able to provide same level of support to all mobile devices.	There is a risk that IT may not be able to provide the same level of support for each and every device that employees bring to the workplace. This may result in the employee not being able to perform their work-related tasks in an effective and efficient manner.	Anderson 2014
7.8	The organisation may leave certain network ports open for ease of connection for employee-owned devices.	There is a risk that the organisation has open ports for employee-owned mobile devices. This may create an opportunity for anyone on the Internet to access a corporation's information system unauthorised.	Markelj and Bernik 2012
8. Obsolescence			
8.1	Mobile device life cycle may shorten.	The mobile device life cycle may shorten. The risk is that the organisation may not be able to keep abreast with all the new devices being used by their employees and this may result in the risks associated with these devices not being adequately and timely addressed.	Entner 2011; Ogie 2016
8.2	Mobile devices may have planned obsolescence built into them.	Manufacturers of mobile devices have planned obsolescence built into their devices. The risk is that the organisation may not be able to keep abreast with all the new devices being used by their employees and this may result in the risks associated with these devices not being adequately and timely addressed.	Keeble 2013; Maycroft 2009

IT, information technology.

were obtained from COBIT 5 Enabler processing guide (ISACA 2012b). A brief explanation as to why a process was considered applicable or why in certain instances a certain process was not applicable for the purpose of this research has been included in the table under the column 'Explanation'.

Figure 1 maps the COBIT 5 processes, which have been identified as being relevant for the purposes of this research, to the risks identified in Table 1. Using these processes to identify possible safeguards, the organisation can reduce the risks to an acceptable level. Many organisations that employ BYOD programmes do not know the number nor do they know which devices are connected to their networks, and many do not have controls in place to mitigate the risks. At governance level, management should identify and take ownership of the risks associated with BYOD. This begins by developing a BYOD strategy as part of its business model, which addresses the challenges related to BYOD; mobile device management and mobile security and access control. A policy should be developed detailing accepted usage of mobile devices, acceptable user behaviour and governing the use of corporate and other third-party applications. Information technology departments should have a clear project plan and should work with end users to implement BYOD. A compliance officer should monitor compliance with the plan and policy as well as regulatory requirements affecting data security, which will improve logging, monitoring and follow-up of access to the enterprise's information systems and data.

Users should be educated on BYOD, its associated risks and accepted usage policies. Support services should also be made available. The IT departments should focus on access security and data protection by doing the following:

TABLE 2: COBIT process selection.

Processes		Relevant to BYOD	Applicable to research	Explanation
Evaluate, direct and monitor				
EDM01	Ensure governance framework setting and maintenance	Yes	Yes	It is important that the organisation adopts a BYOD programme if it assists the organisation in achieving its business imperatives. Once it has been determined that BYOD will add value to the organisation, it is important that proper structures, processes and practices are put in place in order to ensure that the business imperatives are met and that any risks associated with deploying a BYOD programme are reduced to an acceptable level.
EDM02	Ensure benefits delivery	No	No	The employee is primarily responsible for investment in the mobile device which is used to access personal and corporate information.
EDM03	Ensure risk optimisation	Yes	Yes	Prior to deciding to launch a BYOD programme, it is important that those charged with governance at the organisation first identify the entity-specific risks that they will be exposed to as a result of adopting the BYOD programme and they should determine to what extent they would like to be protected from these risks as this will assist them in determining what controls they should be implementing.
EDM04	Ensure resource optimisation	Yes	Yes	In order to successfully run a BYOD programme, the organisation needs to ensure the IT department has the necessary knowledge, skills and time available to properly manage and support the BYOD programme.
EDM05	Ensure stakeholder transparency	No	No	It is not necessary to report to the outside stakeholders on the successful adoption or running of the BYOD programme.
Align, plan and organise				
APO01	Manage the IT management framework	Yes	Yes	The adoption of a BYOD programme and the running thereof should be to support the overall governance objectives of the organisation.
APO02	Manage Strategy	Yes	No	The BYOD programme would be a current initiative which the organisation has adopted. Whilst it may be a current business strategy of the organisation, it was not included as part of the focus of this research.
APO03	Manage enterprise architecture	Yes	No	Whilst having proper architectures in place to govern the BYOD programme adopted by an organisation is important, it was not included as part of the focus of this research.
APO04	Manage innovation	Yes	Yes	BYOD is an innovative business trend. There are lots of benefits which the organisation can obtain through the successful implementation of a BYOD programme.
APO05	Manage portfolio	No	No	Whilst BYOD may form part of the overall investment or related portfolios of the organisation, it was assumed that the BYOD programme was a priority for the purpose of this research and hence no adjustments needed to be made.
APO06	Manage budget and costs	Yes	Yes	The organisation needs to identify that there is a financial benefit which they can derive before adopting a BYOD programme. Whilst this is important, it was not included as part of the focus of this research.
APO07	Manage human resources	No	No	BYOD should not directly impact the management of human resources at the organisation. Whilst the skill and ability of the IT department need to be considered when adopting a BYOD programme, it was not included as part of the focus of this research.
APO08	Manage relationships	Yes	No	Whilst the relationship between those employed in the operational side of the organisation and the IT side of the organisation is important, the quality of their relationship was not included as part of the focus of this research.
APO09	Manage service agreements	Yes	No	It is important that the organisation first identifies its business imperatives. If it was concluded that the adoption of the BYOD programme would assist in the achieving of the organisation's business imperatives, then the BYOD programme should be adopted. The consideration of whether or not a BYOD programme would assist the organisations in achieving their business imperatives was not included as part of the focus of this research.
APO10	Manage suppliers	No	No	The adoption of a BYOD programme does not involve the supply of any goods or services by outside suppliers directly to the organisation. The employee deals with the supplier of the mobile device.
APO11	Manage quality	Yes	No	Defining the communication of quality requirements in all processes and procedures is of key importance for every organisation. The defining and communication of BYOD processes was however not included as part of the focus of this research.
APO12	Manage risk	Yes	Yes	It should be a priority for the organisation to continually identify, assess and reduce the risks that arise as a result of the adoption of a BYOD programme. Failure to do so could have adverse consequences on the organisation.
APO13	Manage security	Yes	Yes	Security of the corporate information should be a priority at all times. The safety of information is definitely a concern in a BYOD as a result of cyber theft.
Build, acquire and implement				
BAI01	Manage programmes and projects	Yes	No	The BYOD programme needs to be managed as one of the organisation's programmes. The management aspect of a BYOD programme was however not included as part of the focus of this research.
BAI02	Manage requirements definition	Yes	No	It is essential that the organisation first conducts a detailed analysis as to whether or not a BYOD programme will assist it in the achievement of its business imperatives. The pre-adoption analysis of a BYOD programme and the feasibility thereof was however not considered as part of this research.
BAI03	Manage solutions identification and build	Yes	No	The deployment of a BYOD programme may be one of the solutions which an organisation could employ in order to achieve its business imperatives. This was however not considered as part of this research.
BAI04	Manage availability and capacity	Yes	No	The availability of enough skilled IT staff to support a BYOD programme may be something that an organisation should be interested in. It was however not considered as part of this research.
BAI05	Manage organisational change enablement	Yes	No	The adoption of a BYOD programme for the very first time by an organisation will definitely affect all the stakeholders in the organisation. The first time adoption of a BYOD programme at an organisation was however not considered as part of this research.
BAI06	Manage changes	Yes	No	The initial adoption of a BYOD programme by an organisation will definitely require significant attention. It would be a change from the normal way of accessing and processing sensitive corporate information. The initial adoption of a BYOD programme at an organisation was however not considered as part of this research.
BAI07	Manage change acceptance and transitioning	Yes	No	The initial period from pre-adoption to initial adoption of the BYOD programme needs to be planned successfully to ensure that all significant risks have been identified and that sensitive corporate data are safeguarded at all times. The initial adoption of a BYOD programme in an organisation was however not considered as part of this research.
BAI08	Manage knowledge	Yes	No	It is important that the IT department has the relevant skills in order to manage and support a BYOD programme. The maintenance of knowledge to be able to do so successfully was however not considered as part of this research.
BAI09	Manage assets	Yes	Yes	The organisation does not own the mobile devices being used to access the organisation's sensitive information. The IT department however should be in a position where they are able to assist the users of the mobile devices with certain technical issues that arise with the devices. It is also extremely important that software licenses of these devices are understood as the organisation may be in breach if the employee uses software on the mobile device for business purposes when in fact it is a personal use software license which the employee possesses.
BAI10	Manage configuration	Yes	No	It is extremely important that the configurations of all devices connecting to the organisation's network are defined and maintained. This is applicable in a BYOD environment as devices will be connecting to the organisation's network. Defining and maintaining descriptions and relationships of resources and capabilities required by IT-enabled services was however not considered as part of this research.

Table 2 continues on the next page →

TABLE 2 (Continues...): COBIT process selection.

Processes		Relevant to BYOD	Applicable to research	Explanation
Deliver, service and support				
DSS01	Manage operations	Yes	Yes	The execution of IT procedures effectively in managing and securing mobile devices is essential to ensure the safeguarding of sensitive corporate information.
DSS02	Manage service requests and incidents	Yes	Yes	The IT department should be in a position to assist the mobile device user with support with troubleshooting required by the user, which will enable them the ability to access and process work-related activities on their mobile devices.
DSS03	Manage problems	Yes	Yes	
DSS04	Manage continuity	Yes	No	It is important that the organisation has a plan in place for incidents such as mobile device or Wi-Fi downtime as this will disrupt the organisation's ability to function properly. The establishment and maintenance of a plan of this nature was however not considered as part of the research conducted.
DSS05	Manage security services	Yes	Yes	It is essential that the organisation conducts a proper risk analysis (which will include security-related risks) in relation to the adoption of a BYOD programme.
DSS06	Manage business process controls	Yes	Yes	Once the risk analysis has been conducted, it is important that the organisation identifies suitable controls which will reduce the risks to an acceptable level.
Monitor, evaluate and assess				
MEA01	Monitor, evaluate and assess performance and conformance	Yes	No	It is essential that the success of the BYOD programme, control environment and the controls affecting the BYOD programme should be monitored on a regular basis. Failure to do so could result in the organisation suffering major losses (e.g. data theft). The monitoring of the success of the BYOD programme and controls affecting the BYOD programme was however not considered as part of this research.
MEA02	Monitor, evaluate and assess the system of internal control	Yes	No	
MEA03	Monitor, evaluate and assess compliance with external requirements	Yes	Yes	It is essential that the organisation evaluates whether or not it is complying with the rules and regulations affecting the organisation. This is especially true in a BYOD environment where different industries and different geographical regions have different rules and regulations which govern them. The organisation should map the risks and controls identified to reduce the risks to an acceptable level.

BYOD, Bring Your Own Device; IT, information technology; MEA, Monitor, evaluate and assess; DSS, Deliver, service and support; BAI, Build, acquire and implement; APO, Align, plan and organise; EDM, Evaluate, direct and monitor.

FIGURE 1: Mapping risks to possible safeguards.

Number	Summarised risk identified	EDM01	EDM03	EDM04	APO01	APO12	APO13	BAI09	DSS01	DSS02	DSS03	DSS05	DSS06	MEA03	Possible safeguard
1.1	Deployment of malware into Organisation's system.	■	■		■	■	■					■			1.1.1 The organisation should have a policy stating that mobile device users are only able to connect to the network if they have installed anti-malware software. 1.1.2 The anti-malware software should be updated on a regular basis.
1.2	Malicious software targets smartphones and tablets.	■	■		■	■	■					■			1.2.1 Employees should be educated about what impact malware could have on the organisation's sensitive data as well as the manner in which malware infiltrates the device. [Refer to 1.1.1 and 1.1.2].
1.3	Hackers' ability to control computer systems.	■	■		■	■	■					■			1.3.1 The organisation should encrypt their data. 1.3.2 The organisation should have strong authentication methods in place to access the network. An example of this will include the use of tokens. 1.3.3 Unauthorised devices which have been detected by the network access control software should block these devices immediately.
1.4	Data stolen or damaged.	■	■		■	■	■					■			[Refer to 1.3.1 and 1.3.2].
1.5	Device disabled.	■	■		■	■	■					■			[Refer to 1.1.1, 1.1.2 and 1.2.1].
1.6	Use of unapproved applications.	■	■		■	■	■					■			1.6.1 The organisation needs to have a policy stating which applications employees are permitted to download onto their devices. The policy should be updated on a regular basis to take into account the new malicious applications that have been brought to the attention of the IT department. 1.6.2 The organisation could have a policy where they do spot-checks on the mobile devices used by their employees. Where unapproved applications have been identified, the owner of the device should be requested to delete the application immediately.
2.1	Data leakage is a greater problem than malware.	■	■		■	■	■					■			2.1.1 Employees should be educated about the impact that data leakage could have on the organisation and how it occurs.

Figure 1 continues on the next page →

FIGURE 1 (Continues...): Mapping risks to possible safeguards.

Number	Summarised risk identified	EDM01	EDM03	EDM04	APO01	APO12	APO13	BAI09	DSS01	DSS02	DSS03	DSS05	DSS06	MEA03	Possible safeguard
2.2	Employees sync mobile device with infected home computer.														2.2.1 Employees should be educated about the risks involved with syncing their mobile device with their home computer. 2.2.2 The employee should be advised to run their antivirus software on a regular basis.
2.3	Unpatched vulnerabilities on home computer grant cybercriminals access to sensitive data.														2.3.1 The organisation should invest in on-device containerisation technology. 2.3.2 The organisation should consider making use of a virtual desktop environment. [Refer to 1.3.1].
2.4	Loss of control over data stored in the Cloud.														2.4.1 The organisation should provide employees with a convenient method of securely sharing documents and collaborating on mobile devices.
2.5	Unauthorised access to sensitive data.														2.5.1 Employees should be educated about the risks involved with storing confidential data in the Cloud. [Refer to 1.3.1].
2.6	Potential outflow of finances as a result of data breach.														2.6.1 The organisation should have sufficient insurance to cover any financial outflows that arise as a result of data breach.
3.1	Lost mobile devices create a security threat.														3.1.1 The organisation can use remote wiping facilities to delete all organisation-related information that is stored on the device. [Refer to 1.3.1].
3.2	Criminals may gain access to confidential information.														[Refer to 1.3.1 and 3.1.1].
3.3	Information may not be password protected.														3.3.1 Employees should be educated about the advantages and disadvantages of not having a secure password on their mobile device. [Refer to 1.6.2].
3.4	Data may not be encrypted.														3.4.1 The organisation should have a policy that all data transmitted to employee's mobile devices should be encrypted at all times.
3.5	Mobile devices are easily stolen as a result of size.														3.5.1 Employees should be encouraged to be mindful of the whereabouts of the mobile devices at all times. 3.5.2 Mobile device tracking facilities could be used to locate the mobile device. [Refer to 3.1.1].
3.6	Data on mobile device which has been lost or stolen may be compromised.														[Refer to 1.3.1].
3.7	Lost or stolen mobile devices may have personally identifying and confidential client information.														3.7.1 The organisation should have sufficient insurance to cover possible lawsuits as a result of confidential information relating to their clients being revealed. [Refer to 1.3.1 and 3.1.1].
3.8	Organisation cannot remotely wipe lost mobile device.														3.8.1 The organisation should invest in software that will enable it to remotely wipe sensitive data off an employee's mobile device which has been lost or stolen. [Refer to 1.3.1].
3.9	Employees do not know what to do when their device is lost or stolen.														3.9.1 The organisation should have a policy informing employees what they need to do in the event that their mobile device is lost or stolen.
4.1	Bluetooth device may be discoverable.														4.1.1 Employees should be educated about the risks involved with leaving their mobile devices on discoverable mode.

Figure 1 continues on the next page →

FIGURE 1 (Continues...): Mapping risks to possible safeguards.

Number	Summarised risk identified	EDM01	EDM03	EDM04	APO01	APO12	APO13	BAI09	DSS01	DSS02	DSS03	DSS05	DSS06	MEA03	Possible safeguard
4.2	Unauthorised data downloads.														4.2.1 The organisation should make use of network access control technology. Any unauthenticated device should be immediately blocked. 4.2.2 Employees should be educated about the risks involved with leaving their mobile devices on discoverable mode as well as the risks involved with tethering. [Refer to 1.3.1].
4.3	Non-authenticated devices connecting to network.														[Refer to 4.2.1].
4.4	Bluetooth and Wi-Fi technology are easily infected.														4.4.1 Anti-malware software should be loaded onto the mobile devices. [Refer to 4.2.1].
4.5	Data transmitted may be compromised.														[Refer to 1.3.1].
5.1	Applications downloaded may steal or damage data.														5.1.1 Employees should be educated about the risks involved with downloading applications onto their mobile devices. [Refer to 1.3.1].
5.2	Unapproved applications may be stored on mobile devices.														5.2.1 The organisation should have a policy indicating which applications employees are permitted to download onto their devices.
5.3	Unapproved applications may not be easily detectable.														[Refer to 1.6.2].
5.4	Employees unaware of risky apps.														5.4.1 The organisation should have a policy where the IT department sends out regular email communication to employees about which popular applications are risky as well as what the potential consequences are if they download one of these applications.
6.1	Organisations may not be complying with laws and regulations.														6.1.1 The organisation should have a compliance officer who identifies which laws and regulations affect the organisation.
6.2	Organisations may be unaware of specific geographical laws and regulations.														[Refer to 6.1.1].
6.3	Communication laws may be violated.														6.3.1 The organisation should inform their employees which laws and regulations affect the organisation (including communication laws).
6.4	Organisations may not be able to ensure compliance on employee-owned devices.														6.4.1 The organisation could have the employees sign a contract indicating that if they intentionally violate a law or regulation of which they should have been knowledgeable, then they take personal responsibility for the non-compliance. [Refer to 6.1.1].
6.5	Personal use software may be used for business purposes.														6.5.1 Employees should be informed that they should inspect the software license on their device to identify whether or not it is personal use software prior to using the software for business purposes. 6.5.2 The organisation could have a policy where an employee needs to get the mobile device pre-approved prior to being allowed to use it to access the organisation's sensitive data. Software licenses could be checked by the IT department at this point in time.

Figure 1 continues on the next page →

FIGURE 1 (Continues...): Mapping risks to possible safeguards.

Number	Summarised risk identified	EDM01	EDM03	EDM04	APO01	APO12	APO13	BAI09	DSS01	DSS02	DSS03	DSS05	DSS06	MEA03	Possible safeguard
6.6	Organisations may be liable for additional costs where software licenses have been breached.	■	■		■	■	■					■	■	■	6.6.1 The organisation should have sufficient insurance to cover itself in the event that it is found to have breached a software licensing agreement. [Refer to 6.5.2].
7.1	IT may not be able to manage all mobile devices.	■	■	■	■	■	■	■	■	■	■	■	■		7.1.1 The organisation may establish user self-support and third-party support options. 7.1.2 The organisation may re-train existing service desk staff and augment the mobile support team as needed. 7.1.3 The organisation may make use of internal wikis, user forums, email distribution lists, enterprise social networking and other collaboration tools for user self-support.
7.2	IT may not be able to secure all mobile devices.	■	■	■	■	■	■	■	■			■	■	■	7.2.1 The organisation should implement a mobile device management system to reduce the risks associated with not being able to secure all mobile devices.
7.3	IT may not be able to successfully implement mobile security.	■	■	■	■	■	■	■	■	■	■	■	■	■	7.3.1 The organisation may make use of a network access controls system to reduce the risk of unauthorised devices connecting to the network. [Refer to 7.2.1].
7.4	Employees may select a device without considering IT support.	■	■	■	■	■	■		■	■	■	■	■	■	7.4.1 The organisation could have a policy indicating which mobile devices they will support.
7.5	Employee mobile devices may not be configured or locked down.	■	■	■	■	■	■	■	■	■	■	■	■	■	7.5.1 The organisation should implement a mobile device management system to ensure that all mobile devices have been configured correctly.
7.6	IT may not pre-approve all mobile devices.	■	■	■	■	■	■		■		■	■	■	■	7.6.1 The organisation should have a policy whereby it only permits pre-approved mobile devices to connect to the organisation's network.
7.7	IT may not be able to provide same level of support to all mobile devices.	■	■	■	■	■	■	■	■	■	■	■	■	■	[Refer to 7.1.1, 7.1.2 and 7.1.3].
7.8	The organisation may have open ports for employee-owned devices.	■	■	■	■	■	■					■	■	■	7.8.1 The organisation should not have open ports. Employees should use some form of login password to gain access to the network.
8.1	Mobile device life cycle may shorten.	■	■		■	■	■					■	■	■	8.1.1 Employees should be encouraged to keep their mobile phones for the duration of their mobile phone contracts. [Refer to 7.1.2].
8.2	Mobile devices may have planned obsolescence built into them.	■	■		■	■	■					■	■	■	[Refer to 8.1.1].

Note: The shaded areas indicate that the process is mapped to the risk identified.
IT, information technology; MEA, Monitor, evaluate and assess; DSS, Deliver, service and support; BAI, Build, acquire and implement; APO, Align, plan and organise; EDM, Evaluate, direct and monitor.

- adopting a multi-layered approach to security and authentication where both users and devices are encrypted and authenticated
- implementing mobile device management, preventing access to malware and encrypting important information and removing rogue mobile applications
- protecting data at the data file level to prevent unauthorised access to data files, as well as unauthorised moving, copying and/or editing of data files. This must include a containment and remote delete function.

Conclusion

Bring Your Own Device involves allowing an employee to use his or her own mobile device to access his or her organisation's network. Many organisations are embracing this trend in an attempt to create value. This comes at a cost. The aim of the research was to identify the risks which arise as a result of an organisation adopting a BYOD programme as well as using a recognised framework to identify controls which could be implemented to reduce the risks to an acceptable level.

The literature review revealed 50 risks which could arise if an organisation adopts a BYOD programme. The user of this research should note that there may be other incremental risks which may arise at their organisation. This is entirely dependent on the circumstances and control environment found at the organisation. COBIT 5 framework was selected as an acceptable framework to use in identifying controls which could reduce BYOD risks to an acceptable level. Six key risk areas were identified. These can be managed by a control framework which consists of four key elements: (1) policy development outlining acceptable user behaviour and monitoring the compliance thereof, (2) user education and the provision of user support services, (3) a software component addressing device, network and mobile device management systems and (4) a technological component that focuses on anti-malware, encryption, authentication and containment.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationships which may have inappropriately influenced them in writing this article.

Authors' contributions

L.W. is the primary researcher having conducted the research, assisted and supervised by R.R.

References

Anderson, N., 2014, *CISCO enterprise mobility solution: Device freedom without compromising the IT Network*, CISCO, viewed 18 August 2016, from http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/byodwp.pdf

Burt, J., 2011, *BYOD trend pressures corporate networks*, eWeek, s.l., viewed 18 August 2016, from http://www.eweek.com/c/a/Mobile-and-Wireless/BYOD-Trend-Puts-Pressure-on-Corporate-Networks-186705

CISCO, 2012, *The CISCO BYOD Smart Solution*, CISCO, viewed 18 August 2016, from http://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/byod_smart_so.pdf

CISCO, 2013, *CISCO connected world—International mobile security: Survey research highlights and considerations for enterprise IT*, IT world Canada, viewed 18 August 2016, from http://www.itworldcanada.com/assets/cisco-connected-world-international-mobile-security-survey-research-highlights-and-considerations-for-enterprise-it

Deloitte, 2013, *Understanding the bring your own device landscape*, Deloitte, UK, viewed 18 August 2016, from http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/about-deloitte/deloitte-uk-understanding-the-bring-your-own-device%20landscape.pdf

Drew, J., 2012, 'Managing cybersecurity risks', *Journal of Accountancy* 214(2), 44–48.

Entner, R., 2011, *International comparisons: The handset replacement cycle*, Recon Analytics, s.l., viewed 18 August 2016, from http://mobilefuture.org/wp-content/uploads/2013/02/mobile-future.publications.handset-replacement-cycle.pdf

Evangelista, M., 2014, 'Forrester: The total economic impact of IBM managed mobility for BYOD', *TechRepublic*, viewed 18 August 2016, from http://www.techrepublic.com/resource-library/whitepapers/forrester-the-total-economic-impact-of-ibm-managed-mobility-for-byod/

Gatewood, B., 2012, 'The nuts and bolts of making BYOD work', *Information Management* 46(6), 26.

Gupta, A., Milanes, C., Cozza, R. & Lu, C.K., 2013, *Market share analysis: Mobile phones*, Worldwide, 2Q13, Gartner, s.l.

IBM, 2011, *The new workplace: Supporting 'Bring your own'*, IBM, s.l.

IBM, 2012, *Securing end-user mobile devices in the enterprise*, s.n., s.l.

ISACA, 2012a, *COBIT 5: A business framework for the governance and management of enterprise IT*, ISACA, Rolling Meadows, IL.

ISACA, 2012b, *COBIT 5: Enabling processes*, s.n., s.l.

Kanaracus, C., 2012, 'IBM CIO embraces', *Computer World*, viewed 18 August 2016, from http://www.computerworld.com/article/2502805/byod/ibm-cio-embraces-byod-movement.html

Kaspersky, 2012, *Security technology for mobile and BYOD*., s.n., s.l.

Keeble, D., 2013, 'The culture of planned obsolescence in technology companies', Unpublished thesis, OULO University of Applied Sciences.

Klossner, J., 2012, 'Consumerization of IT – BYOD is driving IT "Crazy," says Gartner', *Computer World*, s.l., viewed 18 August 2016, from http://www.computerworld.com/article/2503573/consumerization/consumerization-trend-driving-it-shops--crazy---gartner-analyst-says.html

Koczerginski, M., 2015, 'Bringing sense to BYOD', *Canadian Underwriter* 82(12), 24–25.

Koh, E., Oh, J. & IM, C., 2014, 'A study on security threats and dynamic access control technology for BYOD, smart-work environment', in *Proceedings of the International Multi Conference of Engineers and Computer Scientists*, 2014. II, March 12–14, Hong Kong, pp. 634–639.

Lung Kao, I., 2011, *Securing mobile devices in the business environment*, IBM, viewed 18 August 2016, from https://www-935.ibm.com/services/uk/en/attachments/pdf/Securing_mobile_devices_in_the_business_environment.pdf

Mansfield-Devine, S., 2012, 'BYOD and the enterprise network', *Computer Fraud and Security*, 2012(4), 14–17. https://doi.org/10.1016/S1361-3723(12)70031-3

Markelj, B. & Bernik, I., 2012, 'Mobile devices and corporate data security', *International Journal of Education and Information Technologies* 6(1), 97–104.

Maycroft, N., 2009, *Consumption, planned obsolescence and waste*, Working paper, University of Lincoln, viewed 18 August 2016, from http://eprints.lincoln.ac.uk/2062/1/Obsolescence.pdf

McQuire, N., 2012, *Global BYOD attitudes and best practice for multinational organisations*, White paper, IDC, viewed 18 August 2016, from http://www.vibrantmedia.co.za/m/creativecounsel/vodacomboyd/November2012/IDCWP28U_Web.pdf

O'Brien, F., 2013, *Cut the software compliance risks of BYOD*, Gartner, s.l.

Ogie, R., 2016, 'Bring your own device: An overview of risk', *IEEE Consumer Electronics Magazine* 5(1), 114–119. https://doi.org/10.1109/MCE.2015.2484858

Pelino, M., 2012, *Building the case for a Bring-Your-Own-Device (BYOD) program*, Forrester, Cambridge, MA.

Ponemon Institute LLC, 2012, *Global study on mobility risks*, Ponemon Institute LLC, viewed 18 August 2016, from http://www.ponemon.org/local/upload/file/Websense_Mobility_US_Final.pdf

Rohan, A., 2013, *Bring-Your-Own-Device (BYOD) market poise $181.39 billion by 2017*, SBWire, viewed 18 August 2016, from http://www.sbwire.com/press-releases/bring-your-own-device-byod-market-poise-18139-billion-by-2017-321838.htm

Rose, C., 2012, 'BYOD: An examination of bring your own device in business', *Review of Business Information Systems* 17(2), 65–70. https://doi.org/10.19030/rbis.v17i2.7846

Rouse, M., 2010, *Definition cloud computing*, Whatif.com, viewed 18 August 2016, from http://searchcloudcomputing.techtarget.com/definition/cloud-computing

Rouse, M., 2011, *Define control framework*, Whatis.com, viewed 18 August 2016, from http://searchcompliance.techtarget.com/definition/control-framework

Staut, M., 2012, *BYOD: A revolution on the rise – Bring your own device' is poised to expand*, CAP Insider, viewed 18 August 2016, from http://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2012/CPA/Apr/RevolutionRise.jsp

Stroud, R., 2012, *5 Essential facts about COBIT 5*, ISACA, viewed 18 August 2016, from https://www.isaca.org/COBIT/Documents/5-Essential-Facts-about-COBIT.pdf

Swanepoel, R., 2015, 'BYOD: Are you missing the boat?', *Accountancy SA*, June, pp. 32–33.

Sylvester, A., Tate, M. & Johnstone, D., 2011, 'Beyond synthesis: Re-presenting heterogeneous research literature', *Behaviour & Information Technology* 32(12), 1199–1215. https://doi.org/10.1080/0144929X.2011.624633

Tibken, S., 2012, *Google ties Apple with 700 000 android apps*, CNet, viewed 18 August 2016, from http://news.cnet.com/8301-1035_3-57542502-94/google-ties-apple-with-700000-android-apps/

Vodafone, 2012, *Bring your own device: A considered approach*, White paper, Vodafone, viewed 18 August 2016, from http://www.vodafone.com/business/global-enterprise/bring-your-own-device-a-considered-approach-white-paper-2012-05-11

Willis, D., 2013, *Bring your own device: The facts and the future*, Gartner, viewed 18 August 2016, from https://l1.osdimg.com/remote-support/dam/pdf/en/bring-your-own-device-the-facts-and-the-future.pdf

Zahadat, N., Blessner, P., Blackburn, T. & Olson, B., 2015, 'BYOD security engineering: A framework and its analysis', *Computer & Security* 55, 81–99. https://doi.org/10.1016/j.cose.2015.06.011