陳志誠、林淑瓊、劉用貴、趙乃青(2018)，『BYOD 導入企業之關鍵管理因素：組織資訊安全管理觀點』，*中華民國資訊管理學報*，第二十五卷，第一期，頁 76-102。

BYOD 導入企業之關鍵管理因素：組織資訊安全管理觀點

陳志誠
大同大學資訊經營學系

林淑瓊*
大同大學資訊經營學系

劉用貴
大同大學資訊經營學系

趙乃青
大同大學資訊經營學系

摘要

企業導入員工攜帶自有行動設備(BYOD)上班已逐漸形成一個趨勢，但企業可能會擔心該實體設備遺失或內載資料被竊取所衍生出來的後續組織管理及資訊安全的嚴重問題。為使企業能對 BYOD 導入有明確的管理決策擬定之依據，探討企業 BYOD 導入需要掌握的關鍵管理因素即成為重要的研究課題。本研究從組織管理觀點思考 BYOD 導入之關鍵管理因素，先由防護技術及行動應用的相關文獻中整理出影響 BYOD 管理策略之四個準則構面及 16 個因子，再以修正式德爾菲法將專家意見轉為共識之研究條件，並結合層級分析法驗證影響 BYOD 管理策略之關鍵因素與因子。研究結果說明，經由關聯程度及相對權重分析出重要的管理準則構面，依序為行動資訊管理(MIM)、行動裝置管理(MDM)、企業風險管理(ERM)與行動應用程式管理(MAM)，各準則構面的重要管理因子依序為資料防護、安全認證管理、公司資安政策、存取控制等。

關鍵詞：攜帶自有行動設備、BYOD、行動資訊管理、行動裝置管理、資料防護。

*本文通訊作者。電子郵件信箱：sclin@ttu.edu.tw
2015/07/22 投稿；2016/11/14 修訂；2017/12/04 接受

Chen,P.S., Lin, S.C., Liu,Y.K. and Chao,N.C. (2018),' Critical management factors for the implementation of BYOD based on the perspective of organizational management concerning information security',
Journal of Information Management, Vol. 25, No. 1,pp. 76-102.

Critical Management Factors for the Implementation of BYOD Based on the Perspective of Organizational Management Concerning Information Security

Patrick Shicheng Chen
Dept. of Information Management, Tatung University

Shu Chiung Lin*
Dept. of Information Management, Tatung University

Yong Kuei Liu
Dept. of Information Management, Tatung University

Nai Ching Chao
Dept. of Information Management, Tatung University

Abstract

Purpose-The concept of Bring Your Own Device (BYOD) has been gaining its popularity and forming a trend in modern business operation. Along with the trend, many issues arise regarding device management and data security. Businesses have concerns about that personal devices can be lost and the confidential information contained in them can be compromised, leading to serious consequence. Meeting the challenges brought forth by the inclusion of personal devices in the business operation, especially equipment mobilization and personal use, and addressing the issues of effective management of confidential information are the main purposes of this study.

Design/methodology/approach- This study analyzes critical management factors affecting business BYOD adoption based on the concept of organization management. This study summarizes BYOD strategic guidelines and impacting factors by consulting available literature and protective techniques in practical use.

* Corresponding author. Email: sclin@ttu.edu.tw ◦
2015/07/22 received; 2016/11/14 revised; 2017/12/04 accepted

The factors are grouped into four different management constructs and 16 factors. The study collects core research elements through interviews with experts and analyzes their opinions using Modified Delphi Method and Analytic Hierarchy Process.

Findings-The result of this study shows the priorities of the enterprise BYOD implementation through the analysis of relevance degree and relative weight can be listed in the following order: MIM, MDM, ERM, and MAM. The most important factor in the MIM construct is data protection, in the MDM construct is security certificate management, in the ERM construct is company information security policy, and in the MAM construct is access control.

Research limitations/implications- The results of this study can help enterprises establish their BYOD strategy and be useful for future academic research.

Practical implications- According to the results, this study suggests that firms must strengthen enterprise internal information security policies, effective action to strengthen identity verification and access control to the equipment, and better application control through information security policy, practices of institutionalization and implementation of effective identity authentication.

Originality/value- This study provides enterprises to know more about the problems of the implementing BYOD impact on organizational operation from the perspective of high management level. The critical management factors of implementing BYOD are also provided to establish a total solution of information security management for enterprises.

Keywords: Bring Your Own Device, BYOD, Mobile Information Management, Mobile Device Management, Data Protection.

壹、緒論

行動技術快速發展，觸發了智慧型手機、平板電腦等行動裝置的風行，更多新的行動服務與行動裝置類型紛紛被推出，深深影響人們的使用習慣與行為，而行動服務大量使用的情形已從日常生活擴展到工作場域中。近年，企業讓員工自行攜帶自有設備(bring your own device; BYOD)在國內外皆已逐漸形成趨勢。員工使用自己喜歡與熟悉的自有設備與行動裝置，無論對企業或員工都有好處，不僅可以提升工作效率與便利性，同時公司也不需要再為員工採購相關的硬體設備，節省企業的營運成本。雖然有不少企業認同 BYOD 的趨勢，卻因為組織內資源設備管理、資訊和資料安全、隱私風險與行動裝置安全控管等問題，很多企業仍在猶豫之中(Miller, Voas & Hurlburt 2012; Thomson 2012; Ghosh, Gajar & Rai 2013; Bello Garba, Armarego & Murray 2015)。

Copeland and Crespi (2012a)於 2012 年發表有關 BYOD 的統計調查，結果顯示全球有 88%的企業員工有攜帶自有行動裝置於工作場域的經驗，並有 79%的企業員工預計在未來 12 個月內會編列預算購買自有行動裝置；此一資訊說明 BYOD 已成為工作者於工作場域中一個很重要的趨勢與氛圍。隨著員工攜帶自有行動設備到工作場域中的現象逐漸擴展，對企業而言，並非是沉醉在節省設備購置成本與提升工作效率的利多中，反而是憂心衍生而來的企業設備與資料管理問題、資訊隱私與使用問題及資訊安全與風險管理問題(Miller et al. 2012; Bello Garba et al. 2015; Kumar & Singh 2015)。這些問題都已悄悄提升成為組織管理階層必需即刻面對的挑戰，企業需要在不影響資訊安全與工作效益的權衡下，取得平衡與解決方案(Gessner et al. 2013)，並且需要教育與管理員工以提升對 BYOD 使用安全的認知(Romer 2014)，進而達到防堵資訊安全弱點與漏洞發生的機會，提升企業整體的安全性。同時，有高達 46%的企業資訊專業人員關心裝載有機密資料的自有行動設備實體遺失或被竊取的問題；另有 46%的專業人員關心如何保護行動裝置上的機敏資料在存取或儲存過程中的機密性和完整性，更有 40%的人認為必須強化行動裝置安全政策(Scarfo 2012)。

目前有關 BYOD 的研究主要是著重在提升資訊安全的技術觀點發展，研究的議題圍繞在 BYOD 造成的資訊安全與隱私違害討論上(Bello Garba et al. 2015; Eslahi et al. 2014; Miller et al. 2012; Tokuyoshi 2013)，包含：轉移 BYOD 風險的程序研究(Kumar & Singh 2015)與 BYOD 轉移策略研究(Ghosh et al. 2013)、BYOD 敏感資料的使用控制與保護(Morrow 2012)、BYOD 環境的企業網路管理研究(Mansfield Devine 2012)、BYOD 的行動裝置管理的管理架構(Song & Lee 2014)；以及 BYOD 的使用效益與影響研究，如：企業 BYOD 政策對員工的影響(Singh 2012)、影響 BYOD 服務採用行為的前置因素研究(Loose, Weeger & Gewald 2013)、BYOD 在組織內使用的效益與管理(Ullman 2011; Song 2014; Marshall 2014)。由這些先前的相關研究得知 BYOD 風險轉移與使用效益是主要的研究方向，然而較少有研究以組織層級觀點探討 BYOD 的資訊安全管理問題；也就是

說，BYOD 導入對於組織營運影響之管理問題較少被提及，而此問題卻是現今企業即刻會面臨到的重要挑戰(Ackerman & Krupp 2012; Marshall 2014)，提出整體解決方案是企業勢在必行的途徑，此也是本研究欲探討的問題。

有關組織導入 BYOD 的管理研究目前尚未有完整的理論架構可供參考，但經由相關文獻的探討與推敲，觀察到現有研究提及影響 BYOD 的管理因素與相關因子，主要是圍繞在裝置、資料、使用者、風險等管理上(Madden 2012; Jaramillo et al. 2013; Song & Lee 2014; Mooney, Parham & Cairney 2014)，這些因素可區分為：行動裝置管理(mobile device management; MDM)、行動應用程式管理(mobile application management; MAM)、行動資訊管理(mobile information management; MIM) (Scarfo 2012; Madden 2012)、以及企業風險管理(enterprise risk management; ERM) (Kumar & Singh 2015)等。所以，因應全球 BYOD 的發展趨勢，企業需要正視與思考 BYOD 使用環境的安全管理問題，並且提出 BYOD 的組織管理策略與使用規範，才能有效降低與轉移資訊安全的風險問題(Thomson 2012; Ghosh et al. 2013; Eslahi et al. 2014; Kumar & Singh 2015)。因此，本研究的主要研究目的是以組織策略層級的資訊安全管理觀點進行企業導入 BYOD 應掌握的關鍵管理因素探討，再由分析結果論述可提供企業參考之具體建議，作為企業 BYOD 導入之資訊安全管理策略的決策依據。

本文其餘內容安排：第二節先針對行動裝置安全相關文獻加以探討；第三節說明研究方法與研究流程及設計；第四節進行問卷調查與建立評估架構及分析評估結果；最後於第五節中說明研究結論與貢獻和研究限制。

貳、文獻探討

由於企業順應時代潮流導入個人攜帶自有行動裝置應用於工作環境中，企業即應重視與考量 BYOD 的便利性和可用性與資訊安全間的衝突問題，以及未來將面對的挑戰(Tokuyoshi 2013; Eslahi et al. 2014)。因而，提供安全的 BYOD 環境儼然成為現今企業的課題，並且 BYOD 使用環境的資訊安全管理問題是需要以組織層級觀點進行企業資訊安全管理的政策擬定與規範。

有關組織導入新資訊科技的相關研究，Tornatzky and Fleischer(1990)提出科技-組織-環境(technology-organization-environment)架構，科技構面說明組織的技術水準與市場上可取得的技術；組織構面說明組織大小與範圍、管理結構的複雜度、人力資源的品質與內部可取得的閒置資源；環境構面說明組織與其他競爭者在資源上的競爭或使用情形，此架構直接影響到組織創新科技的採用與建置。Laudon 等 (2000)也說明組織引進資訊系統可分為內部制度因素與外部環境因素，前者包含：制度因素、價值、規範與利益，後者包含：環境因素、不確定性與機會，這些因素影響組織開發、使用、引進與管理資訊系統。Tornatzky and Fleischer(1990)與 Laudon 等 (2000)皆分別說明組織與環境因素對資訊科技導入的影響，但組織技術水準與市場上可取得的技術更是新資訊科技導入不可以或缺的部份(Tornatzky & Fleischer, 1990)，因而本研究的研究核心是以 Tornatzky and

Fleischer(1990)於科技構面中的說明為理論基礎，探討組織導入 BYOD 應掌握的關鍵管理因素，並且以 Scarfo(2012)與 Madden(2012)在行動裝置管理的研究為核心，結合企業資訊安全風險管理進行思考(Mooney et al. 2014)，以降低風險的發生與造成的損失(Stoneburner et al. 2001; Lin et al. 2014)。

Scarfo(2012)提出三項行動裝置管理建議：(1)以人為中心的管理，針對存取控制(Access Control)考慮管理方向；(2)以裝置為中心的管理，針對裝置管制(device control)考慮管理方向;(3)以資料為中心的管理,針對資訊管理(information management)考慮管理方向。而 Madden(2012)將行動裝置管理區分為行動裝置管理、行動應用程式管理、以及行動資訊管理三類,提供企業行動裝置管理的方向。雖然 Scarfo(2012)與 Madden(2012)分別對行動裝置的管理提出不同的說法，但二者在分類上有不謀而合之處，皆分別對裝置、資訊與應用程式存取進行管理說明，此三類也是企業導入 BYOD 最需要重視與建立管理方針的部份。同時，企業導入 BYOD 可能導致的企業風險是不能被忽視的，一旦風險發生企業要面對風險控制、評估與規避等的問題，且要有立即處理與制定相關管理策略的能力(Ghosh et al. 2013; Kumar & Singh 2015)。

一、行動裝置管理(MDM)

MDM 是企業透過第三方軟體整合方案在遠端對行動裝置進行監控、鎖定、操控、加解密、安裝程式及套用政策，進而達到遠端管理行動裝置與實體機器的目的(Scarfo 2012; Pogarcic et al. 2013; Security for Business Innovation Council (SBIC) 2012)。例如：當行動裝置遺失時，企業可以利用遠端操作方式，將存於此裝置上之機密資料刪除，避免資安事件發生。在資訊周刊進行的行動運算風險(the risks of mobile computing)調查中，有 84%的資訊安全專業人員認為「遺失或被盜的裝置」是最大的隱憂(InformationWeek 2012)，手持式行動裝置資料遺失或被盜是亟需要克服的問題。

Redman 等(2011)認為 MDM 管理可歸納為四部份：(1)軟體部署(software distribution)：包括支援及管理移動裝置應用程式部署、安裝、升級、移除或中斷；(2)政策管理(policy management)：是指對企業中使用的行動裝置進行開發、控制、操作等的管理政策，在研究中為了與 MIM 中的政策管理區別，本研究將之稱為裝置政策管理；(3)元件管理(inventory management)：基本裝置管理、調配和支援(provisioning and support)管理；(4)安全認證管理(security certificate management)：裝置的安全性、認證的強制執行和加密服務管理。此外，在一些資安事件中也曾發現，雖有 MDM 的實施，駭客仍有能力將行動裝置網路連線癱瘓或使其失效，進而阻止企業遠端使用命令及指令抹除資料的動作。對於使用者而言，因為企業管理程式的限制，可能使原本操作的方便性降低而影響工作效率(Leavitt 2013)，因而明確的 MDM 管理架構是有其必要的，以提升 MDM 的安全與效益(Song & Lee 2014; Jaramillo et al. 2013)。所以，當企業允許 BYOD 時，MDM 要考量的因素包含：管理行動裝置的安全系統佈建、管理元件的功能操

作、行動裝置的身份確認與遺失風險評估等(Redman et al. 2011; SBIC 2012; Standard & Poor's 2007)，企業 MDM 準則構面之影響因子可具體說明如表 1。

表 1：影響 MDM 之關鍵因子

關鍵因子	說明	相關文獻
軟體部署 software distribution	進行支援及管理移動裝置應用程式部署、安裝、升級、移除或中斷等。	Redman et al. 2011
元件管理 inventory management	進行基本的裝置元件管理，以及調配和支援的管理。	Redman et al. 2011
安全認證管理 security certificate management	裝置的安全性、認證的強制執行和加密服務的安全管理。	Redman et al. 2011
裝置失竊管理 lost or stolen devices management	裝置遺失會被竊取之風險管理。	SBIC(2012); Standard & Poor's(2007)

二、行動應用程式管理(MAM)

MAM 是企業管理與限制行動裝置上的應用程式使用之功能，主要是對遠端行動裝置上的程式進行監控與管理，進而達到在遠端管理行動裝置上的程式使用之目的，包括：安全的遠端部署、保護程式及企業資料使用。MAM 主要是限制員工不得使用未經核准的應用程式存取企業網路資料，透過權限管制可以使企業內部資料安全的被隔離，以防止被不信任的程式盜取或誤用(Leavitt 2013)。但是企業利用 MAM 築起一道虛擬的防火牆，在安全上仍是有限的，MAM 只能限制企業部署在自有行動裝置上的代理程式，透過代理程式傳送及收發所有的封包訊息，資料安全性可以有效的控制(Marques et al. 2001)，然而卻無法防止同一裝置上其他應用程式的違法竊取行為，例如：畫面擷取、封包側錄的程式行為(Scarfo 2012)。

企業對行動裝置提供遠端應用程式服務部署時，常因為資料安全的限制，必須套用客製化的管理政策保障資料傳輸過程的安全。Copeland and Crespi (2012a) 提出政策樹(policy tree)的概念闡釋軟體傳輸服務政策，分為四大類：(1)用戶/裝置政策(user/device policy)：針對終端裝置的過濾篩選、使用者權限等設定政策，管理使用者或限制裝置存取權限；(2)服務政策(service policy)：針對通信服務品質等級提供不同層級的服務；(3)場次政策(session policy)：針對任務活動或是重大任務執行之特殊授權或服務範圍之通訊管理政策，在本研究中稱為通訊場次政策；(4)網路政策(network policy)：針對網路傳輸進行管理。因此，當企業允許 BYOD 時，MAM 要考量的因素包含：應用程式的存取控制與權限、應用程式的安全性與弱點、行動裝置進行溝通的軟體權限與服務品質等，影響企業 MAM 準則構面之影響因子可分為：(1)存取控制；(2)代理程式安全；(3)通信軟體管理元件；(4)通信服務品質；(5)軟體缺陷(Copeland & Crespi 2012b; SBIC 2012; Marques

et al. 2001; Scarfo 2012)，如表 2。

表 2：影響 MAM 準則構面之關鍵因子

關鍵因子		說明	相關文獻
存取控制	服務規則政策 service rules policy	針對應用程式服務品質等級分別提供不同層級的服務。例如：依不同應用程式服務等級提供頻寬使用限制、服務內容。	Copeland & Crespi (2012b)
	服務政策 service policy	針對使用者服務品質等級分別提供不同層級的服務。例如：依不同職務等級提供頻寬使用限制、服務內容。	SBIC (2012)
代理程式安全	追蹤元件 tracking component	讓每個中央管理應用程式透過 Mobile-agent 持續追蹤及管理本地或遠端的行動裝置。	Marques et al. (2001)
	安全元件 security component	透過安全驗證與授權方式，遠端執行應用程式或服務，達到資料使用的安全。	Marques et al. (2001)
通信軟體管理元件 mobile-agent management component		Mobile-agent 管理元件能在行動裝置上使用之控制機制，可遠端控制及監控的機能與可隨時與其他元件交互運作與管理。	Scarfo (2012); Marques et al. (2001)
通信服務品質	通訊元件 communication components	以同步或非同步的形式透過資料交換與行動裝置上執行的其他應用程式進行溝通及傳遞資料。	Marques et al. (2001)
	網路政策 network policy	為網路傳輸的管理政策，例如：資料流品質、路由方式、頻寬提供與限制、網路服務品質(QoS)等。	Copeland & Crespi (2012b)
軟體缺陷	惡意軟體 mobile malware	移動設備惡意軟體攻擊之風險。	SBIC (2012)
	軟體漏洞 software vulnerabilities	軟體漏洞造成資安之風險。	SBIC (2012); Standard & Poor's (2007)

三、行動資訊管理(MIM)

由於現今使用者可在不同裝置上使用程式存取雲端伺服器上的資料(Scarfo 2012)，例如：在 Dropbox 上進行資料的存取，因而衍生出許多資料管理的安全問題。MIM 是透過雲端資料儲存服務方案管理及控制資料的安全問題，專為個人資訊管理(personal information management; PIM)提供資料安全的防護服務，包含：電子郵件、行事曆、工作排程與通訊錄等。另有研究使用行動資料管理(mobile data management; MDM)這個名詞(Bisdikian et al. 2011)，本研究為避免與前面描述的裝置管理(device management)產生混淆，將於全文中直接使用 MIM 加以區分，透過 MIM 進行管理及控制資料與資訊在不同裝置上的存取安全問題(Mallick

2003; Scarfo 2012)。

目前 MIM 相關應用皆以大型服務方式提供，如：電子郵件或行事曆程式部署在用戶端使用，Jaramillo et al.(2013)在資料隔離策略中提出，需要能有效將個人資料及企業機敏資料依自有行動裝置的功能面進行控制及區分管理，並且分為四種管理面向：(1)裝置查詢(device query)：指對行動裝置的資訊進行專一性資料蒐集的功能，如：識別資訊、記憶體、儲存設備、GPS 位置資料等；(2)政策管理(policy management)：指建立明確的行動裝置使用資訊的管理規範，如：密碼長度與強度、控制資料儲存於雲端、防毒軟體強制執行等，而此政策管理與 MDM 指的政策管理內容不盡相同，本研究將之稱為資訊政策管理；(3)資料保護(data protection)：是指裝置使用資料管理控制保護功能，如：限制複製及貼上功能的使用、限制讀取機敏電子郵件資料、防止重要機敏資料外洩等；(4)裝置動作(device actions)：指對行動裝置內的資訊執行相關資訊處理的功能，如：從裝置管理系統中執行部分或全部資料抹除、遠端鎖定裝置、遠端重設密碼、阻斷接收電子郵件、遠端發送訊息等。

此外，Redman 等(2011)在 MDM 中提及的政策管理與 Jaramillo et al. (2013)在 MIM 提及的政策管理，二者在概念與內容上皆是不相同的，前者是指對行動裝置本身的政策管理，本研究將之稱為裝置政策管理，後者是指對行動裝置使用之資訊的政策管理，本研究將之稱為資訊政策管理。當企業允許 BYOD 時，在 MIM 要考量的因素包含：資料存取的權限與安全、資料蒐集與使用的權限、資料保護的方法，所以影響企業 MIM 準則構面之影響因子，可具體說明為資料防護、資料查詢與資料使用(Jaramillo et al. 2013; SBIC 2012)，如表 3。

表 3：影響 MIM 準則構面之關鍵因子

關鍵因子	說明	相關文獻
資料防護 data protection	裝置使用資料之管理、控制與保護功能，例如：限制複製及貼上功能的使用、限制讀取機敏電子郵件資料、防止重要機敏資料外洩等。	Jaramillo et al. (2013)
資料查詢 data query	裝置資訊查詢與蒐集具專一性資料功能，例如：識別資訊、記憶體、儲存設備、GPS 位置資料等。	Jaramillo et al. (2013)
資料使用 data actions	在裝置上執行資訊處理功能，例如：執行部分或全部資料抹除、遠端鎖定裝置、遠端重設密碼、阻斷接收電子郵件、遠端發送訊息等。	Jaramillo et al. (2013); SBIC (2012)

四、企業風險管理(ERM)

由於現今手持行動裝置儲存越來越多個人隱私資料，雲端網路開放空間更容易引起不法者的覬覦，根據 Ponemon Institute(2014)的研究指出，在員工遺失或被盜的智慧型手機中，60%有包含機敏訊息，若這些手機含有企業策略或財務資訊，其損害將無以計算，若再含有客戶穩私資料與機密訊息，將可能面臨訴訟的

爭議(SBIC 2012)，為此手機業者都竭盡全力遏止惡意軟體在行動裝置上執行，較常採行的方式是在操作系統上執行應用沙箱(application sandbox)，限制應用程式存取數據及系統資源(SBIC 2012)，行動裝置造成的風險管理問題正衝擊著企業組織。

ERM 是由管理者的角度審視 BYOD 導入政策的風險問題(Mooney et al. 2014)，目的在於認知和分析潛在損失的可能性和可能的衝擊程序，風險管理包含三部份：風險控制、風險評估和風險規避(Skipper 1998; Stoneburner et al. 2001; Lin et al. 2014)。(1)風險評估：分析潛在損失的可能性和可能幅度之程序，企業必須通盤評估 BYOD 進入企業後可能帶來的風險，包含：財務風險、資安風險、實體損壞風險、惡意或蓄意攻擊風險等；(2)風險控制：是管理風險最有效的方法，當 BYOD 進入企業後，公司資安政策可針對已知風險制定管理控制對策，將預期風險降低，包含：預防損失、降低損失幅度與避免潛在的損失危險，以及風險控制最佳實務等(Standard & Poor's 2007; SBIC 2012)；(3)風險規避：BYOD 進入企業後針對非預期或未知風險制定管理應變對策及標準作業程序，提供相當資金及處理潛在損失的技巧與方法，以期規避非預期風險，包含：提供資金、處理潛在損失的措施等。

當 BYOD 進入企業後，企業面臨的風險將是可以預期的，BYOD 非僅是資料安全的管理問題，而是整體企業網路安全管理的策略問題(Mansfield Devine 2012)，企業將可依上述三個管理法則進行風險管理，透過風險評估產出風險控制對策，針對已知風險制定管理控制對策，並配合非預期風險提出風險規避策略，以達到 BYOD 進入企業後的企業風險管理目的。當企業允許 BYOD 時，ERM 要考量的因素包含：風險的防範與資訊安全的政策、惡意程式攻擊與風險損失評估、資訊與人員的使用權限等。影響 ERM 準則構面之影響因子，可具體說明為財務風險、公司資安政策、病毒威脅、錯誤操作行為(Standard & Poor's 2007; SBIC 2012; Copeland & Crespi 2012b)，如表 4。

表 4：影響 ERM 準則構面之關鍵因子

關鍵因子		說明	相關文獻
財務風險	財務風險 financial risk	資本可及性、信用、財務市場風險、通貨膨脹、利率、流動性。	Standard & Poor's (2007)
	供應風險 supply risk	商品價值、供應鏈。	Standard & Poor's (2007)
公司資安政策	管理風險 management risk	公司治理、資料安全措施、智慧財產權管理、員工技能問題、管理複雜度、委外問題、專案管理、科技管理。	Standard & Poor's (2007)
	管理場次政策 mnagement session policy	主要針對提供任務活動或是重大任務執行範圍等管理層面之政策，通常礙於企業預算政策面的考量而有所限制與不同。	SBIC (2012); Copeland & Crespi (2012b)
病毒威脅		移動設備惡意軟體攻擊之風險。	SBIC (2012)

mobile malware		
錯誤操作行為 end-user behavior	終端使用者行為錯誤之風險。	SBIC (2012)

參、研究方法

經由上述文獻探討，本研究先彙整影響企業 BYOD 導入之關鍵管理因素的準則構面與關鍵因子，再以修正式德爾菲法(modified delphi method; MDM)進行專家訪談，接著整理專家對於企業導入 BYOD 關鍵管理因素的意見，作為後續研究構面與影響因子之擬定，同時設計專家問卷進行意見調查，並且以層級分析法(analytic hierarchy process; AHP)分析各準則構面與因子的權重，以及建立企業導入 BYOD 關鍵管理因素的層級架構圖。本研究的分析單位為組織層級。

一、準則構面之操作型定義及影響因子擬定

根據文獻探討分析，本研究依 Scarfo(2012)以人、裝置、資料為中心的管理概念，與 Madden(2012)對行動裝置管理的分類研究結合企業風險管理，進行企業 BYOD 導入之關鍵管理因素準則構面的擬定，分別為：以人為中心的行動應用程式管理(MAM)，以裝置為中心的行動裝置管理(MDM)，以資料為中心的行動資訊管理(MIM)，以及避免行動裝置管理過程發生資訊風險問題的企業風險管理(ERM)。四個準則構面的操作型定義與各構面的影響因子整理如表 5，再由此發展第一階段修正式德爾菲法的調查問卷。

表 5：準則構面的操作型定義及影響因子

準則構面	操作型定義	影響因子	參考文獻
行動裝置管理(MDM)	企業以軟體整合方案在遠端對行動裝置進行監控、鎖定、遠端操控、加解密、安裝程式及套用政策等，進而達到遠端管理行動裝置實體機器之目的。	軟體部署、元件管理、安全認證管理、裝置失竊管理	Scarfo(2012)、Pogarcic et al.(2013)、SBIC(2012)
行動應用程式管理(MAM)	企業在遠端對行動裝置上的應用程式進行管理、權限使用控管與監控，進而達到在遠端管理行動裝置上的程式之目的。	存取控制、代理程式安全、通信軟體管理元件、通信服務品質、軟體缺陷	Scarfo(2012)、SBIC(2012)、Copeland & Crespi(2012b)
行動資訊管理(MIM)	企業在遠端對於儲存在行動裝置上的資訊與資料進行管理，以及控制資料在不同裝置上使用程式與存取雲端伺服器資料的安全問題。	資料防護、資料查詢、資料使用	Scarfo(2012)、Mallick(2003)
企業風險管理(ERM)	企業認知和分析潛在損失的可能性和可能幅度之程序，風險控制	財務風險、公司資安政策、	Standard & Poor's(2007)、

	包括避免潛在損失危險、預防損失、降低損失幅度，以達到企業風險管理的目的。	病毒威脅、錯誤操作行為	SBIC(2012)

二、修正式德爾菲法

德爾菲法(delphi method)為一種採取匿名式的專家集體決策技術，保有專家團體決策的優點，也能避免調查成員面對面的溝通干擾，同時結合統計分析判定受訪者對探討項目有否達到一致共識的方法(Dalkey & Helmer 1963; de Meyrick 2003)，Okoli and Pawlowski (2004)認為德爾菲法是資訊相關研究領域用於擬定管理決策順序的有效工具。Murry and Hammons(1995)提出修正式德爾菲法(modified delphi method)，主要是將原本第一回合開放式問卷調查改以參考相關文獻的研究結果或以研究者的規劃替代，亦可用專家訪談的方式進行，以直接建構第一回合結構性的問卷調查內容。此法最主要是讓參與的專家小組成員能夠集中在研究主題上，省去對開放性問卷的揣摩臆測進而提高問卷的回收率。

本研究問卷採用李克特五等尺度量表(Likert 1932)，依受訪專家評估該項因素對企業導入 BYOD 後之影響的重要性程度，分為：5 分非常重要至 1 分非常不重要。德爾菲法在進行統計分析時主要採用眾數、中位數、平均數與四分位數等方法，用以呈現專家學者的意見達到一致性與取得共識的結果(Green et al. 1999)，本研究的分析方法說明如下：

(1)總數(T)：指標項目在所有專家勾選重要程度的總分數。

(2)平均數(M)：屬於集中量數，表示專家意見的集中趨勢，平均數大於 3 的題項予以保留(Holden et al. 1993)。

(3)眾數(MO)：一組數據中，專家選擇出現最多次的數值。

(4)眾數與平均數差之絕對值｜MO-M｜：若絕對值≦1 者，表示專家意見的一致性相當高；若絕對值≧1 者，表示專家意見分歧(Holden et al. 1993)。

(5)標準差(SD)：呈現一組數據離散程度的最佳指標，數值越大表示離散程度越大，數值越小表示專家意見越集中。

(6)四分位差(Q)：利用四分位差呈現群體回饋的變異程度。當四分位差的數值≦0.6，可視為該問項已達到高度共識；若四分位差是＞0.6 且≦1，則視該問題達到中度共識；若四分位差＞1，則可視該問項並未達成共識(Holden et al. 1993)。

三、層級分析法

AHP 法乃是將問題進行結構化與系統化處理的過程，透過 AHP 法將研究之複雜系統分解成簡明的因子階層系統以建立層級結構。經過評比以找尋各階層各要素間的權重，以 AHP 法建構能力指標相對權重體系是使專業理念、知識與數理統計分析做一個結合的過程。AHP 法主要步驟有四：

(1)將影響問題的因素組合成多個層級，基本假設是每一層級只影響下一層級，同時僅受另一層級的影響。層級的結構可從方案的整體目標、子目標、及子

目標的影響要素形成。研究者可透過文獻回顧、專家訪談與調查問卷等方法，建立問題之影響構面與因子間的關係；

(2)建立評估構面和各構面之因子的成對比較矩陣。AHP 法是利用特徵向量法求取因子間的權重，並且採用比率尺度衡量成對比較矩陣，主要分為五項等級(同等重要、稍重要、頗重要、極重要和絕對重要)加上四個中介尺度(介於上述每兩者之間)，共九個尺度分別給予 1 至 9 之比重。研究中先建立決策模型，再以 Expert Choice 2000 建立成對比較矩陣與進行分析，透過一對一的比較和變數間的相對重要性進行重要因子的判斷。

(3)計算各因子之相對權重和各構面的相對評估值。

(4)一致性檢定：是為了驗證及檢定決策者在計算特徵向量值後，回答成對比較結果是否合理。Saaty(1980)建議以一致性指標(consistency index; C.I.)與一致性比率(consistency ratio; C.R.)檢定成對比較矩陣。一致性指標是確定決策者判斷前後的一致性，從評估尺度產生的正倒值矩陣，會因矩陣內的階數產生不同的 C.I.值，其值主要會隨著矩陣內階層數目的增加而增加，稱為隨機指標(random index; R.I.)，R.I.值參考自 Saaty(1980)整理的隨機指標表。各指標的標準值如下說明：

C.I. ≤ 0.1 時，一致性程度可以接受。

C.R. = (C.I.) / (R.I.)

C.R. ≤ 0.1 時，其一致性程度達可接受的水準。

四、結合修正式德爾菲法與層級分析法進行二階段分析

Khorramshahgol and Moustakis(1988)結合德爾菲法與層級分析法的優點提出德爾菲層級程序法(delphi hierarchy process; DHP)的概念進行二階段分析，第一階段先以德爾菲法建立層級結構與成對比較矩陣，再以 AHP 法進行第二階段階層分析問題之邏輯運算，例如：Di Zio and Maretti(2014)的能源可接受性研究。近年，即有許多研究以 Khorramshahgol and Moustakis(1988)的 DHP 法為概念基礎，以修正式德爾菲法(Murry & Hammons 1995)取代德爾菲法(Dalkey & Helmer 1963)進行二階段的分析，並且常應用於績效指標評選與管理決策制定的研究議題上，例如：Hsu, Chiang and Wang(2011)建立國際展覽會代理商的評選機制、Hsu, Tsai and Chen(2014)商業電視台旅遊方案主辦單位最佳化研究、Cao 等(2014)探討軟體可靠度評估模式、Chen 等(2015)探討金融機構資訊資產評估、Min(2016)發展導遊服務品質指標、Kim and Gausdal(2017)探討運輸中領導模式的加權安全研究等。

第一階段修正式德爾菲法的問卷篩選標準係依四分位差(quartile deviation, Q)、平均數、眾數及中位數作為檢測題項是否達到一致性的共識為標準。Holden 等(1993)研究指出當四分位差之數值 Q≦0.6，該關鍵因子被認定為具有專家一致性共識；當｜Mo-M｜≦1 則表示專家意見一致性高，並且平均數須大於 3 的題項才予以保留。利用這些指標作為專家問卷的同意程度，以及篩選主準則構面之

依據，若其中一點不符合時則予以刪除。若有 85%以上題項達到中度共識以上程度，則可結束調查。第二階段再以前階段得到的準則構面及關鍵因子建立 AHP 層級架構，再依層級架構進行問卷設計。

在問卷填答部份以兩兩問題相互比較其相對的重要程度為題項設計之依據，填答者分別對每一題項進行二者重要性程度的差異比較，主要分為九個不同權重強度之權重分數等級，其分數為 1-9 分的等級尺度，並以網路問卷及電子郵件問卷進行發放。

五、調查對象

由於本研究是以修正式德爾菲法(MDM 法)與 AHP 法二階段進行企業 BYOD 導入之關鍵管理因素之架構與分析，在進行修正式德爾菲法的專家調查訪談時，若受訪專家間的異質性較高時，邀請 5-10 位專家參與即足夠，10 位以上的群體誤差較低且可信度較高(Dalkey 1969; Delbecq et al. 1975; Brooks 1979; Parente & Anderson Parente 1987)。本研究在進行受訪專家選定時，即以先前學者的建議與 BYOD 導入之管理問題進行思考，鎖定尋找異質產業的專家，共邀請 14 位資深專家參與二階段的問卷調查(Delbecq et al. 1975)，如表 6 所示。第一階段的修正式德爾菲法邀請七位專家對各構面之準則問題進行意見表達；第二階段則再增邀請七位資訊科技業的專家參與 AHP 法的問卷調查。此外，為了能瞭解不同屬性專家的意見，在分析部份除了進行全體專家的資料分析外，更進一步將專家區分為二群組(高階主管組、資訊科技組)進行分析比較。

表 6：修正式德爾菲法與層級分析法受訪專家資料

項次	產業類型	受訪者服務單位	職稱	學歷	工作年資	MDM 法	AHP 法
1	學術	大學	教授	博士	30	✓	✓
2	醫療	教學醫院	副院長	博士	30	✓	✓
3	電信	電信公司	經理	碩士	30	✓	✓
4	製造業	工業公司	經理	學士	17	✓	✓
5	網際網路業	網際網路公司	系統設計師	博士	22	✓	✓
6	生技業	生技公司	執行長	碩士	15	✓	✓
7	證券	證券公司	副理	學士	25	✓	✓
8	軟體服務業	軟體服務公司	資深協理	碩士	30		✓
9	軟體服務業	軟體服務公司	技術處長	學士	20		✓
10	軟體服務業	軟體服務公司	技術處長	專科	22		✓
11	軟體服務業	軟體服務公司	技術經理	碩士	20		✓

12	管理顧問	企業管理顧問公司	董事長	專科	30		✓
13	通訊	通訊科技公司	副總經理	碩士	25		✓
14	軟體服務業	科技公司	執行長	碩士	28		✓

肆、資料分析與討論

依據研究方法與設計進行修正式德爾菲法與 AHP 法的資料蒐集與分析。

一、修正式德爾菲法問卷分析

研究中以四個準則構面及 16 項關鍵影響因子整理出修正式德爾菲法問卷，並於 2014 年 11 月 1～7 日發放，共發出 7 份問卷，回收 7 份。接著進行一致性比率(consistency ratio; CR)與一致性指數(consistency index; CI)分析，結果說明 C.I. 值>0.1 的問卷有 5 份，再挑出不符合一致性檢定之 2 份問卷，並且與填寫該份問卷之專家進行深入訪談，比對問卷的不一致性，使其了解其所填問卷不一致之處，予以更正後再重新設計問卷與發放。待所有問卷均符合一致性之要求，再求取每位專家對於各關鍵因子之評比。各準則構面與影響因子的修正式德爾菲法問卷結果分析如表 7 與表 8 所示，二表中分別說明 4 個準則構面與 16 個影響因子的分析數據皆符合修正式德爾菲法的門檻，予以保留；接著再進行準則構面與關鍵因子問項的一致性分析，分析結果僅有 1 個「裝置失竊管理」之關鍵因子問項的四分位差(Q)為 0.75，是介於門檻值 0.6 與 1 間的值，為中度的一致性程度，其餘問項的四分位差(Q)皆為小於 0.6 門檻值，具有高度一致性程度，因此本研究的問項皆達到中度以上共識，如表 9 所示。

表 7：準則構面之修正式德爾菲法問卷結果分析

編號	準則構面	總數(T)	平均數(M)	眾數(MO)	|MO-M|	標準差(SD)	四分位差(Q)	保留
1	行動裝置管理	30	4.29	5	0.71	0.76	0.5	✓
2	行動應用程式管理	28	4	4	0	0.58	0	✓
3	行動資訊管理	33	4.71	5	0.29	0.49	0.25	✓
4	企業風險管理	32	4.57	5	0.43	0.53	0.5	✓

表 8：影響因子之修正式德爾菲法問卷結果分析

編號	準則構面	影響因子	總數(T)	平均數(M)	眾數(MO)	|MO-M|	標準差(SD)	四分位差Q	保留
1	行動裝置管理	軟體部署	27	3.86	4	0.14	0.38	0.00	✓
2		元件管理	24	3.43	3	0.43	0.79	0.25	✓
3		安全認證管理	31	4.43	5	0.57	0.79	0.50	✓
4		裝置失竊管理	30	4.29	5	0.71	0.95	0.75	✓

5	行動應用程式管理	存取控制	31	4.43	5	0.57	0.79	0.50	✓
6		代理程式安全	27	3.86	4	0.14	0.69	0.25	✓
7		通信軟體管理元件	29	4.14	4	0.14	0.38	0.00	✓
8		通信服務品質	27	3.86	4	0.14	1.07	0.50	✓
9		軟體缺陷	28	4.00	4	0.00	0.58	0.00	✓
10	行動資訊管理	資料防護	32	4.57	5	0.43	0.53	0.50	✓
11		資料查詢	25	3.57	3	0.57	0.79	0.50	✓
12		資料使用	27	3.86	4	0.14	0.69	0.25	✓
13	企業風險管理	財務風險	29	4.14	4	0.14	0.69	0.25	✓
14		公司資安政策	32	4.57	5	0.43	0.53	0.50	✓
15		病毒威脅	29	4.14	4	0.14	0.69	0.25	✓
16		錯誤操作行為	27	3.86	4	0.14	0.38	0.00	✓

表 9：各構面與影響因子的一致性分析

一致性程度	四分位差	題項		百分比
		準則構面	影響因子	
高度	Q≦0.6	4	15	95%
中度	0.6<Q≦1	0	1	5%
低度	Q>1	0	0	0

二、AHP 法問卷資料分析

經修正式德爾菲法分析後，建構企業 BYOD 導入之關鍵管理因素層級架構圖，如圖 1 所示。接著，再發放 14 份問卷並進行 AHP 法分析，時間為 2014 年 12 月 14～31 日，有效回收率 100%，受訪對象男性占多數，年齡層分佈在 36-65 歲，教育程度以研究所居多數，工作內容性質多為管理職務，職務性質則以決策、管理及執行為主，表 10 為受訪者基本資料。表中說明有 7 位受訪者「工作單位有提供行動裝置」，有 2 位受訪者的「個人行動裝置沒有使用在工作單位」，但 14 位受訪者「最常使用的行動裝置」分別是：14 位使用智慧型手機、3 位使用平板、8 位使用筆記型電腦，表示受訪者皆有使用行動裝置，只是提供行動裝置的來源有所不同。本研究推論此 7 位的工作單位有提供行動裝置的受訪者，其使用的行動裝置是專屬於受訪者使用。另有 2 位受訪者雖然沒有將個人行動裝置使用於工作單位中，但本研究推論受訪者是於工作環境中使用工作單位提供的行動裝置，所以有這二部份情況的受訪者，其使用過程也是符合本研究要探討的資訊安全管理問題。此外，這幾位受訪者是以專家的身份提供意見，而這些專家都是業界的資深管理者，因此受訪者的資格是符合本研究研究設計的專家資格。

在 AHP 法的分析部份，本研究分成三群進行資料分析與比較，首先進行全體受訪者 14 份問卷資料分析，再進行 7 位高階主管受訪者的問卷資料分析，以及 7 位資訊科技業受訪者的問卷分析，並比較三群的分析結果。在一致性分析部份三群的分析結果，其 C.I.<0.1 且 C.R.<0.1，皆符合 AHP 法一致性的標準，如

表 11 所示。

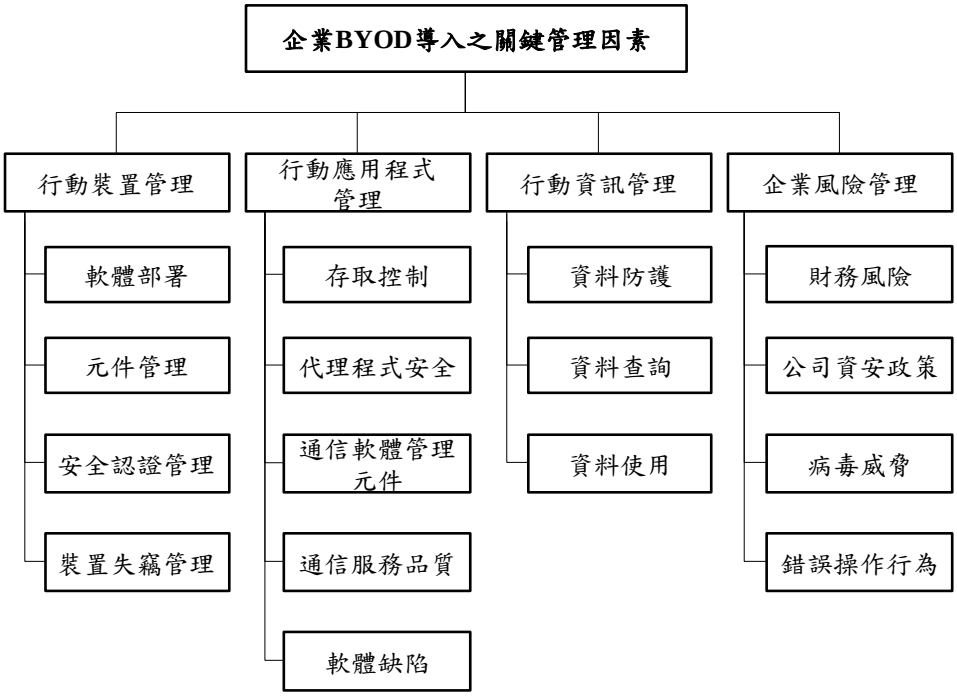

圖 1：企業 BYOD 導入之關鍵管理因素架構圖

表 10：受訪者基本資料分析

項目	選項	人數	比例	項目	選項	人數	比例
性別	男性	13	92.86%	職務性質	決策	5	35.71%
	女性	1	7.14%		管理	6	42.86%
年齡	36-40 歲	1	7.14%		執行	3	21.43%
	41-45 歲	4	28.57%	工作內容性質	研發	2	14.29%
	46-50 歲	3	21.43%		管理	9	64.29%
	51-55 歲	3	21.43%		資訊	3	21.43%
	56-60 歲	1	7.14%	工作年資	15 年以上	14	100.00%
	60 歲以上	2	14.29%	最常使用的行動裝置(可複選)	智慧型手機	14	100%
教育程度	專科	2	14.29%		平板	3	21%
	學士	3	21.43%		筆記型電腦	8	57%
	碩士	6	42.86%	個人的行動裝置使用在工作單位	有	12	86%
	博士	3	21.43%				
產業性質	學術	1	7.14%		沒有	2	14%
	醫療	1	7.14%				
	電信	1	7.14%	工作單位有提供行動裝置	有	7	50%
	製造業	1	7.14%		沒有	7	50%
	網際網路	1	7.14%				

項目	選項	人數	比例	項目	選項	人數	比例
	業						
	生技業	1	7.14%	工作單位提供的行動裝置 (可複選)	智慧型手機	5	36%
	證券	1	7.14%		平板	3	21%
	管理顧問	1	7.14%		筆記型電腦	8	57%
	通訊	1	7.14%				
	軟體服務業	5	35.71%				

表 11：三群受訪者準則構面一致性分析

構面	C.I.	C.R.	C.I.建議值	C.R.建議值	結果
全體受訪者					
行動裝置管理	0.00	0.00	<0.1	<0.1	接受
行動應用程式管理	0.01	0.02	<0.1	<0.1	接受
行動資訊管理	0.00	0.00	<0.1	<0.1	接受
企業風險管理	0.00	0.00	<0.1	<0.1	接受
高階主管受訪者					
行動裝置管理	0.01	0.02	<0.1	<0.1	接受
行動應用程式管理	0.01	0.02	<0.1	<0.1	接受
行動資訊管理	0.00	0.00	<0.1	<0.1	接受
企業風險管理	0.01	0.01	<0.1	<0.1	接受
資訊科技業受訪者					
行動裝置管理	0.01	0.02	<0.1	<0.1	接受
行動應用程式管理	0.01	0.02	<0.1	<0.1	接受
行動資訊管理	0.00	0.00	<0.1	<0.1	接受
企業風險管理	0.00	0.00	<0.1	<0.1	接受

三、準則構面與關鍵因子之權重分析與比較

首先對全體 14 位受訪者的意見進行分析，透過建立成對比較矩陣取得相對的權重值分析後，全體受訪者準則構面之權重結果如表 12，準則中最受重視依序是行動資訊管理(0.374)、行動裝置管理(0.246)、企業風險管理(0.216)與行動應用程式管理(0.164)。表 12 中亦說明全部影響因子整體權重排序，最重要的三者依序為：資料防護(0.192)、安全認證管理(0.109)與資料使用目的與方式(0.092)。

表 12：全體受訪者的關鍵管理因素權重分析表

準則	權重	準則權重排名	影響因子	影響因子權重	影響因子排名	影響因子整體權重	影響因子整體排名
行動裝置管理(MDM)	0.246	2	軟體部署	0.152	4	0.038	11
			元件管理	0.160	3	0.039	10
			安全認證管理	0.444	1	0.109	2
			裝置失竊管理	0.245	2	0.060	6
行動應用程式管理(MAM)	0.164	4	存取控制	0.359	1	0.059	7
			代理程式安全	0.173	3	0.028	14
			通信軟體管理元件	0.182	2	0.030	13
			通信服務品質	0.166	4	0.027	15
			軟體缺陷	0.121	5	0.020	16
行動資訊管理(MIM)	0.374	1	資料防護	0.513	1	0.192	1
			資料查詢	0.240	3	0.090	4
			資料使用	0.247	2	0.092	3
企業風險管理(ERM)	0.216	3	財務風險	0.236	3	0.051	9
			公司資安政策	0.347	1	0.075	5
			病毒威脅	0.268	2	0.058	8
			錯誤操作行為	0.149	4	0.032	12

接著進行七位受訪高階主管的分析，高階主管們在準則構面的重視程度依序是企業風險管理(0.364)、行動資訊管理(0.306)、行動裝置管理(0.178)、行動應用程式管理(0.152)，可知企業風險管理是高階主管們最重視的問題，如表 13 所示。表中亦說明全部關鍵因子整體權重排序，最重要的三者依序為：資料防護(0.169)、公司資安政策(0.122)與財務風險(0.102)。在 ERM、MIM、MAM 中，高階主管最關心的問題與全體受訪者無異，然而在 MDM 準則構面中，卻最在意裝置失竊管理，擔心設備失竊對企業的衝擊。

表 13：高階主管群的關鍵管理因素權重分析表

準則	權重	準則權重排名	影響因子	影響因子權重	影響因子排名	影響因子整體權重	影響因子整體排名
行動裝置管理(MDM)	0.178	3	軟體部署	0.160	3	0.028	12
			元件管理	0.095	4	0.017	16
			安全認證管理	0.277	2	0.049	9
			裝置失竊管理	0.467	1	0.083	5
行動應用程式管理(MAM)	0.152	4	存取控制	0.337	1	0.051	8
			代理程式安全	0.197	2	0.030	11
			通信軟體管理元件	0.137	5	0.021	15

			通信服務品質	0.182	3	0.028	12
			軟體缺陷	0.148	4	0.022	14
行動資訊管理(MIM)	0.306	2	資料防護	0.551	1	0.169	1
			資料查詢	0.225	2	0.069	6
			資料使用	0.225	2	0.069	6
企業風險管理(ERM)	0.364	1	財務風險	0.281	2	0.102	3
			公司資安政策	0.336	1	0.122	2
			病毒威脅	0.257	3	0.093	4
			錯誤操作行為	0.126	4	0.046	10

針對資訊科技業軟體工程師受訪專家的分析，顯示軟體工程師的重視程度依序是：行動資訊管理(0.408)、行動裝置管理(0.324)、企業風險管理(0.138)、行動應用程式管理(0.130)，如表 14 所示，結果說明軟體工程師認為在行動資訊管理上需要特別重視及加強；此與全體受測者群組的意見一致，且在各個構面中最重視的各影響因子，也與全體群組是相同。表中亦說明全部關鍵因子整體權重排序，最重要的三者依序為：資料防護(0.218)、安全認證管理(0.139)與資料使用(0.096)。

表 14：資訊科技業群的關鍵管理因素權重分析表

準則	權重	準則權重排名	影響因子	影響因子權重	影響因子排名	影響因子整體權重	影響因子整體排名
行動裝置管理(MDM)	0.324	2	軟體部署	0.169	3	0.055	6
			元件管理	0.141	4	0.046	9
			安全認證管理	0.428	1	0.139	2
			裝置失竊管理	0.262	2	0.085	5
行動應用程式管理(MAM)	0.130	4	存取控制	0.409	1	0.053	8
			代理程式安全	0.161	2	0.021	13
			通信軟體管理元件	0.129	3	0.025	12
			通信服務品質	0.125	4	0.016	15
			軟體缺陷	0.114	5	0.015	16
行動資訊管理(MIM)	0.408	1	資料防護	0.534	1	0.218	1
			資料查詢	0.230	3	0.094	4
			資料使用	0.236	2	0.096	3
企業風險管理(ERM)	0.138	3	財務風險	0.185	3	0.026	11
			公司資安政策	0.392	1	0.054	7
			病毒威脅	0.283	2	0.039	10
			錯誤操作行為	0.140	4	0.019	14

四、討論

經由以上分析，接著進行三群組的分析結果比較，如表 15 所示。在準則構面部份，全體受訪者與資訊科技群最重視行動資訊管理(MIM)，而高階主管群則最重視企業風險管理(ERM)，說明高階決策者對於企業整體的風險安全最為重視，以能在安全無虞的環境中維持企業正常的運作，以及面臨風險時如何進行有效的解決與管理；反觀資訊科技群對於行動資訊使用的管理最為重視，主要是因為企業使用者可隨身攜帶行動裝置與隨時存取企業內部的資訊，並將資料儲存於行動裝置內，一旦資料曝露時將面臨許多風險的問題。因此，如何有效的進行行動資料管理成為資訊科技人員最為重視的管理問題，此問題也與 Scarfo(2012)的研究和 Thomson(2012)的研究說明企業應提供安全的網路與資料供員工進行資訊存取相互呼應。

而在各準則構面的關鍵影響因子分析部份，行動裝置管理(MDM)準則構面的關鍵影響因子，全體受訪者與資訊科技群最重視安全認證管理，高階主管群較注重裝置失竊管理，主要是因高階主管群多為高階決策者，在決策考量時，會較注重裝置失竊對組織的衝擊，並且三群對裝置失竊管理及安全認證管理的重視程度皆為權重評分之前兩名，顯示這兩者重要性較高。因此，在安全認證管理方面針對使用者身分的確認與驗證較需重視與處理，身分驗證機制強弱與否關係到整個公司資訊安全議題，如能採用多因素認證辨識系統，應可加強驗證安全性。在行動應用程式管理(MAM)準則構面的關鍵影響因子中，三群最重視的皆為存取控制，表示在存取控制方面針對使用者權限控制與管理較需重視與管理設定。行動資訊管理(MIM)準則構面的關鍵影響因子中，三群最重視的皆為資料防護，顯示注重機敏資料防護刻不容緩。在企業風險管理(ERM)準則構面的關鍵影響因子中，三群皆最重視公司資安政策，表示較需特別注意政策之訂定、宣示、規畫與執行。由此可知，各準則構面的關鍵因子也為企業導入 BYOD 應加以重視的因素，企業若能有效掌握導入 BYOD 的關鍵管理因素與影響因子，才能明確訂定企業的 BYOD 管理策略，以加強攜帶自己設備的管理原則與提升企業的資訊安全(Bello Garba et al. 2015)，同時企業有明確的 BYOD 政策對員工的工作效率與企業獲利皆具有正向的影響(Singh 2012)。

表 15：三群受訪者最重視的準則構面與影響因子比較

準則構面	全體受訪者	高階主管群	資訊科技群
BYOD 導入之關鍵管理因素	行動資訊管理	企業風險管理	行動資訊管理
行動裝置管理	安全認證管理	裝置失竊管理	安全認證管理
行動應用程式管理	存取控制	存取控制	存取控制
行動資訊管理	資料防護	資料防護	資料防護
企業風險管理	公司資安政策	公司資安政策	公司資安政策

伍、結論與建議

行動裝置的盛行，已成為現今人人必備用以儲存資料與通訊的重要工具，並

且也在不知不覺中與職場環境融合在一起，成為攜帶自己行動裝置用於工作中的普遍現象，雖然對職場帶來許多工作的便利性，但也引發許多令企業管理層級擔憂的問題。本研究即以組織管理層級的觀點探討企業 BYOD 導入之關鍵管理因素，分析出影響 BYOD 導入之關鍵管理因素的四項重要準則構面，為：行動裝置管理(MDM)、行動應用程式管理(MAM)、行動資訊管理(MIM)與企業風險管理(ERM)，而這四個準則構面共包含 16 項影響因子，這些都是企業導入 BYOD 在管理上極需要重視的部份，企業也由掌握這些關鍵管理因素與影響因子才能制定安全導入 BYOD 的政策，並且降低發生行動裝置使用的資訊安全相關問題。

由於攜帶自有行動設備用於工作中，有可能帶來資料遺失與被竊取方面的問題，也是自有行動裝置導入企業環境的最大阻礙因子。研究中以高階主管的觀點與資訊科技人員的觀點進行分析，在各項準則中二群受訪者有意見相同亦有相佐之處，高階主管最重視企業風險管理(ERM)的問題，而資訊科技人員最重視行動資訊管理(MIM)的問題。而各準則構面的影響因子也有相同與相異之處，高階主管最重視的前三項影響因子為：資料防護、公司資安政策與財務風險，資訊科技人員最重視的前三項影響因子為：資料防護、安全認證管理與資料使用。這二群的受訪者雖然有些觀點不同，但是也反應出企業管理面與執行面對於企業導入 BYOD 政策具有不同的隱憂，高階主管群從企業風險管理的角度思維整體風險管理的重要性，期望在任何行動裝置使用過程中造成的風險問題，皆能在有效的公司資安政策維護下，降到最低的風險損失，包含財務風險等，以及加強對於資料防護的重視程度；資訊科技群則從行動資訊管理的執行角度思維資料防護與資料使用的重要性，在使用者使用行動裝置於任何時間與地點存取企業資料時，皆需要進行完整的身份認證程序，並且企業要建立清楚的行動資料保護方式與使用規範，以提升行動資訊管理的安全。

經由研究分析結果說明，行動資訊管理(MIM)準則構面中的資料防護被受訪專家認為是 BYOD 導入之關鍵管理因素最重要的問題，也就是說在現今高度行動化的環境中，企業在導入 BYOD 時應特別重視資料保全的問題，不僅要強化機敏資料的防護，並且應建立企業的資安政策與善用資安技術，此也為企業導入 BYOD 的首要關鍵管理因素。同時企業也應強化與落實資訊安全政策，有效進行行動設備及應用程式的身分驗證及存取控制的管理，以及徹底讓資安政策與實踐制度化，也為企業導入 BYOD 的關鍵管理因素，共同提升企業導入 BYOD 的資訊安全與管理品質。本研究貢獻在於由組織管理觀點分析影響企業 BYOD 導入之管理策略的重要準則構面與影響因子，經由關聯程度及相對權重分析出重要準則構面，依序為 MIM、MDM、ERM 與 MAM，並且提出企業導入 BYOD 的具體建議：(1)企業應優先重視 MIM 以強化對機敏資料的防護；(2)企業應重視內部資訊安全政策，有效針對行動設備及應用程式強化其身分驗證和存取控制；(3)落實行動設備之應用目的控管，並使資安實踐制度化。

本研究採用修正式德爾菲法進行專家意見的調查，第一回合的問卷題項內容是經由文獻探討產生，並且於第一回合的調查中受訪專家即已達成共識，但對於

受訪專家的實務經驗尚未經由研究調查取得，並且本研究僅著重在組織的資訊安全管理觀點，探討企業導入 BYOD 對企業資訊安全管理影響的核心主軸與應掌握之關鍵因素，因此面對 BYOD 不斷快速擴展的成長趨勢，取得受訪專家實務觀察與經驗知識至為重要，此也為未來研究可以繼續深入探討的議題。此外，由於本研究的主要研究核心是以組織資訊安全管理的觀點出發，思考企業 BYOD 導入的相關資訊安全管理問題，因而本研究僅將研究議題鎖定在探討組織對於 BYOD 導入要在資訊安全上掌握的關鍵因素進行研究，其它有關於組織管理與經營對 BYOD 導入會產生影響的問題就較少觸及，所以在此研究脈絡的思考過程中查詢到 Scarfo(2012)與 Madden(2012)二位學者對於行動裝置使用之資訊安全問題有許多的見解，因此本研究融合二位學者的研究洞見成為本研究的主要構面基礎，並且因 BYOD 導入對企業帶來的資安風險問題即刻出現，本研究也在理論探討過程中參考相關文獻指出，一旦風險發生企業要面對風險控制、評估與規避等的問題，且要能有立即處理的能力與制定相關管理策略，因而將此構面納入為企業 BYOD 導入時組織管理應要有的思考。由此形成本研究初步的理論概念模型，在行動裝置管理部份分為裝置、資源與應用程式存取的管理，以及企業風險的管理上。也因為本研究希望能將研究的內容集中在企業導入 BYOD 與對企業資訊安全管理影響的核心主軸，因此對於組織其它構面的探討則沒有列入本研究中，至於掌握組織內部與 BYOD 導入有關的因素，例如：企業資源、組織支持、組織彈性、領導風格等因素，對於 BYOD 導入會帶來那些影響？也是值得後續繼續研究的議題，以能對企業 BYOD 導入之管理有更多的深入探討與解決現今企業皆面臨的資訊安全問題。

誌謝

作者感謝主編與二位匿名審查學者給予本論文諸多寶貴意見，使本論文內容更臻完善；本研究承蒙大同大學基礎研究案經費支持，計畫編號：B105-N01-030，謹致謝忱。

參考文獻

Ackerman, A.S. and Krupp, M.L. (2012), 'Five components to consider for BYOT/BYOD', *International Association for Development of the Information Society*, pp. 35-41. From http://files.eric.ed.gov/fulltext/ED542652.pdf, Accessed on 2015/7/12.

Bello Garba, A., Armarego, J. and Murray, D. (2015), 'Bring your own device organizational information security and privacy', *ARPN Journal of Engineering and Applied Sciences*, Vol. 10, No. 3, pp. 1279-1287.

Bisdikian, C., Mitschang, B., Pedreschi, D., Tseng, V.S. and Bettini, C. (2011), 'Challenges for mobile data management in the era of cloud and social computing', *2011 12th IEEE International Conference on Mobile Data Management (MDM)*, Vol. 1, p. 6.

Brooks, K.W. (1979), 'Delphi technique: expanding applications', *North Central Association Quarterly*, Vol. 53, pp. 377-385.

Cao, P., Tang, G.C., Zhang, Y. and Luo, Z. Q. (2014), 'Qualitative evaluation of software reliability considering many uncertain factors'. In Ecosystem Assessment and Fuzzy Systems Management, 199-205. Springer International Publishing.

Chen, P.S., Yen, D.C. and Lin, S.C. (2015), 'The classification of information assets and risk assessment: an exploratory study using the case of C-Bank', *Journal of Global Information Management,* Vol. 23, No. 4, pp. 26-54.

Copeland, R. and Crespi, N. (2012a), 'Analyzing consumerization - Should enterprise business context determine session policy?' *2012 16th International Conference on the Intelligence in Next Generation Networks (ICIN).*

Copeland, R. and Crespi, N. (2012b), 'Establishing enterprise business context (eBC) for service policy decision in mobile broadband networks'. *2012 21st International Conference on the Computer Communications and Networks (ICCCN).*

Dalkey, N.C. (1969), 'The Delphi method: An experimental study of group opinion'. Santa Monica, CA: The Rand Corporation.

Dalkey, N. and Helmer, O. (1963), 'An experimental application of the Delphi method to the use of experts'. *Management science,* Vol. 9, No. 3, pp. 458-467.

de Meyrick, J. (2003), The Delphi method and health research. *Health education,* Vol. 103, No. 1, pp. 7-16.

Delbecq, A.L., Van de Ven, A.H. and Gustafson, D.H. (1975), 'Group techniques for program planning: a guide to nominal group and Delphi processes'. Chicago, NJ: Scott. Foresman and Company.

Di Zio, S. and Maretti, M. (2014), 'Acceptability of energy sources using an integration of the Delphi method and the analytic hierarchy process'. *Quality & Quantity*, Vol. 48, No. 6, pp. 2973-2991.

Eslahi, M., Naseri, M.V., Hashim, H., Tahir, N.M. and Saad, E.H.M. (2014), 'BYOD: current state and security challenges'. *2014 IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE),* pp. 189-192.

Gessner, D., Girao, J., Karame, G. and Li, W. (2013), 'Towards a user-friendly security-enhancing BYOD solution'. *NEC Technical Journal*, Vol. 7, No. 3, p. 113.

Ghosh, A., Gajar, P.K. and Rai, S. (2013), 'Bring your own device (BYOD): security risks and mitigating strategies'. *Journal of Global Research in Computer Science*, Vol. 4, No. 4, pp. 62-70.

Green, B., Jones, M., Hughes, D. and Williams, A. (1999), 'Applying the Delphi technique in a study of GPs' information requirements'. *Health & social care in the community*, Vol. 7, No. 3, pp. 198-205.

Holden, M.C. and Wedman, J.F. (1993), 'Future issues of computer-mediated communication: the results of a Delphi study'. *Educational Technology Research and Development,* Vol. 41, No. 4, pp. 5-24.

Hsu, P.F., Chiang, H.Y. and Wang, C.M. (2011), 'Optimal selection of international exhibition agency by using the Delphi method and AHP'. J*ournal of Information and Optimization Sciences,* Vol. 32, No. 6, pp. 1353-1369.

Hsu, P.F., Tsai, C.W. and Chen, K.C. (2014), 'Optimizing the host of a travel program for commercial tv stations by using the AHP and sensitivity analysis'. *International Journal of Decision Support System Technology (IJDSST),* Vol. 6, No. 3, pp. 30-42.

InformationWeek (2012, March), '2012 State of mobile security'. From http://reports.informationweek.com/abstract/18/8792/Mobility-Wireless/research-2012-state-of-mobile-security.html?cid=rpt_cync, Accessed on 2015/4/10.

Jaramillo, D., Katz, N., Bodin, B., Tworek, W., Smart, R. and Cook, T. (2013), 'Cooperative solutions for bring your own device (BYOD)'. *IBM Journal of Research and Development*, Vol. 57, No. 6, pp. 5:1-5:11.

Khorramshahgol, R. and Moustakis, V.S. (1988), 'Delphi hierarchy process (DHP): A method for priority setting derived from the Delphi method and analytic hierarchy process'. *European Journal of Operational Research*, Vol. 37, pp. 347-354.

Kim, T.E. and Gausdal, A.H. (2017), 'Leading for safety: a weighted safety leadership model in shipping'. *Reliability Engineering & System Safety*, Vol. 165, pp. 458-466.

Kumar, R. and Singh, H. (2015), 'A proactive procedure to mitigate the BYOD risks on the security of an information system'. *ACM SIGSOFT Software Engineering Notes*, Vol. 40, No. 1, pp. 1-4.

Laudon K.C. and Laudon J.P. (2000), *Management Information Systems: Organization and Technology in the Networked Enterprise*, 6th Edition. New Jersey: Prentice Hall.

Leavitt, N. (2013), 'Today's mobile security requires a new approach'. *Computer,* Vol. 46, No. 11, pp. 16-19.

Likert, R. (1932), 'A technique for the measurement of attitudes'. *Archives of Psychology,* Vol. 140, pp. 1-55.

Lin, S.C., Chen, P.C., and Chang, C.-C. (2014), 'A novel method of mining network flow to detect P2P botnets'. *Peer-to-Peer Networking and Applications*, Vol. 7, No. 4, pp. 645-654.

Loose, M., Weeger, A. and Gewald, H. (2013), 'BYOD–The next big thing in recruiting? Examining the determinants of BYOD service adoption behavior from the perspective of future employees'. *19th Americas Conference on Information Systems (AMCIS)*.

Madden, B. (2012), 'What is MDM, MAM, and MIM? (And what's the difference?)'. From http://www.brianmadden.com/blogs/brianmadden/archive/2012/05/29/what-is-mdm-mam-and-mim-and-what-s-the-difference.aspx, Accessed on 2014/3/20.

Mallick, M.(2003), 'Mobile and wireless design essentials' (C. Long Ed.): Robert Ipsen.

Mansfield Devine, S. (2012), 'Interview: BYOD and the enterprise network'. *Computer fraud & security*, Vol. 2012, No. 4, pp. 14-17.

Marques, P., Simoes, P., Silva, L., Boavida, F. and Silva, J. (2001), 'Providing applications with mobile agent technology'. *2001 IEEE Proceedings in the Open Architectures and Network Programming*.

Marshall, S. (2014), 'IT consumerization: A case study of BYOD in a healthcare setting'. *Technology Innovation Management Review*, Vol. 4, No. 3.

Miller, K.W., Voas, J. and Hurlburt, G.F. (2012), 'BYOD: security and privacy considerations'. *It Professional*, No. 5, pp. 53-55.

Min, J.C. (2016), 'Guiding the guides: developing indicators of tour guides' service quality'. *Total Quality Management & Business Excellence*, Vol. 27, No. 9-10, pp. 1043-1062.

Mooney, J.L., Parham, A.G. and Cairney, T.D. (2014), 'Mobile risks demand c−suite action!' *Journal of Corporate Accounting & Finance*, Vol. 25, No. 5, pp. 13-24.

Morrow, B. (2012), 'BYOD security challenges: control and protect your most sensitive data'. *Network Security*, Vol. 2012, No. 12, pp. 5-8.

Murry Jr, J.W. and Hammons, J.O. (1995), 'Delphi: a versatile methodology for conducting qualitative research'. *Review of Higher Education*, Vol. 18, No. 4, pp. 423-36.

Okoli, C., and Pawlowski, S.D. (2004), 'The Delphi method as a research tool: an example, design considerations and applications'. *Information & management*, Vol. 42, No. 1, pp. 15-29.

Parente, F., and Anderson-Parente, J. (1987), 'Delphi inquiry systems', In Wright, G., and Ayton,P. (Eds.), Judgmental Forecasting, John Wiley & Sons, pp. 129-156.

Pogarcic, I., Gligora Markovic, M. and Davidovic, V. (2013), 'BYOD: a challenge for the future digital generation'. *2013 36th International Convention on the Information & Communication Technology Electronics & Microelectronics (MIPRO)*.

Ponemon Institute (2014), 'The cost of insecure mobile devices in the workplace'. From http://www.ponemon.org/local/upload/file/AT%26T%20Mobility%20Report%20FINAL%202.pdf, Accessed on 2017/7/9.

Redman, P., Girard, J. and Wallin, L.-O. (2011), 'Magic quadrant for mobile device management software'. Gartner research, G00211101. Form http://www.air-watch.com/downloads/analyst-reports/gartner-mdm-magic-quadrant-2011.pdf, Accessed on 2015/7/11.

Romer, H. (2014), 'Best practices for BYOD security'. *Computer Fraud & Security*, Vol. 2014, No. 1, pp. 13-15.

Saaty, T.L. (1980), 'The analytic hierarchy process'. New York, NY: McGraw-Hill.

Scarfo, A. (2012), 'New security perspectives around BYOD'. In *Proceedings of the 2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications* (BWCCA), 446-451. IEEE Computer Society.

Security for Business Innovation Council (SBIC) (2012), 'Security for business innovation council report paper presented at the RSA conference EUROPE LONDON 2012'. From http://www.emc.com/about/news/press/2012/20121009-02.htm and http://www.emc.com/collateral/industry-overview/h11109-rsa-realizing-mobile-enterprise.pdf, Accessed on 2014/11/28.

Singh, N. (2012), 'BYOD genie is out of the bottle–"devil or angel"'. *Journal of Business Management & Social Sciences Research*, Vol. 1, No. 3, pp. 1-12.

Skipper, H.D. (1998), 'International risk and insurance: an environmental-managerial approach', (Ed). Chicago, IL: Irwin/McGraw-Hill.

Song, M. and Lee, K. (2014), 'Proposal of MDM management framework for BYOD use of large companies'. *International Journal of Smart Home*, 8(1), pp. 123-128.

Song, Y. (2014), '"Bring Your Own Device (BYOD)" for seamless science inquiry in a primary school'. *Computers & Education*, Vol. 74, pp. 50-60.

Standard and Poor's (2007), 'Public Finance Criteria'. New York: Standard & Poor's.

Stoneburner G., Goguen A. and Feringa A. (2001), 'Risk management guide for information technology systems', *National Institute of Standards and Technology (NIST), Special Publication* Vol. 800, No. 30.

Thomson, G. (2012), 'BYOD: enabling the chaos'. *Network Security*, Vol. 2012, No. 2, pp. 5-8.

Tokuyoshi, B. (2013), ‘The security implications of BYOD’. *Network Security*, Vol. 2013, No. 4, pp. 12-13.
Tornatzky, L.G. and Fleischer, M. (1990), ‘The process of technological innovation’, *Lexington Books*, Lexington, MA.
Ullman, E. (2011), ‘BYOD and security’. *Technology & Learning*, Vol. 31, No. 8, pp. 32-36.