基於 ISO 27001 之手機資安管理稽核分析

- 以國軍某後備單位為例

劉家驊 教授　　顏建富 研究生

醒吾科技大學資訊　　國防大學管理學院

科技應用研究所　　資訊管理研究所

089005@mail.hwu.edu.tw　　warsukes@gmail.com

摘　要

隨著科技和網路的快速發展，現代社會的網路應用已深入每個生活環節，而近年智慧型手機的普及則更多元地影響人們的生活型態；以企業經營需求而言，資訊的便利與應用效率的提升是其正面的貢獻，但從資安管理角度分析其帶來的負面安全影響，則必須予以妥善管理與整體規劃。軍事單位的資訊管理與應用因應其特殊的工作背景與安全需求，其管理嚴格程度較為殷切，而手機開放入營的現況，應如何掌握資安全生命週期各階段與各實務面向需求，實為重要課題。本研究即基於 ISO 27001 之架構來探討國軍智慧型手機管理政策，其實務管理需求則整合專家經驗來進行資安稽核項目分析，藉「政策管理、系統管制」等手段，期能降低智慧型手機入營後之可能肇生之資安風險與管理漏洞。其中應用單位在智慧型手機管理系統控制措施實施後，最符合資安稽核要求。稽核評核量表模式及整體研究結論將可用於管理精進的方向應用及提供目標管理政策擬定參考

關鍵詞：資安管理、ISO 27001、智慧型手機、資訊稽核

Abstract

Accompanied with the popular of network applications, the influence of network have deep into the every level of our life. The usage of smart cellphone have more serious effects on inner matter of lifestyle. The information usage convenience and efficiency are the positive contribution for enterprise, however, it also bring a lot problems and challenges for data security. How to proper managed and planned are important tasks. The circumstance in military unit will be a more serious case needed to solve, it is permitted to use smart cellphone inside military camp now, and thus, how to control the detail steps in the lifestyle of data security will be a major topic to study. Therefore, in this study, based on the standard of ISO 27001 for military units audit are proceeded. The terms are investigated from the experts of related areas, by usage the principle of"political managed and system control", the evaluation results will be a useful means to improve the secure problem of cellphone usage. The evaluation process and the audit result could be used for goal management and policy planning in the future.

Keywords: data security management, ISO27001, smart cellphone, information audit ,

1. 緒 論

進入二十一世紀後，隨著科技的快速進步發展與網路應用的普及，讓我們的工作或生活所產生的各項資訊皆成為可以分析利用的資訊，而現代社會的網路應用已深入每個生活環節，其中尤以近年智慧型手機的普及則更多元地影響人們的生活型態；以企業經營需求而言，資訊的便利與應用效率的提升是其正面的貢獻，但從資安管理角度分析其帶來的負面安全影響，則必須予以妥善管理與整體規劃。[1,2]軍事單位的資訊管理與應用因應其特殊的工作背景與安全需求，其管理嚴格程度較為殷切，而手機開放入營的現況，應如何掌握資安全生命週期各階段與各實務面向需求，實為重要課題。[12,16]本研究即基於 ISO 27001 之架構來探討國軍智慧型手機管理政策[18]，其實務管理需求則整合專家經驗來進行資安稽核項目分析，藉「政策管理、系統管制」等手段，期能降低智慧型手機入營後之可能肇生之資安風險與管理漏洞。研究結論將可用於管理精進的方向應用及提供目標管理政策擬定參考

1.1 研究動機

本研究主要目的在探討國軍智慧型手機管理政策在ISO 27001稽核下之管理方式與應注意之資安漏洞。因此為因應智慧型手機開放入營後之管理，國軍嘗邀集各軍司令部、指揮部業務主管及承辦人，及中科院專業人員，共同研討智慧型手機開放所伴隨之資安問題，據以研擬智慧型手機管理政策；另請中科院研發管控軟體，藉「政策管理、系統管制」等手段，降低智慧型手機入營可能肇生之風險[13,14]。惟所屬官兵在使用之際，常易忽略了政策要求及智慧型手機所伴隨的資安問題，以致肇生多起違規事件，雖尚未因智慧型手機產生洩密情事，但已嚴重的影響國軍形象，進一步即容易威脅國防安全，因此，如何有效管控智慧型手機，已變成了現今國防資訊安全的重要課題。

1.2 主要探討問題

(一) 分析國軍智慧型手機管理政策在ISO 27001稽核下資安漏洞

(二) 稽核現有智慧型手機管理政策，並利用某後備單位進行實務需求

分析，已掌握資安管理、風險評鑑等項目的問題內容。

1.3 論文架構

本論文架構說明如下:第一節說明研究動機與目的，第二節回顧基於ISO 27001與資安稽核之相關概念及創新智慧手機運用管理之相關文獻，第三節說明主要研究方法與稽核項目設計，第四節敘述稽核分析實務研究結果與分析歸納，第五節為研究結論與未來研究建議。

2. 文獻探討與相關技術

本研究的目的為探討網路應用環境中智慧型手機的資安管理政策在ISO 27001稽核下，現有政策缺陷不足及須改進的地方，並以某後備部隊為例，先期訪談相關單位中智慧型手機業務方面專家，挑選ISO 27001適用於智慧型手機管理條文，再運用條文至後備部隊實施驗證，藉資料蒐集及單位執行現況，研擬分析出現行政策不足之處，作為後續手機應用管控之參考方式，期能創造軍方低資安風險的手機使用環境。因此，文獻探討將分為五大部分進行說明，第一部份為資訊

安全定義；第二部份智慧型手機定義、及相關系統發展；第三部份為簡介軍方智慧型手機開放使用政策、執行現況；第四部份為ISO 27001資訊稽核背景與特性，第五部份為資訊安全相關指標建構文獻，以下僅就各部份文獻探討說明如下，藉以做為研究之依據。

2.1.1 資訊安全定義

隨著個人電腦於 1980 年代逐漸普及化及網際網路於 1990 年代快速成長，所有使用者的電腦都連在一起，使得病毒傳播及駭客攻擊更加方便有效。「資訊安全」議題在國內外均有學者加以研究定義如表 1，而資訊安全政策之目標，即是達成資訊系統中之機密性(Confidentiality)、完整性(Integrity)、可用性(Availability)及責任性(Accountability)[3~5]。而資安稽核是檢查和評核機構內的資訊安全的重要運作環節。圖一顯示資訊稽核是資通安全運作中重要的一環。

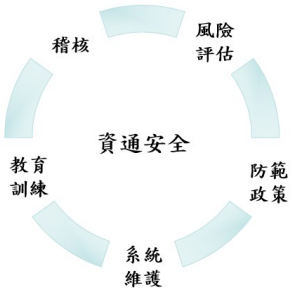

圖 1: 資通安全運作流程

2.1.2 軍方資訊安全涵義

「資訊安全」是防護資訊與資訊系統，對抗非授權連線或資訊修改，不管是在儲存、處理或針對授權使用者拒絕服務，資訊安全包含偵測設施與因應威脅作為之文件，以確保國家各項行政或國防事務產生之資訊避免遭受洩漏或損害，故我國明確律訂相關資訊安全政策及法規，供從事公家機關及國防事務的人員及團體有所依循。[11,12,13]

現行軍事各級單位及人員在運用網際網路及內部網路的使用量日趨龐大，在網際網路方面，無論是全民國防推動、災害防救、採購公告等等，均須使用到網際網路；而內部網路更是國軍人員各項作業不可或缺的重要工具。目前各單位部分辦公室均同時設有網際網路及內部網路，如不慎混接網路後果將不堪設想。[8,9]

而手機等各類行動裝置的資訊安全與管理已成為企業經營管理中保護機敏資料的重要議題，早期資訊安全的防護原本較專注於電腦的惡意軟體攻擊問題亦已移轉到手機及應用程式上，企業管理者與手機製造商也已經意識到這個問題的嚴重性，所以增加許多資安上面的研究投入。[6, 7]

國軍近年來亦戮力於推展資訊安全防護的工作與宣導行動，資訊安全的基礎發展以達成「資訊作業不間斷」、「軍事資料不外流」為目標，提供全體人員一個安全的資訊作業環境，因此落實「資訊安全」是軍方全體同仁的責任，也是落實國防安全的重要關鍵。[15,16]

2.2.3 智慧型手機定義

智慧型手機這個名詞自今尚無統一且明確的定義，依據研究分析[8]智慧型手機須具備以下五項功能，才能稱之為智慧型手機：

一、基本功能： 具備內嵌式數據與語音之無線通訊功能模組。

二、數據通訊： 具備PIM 功能，包含行程表、通訊錄、工作表、記事本、與電腦同步等功能，並可連結internet、收發e-mail。

三、語音通訊： 具備內嵌式語音通訊功能。

四、輸入方式： 觸控式、按鍵式、或語音輸入等。

五、處理器與作業系統： 擁有多工的嵌入式微處理器與作業系統。

智慧型手機就是一隻可依個人需求安裝或移除各種應用軟體的手機，所有的應用軟體是基於核心作業系統的支援來運作，目前市場主流的智慧型手機作業系統如下：Apple 的 iOS、Google 的 Android、Microsoft 的 Windows Mobile、Nokia 的 Symbian OS 及 RIM 的 BlackBerry 等。

2.2.4 ISO 27001 資訊稽核背景

ISO 主要為負責制定全世界工商業國際標準，是全球最具規模的國際標準的出版及研發機構。其產出一致同意並列入正式紀錄的文件化協定訂定標準(Documented Agreement)，範圍涵蓋技術規格、引用為規範特性之規則、指引或定義之準據，標準之運用主要為確保物質、產品、製程以及服務等均能符合使用目的。ISO 27001 是一個產業資安水準的參考指標，亦是一張資安認證，但對於某些產業的營運發展而言，其具有正面效益，在技術規範上跟現在的 IT 技術潮流，如智慧型手機的控管，也提供一個更高的標準架構，供企業重新界定新版標準和其他類似標準的整合。[17,18]一個組織的資訊資產端賴於資訊與通訊技術，這些技術使得組織能更順利的執行資訊的創作、處理、儲存、傳送、保護與銷毀。而正當全世界企業環境的相互聯繫廣度與長度不斷擴張時，所有資訊因而暴露在更廣泛及多變的威脅中而容易受傷，因此保護資訊安全的需求也日漸升高。[20]而對電子商務、保健、通信、汽車業、以及其它在商業及政府部門方面之運用而言，標準化之資訊安全技術已成為強制性之要求。而 ISO/IEC 27001:2013 配合其他 ISO/IEC 27000 各項標準，其目的即是在於協助組織更有效的達成其適當之資訊安全水準。其發展沿革如下圖 2:

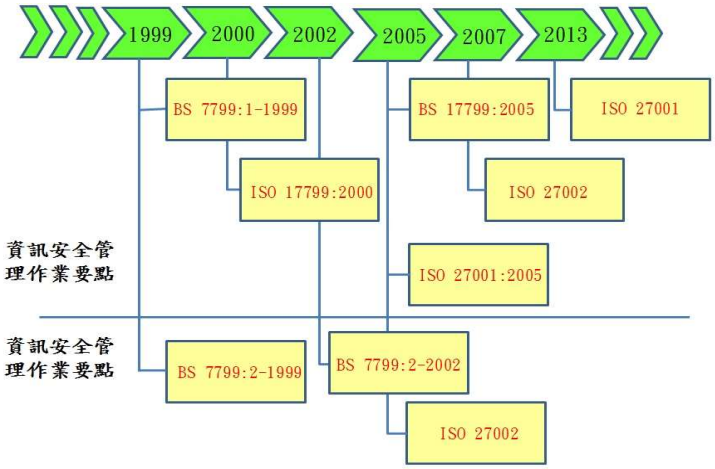

圖 2 ISO 27001 發展沿革圖（資料來源：本研究整理）

ISO 27001 主要內容涵蓋了的資訊安全控制措施以及施行資訊安全的最佳方法(Best Practice)，提供資訊安全管理系統的建立、實施、維護與書面化的具體要求，2013 年發表新版 ISO 27001 標準不再獨尊先前以資訊資產、弱點、威脅為主要考量面向之風險評鑑方式，原本定義 11 個資 訊安全管理領域 (Domain)，共 133 項控制措施，在新版標準調整為 114 項控制措施，將通訊與作業管理分成兩個獨立的領域，而「供應商關係管理 (Supplier relationships management)」及「加密（encryption)」兩項比較重要之控制目標提升為新的領域；另在控制措施方面，因應資訊技術與安全管理之發展趨勢，增加「行動裝置 (Mobile devices)管理」、「資通訊供應鏈管理」及「系統開發管理」之資訊安全要求等控制措施。[19]圖 3 顯示重要變動項目。

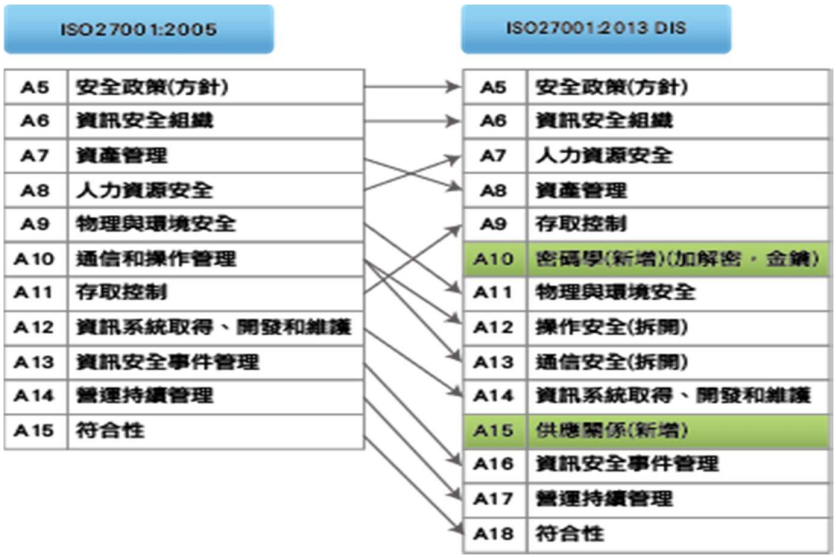

圖 3 :新版 ISO 27001 差異比較圖

2.2.5 智慧型手機開放使用政策

國防部為順應世界資訊趨勢潮流、滿足國軍官、士、兵及聘雇人員使用需求，自 102 年起，由各軍司令部及指揮部遴選部分單位辦理「智慧型手機開放試行」，以了解智慧型手機於營內使用情形，先期消弭相關危安因素，以兼顧國防安全及官兵權益。[10,11]

其中後備部隊再考量通資安全管控無虞的前提下，將整個試行期程區分「試行驗證」及「全面開放」2 個階段實施，初期以由中部地區 TC 縣市擔任試行單位，開放人員使用「智慧型手機」，並於營區內相關機敏及辦公處所劃定為「禁止使用區」，藉嚴禁攜入、部分功能管制及違規懲處等手段，要求人員確依通資安全規定落實執行，確保整體安全；另配合國防部評估檢討及技術導入等政策，作維爾後全面開放之參據，達成「安全為先，有效管理」目標。[12]

3. 研究方法

本研究採用文獻探討、專家訪談及質性研究法，主要流程如下：

1. 研究背景為國軍智慧型手機現有管理政策在資訊安全管理制度標準規範 ISO 27001 稽核下，政策不足之處，作為爾後政策修訂依據，研究主題為「基於 ISO 27001 之國軍手機資安管理體系稽核分析」，並以某後備部隊為例進行實務項目分析。
2. 蒐集智慧型手機系統及發展趨勢，初步歸納彙整智慧型手機功能，及對國軍單位、位置、資訊資產及機敏資料等可能產生之資安風險。
3. 安排與幾位具有實務經驗專家實施一對一訪談，針對 ISO 27001 控制項目遴選出與國軍智慧型手機管理相關之條文，作為稽核要項，並建立基礎評核表。
4. 至後備部隊個案單位實地查察及檢視單位紀錄資料，進行評量審查
5. 依評核結果完成資料分析與歸納。
6. 最後根據研究結果提出本研究論文結論與建議。

本研究彙整ISO 27001:2013的主要內容，經由專家訪談獲得適合國軍智慧型手機管理的項目，並參考李克特總加量表法(Likert scale)，依據ISO 27001的控制要項、控制目標與控制措施設計出四分量表，運用ISO驗證稽核的方式進行探討。

各項研究議題皆可採取不同的研究策略，不同的研究策略會造成研究方向與研究深度的差異，因此應審慎衡量不同的研究問題特徵，選擇適當的研究策略，表3-1為質性研究法的策略選擇原則，在五種質性研究方法中，依「研究問題的型態」、「對行為事件的控制要求」與「是否著重於當代事件」為考量，從中選擇適合的研究方法。根據本研究設計的評核表與訪談稽核方式，絕大多數屬於「How」與「Why」的問題類型，且遵循質性研究自然主義的精神之下，不需要(也不容易)針對某一行為事件進行控制，此外本研究探討個案業者當下的現況，一般的次級資料無法完全闡明其運作情形，必頇藉由研究者實地親訪方能瞭解實際的情況，綜合以上條件，「個案研究法」是本研究主題最理想的研究方法，藉由實地訪查，了解各縣市後備指揮部管理智慧型手機實際情形，如此能夠得到接近事實的資料，並洞察ISO 27001所建立之基礎評核表，

與單位實際執行管控各項措施其中的相互關係。[17,18]

4. 稽核分析

(一)建立 ISO 27001:2013 為基礎之評核表

ISO 27001:2013 的控制要項涵蓋了「安全政策」、「資訊安全組織」、「人力資源安全」、「資產管理」、「存取控制」、「密碼學」、「物理與環境安全」、「操作安全」、「通信安全」、「資訊系統取得、開發和維護」、「供應安全」、「資訊安全事件管理」、「營運維持管理」及「符合性」等 14 項範圍，若依此評估驗證國軍現行智慧型手機資安政策，恐無法全數適用，因此，本研究先藉由專家訪談方式，由專家遴選出適合稽核之範圍，並針對範圍完成基礎評核表建立，以利執行訪談與實地查察的作業。同時運用李克特總加量表法之四等級模式，進而發展四分量表，評核表的題號編排直接參照 ISO 27001 之控制要項、控制目標與控制措施的編號，不再另行編碼。

(二) 實施稽核

本研究的評估模式係以 ISO 27001 之資訊安全管理系統的要求事項為評核依據，[19]其相關評核作業的標準定義如下：

一、評核方式：

依據「ISO 27001基礎評核表」作為訪談以及實地查察的基礎，並就評核結果與事實發現於評核表上作勾選記錄。

二、評核量化：

評核量化之依據採稽核驗證的方式，其界定標準與評分準則如下：

●完全符合：符合控制措施的內容精神與要求，作業、流程與文件皆完整、完善，量化值為3分。

●次要缺失：符合控制措施的內容精神與要求，部分作業、流程與文件有輕微瑕疵，組織風險性程度屬於低度風險，量化值為2分。

●主要缺失：不完全符合控制措施的內容精神與要求，部分作業、流程與文件有重大瑕疵，組織風險性程度屬於中、高度風險，量化值為1分。

●不符合：完全不符合控制措施的內容精神與要求，亦缺乏相關作業、流程與文件，量化值為0分。

4.1.1 完全符合項目

實務專家均認為表 1「A.5 資訊安全政策」為整個政策之核心，包含國防部的政策指導、國防部各聯參單位針對業管項目之評估、智慧型手機攜帶入營區之限制範圍、使用之規範及使用的時間、地點等，完成整體評估後，訂定出整個管理指導方針及政策，各軍種再依政策指導方向，

擬定適用於單位的智慧型手機管理規定，如此才能符合單位需求，因此資訊安全政策內 2 個控制措施應全數納入。

表 1:ISO 27001「A.5 資訊安全政策」控制項目

A.5 資訊安全政策						
控制目標	A.5.1	資訊安全之管理指導方針		是否適用		
控制項	A.5.1.1	資訊安全政策	資訊安全政策應由管理階層定義並核准，且對給所有員工及相關外部各方公布及傳達。			
	A.5.1.2	資訊安全政策之審查	資訊安全政策應依規劃之期間或發生重大變更時審查，以確保其持續的合宜性、適切性及有效性。			

（本研究整理）

4.1.2 部分符合項目

針對「A.6 資訊安全之組織」、「A.7 人力資源安全」、「A.8 資產管理」、「A.11 實體及環境安全」、「A.16 資訊安全事故管理」、「A.18 遵循性」內各項控制項目，僅有部分適合本研究，針對各項控制項目，本研究採 2 位以上專家遴選出之控制項目為評核表，如僅有 1 位則不納入，遴選後各控制項目如表 2。

表 2-1ISO 27001 部分符合之控制項目

A.6 資訊安全之組織						
控制目標	A.6.1	內部組織		是否適用		
控制項	A.6.1.1	資訊安全之角色與責任	應定義及配置所有資訊安全責任。			
	A.6.1.3	與權責機關之聯繫	應維持與相關權責機關之適切聯繫。			
控制目標	A.6.2	行動裝置及遠距工作		是否適用		

控制項	A.6.2.1	行動裝置政策	應採用政策及支援之安全措施，以管理因使用行動裝置所導致之風險。			
A.7 人力資源安全						
控制目標	A.7.1	聘用前		是否適用		
控制項	A.7.1.2	聘用條款及條件	施行單位與員工及承包者簽訂之契約化協議書，應敘明雙方對資訊安全的責任。			
控制目標	A.7.2	聘用期間		是否適用		
控制項	A.7.2.1	管理階層責任	管理階層應要求所有員工及承包者，依施行單位所建立政策及程序施行資訊安全事宜。			
	A.7.2.2	資訊安全認知、教育及訓練	施行單位內所有員工及相關之承包者，均應接受及其工作職務相關的組織政策及程序之適切認知、教育及訓練，並定期更新。			
	A.7.2.3	懲處過程	應具備正式即已傳達之懲處過程，以對違反資訊安全之員工採取行動。			
A.8 資產管理						
控制目標	A.8.1	資產責任		是否適用		
控制項	A.8.1.1	資產清冊	應識別與資訊及資訊處理設施相關聯之資產，並製作及維持此等資產之清冊。			
控制目標	A.8.2	資訊分級		是否適用		
控制項	A.8.2.1	資訊之分級	資訊應依法律要求、價值、重要性及其對未經授權揭露或修改之敏感性分級。			
	A.8.2.2	資訊之標示	應依施行單位所採用之資訊級方案，發展及實作一套適切的資訊標示程序。			
A.11 實體及環境安全						
控制目標	A.11.1	安全區域		是否適用		

控制項	A.11.1.1	實體安全周界	應定義及使用安全周界，以保護收容敏感或重要資訊及資訊處理設施之區域。			
A.13 通訊安全						
控制目標	A.13.1	網路安全管理		是否適用		
控制項	A.13.1.1	網路控制措施	應實施網路控制措施，維護網路安全。			
	A.13.1.3	網路之區隔	應區隔各群組之資訊服務、使用者及資訊系統使用的網路。			
A.16 資訊安全事故管理						
控制目標	A.16.1	資訊安全事故及改善之管理		是否適用		
控制項	A.16.1.1	責任及程序	應建立管理責任及程序，以確保對資訊安全事故做迅速、有效及有序之回應。			
	A.16.1.2	通報資訊安全事件	應循適切之管理管道，儘速通報資訊安全事件。			
	A.16.1.4	資訊安全事件評估及決策	應評鑑資訊安全事件，並決定是否將其歸類為資訊安全事故。			
	A.16.1.6	由資訊安全事故中學習	應使用獲自分析及解決資訊安全事故之知識，以降低未來事故之可能性及衝擊。			
A.18 遵循性						
控制目標	A.18.2	資訊安全審查		是否適用		
控制項	A.18.2.2	安全政策及標準之遵循性	管理人員應以適切之資訊安全政策、標準及其他安全要求事項，定期審查其責任範圍內之安全處理及程序的遵循性。			

4.1.3 完全不符合項目

「A.9 存取控制」、「A.10 密碼學(加密控制)」、「A.12 運作安全」、「A.13 通訊安全」、「A.14 系統獲取、開發及維護」、「A.15 供應者關係」、「A.17 營運持續管理之資訊安全層面」等項目，

專家認為不適合用與本研究，主要為智慧型手機屬個人資產，對於軍中的資訊本無存取權限，且相關運作與各項資訊系統毫無關聯，均認為上述控制措施不適用本研究性質，可予以忽略。

4.2 評核結果分析

以資訊安全政策項為例:安全政策包含 1 個控制目標「資訊安全政策」以及 2 項控制措施。個案單位於安全政策的符合狀況，如表 3 所示；個案業者於安全政策的符合程度，如圖 4 所示。

表 3:個案單位於安全政策之符合狀況

題號	評估項目	量化分數 TP	NN	TY	ML	TC	NT	NN	KS	PT	平均
A.5	資訊安全政策(2項控制措施)										
A.5.1.1	資訊安全政策	2	3	3	3	1	3	2	2	3	2.4
A.5.1.2	資訊安全政策之審查	2	3	3	2	2	2	3	3	3	2.6
平均		2	3	3	2.5	1.5	2.5	2.5	2.5	3	2.5

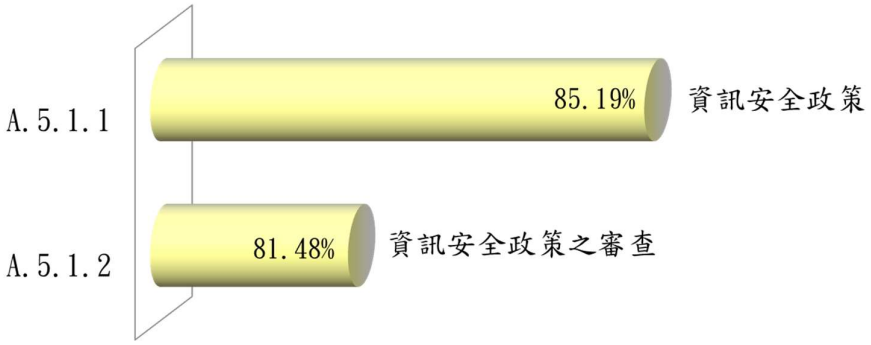

圖 4:個案單位於安全政策之符合程度

5. 結論

隨著科技和網路的快速發展，現代社會的網路應用已深入每個生活環節，而近年智慧型手機德普及則更多元地影響人們的生活型態；以企業經營需求而言，資訊的便利與應用效率的提升是其正面的貢獻,但從資安管理角度分析其帶來的負面安全影響,則必須予以妥善管理與整體規劃。軍事單位的資訊管理與應用因應其特殊的工作背景與安全需求，其管理嚴格程度較為殷切，而手機開放入營的現況，應如何掌握資安全生命週期各階段與各實務面向需求，實為重要課題。本研究即基於 ISO 27001 之架構來探討國軍智慧型手機管理政策，其實務管理需求則整合專家經驗來進行資安稽核項目分析，藉「政策管理、系統管制」等手段，將 ISO 27001:2013 內 14 個資訊安全管理領域(Domain)、35 個控制目標、114 項控制措施，並將其控制要項分為「策略面」、「管

理面」以及「作業面」，方便組織各負責單位的執行，研究結果依實務專家挑選 20 個控制措施加以分類，可有利區別智慧型手機違規案件應從哪方面著手改進。整體研究結果期能降低國軍部隊智慧型手機入營後之可能肇生之資安風險與管理漏洞。研究結論將可用於管理精進的方向應用及提供目標管理政策擬定參考。

參考資料

[1] 吳世璋，2016，網路資料中心資訊安全防護能力之研究—以空軍網路資料中心為例，國防大學管理學院資訊管理研究所碩士論文。

[2]徐弘昌，2009，以ISO 27001為基礎評估電信業資訊安全管理-以第一類電信業者為例，國立交通大學管理學院碩士論文。

[3]周哲賢、黃邦平，2015，從 ISO 27001 新版標準 看企業資安管理之挑戰與因應。

[4]行政院國家資通安全會報，2013年，國家通訊安全發展方案。

[5]李仁鍾、潘季豪、林辰諶、楊明仁，2014，企業對員工可攜式設備管理之研究-以H公司為例，華梵大學資管系。

[6]楊欣哲，林裕倫，2014，企業網站設計之資訊安全的評估模式與評量工具之研究，資訊管理學報，第21卷・第2期：107～138頁。

[7]簡唯倫，2002，智慧型手機功能發展趨勢與造形風格演變之研究-以Apple iPhone為例，大同大學工業設計研究所碩士論文。

[8]楊銀濤，1999，智慧型手機發展的趨勢研究，國立成功大學企業管理系碩士論文。

[9]黃亮宇，1992，資訊安全規劃與管理，松崗電腦圖書公司。

[10]國防部，2010，國軍資訊安全政策，臺北：國防部參謀本部通信電子資訊參謀次長室。

[11]國防部參謀本部通信電子資訊參謀次長室，2010，國軍資訊安全政策。

[12]國防部參謀本部通信電子資訊參謀次長室，2013，國軍營內智慧型手機試行要點。

[13]國防部後備指揮部，2013，智慧型手機試行實施計畫。

[14]國防部後備指揮部，2013，智慧型手機全面試行實施計畫。

[15]國防部參謀本部通信電子資訊參謀次長室，2015，國軍營內民用通信資訊器材管理要點。

[16]國防部參謀本部通信電子資訊參謀次長室，2013，國軍資通安全獎懲規定。

［17］Barafort, B., Humbert, J.P. & Poggi, S., 2006, 'Information security management and ISO/IEC 15504：the link opportunity between security and quality', Proceedings of the SPICE 2006 conference, Luxembourg, May 4～5.

[18]ISO/IEC, ISO/IEC 27001：2013 Information technology --Security techniques --Information security management systems –Requirements, 2013.

[19]ISO/IEC, ISO/IEC 27002：2013 Information technology --Security techniques --Code of practice for information security controls, 2013.

[20]McClure, C.,1994, Network literacy: a role for libraries? Information Technology and Libraries. 13(2), 115-125.