表5　各國通過ISO27001認證統計

Japan	3,378	Slovenia	13	Portugal	3
India	484	France	12	Vietnam	3
UK	407	Netherlands	12	Belgium	2
Taiwan	386	Saudi Arabia	12	Cyprus	2
China	251	Pakistan	1	Isle of Man	2
Germany	135	Bulgaria	10	Kazakhstan	2
Korea	106	Norway	10	Morocco	2
USA	95	Russian Federation	10	Ukraine	2
Czech Republic	85	Kuwait	9	Argentina	1
Hungary	66	Sweden	9	Armenia	1
Italy	58	Slovakia	8	Bangladesh	1
Poland	40	Bahrain	7	Belarus	1
Spain	39	Colombia	7	Bosnia Herzegovina	1
Austria	32	Indonesia	7	Denmark	1
Hong Kong	31	Iran	7	Dominican Republic	1
Australia	29	Croatia	6	Kyrgyzstan	1
Ireland	29	Switzerland	6	Lebanon	1
Malaysia	27	Canada	5	Luxembourg	1
Mexico	26	South Africa	5	Macedonia	1
Thailand	26	Sri Lanka	5	Mauritius	1
Greece	25	Lithuania	4	Moldova	1
Romania	25	Oman	4	New Zealand	1
Brazil	23	Qatar	4	Sudan	1
Turkey	20	Chile	3	Uruguay	1
UAE	18	Egypt	3	Yemen	1
Philippines	15	Gibraltar	3		
Iceland	14	Macau	3		
Singapore	13	Peru	3	Total	6,099

資料來源：ISMS International User Group，2010年1月[26]。

3,713個重要政府機構建立一個完整的資通安全整體防護體系，同時針對20個影響國家安全、社會安定的國家重要基礎建設資訊系統實施嚴格管制。其中並依國防、行政、學術、四大類事業體（經濟、交通、財政、衛生）劃分，並且就縱向屬性類別下再區分「A級」—「重要核心單位」、「B級」—「核心單位」、「C級」—「重要單位」及「D級」—「一般單位」等四個不同橫向等級單位。政府體系中的國土安全、金融服務、能源設施、供水系統、電信郵政、交通運輸及醫療保健等，均屬A級單位，必須在第二期(2005～2009)會報內，通過資訊安全管理系統認證。[27]

導入國際安全標準已成為未來潮流，目前臺灣已完成了資通安全相關國家標準（包括資通安全產品認證、管理系統認證及資安技術相關標準等），且已有386家公、私機構取得ISO認證，成果排名全世界第4名，這都顯示臺灣重視相關認證標準，而導入認證儼然成為臺灣資安工作的一項重要指標。

㈤CNS標準

「臺灣資訊安全管理系統標準」從2002年依照ISO17799及BS7799的標準演變至今，最新的CNS 27001及27002已於2007年10月24日公告。（如圖6）

資訊安全管理認證標準中要求組織完成資產清查與責任，並規範人力、實體與環境、網路、系統文件等安全標準、資安事件處理與改進程序及營運管理、稽核等部分。換言之即建立ISMS採用PDCA過程的模式。（如圖7）

26 http://www.iso27001certificates.com/, <Accessed,Jan/2010>

27 徐國祥，「逐步堅實推動國家資通安全防護—專訪政務委員林逢慶」，資安人雜誌，2005年1月。

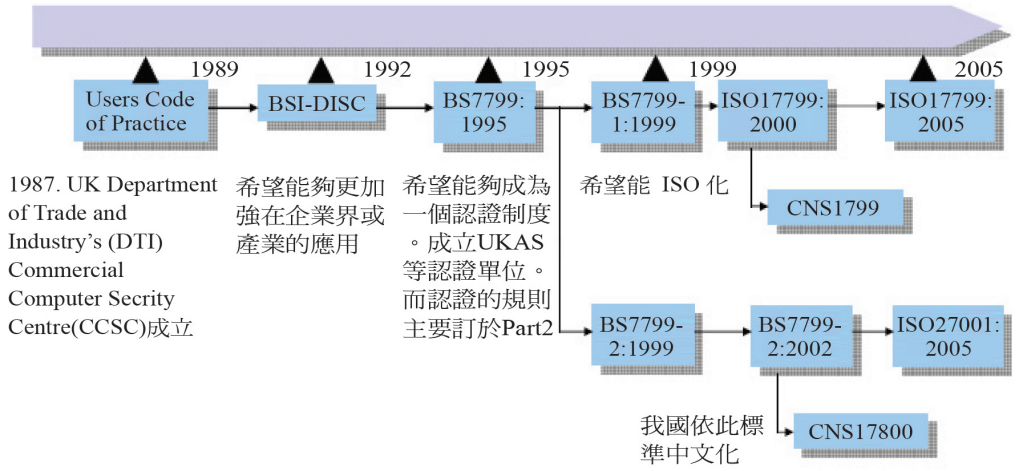

圖6　資安管理制度演變[28]

資料來源：IDC，資策會MIC整理。

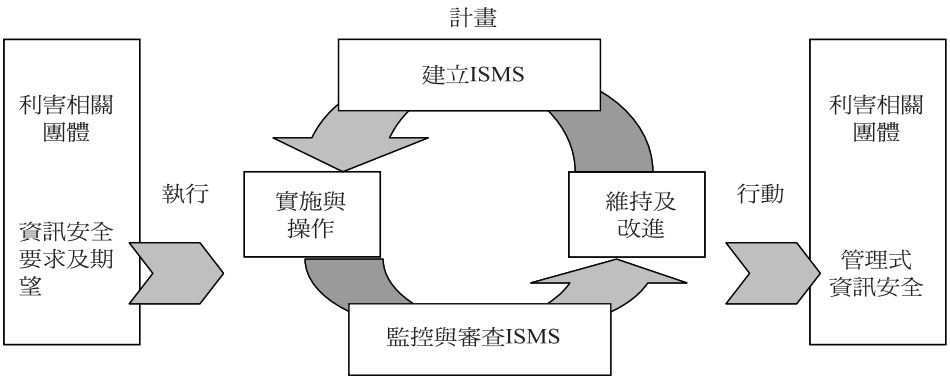

圖7　適用於ISMS的PDCA模型[29]

國內推動資安管理制度已有一段時間，行政院資通會報考量政府機關推動時，應採用國家標準還是政府規範的兩難，以及政府規範如何訂定及推動，在2010年完成5項資安認證作業規範。[30]

三、資訊資產管理目標

從第一章所列舉的資訊安全事件中，我們可以了解到重要的資訊資產應在組織中予以辨識，並加以控管，以降低資訊安全事件發生的機率：從本章探討ISO17799的國際規範、資訊安全的演進及國內外資訊安全管理系統的發展中，不論在服務及產品、或是各國通過ISO認證的機構數量，皆顯示資訊安全管理議題是極需重視且執行的。

ISO17799提出對於資訊資產分類與管理的二大目標如后：

㈠維持對於組織之資產的適當保護：所有重要的資訊資產皆應有明確的管理者。每一個業務處理流程的管理者，在所負流程中，確認重要資訊資產，公司可依資訊資產的價值及重要程度提供相對應的保護措施。

㈡確保資訊資產受到適當程度的保護：資訊資產應分類並規劃適度之控管，分類等級較高的資訊資產可能需要額外的控管。組織應擬訂一個資訊資產分類的方法，以利於規劃適宜的保護等級之控管措施。

資訊資產分類與管理的工作，就好比

28 查士朝，「BS7799/ISO17799/ISO27001資訊安全管理制度介紹與導入實務」，2006年。
29 CNS27001「資訊技術—安全技術—資訊安全管理系統—要求事項」，經濟部標準檢驗局，頁6。
30 吳依恂，〈參照國際標準、兼顧國內需求揭開ISMS新頁〉，《資安人雜誌》，2009年12月，頁49。

要蓋一棟大樓的基礎建設，如果基礎不夠紮實，將無法完成一個經得起時間及各項威脅的成品。然而，萬事起頭難，單位往往不知這個根基的工作該從何下手。在導入資訊安全管理系統的時間壓力下，可能就在尚未了解資訊安全的精神，且未深入評估選擇該單位特性、文化的方法下，即貿然進行。

參、單位資訊特性及資訊資產等級

本段區分三部分，分別介紹單位的資訊特性、探討資訊資產等級如何定義，最後綜整前二部分之資訊，探討其等級變動性，以提供單位決定資訊資產的分類及實施控管。

一、單位資訊特性

國軍不同於政府其他部門和民間企業，在遂行戰訓本務，打造堅實國防戰力的過程中，必然擁有許多具有高度機敏性的重要資料，若資訊安全出現漏洞，等於敞開國家安全大門，國土資訊安全必定受到威脅。

後備司令部主要業務有新兵訓練、動員演訓、後備軍人管理與服務、召集訓練等，其中牽涉到的資訊類型包含個人（現役及後備軍人）的基本資料、物力動員的廠商和徵用數量，動員編成名冊及戰備演訓計畫等。

其他的資訊資產則包含了大型主機、伺服器、桌上型電腦、可攜式電腦、儲存媒體、印表機與網路設備等硬體，以及業務、系統維運所必須的各項作業系統與程式（包含了人事戰備、用兵後勤系統、演訓系統和其他行政支援系統）。

國軍從民國2000年開始購進大量電腦設備，並於2001年開始配合政府政策，由國防部通資次長室訂定了許多資訊管理的規定及做法。而為有效管理國軍各級單位資訊資產數量，策頒了「國軍資訊資產管控規定」，置重點於管控連接軍、民網電腦硬體終端設備、移動式儲存媒體，遵循現行國軍財產、軍品及物品管理之登記、經管、報廢、帳籍轉移等規定，以策進掌控資安作為，提供適當安全防護管理與措施，俾利降低資訊作業風險。[31]

後備司令部則依據通次室規定研擬「資訊設備帳籍管理作業規定」，[32]其管理的範圍僅侷限在電腦設備、儲存媒體及印表機等硬體設備，卻忽略了軟體類及管理類資產。

由於本研究主要探討單位導入資訊安全管理系統，落實ISO17799之資訊資產分類與控管之做法，將以單位之資訊資產特性，進行分析及探討。

二、資訊資產等級定義

從第一章所列舉之資訊安全事件案例可以發現，資訊安全事件的發生，多起因於組織未將重要資訊資產予以辨識，並依據針對該資訊資產的風險評估，做有效之風險管理所致。依據ISO17799：2005對資訊資產分類控管的要求為：依照資訊資產之運作流程與資產價值，將資訊資產予以分類，並規劃不同分類等級資產所需之保護措施。故在資訊資產分類時，應就組織資訊資產之特性及組織資訊安全需求，擬訂組織資訊資產分類等級定義，以下就本研究整理之管理類資產分類方法詳列如后：

㈠資訊資產之三級制

31〈國軍資訊資產管控規定〉，民98年，第1頁。

32〈98年資訊設備帳籍管理作業規定〉，民98年，第1-3頁。

茲將臺灣財政部臺灣省北區國稅局、美國華盛頓大學及夏威夷健康資訊機構對資訊資產的等級定義說明及範例整理如表6。

㈡資訊資產分類之四級制

將蘇格蘭兒童通報機構(The Scottish Children's Reporter Administration, SCRA)對資訊資產的分類等級定義說明及範例整理如表7。

表6　資訊資產分類表（三級制）

財政部臺灣省北區國稅局 [33]	機密	敏感	一般
定義	無明確說明	無明確說明	無明確說明
範例	稅捐稽徵法第三十三條規定之稅務資料。	如「電腦處理個人資料保護法」中所定義之個人資料。	

美國華盛頓大學 [34]	Confidential	Official Use Only	Public
定義	以need-to-know基礎開放存取權限。	僅對校內有合理需求使用者開放存取權限，未經授權不得對外公開。	所以對校內及校外公開的資訊。
範例	個人資訊、財務資料、採購資訊、廠商合約。	教材、校內電話簿。	學校刊物。

夏威夷健康資訊機構(HHIC) [35]	Confidential	For Internal Use Only	Public
定義	該資訊未經授權的外洩會對組織、病人及協同廠商等有不利的影響。	1. 不屬於Confidential及Public者。 2. 該資訊未經授權的外洩不預期會對組織、病人、員工及協同廠商等有不利的影響。	可以對外公開的資訊，該資訊的散佈無潛在之傷害。
範例	病歷資料、採購資料、廠商合約。	公司電話表、新進同仁訓練資料。	服務小冊子。

表7　資訊資產分類表（四級制）

蘇格蘭兒童通報機構(SCRA) [36]	RESTRICTED	SENSITIVE	INTERNAL USE ONLY	UNMARKED
定義	任何與高度敏感案例相關之資料。	個人資料保護相關法規所包含之與個人有關的資料。	任何與組織運作有關的資訊。	任何合理可對外公開之資料。
範例	個人資料、非常敏感的客戶訊息、安全報告。	個人資料、組織計畫。	內部通訊資料、內部網路資料。	年報、網頁資訊、宣傳資料。

33 財政部臺灣省北區國稅局，「資訊安全政策」，http://www.ntx.gov.tw/FrontEnd/otherfiles/ntx_sec.doc, <Accessed, 2005年5月23日>。

34 George Washington University, “Data Classification Policy”, http://my.gwu.edu/files/policies/DataCla ssficationPolicy.pdf, 2005年5月23日。

35 HIPAA Readiness Collaborative Security Policies Committee, “Data Classification Policy,” http://www.hhic.org/hipaa/documents/Data%20Classification%20Policy%20Rev%20-%20FINAL.doc, <Accessed, 2005年5月24日>。

36 Cumbria Constabulary, “Government Protective Marking Scheme Policy,” http://www.cumbria.police.uk/aboutus.htm, <Accessed, 2005年5月23日>。

表8　資訊資產分類表（五級制）

	Top Secret	Highly Confidential	Proprietary	Internal Use Only	Public Document
定義	非常敏感的內部的資料，若資料外洩將對組織有嚴重影響。	如果被公開或者在組織內分享，能嚴重的妨礙組織的運作。	通常僅供個人使用。	資料的外洩對組織及管理有影響，但不致產生財物損失及組織誠信的問題。	可公開的資料。
說明	待決的購併案、投資策略、計畫、設計。	財務資料、敏感客戶的銀行資料、病患的醫學記錄。	專案計畫、工作程序書。	內部的備忘錄、會議記錄、內部專案報告。	年報。

㈢資訊資產分類的五級制

將資訊安全廠商對資訊資產的分類等級定義說明及範例整理如表8。

三、資訊資產等級之變動性

資訊資產的等級並非是其本體的價格而定，而是取決於對組織的價值，由於部分資訊資產本身的特性，使得其等級會隨著時間而改變，亦即在管制期限內與管制期限外的等級會有所不同。

就管理類資產而言，例如國軍作戰計畫或採購案件，依據「國家機密保護法」經權責長官核定及審認後，通常會有一定的機密性，一旦公開或外流，除了可能影響國家安全外，更因其機密程度的改變，造成機密要件喪失。又如個人資料，受「電腦個人資料保護法」的規範，其本身的特性不會因時間、空間等變化而變動，故其敏感性是不變的，亦即其管制期限為無限期，也不會因為部分曾被公開過而改變。針對個案單位管理類資訊資產的特性，分析資訊資產等級之變動性（如圖8）。

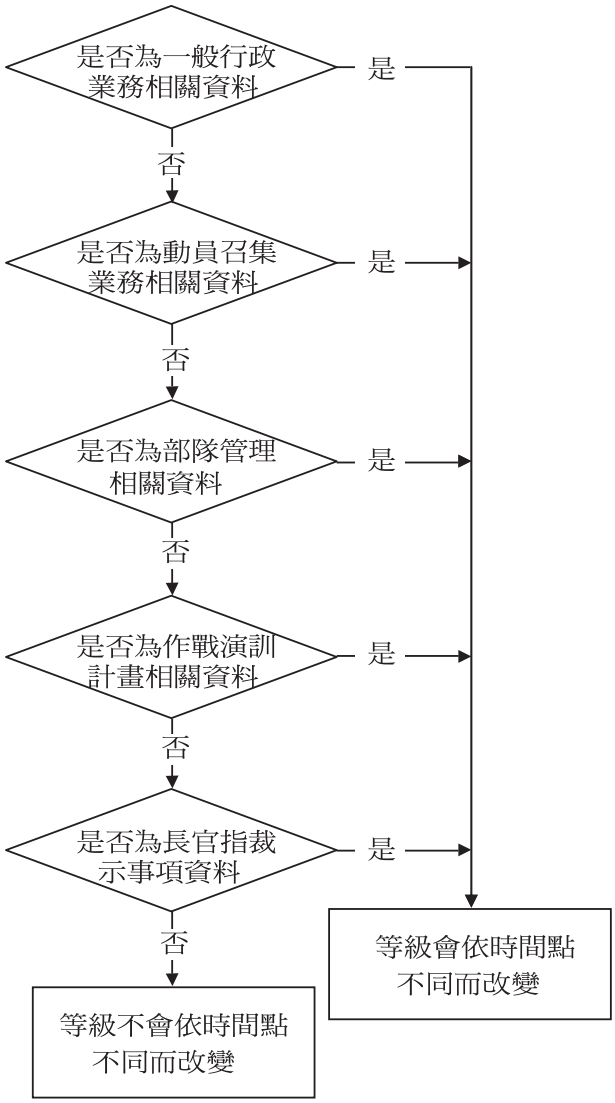

圖8　資訊資產等級之變動性

資料來源：本研究整理。

肆、資訊資產控管方法分析

就資訊系統、流程或資訊資產來說，本

身一定會有弱點，而弱點就會面臨到外在的威脅；所以要透過資訊資產的明確分類，從而規劃相對應的控管措施，以符合經濟效益及避免造成使用者怯步的反效果[37]。

一、資訊資產分類之決定方法

資訊資產分類的目的，在於後續將據此規劃各類資訊資產的控管措施，然而任何管理上或技術上的控管皆直接影響組織的成本，在分類上亦需考量相同的問題。

㈠資訊資產分類定義

依據個案單位所擁有之重要資訊資產種類及特性，及上一節各種分級的方式，三級制之分類恐過於粗略。若傾向保守做法，將大部分重要資訊資產歸於機密分類等級，可能導致重要資訊資產皆施以最嚴密之控管措施，這不但增加管理上的成本，同時亦使資訊的使用方便性下降；反之，若傾向開放做法，將大部分重要資訊資產歸於敏感分類等級，則可能導致重要資訊資產因疏於控管，而造成風險的上升；而五級制之分類對於個案單位來說則過於細微，使得在規劃上即需投入相當程度的資源。參照行政院對於核心資訊資產劃分四級原則，並依國軍資訊資產對國防及單位重要性，區分四級制如表9。

㈡資訊資產分類決定方法

單位在擬訂資訊資產分類等級之定義後，緊接著即是透過方法的運用，判定單位資訊資產之分類等級。由於單位內的資訊資產龐雜，往往摸不著頭緒，不知從何下手。

以臺灣的政府及企業機構為例，通常是以問卷的方式為之。從企業運作、財務健全面、法律面、義務聲譽考量、形象以及是否為客戶資料等方向設計問卷，對機構內部進行調查計算資訊資產之價值，進而分析其分類等級。

本研究係針對上一章實務上所使用之定義及範例，根據單位資訊資產之特性及需求，統整分析後，規劃其資訊資產分類表。

表9　資訊資產分類表

個案單位	A-作戰指管類	B-戰備訓練類	C-管理資訊類	D-行政教育類
定義	凡直接用於作戰指管系統之資訊資產均屬之，是類資訊資產遺失、損壞及存取管制失當，均將影響國軍指管任務之遂行。	凡直接用於戰備或演訓系統之資訊資產均屬之。	凡用於作業管理系統之資訊資產均屬之，其遺失、損壞及存取管制失當將造成管理資訊作業中斷。	凡用於行政作業或一般教育訓練系統之資訊資產均屬之。
範例	指管通情系統（衡山戰情系統、博勝系統、陸捷系統）、資訊戰、情報系統等作戰使用之資訊資產。	戰備系統（人事戰備、用兵後勤、通資電戰力系統）及演訓系統（兵棋裁判、戰術模擬、武器模訓系統）使用之資訊資產。	政戰、人事、主財、後勤、計畫、行政、醫療及通資電系統等使用之資訊資產。	連接民網、教育訓練及備用之資訊資產。

資料來源：本研究整理，部分摘自國軍資訊資產管控規定[38]。

37 同註31。

38 同註31，頁2-3。

二、資訊資產分類等級決定之進行方式

依上一節將資訊資產分類等級決定之方法確定後，單位可選擇運用資訊系統輔助或以紙本問卷進行，將組織裡的資訊資產一一清點，並由資訊資產管理部門之主辦人員依分類等級決定方法，判定資訊資產之分類等級，最後再由權責長官加以審核其判定之合理性，完成後即可彙整編製資產清冊。

以目前國軍所執行的資訊資產管控規定僅針對大型主機、伺服器、個人電腦、儲存媒體、印表機及網路設備等硬體設備有明確之規定區分，而資訊軟體、文件資產（書面報告、磁性媒體、電子訊息及檔案資料等）及操作人員等規範較不明確，不論是獲得、產製、區分、編號、標示、遺失等相關做法均未納入規定；[39]雖然國軍仍可依照「國家機密保護法」及相關法律來實施審認及管控，但是由於承辦單位不同，易造成管理上之漏洞及安全的風險。

單位在實施資訊資產分類評估的時，應依資訊資產的重要性及本身的弱點來評估，當威脅利用到這些弱點時，就會發生資安事件，而造成衝擊；因此資安風險可以說是這些可能發生資安事件的影響。而在評估方法上，按照ISO國際標準，[40]可分為基準法、正式法、非正式法、混合法四種。

其中正式法主要是針對可能發生的資安事件，進行細部的分析，又可以分為定性法與定量法二種，分別利用質化或量化的方式進行分析；而基準法則不進行詳細的風險分析，而以市面上的Best Practice或其他標準為基準，其中與Best Practice的差異為風險。

目前國軍採用的通常為非正式法或混合法，非正式法即由群體共同討論，決定可能遭遇的資安事件，發生的機率，以及可能造成的衝擊等，並共同決定風險。而混合法則用非正式法決定哪些部分特別重要，重要的部分採用正式法進行風險評估，而其他的部分則採用基準法。

本研究參照ISO17799的資訊資產分類方式，最後的資訊資產清冊應包括硬體資產的6大類，並將其等級區分如表10。

三、資訊資產分類之控管分析

㈠資訊資產分類的主要目的

資訊資產分類的主要目的，在於擬訂各分類等級之資訊資產之適度控管，以達到資源合理之分配，故應力求詳細列出各種使用及處理狀況，包含複製、儲存、傳輸及丟棄等。[41]亦即等級高的資訊資產需較多且周

表10　資產類別區分表

資產類別	內容
硬體資產	電腦設備、網路設備、儲存媒體、週邊。
軟體資產	作業系統軟體、應用系統、商用套裝軟體等。
支援資產	電源供應器、空調系統、辦公設施。
資料資產	系統資料庫、系統文件、使用及操作手冊。
管理資產	資訊政策及組織、管控程序等。
人員資產	機房維運、資安管理人員、行政作業人員。

資料來源：本研究整理。

39 同註31，頁3-5。

40 ISO/IEC 27005, 2008.

41 同註9。

延的控管，等級低者則較不需要規劃控管機制，甚至是不需要任何控管。單位的資源有限，控管對於單位而言即是管理成本，單位裡過多的控管，將增加無謂的管理成本；控管不足，則容易提高威脅發生的機率。

㈡資訊資產分類與控管

本研究針對個案單位的特性，以四級制資訊資產分類，說明如何規劃對於不同分類等級之資訊資產，在儲存、存取、複製、標示、備份、傳輸、銷毀、稽核及等級變更等不同的使用處理下，應有的控管方式（如表11）。該資訊資產分類與控管表之設計主要基於以下論點：

1. 儲存媒體區分為固定及可移動兩

表11　資訊資產分類與控管表

處理＼分類	A-作戰指管類	B-戰備訓練類	C-管理資訊類	D-行政教育類
儲存於固定之媒體	加密	加密	加密	不須加密
儲存於可移動之媒體	加密	加密	加密	不須加密
資訊存取	資訊資產管理者應定義存取權限並授權	資訊資產管理者應定義存取權限並授權	資訊資產管理者應定義存取權限	不須限制
電子式複製	資訊資產管理者應授予書面權限	資訊資產管理者應授予權限	撰寫者必須有相等或更高的安全許可	不須限制
紙本式複製	資料擁有者或是指定代理人	僅能複製於指定的、安全的且由人操作的輸出設備	僅能複製於由人操作的設備	不須限制
儲存媒體之標示	須標示相關機密等級	須標示相關機密等級	須標示相關機密等級	不需要
資料標示	須標示相關機密等級	須標示相關機密等級	須標示相關機密等級	不須限制
資料備份	須加密	須加密	當備份資料儲存於異地或是離開組織控管時應加密	不需要
於單位內各部門之間傳遞(紙本、CD、Floppy)	使用機密公文封上鎖並加註機密等級	使用機密公文封上鎖並加註機密等級	使用內部公文封	使用內部公文封
於單位外傳遞(紙本、CD、Floppy)	使用單位信封，密封後加註機密等級，應由可靠的傳遞者傳遞	使用單位信封，密封後加註機密等級，應由可靠的傳遞者傳遞	使用單位信封並由可靠的傳遞者傳遞	使用單位信封
於內部網路傳遞	加密	加密	加密	不需要
於網際網路傳輸	禁止於網際網路傳遞	須經由資料擁有者授權並加密	加密	不需要
資料丟棄	有管制的實體破壞	有管制的實體破壞	應予以銷毀	應予以銷毀

稽核	所有的存取應被紀錄於分離且安全的系統，該紀錄應保留二年	侵犯性的存取應被紀錄於分離且安全的系統，該紀錄應保留一年	侵犯性的存取應被紀錄	侵犯性的存取應被紀錄
資料分類等級之重新分類	資料擁有者必須取得權責長官書面同意，且必須基於業務所需，始能調整等級	資料擁有者必須取得權責長官書面同意，且必須基於業務所需，始能調整等級	資料擁有者必須取得主管同意始能調整機密等級	不需要

資料來源：本研究整理。

類，其控制點有所不同。個案單位的儲存媒體包含電腦主機、桌上型電腦、可攜式電腦、PDA等，所以需考量在不同儲存設備上的控管方式。

2.為防範資訊資產外洩，需考量資訊存取、複製及銷毀之控管方式。

3.基於災害備援之要求，所以須考量各分類等級資訊資產之備份管理。

4.單位的資訊環境有內部網路(Minet)及網際網路(Internet)，因此須考量資訊資產在不同類型網路上的傳輸安全問題。

㈢資訊資產分類控管說明

本段將列舉動員準備計畫、個人資料及電話紀錄為例，說明在資訊資產分類之控管上的應用。

1.動員準備計畫：對於個案單位來說，動員準備是平時就須要完成的，而戰時能否作戰成功，關係到平時的動員準備是否周延。依照本文表9「資訊資產分類表」，在保密期限內，動員準備計畫應為「作戰指管類」。不論儲存於固定或可移動之媒體及資料的備分，皆以加密處理。資訊資產管理者應定義存取權限並授權取得存取資料；不同形式的資料複製，有不同的控管機制；在傳輸的部份則區分為內部、透過網際網路等傳輸，各種形式的傳輸皆有不同的控管；資料丟棄時，須以有管制的實體破壞方式為之；任何與稽核有關的紀錄應存取於分離且安全的系統並保留規範的年限；該分類等級的變動，必須取得權責長官的書面同意，且必須基於業務所需，始能調整等級。

2.個人資料：不論是軍中同僚或是後備軍人的資料，單位皆應善盡保管的責任。不論國內外，皆有相關法規予以規範，單位必須知悉業務運作所觸及的國家相關法律，以確保符合要求。依照文表9「資訊資產分類表」，個人資料應為「管理資訊類」且保密期限不會隨時間改變的。故不論儲存在固定或可移動之媒體，皆應予加密；資料備份則須適當的管控機制；資訊資產管理者應定義存取權限；不同形式的資料複製，有不同的控管機制；在傳輸的部分則區分為內部、透過網際網路等傳輸，各種形式的傳輸皆有不同的控管；資料丟棄時，應予以銷毀；侵犯性的存取應被紀錄；該分類等級之變動必須取得主管同意，始能調整等級。

3.電話紀錄：單位日常運作的穩定性，除了依靠一般公文往返外，仍須依靠電話紀錄來提升工作效率，尤其當異常狀況發生時，電話紀錄可迅速將長官的指導由上向下傳遞，減少各級等待處理的時間；而完整的電話紀錄，應包含詳盡的工作指導及該領域的部分知識。依照本文表9「資訊資產分類表」，電話紀錄若內容不涉及「作戰指管

類」及「戰備演訓類」，在保密期限內之等級應為「管理資訊類」。故不論儲存在固定或可移動之媒體，皆應予加密；資料備份則須適當的管控機制；資訊資產管理者應定義存取權限；不同形式的資料複製，有不同的控管機制；在傳輸的部份則區分為內部、透過網際網路等傳輸，各種形式的傳輸皆有不同的控管；資料丟棄時，應予以銷毀；侵犯性的存取應被紀錄；該分類等級之變動必須取得主管同意，始能調整等級。

伍、結論與未來研究方向

資訊安全管理已是當今不可忽略的管理議題，其主要之精神乃在於辨識出組織的重要資訊資產及其所面臨的威脅，並在資源有效地分配下，規劃合理之控管，以使得風險降至組織可接受範圍。這是一個風險管理的過程，管理的重點應放在組織機密資料的保護，而非所有資訊資產存取的管道上，如此將造成組織的成本浪費並模糊失焦。近年來國內外層出不窮的資訊安全事件，多為缺乏上述資訊安全風險管理機制所制。

一、結論

為提供個案單位之管理類資訊資產分類與控管的建議方案，本研究從數個國內外資訊安全事件的檢討，反思國軍在資訊安全管理上的不足，試圖從案例歸納資訊資產在分類與控管上的重點。

ISO17799「資訊安全管理作業」要點，對組織導入資訊安全管理提供一份完整的參考。然而ISO17799僅提供原則與建議，如何將這些建議與單位自身的實際情況相結合，建構符合組織自身狀況的資訊安全管理系統，才是真正具有挑戰性的工作。ISO17799在標準裡描述的控制方式並非都適合於每種情況，它不可能將組織系統、環境和技術限制考慮在內，也不可能適合每一個組織。本研究即針對個案單位的特性，參考ISO17799在資訊資產分類與控管的作業要點中，分析對於個案單位有效的建議方案。

本研究發現辨識出組織的重要資訊資產為首要工作，其次是依據組織及資訊資產之特性，以有效之方法決定資訊資產之分類等級，最後，在成本效益的考量下，針對各分類等級之資訊資產，規劃不同的控管方式，並週期性的檢討達到持續改進的目標。

目前國軍各單位均依照通次室規定，對於單位資訊資產加以分類及控管，惟現行作法均以實體資訊資產管制為主，並未針對軟體類與管理類資訊資產加以控管；若能對上述二類資產完成辨識，配合現有的AD權限管理、網域管理，再運用檔案伺服器(FTP Server)管理前述資產及異地備援技術，如此即可減少個人電腦上所需儲存的程式及文件量，應可有效減少使用者電腦遭受攻擊的危險與重要資訊資產遺失與損壞之風險。

現行國軍大力推行數位文件流向管理，若能結合網路分級、檔案存取控管、電子憑證服務及自動加密、數位浮水印等機制；再配合導入ISO國際標準的資訊資產控管措施，將可有效減少數位文件外流的可能。

國防部近年來積極提升資安防護，建立良好電腦使用習慣，除安裝防毒軟體、漏洞修補，依資安設定小幫手自我檢查電腦安全，做好資安預防工作外，並讓所有資安長（官）具備執行資安服務的知識與稽核能力，做好單位的內部控管措施，以建立資安防護共識。資訊安全在於支持各項業務工作，使國軍戰備整備更加堅實，進而強化國防力量。

現有的資安防護管理機制是否符合國防的要求、持續有效及安全，是須要持續不斷的稽核和檢視的。唯有透過定期的資安稽核、弱點掃描與滲透測試，才能了解單位的資安體質情況，有效降低不同資安威脅所帶來的風險。

二、未來研究建議

本研究由於時間的限制，選擇後備司令部較易忽略的管理類資訊資產的分類與控管，做為研究內容；而單位內尚有軟體類、硬體類等資訊資產，諸如簽到系統、門禁系統、伺服器及筆記型電腦等，這些也都屬於資訊安全管理的範疇。

過去國家資通安全會報雖將政府機關的資安等級分為A、B、C、D級，但未明確規定各項防護措施應符合之防護強度，[42]如何強化資安防護面向與強度，以符合未來國家資通安全會報所擬訂的政府版ISMS標準，也是需要被考量的。另外資訊安全管理系統的建置、系統導入的困難、資訊系統的運用及如何遵循PDCA模式等，皆是屬於相關的議題，值得繼續探討研究。

收件：99年05月27日
修正：99年06月17日
接受：99年06月23日

作者簡介

林明武上校，陸軍指揮參謀學院88年班、理工學院電子工程研究所92年班及管理學院戰略班96年班；曾任陸軍通基處供應所所長、通校大隊長、步校主任教官、國防大學陸軍指揮參謀學院教官；現任職於國防大學國防管理學院教官兼隊長。

夏鈞浩中校，志預官87年班、陸軍步校正規班335期、陸軍指揮參謀學院99年班、陸院戰研100年班；曾任排、連長、資參官；現任職於後備904旅營長。

42 同註29，頁51。