以資訊安全管理系統(ISMS)架構檢視陸軍公文管理系統安全維護作業

作者／李正勝中校

提要

一、 隨著科技的進步，資訊技術越來越發達的時代，各行各業對於資訊科技的依賴更是與日俱增，享受著科技帶來的便利及資訊的隨手可得之餘，往往容易忽略便利所帶來的資訊安全之重要性。

二、 建構一個有系統且全面的資訊安全管理機制，已成為企業與政府機關的首要任務，尤其以國防安全與企業機密等機關單位，更需加強資訊安全的意識；而資訊安全治理的推動，更可降低組織資訊安全風險，強化資訊安全防衛能力。

三、 本文透過文獻探討方式，以「國際資訊安全管理標準 ISO27000 系列的規範」做為參考指引，探討本軍公文檔案管理系統維護作業，以作為提升單位內系統維運資訊安全之參考。

關鍵詞：公文檔案管理系統、資訊安全、ISO27001、資訊安全管理系統。

前言

隨著電子化政府推動，政府機關更依賴資訊科技所帶來的便利性。因此，強化資訊安全管理並建立安全及可信賴的網路環境，是當前不可忽視的重要工作。由於資訊化之推動，國軍運用電腦科技將各項作業逐步資訊化，並運用網路快速交換各項資訊，有效增進作業效能、資訊傳遞等；但是相對的資料如有管理不當，極易造成資料的錯誤或洩密情形。

因為地震、颱風、水災等天然災害；或是如駭客攻擊、各電腦病毒感染；或是人員惡意竊取資源；或是人員作業疏忽等等相關因素導致組織資訊外流、損壞、遺失等潛在的、可能的危害，即是資訊安全的威脅，依照威脅來源，大致可分為環境因素威脅、外部人員威脅、內部人員威脅等三項。

根據資策會調查資訊安全的威脅來源統計，外部人員(如駭客)只佔 5%，環境因素(天然災害)佔 15%，內部人員(包含人為疏失、不誠信員工)的比例則高達 80%。其中內部人員包含有合法授權人員與非授權人員，各佔 80%。顯見，資訊安全威脅大部分是來自於內部，當然也不能輕忽來自外部的威脅。[1]

美國傳奇駭客 Kevin Mitnick 在被補出獄後，成為一名安全顧問，曾在 2017 年

[1] 林祝興、張明信，《資訊安全概論》，第二版 (台北：旗標出版股份有限公司，2017 年)，頁 1-3

Chime-Himss 資訊主管論壇上表示，人為因素才是資訊安全的最大弱點[2]。另外，根據一項有關資料外洩事件調查指出，除了駭客攻擊佔約 4 成外，內部人為疏失造成的資料外洩也佔了近 5 成的比例，包含了內部人員疏失、資料遺失遭竊及蓄意偷取資料等，究其真實狀況，包括行動裝置遺失、經由外接儲存裝置造成的，或因訪客與廠商造成的資料外洩，以及資訊安全教育不足等等，皆反映了資訊安全防護是一項全面性的管理，抵禦入侵與內部防禦同等重要[3]。因此，為了預防人為管理漏洞所致的資安漏洞，建置一套運作制度完善的資訊安全管理系統，具有其必要性。

資訊安全管理是一項整體性的工作，其中包括管理、技術及實體等三個不同的面向，在多數人的觀念裡，資訊安全似乎多著重在實體層面與技術層面，例如，系統存取控制、建置防火牆，管制人員進出，安裝入侵偵測系統、防毒軟體、防制人為破壞等等，而忽略了管理層面的重要性。

在管理方面，組織必須制定完善的資訊安全相關的政策、規範與程序，以利明確將資訊安全各項要求落實到每個人的工作之中。其中，風險管理是整個管理制度的核心工作，確立風險所在，才能有效進行資訊安全管控。此外，要長期有效的維護資訊安全，需要建立稽核制度，以便即時發覺問題，並持續改善，才能達到降低風險，提高資訊安全管理之成效。而資訊安全管理系統(Information Security Management System, ISMS)即是一套有系統地分析和管理資訊安全風險的方法，透過控制方法，把資訊風險降低到可接受的程度內。

資訊安全定義與目標

資訊可能以事實、數據、說明等不同媒介的方式存在，是經由資料的整理、分析、彙整而來，屬於一種具備意義且必須被妥善保護的重要資產[4]。

而資訊安全是為了預防天災或是人為刻意或無心破壞，以保護系統和資料的產生、儲存、使用、傳送、展示及控制等用途，進而達成防止未經授權的存取或更改與保障合法使用者可用性的目的。此外，資訊安全的範圍需同時涵蓋技術層面和管理層面，兩者缺一不可[5]。

因此，資訊安全是組織管理的過程，而不僅是技術的導入，須透過準則與規範的制定來達成資訊安全之標的，而資訊安全的目標即需符合一般簡稱的 C-I-A 三原則，

---

[2] 謝明珊，〈傳奇駭客談網路安全：人為因素為是最大弱點〉，https://www.digitimes.com.tw/iot/article.asp?cat=158&cat1=20&id=0000495023_8rel8 51o3dact122rmtii，2016/12/20 下載。

[3] 〈駭客攻擊與人為疏失並列企業資料外洩主因〉《資安人》，https://www.informationsecurity.com.tw/article/article_detail.aspx?aid-7108，2016/12/20 下載。

[4] 張正宏，〈探討銀行業 ISO/IEC 27001:2005 資訊安全管理現況-以 T 銀行為例〉(國立中央大學碩士論文，2012 年)，頁 5。

[5] 同註 4，頁 6。

也須同時涵蓋此三者才可算是完整：(如圖一)

一、機密性(Confidentiality)

意即確保只有經授權的人，方能允許存取資訊。各類資料和資源應具有適當的安全機制予以保護，以避免無權限人員取得而危害資訊安全目標，其目的就是要確保資料在傳輸、儲存與處理理之，不被非授權人員讀取、使用或修改。

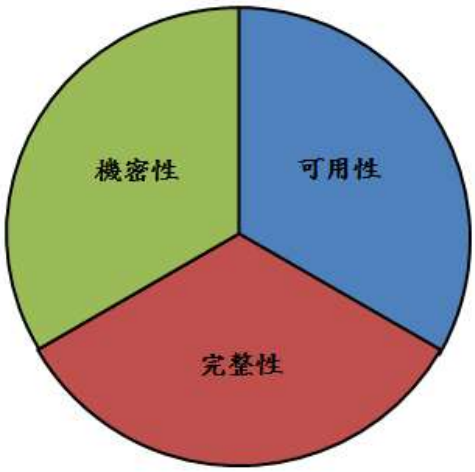
二、完整性(Integrity)

意即確保資訊內容及資訊處理方法為正確且完整。不論是外部或內部資料都應保持一致性，並避免其在傳送、接收或儲存的過程遭到修改或損毀。此外，要注意的是，不是只有遭受攻擊才會喪失資料完整性，人為的操作錯誤、設備損壞等都會是可能的因素。

三、可用性(Availability)

意即確保經授權的使用者當需要時，能存取資訊及使用相關的資產。資訊系統要能夠持續提供服務、正常運作，當合法使用者要使用資訊系統時，必須要能在一定的時間內回應使用者，並且須與上述的機密性與完整性配合在一起，不可為了確保機密性與完整性，進而影響系統的回應時間或導致系統效能降低。

圖一 資訊安全三要素



資料來源：作者繪製。

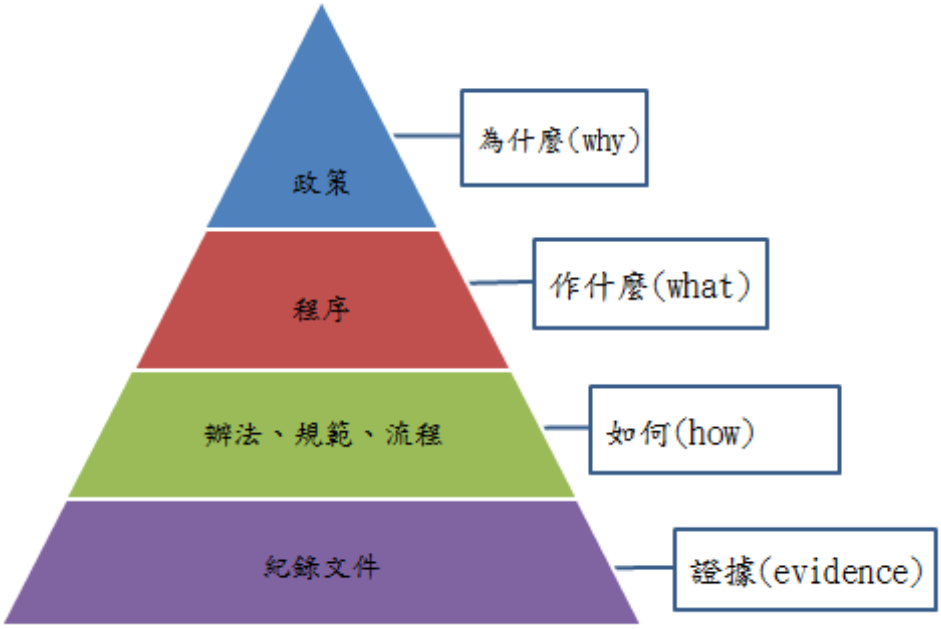
資訊安全政策

資訊安全政策是組織建置資訊安全管理制度相當重要的一環，是管理階層依照組織運作要求、相關規範等，所提出有關資訊安全管理所應遵行並執行的方向，其目的是在於強化包含：資料、系統與相關設施等的資訊資產的保護，也針對各項工作執行人員，包含往來廠商等，均應納入資訊安全政策的規範之中。

為了使檢驗或稽核組織內各項作業或活動，ISO27001 要求資訊安全管理系統文件必須以 4 階層架構呈現，分別為安全政策手冊、作業程序、作業辦法(規範或流程)及

紀錄文件等 4 種，用以查驗各項活動是否符合資訊安全政策所律定之範圍。(如圖二)

圖二 資訊安全管理系統文件體系



資料來源：作者繪製。

4 階層文件的效力是由上而下，例如：作業程序要求不得違反安全政策性文件所規範事項。各階層文件主要內容說明如下：

一、 安全政策手冊

為資訊安全管理系統主要架構之根本，包含資訊安全政策、目標及適用範圍。此為最高指導原則，提示為什麼要執行資訊安全管理，也就是述明組織內所要管理與保護資訊為何，並明確律定可為與不可為之事項。

二、 作業程序

為描述作業人員權責、作業時機、地點及程序等，是依政策文件所發展之文件，涵蓋實體、管理與技術層面的安全管控項目，並適用組織內各項作業或活動。

三、 作業辦法(規範或流程)

描述應如何完成工作，乃是依照作業程序所制訂的可行方法，此處的文件將細分為適用於特定的工作或資訊資產，具體說明達成要求所需的實際作業步驟。

四、 紀錄

執行上述各項作業之相關客觀證據，如訪客登記簿、權限異動申請等文件。紀錄的保存有利於定期的檢驗，若發現有不符合安全政策項目者，即可實施調整或矯正。

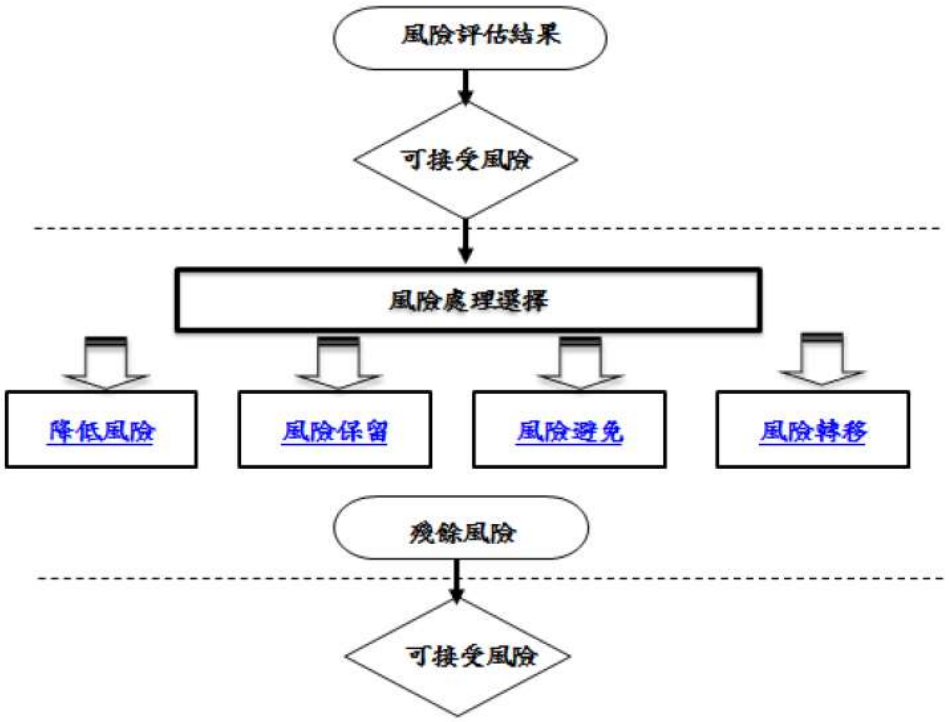
風險管理

資訊安全管理是建立在風險評鑑與管理的基礎上，良好的風險管理可以協助避免

資源的損失與浪費。風險管理是一個管理過程，包括對風險的定義、測量、評估和發展因應風險的策略。其過程主要包含風險評估與風險處理等二個部分。

風險評估包含風險識別、風險分析與風險評價等三個部分，主要是辨識出威脅或弱點為何，並分析威脅或弱點遭利用時，對組織造成的衝擊，並將其發生的機率納入考量，避免將資源投注在不太可能發生的風險上，導致資源浪費，最後進行在風險降低後，評估是否在可接受的程度內。如果不是，則必須考量在風險處理的步驟，採取更多的措施，以進一步降低風險。(如圖三)

圖三 風險管理步驟



資料來源：黃郁育，〈資訊安全管理系統版本差異之導入流程整合〉(國立中山大學碩士論文，2014 年)，頁 15。

風險處理可採取風險降低、風險保留、風險避免及風險轉移等四種方法[6]：

一、風險降低：預防損失發生，以及降低損失的嚴重性。

二、風險保留：自行承擔不願或無法轉給他人的負面風險。

三、風險避免：迴避風險發生的可能性，意即放棄或不進行可能帶來損失的活動或工作。

四、風險轉移：找尋能共同分擔風險的單位，如保險公司或是系統維護廠商等，將風險轉移出去。

要有效管理風險，就必須正確地去判斷相關資料與指標，清楚掌握組織環境變動，並讓相關人員確實了解配合。然而，要明白的是，再完全的管控措施也難保不會發生

[6] 黃郁育，〈資訊安全管理系統版本差異之導入流程整合〉(國立中山大學碩士論文，2014 年)，頁 16。

資安事件。因此，要了解到風險管理並不是 100%避開風險，而是確切瞭解風險在哪裡，並藉由適當的手段與方法，以降低或轉移風險，讓組織確立所能容忍的風險水準為何，而非一味的追求最小風險或是零風險。更重要的是，風險管理是需要持續不斷的進行監控，監視殘餘風險並識別是否有新的風險，才能確保有效管理。

資訊安全管理系統

ISO 27001 是資訊安全管理系統的國際驗證標準，以 PDCA 過程導向模式管理資訊安全管理系統，配合週期性的第三方稽核作業，驗證組織資訊安全管理系統的有效性。PDCA 循環，或稱戴明循環是 Plan-Do-Check-Action 的簡稱，處理來自「利害相關者」的資訊安全要求，以及期望並產出「受管理的資訊安全」，圖四簡要說明了 PDCA 循環如何運用在資訊安全管理系統上，包括：

一、 Plan-規劃(建立 ISMS)

建立與管理風險及改進資訊安全相關之 ISMS 政策、目標、過程(Process)以及程序(Procedure)。

二、 Do-執行(實行與運作 ISMS)

實行與運作在規劃階段所制定的政策、目標、過程與程序。

三、 Check-審查(監視與審查 ISMS)

依據制定的政策、目標及實際經驗，評鑑並測量過程與程序的有效性，並將結果回報給管理階層以進行審查。

四、 Act-行動(維持與改善 ISMS)

基於 ISMS 內部稽核、管理審查的結果，或其他相關資訊採取矯正與預防措施，以達成 ISMS 的持續改善。

五、 管理系統輸入

利害相關者對於資訊安全的要求與期望，這個部分說明了整個人資料訊安全管理系統為何建置。

六、 管理系統輸出

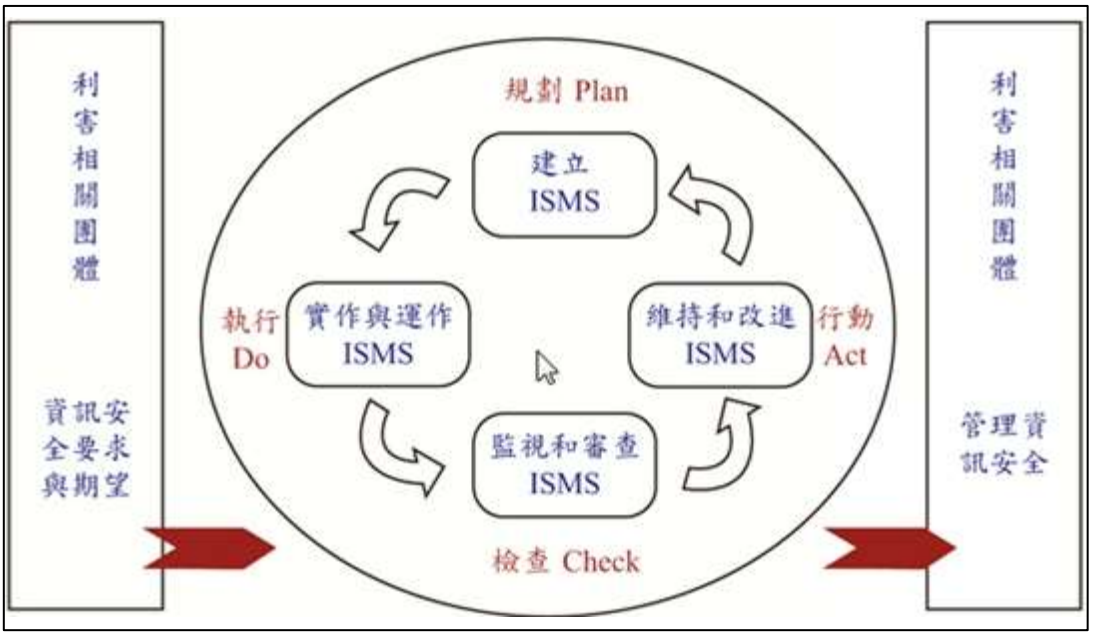
受到管理的資訊安全，此部分對應到管理系統輸入的部分，期望這樣的輸入透過 ISMS 後，可以得到「受到管理的資訊安全」。

相關研究

國防大學管理學院資管系練兆欽於〈軍事機關導入 ISO 27001 資訊安全管理成功因素之研究〉乙篇論文結論歸納[7]：

[7] 練兆欽，〈軍事機關導入 ISO 27001 資訊安全管理成功因素之研究〉(國防大學管理學院碩士論文，2011 年)，頁 82。

圖四 ISMS 系統之 PDCA 示意圖



資料來源：《凌群電子報》，http://www.syscom.com.tw/，2016/12/20 下載。

在導入 ISO27001 後，就「資訊安全政策文件」和「系統文件的安全」部分改善最多，彰顯國防部在專責資訊安全政策擬訂與策頒，統籌資訊安全管理、協調及推動，責成各級單位主官管負資訊安全責任，設置各級單位資訊安全長協助推動資安，確保全般事宜等作為的成效。此項管理工作經各級的重視及不斷修正，已逐步建立人員的資安觀念及架構，奠定相關工作推動的基礎。

國立彰師大資管學系程雅雯在〈以 ISMS 為基礎探討政府資安事件管理-以某縣市政府為例〉乙篇論文結論歸納[8]：

資訊安全須透過資安政策的制定及人員執行的配合度，再加上設備的提升，才能真正達到實質的提升資安事件防禦，也呼應以 ISMS 提倡透過管理，方能有效地提升資安係數。此外，必須了解到 ISMS 規範係屬全體性之管理規範，並非所有系統及單位都適用。根據本研究了解，一個好的管理規範及辦法，應該是針對單位各系統性質及使用者群組的使用習慣去做細部分析及評估，再配合 ISMS 規範中，適合組織單位內實體環境中可採用的管理模式。

國立中央大學資訊管理系張正宏於〈探討銀行業 ISO/IEC27001:2005 資訊安全管理現況-以 T 銀行為例〉乙篇論文結論歸納[9]：

在 ISO27001(2005)的 133 項控制措施，對銀行業最為關鍵的控制措施共 10 項，經問卷調查個案銀行後發現，133 項控制措施的重要程度並非一致。因此，隱含了部分控制措施對銀行而言，的確具有比較重要的意義。

[8] 程雅雯，〈以 ISMS 為基礎探討政府資安事件管理-以某縣市政府為例〉(國立彰化師大碩士論文，2009 年)，頁 70。
[9] 同註 4。

從實際查核結果顯示，部分高缺失的領域(構面)被重視的程序仍然不足。個案銀行之「通訊與作業管理」、「存取控制」以及「資訊系統獲取、開發及維護」三個構面查核缺失遠較其他構面來得高，但受訪者並沒有給予相對的重視程序，此現象值得重視，並加強人員的教育訓練，提高內部員工的資安認知。

ISMS 對於組織資訊安全能提供一定程序的幫助，且不致影響到組織的行政效率。研究發現，ISMS 的導入不僅可以提供強化組織的資訊安全，比較特別之處是對於銀行的行政效率也不產生妨害，此部分或許和銀行業原本資安管制就已經相當落實，且員工已經習慣相關管制措施有關。

綜整上述三篇論文發現，可了解有關資訊安全管理系統對於組織的資訊安全有其一定程序的助益，筆者也歸納出以下幾點，可供參考：

一、管理階層的支持與重視是必要的。

二、針對單位內所有的人員持續推廣資訊安全觀念。

三、完善的資訊安全管理機制。

四、資訊安全政策、目標、活動要能與業務結合。

五、對於風險審查、管理與資訊安全需求要充分了解。

六、資訊安全管理方法與架構要針對不同系統實施細部分析與評估，而非一體適用。

本軍資訊安全政策

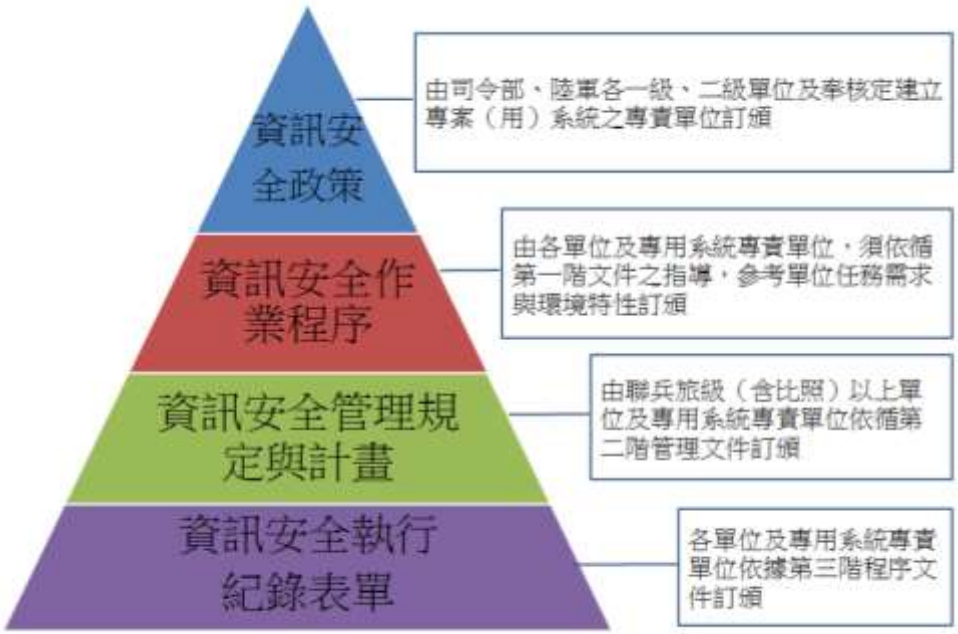
本軍於 1996 年間成立通資安全組，專職負責通資安全相關業務以來，對於各項資訊安全管理工作不遺餘力的推動，以強化本軍各級單位資訊安全防護。其於 103 年訂頒資訊安全政策 4.0 版中，即明確指出本軍資訊安全以「定義」、「達成」與「維護」國防資訊及資訊處理設施等一切與國防事務相關之資訊資產的機密性、完整性、可用性、不可否認性、可歸責性、鑑別性及可靠度為目的[10]。並且逐級要求各級依其單位任務需求與環境特性，訂定相關文件，並依照 CNS 27001 附錄表列 11 項控制領域中的 39 項控制目標，逐項訂立資訊安全政策要求。(如圖五)

公文檔案管理系統維護作業之建議

為健全政府機關檔案管理，促進檔案之開放、運用與管理效能持續提升各機關檔案管理系統之品質，並同時確保公文檔案從產生、應用至保管週期過程中，能有共通的格式與標準，行政院訂頒「文書及檔案管理電腦化作業規範」，此為機關推動公文及檔案管理資訊化重要依據。

[10] 《陸軍資訊安全管理政策》，4.0 版(桃園：國防部陸軍司令部)，民國 103 年 11 月 28 日，頁 5。

圖五 陸軍資訊安全管理文件體系



資料來源：作者繪製。

陸軍為符合上述規範要求，自民國 95 年 5 月由司令部先行導入現行公文檔案管理系統，經近一年的試行後，於 97 年底完成全軍部署，凡屬機關文書單位，均要求運用公文檔案管理系統遂行各項文書處理、稽催管制、發文作業、檔案管理等相關業務。

以下僅就筆者觀察所見提出幾項建議：

一、 建立基礎故障排除能量

公文系統自建置以來，均由司令部業管權責單位編列預算，每年進行維護採購作業，每季由得標商依契約進行定期系統維護作業、依國防部更新版本發布執行系統改版，以及不定期的故障報修處理。

然而，系統業管權責單位多歸責於文書檔案單位，相關人員多數無資訊相關基礎背景，面對問題時，完全依賴維護廠商，如向單位資訊業管部門詢問，少部分單位多以非其業管權責或不熟悉系統，而無法提供協助。

維持系統運作，讓合法使用者能正常使用系統是資訊安全政策的要求之一，本軍各級單位均有資訊組編制，主要任務為確保單位資訊網路及系統安全為目的，遂行單位資訊機房各項軟硬體設備維護、系統服務維運與網路連線檢測，並從平時作業與維護中實施訓練與學習。因此，須使各單位資訊部門人員應具備單位內各項系統基礎故障排除能力，藉以協助單位各項資訊系統運作正常。

二、 建立系統備援機制

系統備援是維護資訊系統可用性與完整性的重要工作之一 。由於系統可能因各類因素失效以致無法正常提供服務，如硬體故障、軟體漏洞、天然災害或是遭受病毒或

駭客攻擊等，都是導致系統無法持續提供服務的原因。因此，可靠的備援機制即可讓損失降至最低。

公文檔案管理系統依建置單位及所屬使用單位人數多寡，配置不同規模之資料庫伺服器，小單位為單一伺服器，大單位則多加配屬一部儲存設備，儲存空間均採 RAID 5 架構，具備基本之安全措施，此外，利用 Windows 內建工作排程器排定每日夜間執行系統備份作業。

雖然備份是由排程每天進行，但是公文系統是每日持續不斷運作，備份與實際使用的資料會有一定的差異，除了考量資料完整及差異備份外，應將交易記錄也列入備份計畫，在不影響設備狀況與系統執行效能之下，以最密集的方式，執行交易備份，若發生資料庫毀損時，可將資料遺失的程序降至最低。

在預算允許的狀況下，建立資料庫備援機制才能確保系統服務不中斷，某單位就曾發生過 RAID 5 的磁碟陣列發生同時損壞兩顆硬碟的記錄，雖然先利用備份檔還原讓系統上線運作，最後仍花費了近一個星期的時間，才將所有資料補齊，如有妥善的備援機制，當重大資安事件發生時，才能在可接受的時間內恢復服務。

三、落實機房維護管理

傳統的實體安全只著重於資訊中心機房內的安全設施，現代的實體安全需要整合實體安全與資訊管理為一體，才能完成實體安全的任務。實體安全涵蓋的範疇很廣，從外部環境到內部資訊設備皆是實體安全所包含的範疇，如冷熱通風系統、火災防護、監視系統、消防系統、門禁系統等。

各單位公文系統均統一置放於單位資訊機房，依陸軍機房管理作業規定要求，機房值班人員應隨時注意電力、空調、消防及不斷電系統是否正常運作，如有異常立即通知檢修及採取應變措施。曾有單位因空調設備無備援，又不堪長時間運轉導致設備故障，使各類主機處於高溫下運作；另有單位將不斷電系統僅供網路設備及特定系統使用，而非提供機房內所有設備使用，均曾導致公文系統故障。

公文系統建置單位遍及臺灣本島各地及外島地區，各地氣候環境均不同，對於環境管理控制必須要因地制宜。天氣炎熱的，加強空調系統；電力不穩定或常有雷擊的，加強不斷電系統或避雷措施。且依相關管理作業規定要求，凡置放於機房內之各類資訊設備、系統，均應依相同標準實施維護管理，避免設備因人為因素導致損壞。

結論

美國知名管理學家勞倫斯．彼得曾提出木桶理論，也就是短板理論，該理論講的是：組成木桶的木板如果長度都不一樣，那麼決定木桶的盛水量的，不是取決於最長的那一塊木板，而是取決於最短的那一塊木板。若將組織視為一個木桶的話，桶子裡

的水就是公司的資源，如何確保桶子裡的水不會輕易的往外流，就是取決於木板的長度，組織的每一份子，包含各項軟、硬體設備，都是組成桶身的木板。因此，組織資訊安全的強度，不是取決於最長的木板，而是最短的木板，各類的威脅必定是在最弱的地方所產生的。

資訊安全管理系統就是以風險管控的角度出發，在明確釐清想要管控的範圍後，實施風險評鑑，確定可接受的風險程度為何之後，逐步就相關管理規則及作業程序之要求，完成相關規定的訂定，並加以施行及記錄。最後，依 PDCA 循環的方法，持續的檢測、精進相關安全管理作法，方能使組織所須面對的資訊安全風險降至最低。

本篇文章僅就筆者觀察所得，未進行較為客觀與量化之調查及統計，未來可針對 ISO27001 所定義之各控制措施實施細部深入探討，以取得客觀且足供參考佐證研究。

參考文獻

一、侯皇熙，〈植基於 BS7799 探討政府部門的資訊安全管理-以海關資訊部門為例〉(國立成功大學碩士論文，2004 年)。

二、林麗英，〈資訊安全管理系統績效評估之研究-以檔案管理局為例〉(朝陽科技大學碩士論文，2010 年)。

三、練兆欽，〈軍事機關導入 ISO 27001 資訊安全管理成功因素之研究〉(國防大學管理學院碩士論文，2011 年)。

四、程雅雯，〈以 ISMS 為基礎探討政府資安事件管理-以某縣市政府為例〉(國立彰化師大碩士論文，2009 年)。

五、徐弘昌,〈以 ISO27001 為基礎評估電信業資訊安全管理-以第一類電信業者為例〉(國立交通大學碩士論文，2009 年)。

六、張鴻正，〈資訊安全管理系統內部稽核管理工具之研究-以國軍某單位資訊中心為例〉(國防大學管理學院碩士論文，2010 年)。

七、聞美晴，〈資訊安全管理系統 ISO27001:2013 與 ISO27001:2005 差異說明〉《金融聯合微信》(臺灣：財團法人金融聯合徵信中心)，第 26 期，2015 年 6 月。

八、Cert Coordination Center, “CERT Statistics,” http://www.cert.org.stats/cert_stats. html, (February 12, 2009), 2016/12/20 下載。

作者簡介

李正勝中校，指職軍官 88 年班、中央大學(資訊管理碩士)94 年班、管理資訊正規班 97 年班，曾任臺長、排長、資訊官、檔案官，現任陸軍通訓中心教官組主任教官。