通資安全管理稽核分析-以國軍資訊系統為例
Communication and Information Security Management Audit Analysis-Taking a military Information System Case

黃志泰	林芳婷
Gai-Tai Huang	Fang-Ting Lin
德明財經科技大學	德明財經科技大學
資訊管理系	資訊管理系
副教授 兼系主任	碩士在職專班研究生
hgt@takming.edu.tw	ftlin1212@gmail.com

摘　要

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的重要性；所以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。

本文透過文獻探討與專家問卷，以「國際資訊安全管理標準 ISO 27000 系列的規範」做為參考指引，訂定適用於國軍體系資訊安全稽核表，藉由調查各資安承辦人對本稽核表項目的看法後得到　各稽核要項按總加量表法之四等級模式予以格式化為四分量表，接著以此稽核表為基礎發展出引用「國際資訊安全管理標準 ISO 27000 系列的規範」建構一套資訊系統驗證的評鑑模式，藉由評鑑模式實際進行驗證工作，再根據實際驗證的結果，分析是否達到各個控制項目的資通安全標準。讓國軍資訊相關單位可依此檢測單位內的資訊安全是否建立完整，並檢視單位內資訊安全要求是否符合 ISO 27001 的精神，可用於提升單位內資訊安全外，亦可於 ISO 27001 內、外部稽核時，加強其稽核要項。

關鍵詞：資訊安全管理、資訊安全稽核、ISO 27001 資訊安全管理系統。

壹、 前言

一、 研究動機

隨著科技的進步，企業、組織甚至於國軍各項資訊系統亦已朝資訊化發展，然在此同時，因資訊系統之內部控管不當而引發之各項問題也越來越多，因資訊安全肇生的問題對企業、組織及國軍所造成之損失是難以估算的。

由於電子化之推動，國軍各項資訊系統逐步朝電腦化發展，並運用網路資訊交換，快速處裡資訊作業，不但增進作業效能、戰情資訊傳遞等；相對地該等資料如有管理不當，極易造成資料的謬誤或洩密情形。為強化國軍資訊單位資通安全管理，維護電腦資源有效運用，應配合資通安全政策之推動，以協助國軍資訊單位了解資通安全之重要性，建立安全及可信賴之作業環境，確保國軍資訊單位辦理資訊作業等相關資料、系統、設備及網路安全，以維護國家安全。

本文即參考 ISO 27001：2013 架構所制定之資訊安全管理控制標準，建構一套資訊安全稽核模式。研究成果除驗證國軍資訊單位不同群組間資通安全作業之差異外，並藉以達成國軍資訊單位資通安全作業改善之目標。

二、 研究目的

依上述研究背景與動機，本研究目的歸類如下：

1. 建構一套資訊安全資訊管理系統驗證的評鑑模式，藉由評鑑模式實際進行驗證工作，再根據實際驗證的結果，分析是否達到各個控制項目的資通安全標準。
2. 提出一適用於國軍體系資訊安全內、外部稽核之資訊系統驗證評鑑系統，提供組織依此系統檢測單位內的資訊安全是否建立完整，讓國軍資訊相關單位檢視資訊安全要求是否符合 ISO 27001 的精神。
3. 針對國軍資訊相關單位管理階層與資訊安全相關人員及後續研究者提供建議。

三、 問題定義

由於國軍資訊人員及駐地單位分布全台各地，對於資訊安全管理機制及控制標準的導入較不易全面推廣，再加上導入成本之考量，國軍單位往往僅能針對重要之資訊相關單位導入資訊安全管理機制。

本研究將訂定適用於國軍體系資訊安全稽核表，讓國軍資訊相關單位可依此檢測單位內的資訊安全是否建立完整，並檢視單位內資訊安全要求是否符合 ISO 27001 的精神，可提升單位內資訊安全，防止機密資訊外洩，達到資訊安全防護的成效。

貳、 相關研究技術

本論文將就資訊安全定義、資訊安全管理標準 ISO 27000 規範及其相關研究進行探討。

一、 資訊安全定義

本研究首先探討資訊安全的定義為如圖 1，說明如下：

圖 1 資訊安全定義

1. 機密性（Confidentiality）：是指個人或團體的資訊或資料不得被未經授權之個人、團體、實體或程序取得或揭露的特性。在電腦中，許多軟體包括郵件軟體、網路瀏覽器等，都有保密性相關的設定，用以維護用戶資訊的保密性，另外木馬軟體或駭客有可能會造成保密性的問題。
2. 完整性（Integrity）：是為確保資料在傳遞過程中，接收者所得到的訊息和發送者所發出的訊息是一樣的，任何被篡改過的訊息便失去了其本身的意義，成為一個無效的資料，更可能影響其他的資訊，造成資訊系統被破壞。
3. 可用性（Availability）：確保經授權的使用者能適時的存取資訊及相關資產，是一種以使用者為中心的設計概念，易用性設計的重點在於讓產品的設計能夠符合使用者的習慣與需求。以網際網路網站的設計為例，希望讓使用者在瀏覽的過程中不會產生壓力或感到挫折，並能讓使用者在使用網站功能時，能用最少的努力發揮最大的效能。

二、 ISO 27001 資訊安全管理系統

資訊安全管理是一套完整的管理流程，提供組織有效建構資訊安全防護機制，透過 ISO 27001 的資訊安全認證即可確保資訊系統的安全和持續運作。

以 ISO 27001 對資訊安全管理系統（ISMS）的整體架構規劃而言，是採用「規劃 － 執行 － 檢查 － 行動」（Plan － Do － Check － Act，簡稱 PDCA）的模式來設計(如:圖 2)；所謂的 PDCA 是指「計畫—執行—檢核—行動」的過程，在最初的計劃階段，單位必須要建立符合維運目標的 ISMS 政策，它定義了單位實施 ISMS 的範圍，並說明資訊安全的目標、需要透過哪些指標去衡量成效，以及管理階層應該擔負的責任。因此，資訊安全政策也可視為管理階層對於資訊安全的宣誓與支持，唯有如此，到了執行的階段，才可依照此一政策來逐步推動各項資安的控制措施，並且建立相關的作業程序。

在依照計畫並且執行後，要得知實施成效時，就進入檢核階段；針對 ISMS 政策、控制目標及實行的過程，依照政策中所設定的指標去分析、評量實施的成果與績效，然後再將此一結果回報給管理階層作為審查之用。最後，再依據審查的結果，若是發現執行過程中有一些不符合的事項，就要透過實際行動來進行改善，也就是採取相對應的矯正和預防措施，持續改進 ISMS 的整體運作。

圖 2 PDCA 架構圖

ISO 27001 標準條文內容一共分為 10 個章節以及附錄，其中第 1 到 3 章，說明了 ISMS 的適用範圍、所引用的其他標準，以及相關名詞的解釋。ISO 27001 條文的重點主要是落在第 4 到 10 章和附錄 A，分別是「資訊安全管理系統」、「管理階層責任」、「ISMS 內部稽核」、「ISMS 之管理階層審查」、「ISMS 之改進」，以及附錄 A 的控制目標與控制措施。

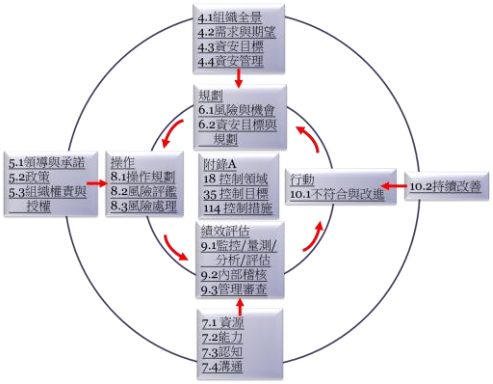

圖 3 ISO 27001 本文條文及 PDCA 循環架構圖

ISO 27001 非常重視持續改進的精神，因此，要求針對每個發生的資安事件擬定矯正措施，以防止類似的資安事件再次發生。

為了落實資訊安全管理系統（ISMS），在 ISO 27001 附錄 A 針對 14 個控制面（A5 － A18）制訂了 35 個控制目標與其相對應之 114 個控制措施，這些控制面與控制目標具體呈現資訊安全管理系統（ISMS）的預防與查核重點，故本研究以附錄 A 之控制目標來訂定適用於國軍體系資訊安全稽核表，讓國軍資訊相關單位可依此檢測單位內的資訊安全是否建立完整，並檢視單位內資訊安全要求是否符合 ISO 27001 的精神。

三、 相關研究探討

1.國防大學管理學院資訊管理系林宏昇提出「植基於 ISO 27001 標準建構資訊安全稽核決策之研究-以股務資訊系統為例」乙篇碩士論文，以條列 8 大稽核控制要項，塑模驗政府務單位之股務資訊系統，完整、明確地評核股務單位之股務資訊系統，亦提供股務單位改善資訊安全內部控制措施之依據。並經過實地驗證後，對個股務單位管理階層提出建議。

該研究過程經由專家訪談方式訂出稽核項目，再運用德非法方式設計出問卷，讓資通安全專家訂出各稽核要項之評分標準，建構一套可運用於股務資訊系統驗證之評鑑模式，再實際至各股務單位執行驗證。最後利用研究中股務單位不同群組間資通安全作業的差異程度，做為各股務單位改善資安管裡的參考依據。

2.國防大學管理學院資訊管理系張鴻正提出「資訊安全管理系統內部稽核管理」乙篇論文，以某國軍單位的資訊中心為例，以其主機房及教育行政管理資訊系統為驗證稽核範圍，構思一套系統化之內部稽核輔助工具，自動產生稽核員在執行稽核工作時所欲使用之各項表格，並透過網路線上系統操作，消除時間與空間之限制，減少紙本作業之時間花費，達成有效之文件管理，且提供歷史稽核記錄查詢與回饋，減少稽核工作之誤差，提供稽核員遵循的指導方針，最終期能透過本系統讓國軍各單位在資訊安全管理系統導入變得輕鬆而確實，且能真正落實資訊安全管理系統之 PDCA 精神，有效支援持續的系統維護工作，解決資訊安全人力不足，系統無法持續維運等問題。

該研究透過專家問卷整理與分析，提出一套內部稽核輔助工具模型，並協助個案單位開發一套內部稽核輔助工具系統，能自動產生單位執行內部稽核所需相關表格及稽核結果輸入功能，並提供矯正措施改善追蹤查詢，可協助稽核人員進行歷史資料查詢及缺點管制，有效降低執行資訊安全管理系統時間，人力與金錢的花費，提高內部稽核工作效率。

3.國防大學管理學院資訊管理系練兆欽提出「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，通過 ISO 27001 認證殊榮國軍單位成員作為研究對象，調查該單位參與 ISO 27001 認證的群體認知，並應用問卷統計資料分析及層級分析法設計研究架構，目的在了解影響國軍資訊安全執行決策因素的優勢方向，與選擇 ISO 27001 認證的優先次序。研究結果具有實用性價值，可以提供國防部做為資通安全決策上改進的依據，也可以做為有意導入 ISO 27001 認證單位的參考。

在問卷統計部分，改善最多為「資訊安全政策文件」和「系統文件的安全」，彰顯了國防部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了相關工作推動的堅實基礎。

在 AHP 部分，權重最多為「證據收集」，顯示國防部重視稽核部份，已運用設定稽核來偵測並記錄影響安全的相關事件，例如未授權的使用者嘗試存取機密檔案或資料夾情形。在稽核物件時，無論物件於何時以某種方式存取，皆會在安全性記錄檔中寫入該事項。各單位亦被要求必須規範要稽核的物件、要稽核誰的動作，以及要稽核的動作類型。稽核一經設定之後，就可以記錄存取某些物件的使用者，並分析安全性的缺失，而記錄所選事件的稽核追蹤會顯示執行動作的人及嘗試執行不允許之動作的人，如此才能遏阻不當企圖及提供偵辦違安事件的有力證據。

4.本研究因考量由於國軍資訊人員及駐地單位分布全台各地，對於資訊安全管理機制及控制標準的導入較不易全面推廣，再加上導入成本之考量，國軍單位往往僅能針對重要之資訊相關單位導入資訊安全管理機制；本研究參考「軍事機關導入 ISO 27001 資訊安全管理成功因素之研究」乙篇論文之論述「國防部重視稽核部份，已運用設定稽核來偵測並記錄影響安全的相關事件」，將訂定適用於國軍體系資訊安全稽核表，讓國軍資訊相關單位可依此檢測單位內的資訊安全是否建立完整，並參考「植基於 ISO 27001 標準建構資訊安全稽核決策之研究-以股務資訊系統為例」乙篇論文之研究方法，建立一套可運用於國軍資訊單位資訊系統之評鑑模式，檢視單位內資訊安全要求是否符合 ISO 27001 的精神，可提升單位內資訊安全，防止機密資訊外洩，達到資訊安全防護的成效。

參、 研究方法

本研究透過量化研究，建置研究架構與流程，先以專家訪談方式參照 ISO 27001：2013 控制項目訂定出稽核項目，並將各稽核要項按總加量表法之四等級模式予以格式化為四分量表，再運用德菲法之方式設計出一份問卷，問卷是依據國軍相關法令規章及標準作業程序，並以 ISO 27001:2013 之資訊安全管理系統驗證規範為基礎，及資安專家認定之可能狀況(非常重要、重要、不重要、極不重要)為內容，據以設計而成，每一控制項目以「非常重要」、「重要」、「不重要」、「極不重要」四個層次表示其重要程度；寄發給參予之資通安全專家，訂出各稽核要項之評分標準，建立一套可運用於國軍資訊單位資訊系統之評鑑模式，藉由評鑑模式實際進行驗證工作，

研究步驟如下：

1.依據國軍相關資訊安全政策、法令規規章及標準作業程序，以專家訪談方式參照 ISO 27001 控制項目訂出稽核要項，並將各稽核要項案總加量表法之四等級模式予以格式化為四分量表。

2.接著運用德菲法之方式設計出一份問卷，寄發給參與之資通安全專家，訂出各稽核要項之評分標準。

3.依據各稽核要項之評分標準，建構一套可運用於國軍資訊系統驗證之評鑑模式。

4.藉由評鑑模式實際至各資訊機房維運管理相關單位進行驗證工作。

5.根據實際驗證之結果，分析各資訊機房維運管理是否達到個控制項目之資通安全標準。

肆、 結論

本研究成果期能驗證國軍資訊單位不同群組間資通安全作業之差異外，並提供國軍資訊單位資通安全作業改善之目標，降低各單位的資安風險，以維護國軍資訊安全為主要貢獻。

參考文獻

[1] ISO/IEC 27001 的官方網頁在<http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>(2015/10/24)。

[2] 林宏昇，2008，「植基於ISO27001標準建構資訊安全稽核決策之研究－以股務資訊系統為例」，國防大學管理學院碩士論文。

[3] 練兆欽，2010，「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。

[4] 張鴻正，2010，「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。

[5] 黃劭彥、林琦珍、邱安安，2011，電腦稽核導入之成效，電腦稽核期刊，23期，16-25頁。

[6] 林玉山，2010，導入ISO 27001 ISMS資訊安全管理系統－以醫療院所核心資料庫安全性的策略和方法為例，電腦稽核期刊，22期，90-102頁。

[7] 洪新原、張碩毅、郭吉原，2011，影響組織採行與應用資訊安全管理系統認證之關鍵因素，電腦稽核期刊，23期，99-112頁。

[8] 吳政叡，2008，ISO 27001「資訊安全管理系統要求」在圖書館的應用， 臺灣圖書館管理季刊，第四卷第二期，89-99頁。