應用失效模式與效應分析評估資訊安全管理系統之風險

Applying FMEA to Assess the Risk of Information Security Management System

韓慧林 (Hui-Lin, Han)
實踐大學高雄校區資訊管理系助理教授

王貴民 (Kuei-Min, Wang)
實踐大學高雄校區資訊管理系助理教授

王振陽 (Chen-Yang, Wang) 劉庭維 (Ting-Wei, Liu) 鄭曳庭 (Yi-Ting, Cheng)
實踐大學高雄校區資訊管理系四年級學生

提　　要

在資訊科技爆炸時代，資訊安全管理系統風險評估已成爲各企業營運或軍事部門優先考量因素；資訊安全漏洞將造成企業或國家之危機，風險發生原因及其影響也將帶來革命性的變化，爲求組織永續發展及營運安全，不斷風險評估、預防管理及立即應變計畫乃必然之防範作爲。本研究應用失效模式與效應分析以評估資訊安全管理系統風險爲例，建立與提供一套資產風險評估與預應之啓發模式，作爲國軍有效評估「國防資訊安全管理系統」之風險參考。

關鍵詞：失效模式與效應分析、資訊安全管理系統

Abstract

In this exploded information technology era, the risk assessment of Information Security Management System (ISMS) has become the major concern by the business management and military department. The vulnerabilities of information security would inflict severe crisis on the enterprise or government easily that, however, the risk with its impact also brings us the revolutionary change for the sake of minimizing the risk. In order to keep the sustainable development and secured operation in organization, the continuous risk assessment, preventive management and immediate contingency plan have to be undertaken as preventive action. This paper is to use Failure Mode and Effect Analysis (FMEA) methodology to establish and provide a new risk assessment, and with heuristic model for studying "The effective risk assessment on ISMS of MND".

Keywords: failure mode and effect analysis (FMEA), information security management system (ISMS)

壹、前　　言

資訊安全(Information Security)，簡言之，乃確保資訊系統提供組織所設定的正常運作及行為，與其所規範之資訊管理作業皆屬之；「資訊安全技術」是指保護資訊資產避免遭到竊取及破壞的技術。而「風險」的定義為「損失或傷害的可能性」，亦指影響任務無法成功完成的潛在干擾因素，任何資訊安全專案之風險包括其可能發生之潛在問題，以及資訊安全管理之風險管理。風險管理規劃的目的是詳細說明誰負責風險的管理，包括規劃、分析、處理和監控、風險如何追蹤、備案如何執行及專案儲備(Project Reserve)使用時機等。因此，專案儲備分為兩類：[1]⑴緊急儲備(Contingency Reserve)；⑵管理儲備(Management Reserve)。緊急儲備是針對已經找到，而且有可能發生的風險(Known Unknowns)，如果風險發生，管理者可掌控並立即應對或防範。而管理儲備是應付那些沒有想到，但是也有可能發生的風險(Unknown Unknowns)，皆要有妥善備用方案。

隨著資訊科技的迅速發展，資訊安全日趨重要；資訊安全事件之個案，層出不窮，未來發生頻率與現今比較，有過猶不及，也將反映出各企業在資訊安全管理上投入心力之不足，而資訊安全管理不足的原因除了天然災害外，反而是人為的風險最大。因此ISO27001資訊安全管理系統(Information Security Management System, ISMS)的11個控制項、39個控制目標、133個控制要點，即提供了企業一套完整的參考文件；而此ISO27001條文要求僅能提供企業參考，再考量企業內部環境、法律、文化及技術等風險，經綜合考量後再與ISO27001做結合，才能發揮較大功用；本研究動機乃賡續王貴民等學者所發表之〈國防資訊安全管理系統之導入專案管理模式建構〉研究，[2]期能提供一套國防資訊安全風險評估之系統方法。

一般申請ISO2007ISMS認證之企業，首先確認申請之範圍如本校以「電算中心」為主，並運用表1之表格逐一檢討其所管轄之資訊資產，進行逐項之威脅弱點評估，而本文之目的在改善此評估方式，建議改用工程上使用之風險評估法（如航空工程）—失效模式與效應分析法(Failure Mode and Effects Analysis, FMEA)，於評估時即將組織之可承受部分納入考量，若超過風險值則提出事先預防之措施，以降低至可接受之風險下。所以，任何企業或組織在資訊安全管理系統之建置或規劃過程中，首先就是有系統和有方法的建立資訊資產風險評估，如「威脅弱點評估法」；組織透過申請驗證範圍所涉及之資訊資產安全風險評估範疇，將可能之威脅及弱點逐一表列，並腦力激盪以威脅及弱點等級為主要考量，區分低、中、高之不同風險等級，並計算其風險值（表1），有系統的探討與進行資訊安全之風險管理，或作為單位每年執行管理審查會議之討論議題，旨在

1 臺灣專案管理學會(TPMA)編制委員會編著，〈國際專案管理知識體系〉（高雄：臺灣專案管理學會，2006年）。

2 王貴民、韓慧林、陳建任、李承漢、陳鼎元、洪全緯，〈國防資訊安全管理系統之專案管理模式建構〉，《國防雜誌》，25卷6期，2010年12月，頁24-36。

表1　現行資訊資產安全風險評估（範例）

威脅	弱點	威脅等級			弱點等級			風險值
		低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	
失竊	範例							
	未保護儲存文件							
	未經控管之資料複製							
	缺乏安全警覺							
	資料銷毀時的不注意							

進行資訊安全風險預防作業或建置ISO27001系統前的資訊安全資產風險評估，對所有資訊資產的價值作一系統性評估或檢視，以及可能損失評估，與避免或降低其發生的機率，然此方法欠缺高風險之因應作為，若無法預先提出因應方案避免高風險因子或防範，則資訊資產風險評估之功效將大打折扣。

由於資訊安全管理問題之範圍十分繁雜、技術日新月異，組織在使用資訊安全系統進行內部管理時，常會覺得無所適從，且無合適的指導方針以提供組織內不同專業單位遵循；而有關之資訊安全政策，其目的不外乎為確保國防部所屬之資訊資產的機密性、完整性及可用性，符合相關法令、法規之要求，使其免於遭受內、外部蓄意或意外之威脅。因此，本研究主要應用企業申請通過ISO27001系統認證之風險評估模式為例，探討其在ISMS中，有關資訊資產風險評估要項、評估方法論與矯正及預防管理時所採用之方法，作為研究資訊安全風險管理之議題。首先，蒐集相關文獻資料以了解資訊安全可能存在的威脅，再探討資訊安全對於企業的重要性，導入ISO27001資訊安全評核規範，並使用FMEA方法，提高資訊安全規劃效益，加強資訊安全管理系統之風險意識，事先避免或降低資訊安全危機的發生，或於資訊安全問題危機發生時能應對自如，以達成及強化資訊安全管理之目標；並期能達到下列目的：(1)應用失效模式與效應分析模式，提出另一不同ISMS風險評估法；(2)建立一套ISMS風險管理的啟發流程方法；(3)提出ISMS的有效防範技術，強化ISMS之可靠度；(4)落實組織ISMS之全面品質管理(Total Quality Management, TQM)；(5)提供各單位申請ISO27001認證之資產風險評估標準作業模式。最後，參照與結合ISO風險評估方法，改善前述表1威脅與弱點分析方法，未能提出預防矯正機制特性之缺失，並提出結論與建議。

貳、文獻探討

一、資訊安全管理系統

資訊對組織來說就是一種資產，和其他重要的營運資產一樣有具高附加價值，因此需要持續、有效的保護與管理。資訊安全若能有效落實於企業文化中，形成組織之作業習慣，將可保護資訊不受各種威脅；因此，如何透過資訊安全政策之宣示、管理範圍確認、風險評估、外部利害關係人與團體之資訊管制、「資產、人力、設備、媒介、方法及環境」管理、資訊安全溝通、內部控制、資訊安全措施與管理，內部資訊安全稽核，確保持續營運，並將資訊安全事件降到

最低，實須一套有效之資訊安全管理系統，方能有效落實資訊安全由政策至執行方案、執行方案至績效落實之有效管理工作。談及「資訊安全威脅」不外乎上述之機密性（入侵行為、惡意程式、資料欄截與插入）、完整性（偽造、竄改）及可用性（意外事件、天然災害、通訊破壞、垃圾文件及怠（罷）工）等效能受到威脅或破壞，達到⑴確保資訊之機密性，保障連線作業單位使用資料之隱私權；⑵確保資訊之完整性，保障單位及部隊使用資訊相關載台或設施之權益；⑶確保資訊可用（必要）性，確保連線作業單位使用資訊系統之品質。[3]

ISO27001對資訊安全的範圍定義為「無論來自人為故意或不經意的，或不可抗性的因素，任何導致資訊安全系統正常運作外的情形或行為皆屬之」，以此為範圍基礎，我們將資訊資產分為實體資產與虛擬資產及人員、作業環境等範圍內之所有問題皆視為FMEA之風險項目，包括機密性、完整性及可用性等三項做為稽查之標準。同時依據其評鑑原則，適當劃分等級高低及依評鑑對象之狀況衡量訂定不可接受之風險等級高低，等級為依照各類資產具有之機密性、完整性及可用性這三項特性區分之，其中屬可接受風險範圍之外者，應訂定風險控制計畫以監督控制；且於申請及準備接受ISO27001系統認證前時，資訊安全風險評估之良窳，更影響系統推展成功與否之舉足輕重地位。

資訊安全風險之評估方法不勝枚舉如FMEA，不僅能將防範及解決各種風險的方法及風險評估文件化外，亦考量風險之等級提出不同之因應方案，使風險評估作業過程更完善化；為因應未來資訊安全風險之問題，能及時解決與防範，降低組織及企業之損失。所以，本研究從風險管理學的方面來探討資訊安全，是為了追求資訊安全品質的最適化，建立資訊安全系統風險評估與管理機制。根據ISO27001的資訊資產分類，可分為資訊資產如資料庫及資料檔等、資料文件包含合約文件及指導文件、軟體資產如由應用軟體、實體資產如電腦及儲存媒介、人力資產如人員、服務性資產如電源和空調，以及無形資產如經驗及內隱知識，因應不同的類別所帶來的不同影響，運用FMEA有系統了解整體ISMS之風險評估模式，建置資訊安全系統前優先預防與管制項目。

資訊安全方法論計有：王志斌結合層級分析法(Analytic Hierarchy Process, AHP)與德菲法(Delphi method)發展資訊安全認知評量表，[4]其使用ISO27001資訊安全科技與標準，透過〈資訊科技安全訓練計畫—以角色與績效為基礎模式〉，建構一套資訊科技安全認知與訓練計畫；吳政叡將ISO27001「資訊安全管理系統要求」運用於圖書館之應用研究，[5]採用「規劃—執行—檢查—行

3 杜偉欽，〈結合HIPAA與ISO27001為基礎探討醫療院所資訊安全管理之研究〉（臺南：國立成功大學工程科學研究所碩士論文，2006年）。

4 王志斌，〈結合層級分析法與德菲法發展資訊安全認知評量表之研究〉（臺北：世新大學管理學院資訊管理學系碩士論文，2009年）。德菲法乃是「一種結構性的團體溝通，過程中允許每位成員就某議題充分表達其意見並受到同等重視，以求得在該複雜議題上意見的共識」。

5 吳政叡，〈ISO27001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4卷，第2期，2008年，頁89-99。資訊安全管理系統之可能威脅包括：駭客入侵、人為操作錯誤、管理人員密碼設

動」(Plan, Do, Check and Act, PDCA)模式，設計與規劃此系統之整合架構，其系統模式包括： 1.建立ISMS（規劃）； 2.實作與運作ISMS（執行）； 3.監視與審查ISMS（檢查）； 4.維持與改進ISMS（行動）。該研究資訊資產主要目的在：確定個別資產的擁有者，以及分析個別資產的價值、弱點(Vulnerability)、威脅(Threat)。

二、失效模式與效應分析

㈠風險管理

導入ISO27001專案風險因應是針對會造成危害的風險，擬定適當的因應措施，以消除或降低其負面效應。風險因應措施必須符合風險的嚴重性及成本效益。而且在此專案執行過程，要定期稽核因應措施是否如預期的產生效果；並區分為4種應對作為：[6](1)避險(Risk Avoidance)：避險是修改專案計畫讓風險不會發生，制定避險策略常需要發揮創意思考；(2)降低(Risk Reduce and Control)：風險降低又稱為風險處理，它是把風險發生的機率或是負面效果降到某一個可以接受的門檻，但是風險降低的成本必須適度；(3)轉移(Risk Transfer)：風險轉移是把風險的後果轉移給第三者去承受，方式是透過合約條款，保險或保固期限要求。風險轉移只是轉移風險並沒有消除風險；(4)接受(Risk Acceptance)：風險接受是接受風險的後果，有積極接受(Active Acceptance)和消極接受(Passive Acceptance)兩種。

葉宇光應用事件樹分析[7](Event Tree Analysis, ETA)於職業安全風險評估之研究，風險評估係考量任何現存控制措施的結果，評估因潛在危害因子而造成的風險，與決定此風險是否為可接受的整個壽命週期流程，風險分析(Risk Analysis)則是系統化的程序了解風險程度的性質並推論風險的等級，風險評析(Evaluation Risk)為比較風險程度與可容忍風險的程序，風險控制(Risk Control)選擇並使用適當的方式降低風險，彼此相輔相成，缺一不可。該研究採事件樹分析法，運用二元邏輯方式，也就是事件的發生為「可能」或「不可能」，或者是設備運作的「失效」或「成功」，並藉由圖形的方式描述由起始事件到可能的後果，起始事件為特定設備失效或人為失誤、零件失效、溫度或壓力的增加或是危害物質洩漏，經由一系列可能的途徑演變至可能的後果或發生機率等評估下，可計算出風險可能導致事件之嚴重程度。張維仁透過犯罪心理與行為之研究中，[8]運用統計檢定方式，以心理學及問卷調查方式進行資訊安全議題之研究，再使用多變量分析(ANalysis Of VAriance, ANOVA)，以量化方式將資安問題明確化。

㈡FMEA相關應用

定不當遭破解、系統管理員離職、天災、硬碟毀損、系統更新程式有臭蟲(Bug)、備份資料失敗、遺失或毀損，由此可知，資訊系統的威脅可能來自各方面：人員、場所、設備、軟體、儲存媒體等，人為或非人為、有意或無意都有可能。

6 同註1。

7 葉宇光，《事件樹於職業安全風險評估應用研究》（桃園：國立中央大學環境工程研究所碩士論文，2009年）。

8 張仁維，《犯罪心理與員工電腦濫用行為之研究》（桃園：國立中央大學資訊管理學系碩士論文），2007年。

Sharon應用品質機能展開圖及FMEA探討產品或服務過程之績效評估。[9]吳貴彬及陳相如認為FMEA是全面品質管理(TQM)的一環，是一種動態且事前預防的工具，藉由專案團隊的運作，以發掘設計與製造的關鍵潛在失效問題及其影響；[10]其論點乃以國際標準系統認證為依據，並以FMEA為個案研究工具，揭露產品在開發製造時的不良模式，並能及早預防與改善。Ellis表示當企業想提升其品質管理系統至高階管理之國際標準規範時，可應用FMEA作為企業可能面臨之風險與落差分析之工具。[11]Shahin表示FMEA所討論之「嚴重性」乃由設計者之角度而非來自顧客觀點，提出矯正率(correction Ratio)與風險優先指數(Risk Priority Number, RPN)結合模式，有效整合管理者、設計者與顧客意見，提升產品市占率。[12]Teng et al., 探討在協同供應鏈下之汽車產業之執行過程，透過嚴重性、可發生機率及可偵測度之排序優先等級，藉由抽樣大小、可靠度及統計檢定、以完成設計驗證與控制計畫所需之FMEA流程，發現協同供應鏈運作困難之問題。[13]Carbone and Tippett[14]及Lanczyck以電子產業為例，[15]應用FMEA於專案風險評估，稱之為RFMEA，提出一套新的電子產業之風險可偵測度之判斷模式，若超過設定之界限，則將由工作團隊處理此立即之風險、訂定應變計畫與改善團隊之作業成效、增加風險控制能力。Segismundo and Miguel以巴西之汽車製造業為例，[16]應用FMEA於新產品開發之最佳化與風險管理。Ahsen探討配送產品可能造成產品失效或偵測出來可能失效之機率，[17]並考量其發生之成本下，進行FMEA之相關作業。洪誌佑以鋼構業為例[18]，於專案品質

9 Sharon, K.J.,“Combining QFD and FMEA to optimize performance”, Annual Quality Congress Proceedings, ABI/INFORM Global, 1998, pp. 564-575.

10 吳貴彬、陳相如，《失效模式與效應分析之應用》（高雄：樹德科技大學工業管理系暨經營管理研究所碩士論文，2003年）。

11 Ellis, M. E.,“FMEA as a gap analysis/transition tool (ISO9001: 2000/TS16949:2002”, Annual Quality Congress Proceedings, ABI/INFORM Global, 2004 pp.43-44.

12 Shahin, A.,“Integration of FMEA and the Kano model: an exploratory examination”, The International Journal of Quality & Reliability Management, 21(6/7), 2004, pp.731-746.

13 Teng S. G., Ho, S. M., Shumar, d., and Liu, P. C.,“Implementing FMEA in a collaborative supply chain environment”, The International Journal of Quality & Reliability Management, 23(2), 2006, pp.179-196.

14 Carbone, T. A. and Tippett, D. D.,“Project risk management using the project risk FMEA”, Engineering Management Journal, 16(4), 2004, pp.28-35.

15 Lanczycki, J. J.,“The basics of FMEA”, Quality Progress, 42(10), 2009, p.67.

16 Segismundo, A. and Miguel, P. A. C.,“Failure mode and effects analysis (FMEA) in the context of risk management in new product development- A case study in an automotive company”, International Journal of Quality & Reliability Management, 25(9), 2008, pp.899-912.

17 Ahsen, A. V.,“Cost-oriented failure mode and effects analysis”, International Journal of Quality & Reliability Management, 25(5), 2008, pp.466-476.

18 洪誌佑，《專案品質管理系統分析與規劃—以鋼構業為例》（高雄：國立高雄應用科技大學工業工程與管理系碩士論文，2008年）。

管理系統分析中，探討品質保證等系列活動之品質管理，包含：學習標竿、流程規劃及FMEA等。Kumar et al.運用FMEA於製藥產業供應鏈研究，[19]透過逆向物流監控系統衡量產業鏈失效模式與風險。廖談坪探討跨功能團隊成員組成條件，[20]以及對FMEA及全面品質管理之影響，讓FMEA成為TQM之有效溝通工具。孫國隆應用資料包絡分析法[21](Data Envelopment Analysis, DEA)於FMEA以增強評估能力之研究，並於FMEA中探討各輸入因子的貢獻值，改善FMEA對風險因子量化之缺失，並以DEA提供各因子的改善尺度，針對關鍵項目，檢討需改善風險因子幅度。

參、FMEA研究方法

一、FMEA方法論概述

FMEA已廣泛使用於評估及發展各種有形產品，如：內燃機、戰車、飛機或飛彈系統及太空梭等國防、航空及工業製造品等之可靠度與安全性，且獲得具體之成效。此方法論對於整體安全性規劃及管理具有明顯功能性；其為可靠度工程分析之技術，主要針對於資產及作業流程的失效預防以提高系統安全性。透過嚴重性、發生機率（頻率）及可偵測度評估，找出實施對策之優先順序，並以文件化方式有效紀錄與備查，透過所見失效項目採取對策，並進行與風險管理上的改善或安全性等有關之設計、製造的改善，使系統效率提高。

FMEA依流程劃分可分為設計階段及製程階段，設計FMEA階段(D-FMEA)主要為作業前的事先性預測及預防，也就是事前控制(Feed Forward Control)。製程FMEA階段(P-FMEA)主要為作業流程之風險安全性管理，依靠D-FMEA之可靠度來管理，即為事中控制(Feed Back Control)。其主要實際作業流程為：⑴選定鑑別項目與分類；⑵表列失效及風險項目；⑶失效及風險造成後果（或嚴重性）預測及分析；⑷探討發生原因；⑸發生頻率分析；⑹目前控制其管理機制的了解與分析；⑺可偵測度分析；⑻研討建議措施並紀錄；⑼計算RPN，對某高風險項目，做出改正措施以降低風險係數；⑽文件化紀錄與持續追蹤改善。

另FMEA可以描述為一系統化的活動，其目的為：⑴發現及評鑑（分析）其潛在的失效及其後果；⑵尋找能避免或減少失效發生的措施；⑶將前述兩項過程文件化，對作業過程更完善化，明確表示必須流程及方法。

二、FMEA跨功能小組發展

跨功能小組(Cross Functional Team)又稱品質改善團隊。沿襲自日式全面品質管制(Total Quality Control, TQC)機能別管理模

19 Kumar, S., Dieveney E. and Dieveney A., “Reflective practice reverse logistic process control measures for the pharmaceutical industry supply chain”, International Journal of Productivity and Performance Management, 58(2), 2009, pp.188-204.

20 廖談坪，〈跨功能團隊成員組成條件對失效模式效應分析及全面品質管理之影響〉（高雄：義守大學管理研究所碩士論文，2009年）。跨功能團隊之組成是一個關鍵，團隊成員各自擁有不同專業背景，其品質規劃及教育訓練、改善措施，亦能透過團隊運作及合作來達到品質要求，同時持續性改善品質。

21 孫國隆，〈應用資料包絡分析法於失效模式與效應分析以增強評估能力之研究〉（桃園：國立中央大學企業管理學系博士論文，2009年）。

式，被用來做為一項持續改善的工具。組織橫跨若干功能別的單位所組成的專案團隊，為了打破部門間溝通的藩籬，強化溝通的效果，取得共識。所以成立「跨功能小組」乃實施或進行FMEA失效模式方法整合及風險管理所必須要完成之重要工作，並決定未來評估資訊安全風險之成敗關鍵，建立其ISMS之機密性、安全性與可用性之保證。以FMEA來建立一套完整資訊安全管理系統，對於各資訊安全問題以風險項目及失效項目研討，亦不失為良方。

三、FMEA與ISMS

相較於風險管理模式，資訊安全的影響不單是實體資產，同時也是造成無形資產損失的最大主因；而FMEA風險管理之優點，乃在加強資訊安全管理的預防與有效落實作業，以FMEA作為資訊安全資產風險預應之研究方法，將任何使實體或是虛擬資產失效的風險，有系統的檢討與連結，並提出可被接受之防範作為，而此有系統、結構化的探討方式，就管理層面言，FMEA對ISMS可有效達到SMART原則：⑴具體化(Specific)：風險項目必須是明確並且可理解的，如缺乏資料（資料、程式與文件）備份造成軟體失效；⑵可衡量的(Measurable)：如同FMEA所設定1～10分之評分標準，可辨識風險之嚴重性、發生機率及可偵測度之等級；⑶可達到的(Attainable)：矯正措施必須是有效的，且在最短時間內可達成或是有效之方案，如加強抽查之頻率等，且其成效可經由主管追蹤管制；⑷相關的(Relevant)：項目不可以與資訊安全問題無關，具問題之針對性以避免浪費管理成本；⑸以時間為基礎(Time)：FMEA應具有動態性，每年必須再行檢視，此模式建立後，具長期性可供每年檢討之依據。資產失效問題，由過去許多品管與可靠度分析管理之案例顯示，FMEA對於資訊安全管理的品質改善效果值得肯定，FMEA方法著重於人為與環境評估以確認可能之資安問題，若能有效建立跨功能小組進行溝通，應用FMEA以系統性的預防手段將人為或環境變動之風險或影響降至最低。

「保密是軍人天職」、「一語外洩、全軍覆沒」，這是身為軍人耳熟能詳之座右銘，且時時提醒我們永遠不能忘記外，還要身體力行；而「不定時炸彈原理」不止用於人為或環境因子之風險，同時也存在於現行預防手段，且對資訊安全而言，尤應更加審慎。若有一筆機密性文件，須對此文件設定一組難以破解之密碼，但又必須假設在此密碼未被破解前，可以確保其安全性。因此，必須針對密碼保護之預防手段進行FMEA方法之風險評估，運用FMEA做為溝通工具，透過跨功能小組之目標設定，從「人員、資訊設備、技術、資訊管理」等多面向不斷修改控制手段，以因應所有可能風險及其控制手段，有系統的規劃與管理，相信任何主官（管）皆能較具信心且廣泛訂定確保機密文件之安全防範管道與應變作為。

四、FMEA之限制

俗話說「計畫比不上變化」，風險評估過程亦會遇到相同之課題，如FMEA運作流程中，亦會存在內部的資訊安全控制方式與外在危險因素間的差距，如「311日本大地震」所造成福島核能發電廠之輻射外洩事件，相信當初之設計構想與防範機制言，考量之狀況必然有所差異，而如今災害之嚴重性與破壞力，超過設計與預演之緊急應變作為；同樣地，隨著資訊科技的日新月異，資

訊安全技術與方法也同樣面臨，「以現今之技術或想法要想像可能之安全防範機制」或「所組成之專家團隊是否為該領域之專家」等問題點或盲點。假使有一設定數組密碼之機密文件，同時已多重備份，然卻有一電腦駭客可運用一個不需經過破解密碼之技能入侵竊取資料，或許彼此對資訊安全認知與該駭客的認知及技術能力間產生明顯差距。所以說，事前、中或後之控制雖都已考量或訂定應變作為，但不可測的意外或人為疏失還是層出不窮，儘管這些責任幾乎可歸咎實施FMEA之人員能力有限，卻是FMEA不足之處。另強調危機處理雖包含事後控制，但事後控制並不等同危機處理，事後控制包括捨棄資產重新建造及馬上停止所有組織活動等控制方法，但危機並未馬上解決僅是暫時減緩，而前述當能力存在差異時（尤其是日新月異的資訊科技），還是要回到FMEA之思考方式加以改善，納入真正專家於跨功能小組活動，發揮「源於規劃，載於計畫」之功，並動態性與系統化的審視與檢核。

肆、國防事務之ISMS風險評估

一、國軍與民間企業資訊安全管理差異分析

整體而言，若由「資訊安全管理內涵、衝擊性、防範措施、可偵測性及防範議題」，進行國軍與民間企業資訊安全管理差異分析（如表2），兩者資訊安全管理之內涵，包括資訊的機密性、完整性及可用性，而如何確保資訊提供者與使用者間之資訊機密性、完整性及可用性，在軍民間之要求並無明顯差異性的，然因軍民間之資訊設備，雖同是一個資訊中心言，軍事院校之電腦設備雖與民間相似，然其所涉及之官士兵個人資訊外洩，與一般民間大學學生資料外洩之嚴重性比較，其所產生之影響或嚴重性前者較高；加諸，與軍事資訊有關之訊息，必然有特定組織進行蒐集或入侵、整合與分析，既使防範措施嚴謹，資訊外洩可偵測性高，資訊安全防範議題及手段推陳出新，致使國軍採取更嚴格之管控方式如資訊網路(Mi-Net)採用實體隔離，且不與網際網路連結；拆除光碟機及封閉USB界面等所有可能與外接儲存裝置；不可攜帶具照相功能之相機，並研發監測軟體(Kerberos)，管控未經核准之輸出與輸入裝置，…等資訊安全管理作為，但仍有防不勝防、力不從心之感。

二、國防事務之ISMS風險評估

本研究主要在提供任何企業或組織在申請ISO27001資訊安全管理系統認證之資訊資產風險評估方法，亦或組織ISMS自我管理，並以實踐大學高雄校區電算中心申請通過認證範圍之資訊資產風險評估流程為依據，經多次與該單位研討與修訂，運用FMEA來制定另一種風險評估流程，完成其資產風險FMEA評估，其整體作業流程與思考模式，

表2　國軍與民間企業資訊安全管理差異分析

	資訊安全管理內涵	資訊資產價值（衝擊）	資訊防範措施	資訊外洩可偵測性	資訊安全防範議題
國軍單位	相同	高	嚴密	高	複雜
民間企業	相同	低	較不嚴密	低	較不複雜
註：國軍單位與民間企業泛指一般型態之組織爲分析之目標，不以個案如台積電、聯電或聯發科等企業作爲比較對象；國軍單位或個別企業之資訊安全管理模式，亦應其組織特性而不同，但整合而言國軍組織較具一條鞭之管理模式，上下層組織之資訊安全管理思維接近。					

亦能提供國軍各軍事機關、單位或部隊，作為資訊安全管理之系統思想與管理方式；並提出一套新的資產安全評估之啟發流程7步驟，以執行FMEA評估：⑴成立跨功能小組；⑵決定驗證範圍與FMEA評估議題；⑶討論與確認FMEA（失效模式對效應的影響、找出嚴重性評價、造成失效模式原因探討、造成失效模式發的機率高低、目前管制方式與能力探討，以及系統或現行作為能偵測出失效原因的能力）；⑷計算風險優先指數；⑸找出高潛在風險因子；⑹預防矯正措施與持續改善；⑺主管追縱與成果確認。

㈠成立跨功能小組

首先，「工欲善其事，必先利其器」，而此處之「器」乃真正專家；也就是先成立具學術與實務能力之專家所組成之跨功能小組，切勿以各單位派「公差」方式組成，其成員來自不同之資訊專業與人格特質者更佳，且為求FMEA之綜效最大化，成員間技能應具備互補性且與目標相呼之特色，先將成員間技能分為專業管理、資訊或電子技能，甚至加諸不同系統管理之經驗亦可考量。專業資訊與電子技能乃針對單位電算中心、資訊室或專案編組等所提出性之ISMS失效項目做出技術性修正或指導。專業管理技能則為人員管理及作業流程管理之失效項目做出修改及技術整合，若能納入各專業人員，建立有效溝通管道，推行全面性資訊安全管理工作，將具事半功倍之效。

跨功能小組成立良窳以及成員能力皆是後續運作成功與否之關鍵，更是在實施FMEA之前，小組成員應妥善規劃教育訓練之因素，不經此步驟便無法達到TQM之目的。所以，跨功能小組成立就是要打破各部門間之藩籬，且為使該小組順利運作，FMEA主要成員必須具備資訊安全之相關知識，包含ISO27001及FMEA風險管理之相關知識。因此，教育訓練實為必須之工作，各單位應有專人接受ISO27001內部稽核員訓練，建立單位溝通平台，讓成員熟悉與不同領域成員合作，熟悉該小組作業流程，對資訊安全管理工作或目標建立共識。

㈡決定驗證範圍與FMEA評估議題

其次，組織應決定其申請認證之範圍，如國防部部本部所有單位、國防部戰略規劃司或參謀本部通信電子資訊參謀次長室，在就此範圍所涉及之ISMS活動進行相關FMEA之議題評估。跨功能小組再針對其作業流程進行風險分析，若以軍事院校言或許申請認證之單位僅為其資訊或電算中心為標的，了解其資訊傳遞及資訊作業對學校教學作業及各功能運作，如圖書館資料庫、資訊教室、軍事院校各單位資訊管理作業與防範機制及外部進入校內之資訊管制作業、…等，宜逐項逐次檢視與規範，皆缺一不可。雖然資訊安全管理之關鍵點或管理範圍為資訊或電算中心，然其作業範圍涉及各單位，如何建立各單位具機密性、整體性及可用性之ISMS量化管理目標，除了促使各單位建立自主ISMS管理機制外，否則再完美之導入ISO27001之專案管理工作或督導，皆無法有效杜絕資訊安全事件之發生。

所以，確認ISMS驗證範圍後，應逐步完成下列風險評估作業：辨識可能造成ISMS風險之潛在因素，透過嚴重性、發生機率及可偵測性，運用定性及定量之方法，評估分析不同層級（高、中、低）風險，並預擬因應方案或應變作為，作為管理、演練與內外部稽核之重點，發揮「80-20重點管理」效果，防止於未然或使其納入可預測之管

控中。如電源不穩定、硬體品質不良或超過使用年限、線路保護措施不良、使用者端中毒、系統漏洞、操作不當、有心人士洩漏資料。此外，FMEA實施效果之關鍵，乃將其客觀性結論文件化，以利ISMS措施的有效運行，保證其持續改之善品質。

㈢討論與確認FMEA要項

本研究以ISO27001為藍本，透過ISO27001以機密性、可靠性、完整性之標準為考量，針對此三項要點作為風險評估方向，和對ISMS之有形及無形資產的影響範圍及大小等評估，並作為小組成員間（包含資訊或電算中心之成員）腦力激盪，以確認FMEA議題、資訊安全要求與潛在失效模式等議題，其潛在失效模式「失竊」要項（如表6範例，包括：未經控管之資料複製、外部人員或清潔人員缺乏人員陪同作業）、軟體失效（沒有軟體測試或軟體測試不夠、開發者的規範不清楚或不完整）、不當維護（專業訓練不足）、儲存媒介的劣化（儲存媒體維護不足／安裝瑕疵）、竊聽（缺乏正確使用通訊設備（照相手機）與訊息控管的政策與執行方案）、…等要項，並完成此文件之表單。

㈣計算風險優先指數

確認潛在失效模式與效應影響要項後，管制要項之文件化可使跨功能小組與相關人員有效溝通及指導，使FMEA實施作業更加有效。然任何風險皆具不同等級特性，若將所歸納之管制要項全部列表管理，則將失去風險管理之要義；如何找出失效模式與效應的影響、嚴重性、失效模式原因、發生的機率、目前管制方式與能力探討、現行作為能偵測出失效原因的能力。

所以，評估風險之等級必然之作為，透過「嚴重性」、「發生機率」及「可偵測度」等評分標準，對某一要項之影響範圍評價，通常分為1～10等級；就「嚴重性」言，級數越高表示影響越大，要減少嚴重性數值，須提出有效防治措施，降低風險之衝擊或破壞力（如表3）；「發生機率」言，是指此風險項目的發生機率，通常以其發生頻率作為判定的依據，並以過去發生頻率之記

表3　「嚴重性」之評分標準

影響	影響的嚴重性	等級
無預警高危險	非常高的嚴重等級將危害設備及作業員，當失效模式影響到設備操作安全和／或牽涉到違反法規時，且失效發生無預警。	10
有預警高危險	非常高的嚴重等級將危害設備及作業員，當失效模式影響到設備操作安全和／或牽涉到違反法規時，且失效發生有預警。	9
中高	嚴重影響作業進行，所有資訊資產報廢；設備無法操作，喪失基本功能。	8
	輕微影響作業程序，資料須檢驗及部分報廢；設備可以操作，但降低功能等級。	7
適中	輕微影響作業程序，部分資料報廢；設備可以操作，但部分功能無法運作，使用者會感受到不便。	6
	輕微影響作業程序，資料可還原；設備可以操作，但少數功能無法運作，使用者會感受到不便。	5
非常低	輕微影響作業程序，資料須查驗，設備操作造成使用者不舒服。	4
次要	輕微影響作業，部分資料可還原，設備操作造成使用者不適。	3
非常次要	輕微影響作業，全部資料可還原，設備操作造成使用者不適。	2
沒有	沒有影響。	1

錄為參數，但應注意頻率將隨外在環境而改變，若評分為「1」時，則表示為發生機率「極低」，分數越高表示發生機率愈高，要減少發生機率數值，則將增加稽核之次數或頻率（如表4）；就「可偵測度」言，為所有偵測風險方式之難易度，其分數越高表示可偵測度越不佳，要減少可偵測度數值，需要提升管理人員之資訊技能與專業能力，自我檢查找出單位潛在缺失並矯正（如表5）。

綜言之，FMEA優先等級判定準則為：若嚴重性分數9～10時，則表示資訊安全議題在此標準下之影響甚巨，各指標皆處於不理想狀態，而級數為1～2時，則資訊安全之議題，較無須投入更深入之管理，三項指標皆呈現佳之狀態。評分的標準乃由各組織之跨功能小組因單位之特性討論與訂定，一般企業於第一次討論建置完成後，每年僅做內容之探討，而不再修訂此評分標準。

資訊安全之資產評估或其風險值RPN之計算，是以嚴重性(S)、發生機率(O)、可偵測度(D)等三項評估指標，各以1到10分的評分項目，由跨功能小組邀請不同專家學者共同評分，再進行平均與討論判斷，而以嚴重性(S)×發生機率(O)×可偵測度(D)三項之乘積（如表6第4、6及9欄），表示該項風險值(RPN)的影響程度（如表5第10欄），RPN的值愈高，表示該風險項目對組織之資訊安全威脅愈高；若以「失竊」項之「人員安全訓練不足」為例，經10位專家學者所評分之平均值為可得其風險值為：5×3×3=45。並由單位對資訊安全要求之敏感度考量與討論後，設定RPN值若未超過150分為可接受之風險值，則表示該項潛在風險之管理，僅須按照現行之軍事院校資安管理措施辦理即可，若RPN>150分，則必須提出矯正作為（但一般軍事單位如國防部部本部單位或參謀本部單位，其資訊安全要求等級高，可將RPN設定為50分甚或更低之數值，以強化單位之資訊安全管理敏感度）；同樣地，若3項評

表4　「發生機率」之評分標準

失效的機率	可能失效的比例	等級
非常高：持續性失效	4次／每一天或≧1／每小時	9～10
高：經常性失效	1～3次／每一天	7～8
中等：偶發性失效	1～4次／每星期	4～6
低：相對少發生的失效	1～3次／每個月	2～3
罕見：失效幾乎不會發生	≦1次／每年	1

表5　「可偵測度」之等級標準

可偵測度	判斷（利用設計管控可以達到的偵測性）	等級
幾乎不可能	現行無任何管制方法可查出失效模式	10
非常些微	現行管制方法有非常些微的機會可以查出失效模式	9
些微	現行管制方法有些微的機會可以查出失效模式	8
非常低	現行管制方法有非常低的機會可以查出失效模式	7
低	現行管制方法有較低的機會可以查出失效模式	6
適中	現行管制方法有適中的機會可以查出失效模式	5
適度高	現行管制方法有適度高的機會可以查出失效模式	4
高	現行管制方法有較高的機會可以查出失效模式	3
非常高	現行管制方法有非常高的機會可以查出失效模式	2
幾乎確定的	現行管制方法幾乎可以查出失效模式	1

分標準存在極端值（單一評比分數為9～10分者，亦可納入上述高風險之作為，提出風險預應作為），也就是說，該資訊資產已不再具備或滿足機密性、完整性及可用性之資訊安全標準要求，必須進行或提出預防及矯正作為。

㈤找出高潛在風險因子

如上所述，RPN>150分的風險發生，即表示該項資產不再滿足單位之機密性、完整性及可用性要求，對資訊安全已產生實值影響，如表6「失竊」項下之「未經控管之資料複製之潛在因子」，其RPN=7×5×5=175>150，表示該項作業可列為了後續預防改進作業之目標，且針對此風險項目的改善措施，一定要提出並確保可降低此數值至150分以下之作為，尤其必須主官（管）之有效確認。

㈥預防矯正措施與持續改善

經由上述之跨功能小組成員的討論後，我們將所有目前預防風險之可行措施記載於FMEA文件內，並保持文件化效果，經由該表可提供現職或新進人員深入了解單位

表6　國防資訊安全管理系統FMEA分析表（範例）

潛在失效模式		顧客要求	潛在失效效應（資產價值）	嚴重性 S	失效等級	發生機率 O	目前預防管制	偵測等級	可偵測度 D	風險值	建議措施	實施日期	措施執行結果 採取措施	嚴重性	發生機率	可偵測度	風險值
失竊	**人員安全訓練不足**	略	1.**實際金錢損失** 2.**工作中斷** 3.**資料遺失** 4.**危害部隊安全**	**5**	**中**	**3**	**加強訓練**	**定期檢測**	**3**	**45**							
	人員評選程序不嚴謹			4	低	2	評鑑中心制		4	32							
	外部人員或清潔人員缺乏人員陪同作業			5	中	3	進出口專人管制	攜帶物品檢查	2	30							
	未保護儲存文件			7	中高	3			4	84							
	未經控管之資料複製			**7**	**中高**	**5**	**資料加密**	**使用記錄查詢**	**5**	**175**	**加強稽查**	**年度內隨機抽查**	**每月抽查3次重新記錄**	**7**	**4**	**2**	**56**
	缺乏安全警覺			4	低	4	加強訓練	定期檢測	4	64							
	資料銷毀的不確實			6	中	3			3	54							
	機密資料的外洩			8	中高	3	存取管制	攜帶物品檢查	4	96							

*資產價值：表示該風險會對資產造成何種影響。
*失效等級(依據資產價值)：1～4（低），5～6（中），7～8（中高），9～10（高）。
*風險值(RPN)＝嚴重性(S)×發生機率(O)×可偵測度(D)，RPN〉＝150則採取預防矯正作為，RPN〈150則無。
*本表單僅列所有FMEA內潛在失效模式之一項；可透過人、機、料、法、環境等構面進行深入之檢討與風險評估。

之資訊安全風險所帶來之影響，以及如何防治或避免的方法，甚至將作為標準化或訂定標準作業程序，每年需因應外在環境變動時於管理審查會議中提出討論與修訂，小組因應此變動做出持續性的改善措施，保持ISMS之適切性及有效性。且為達到預防矯正措施與持續改善作為之有效性，應要求(1)執行風險處理計畫以鑑別適當的管理行動、資源、責任和優先權；(2)為達到已鑑別的管制目標，實施風險處理計畫，包含資金考量及責任分配；(3)實行所選擇的控管項目以符合管制目標；(4)定義如何測量所選之控管項目量化目標的有效性，以及說明這些量測如何能達到管制效果，產生可比較及控管之效果；(5)實行訓練及認知之相關課程；(6)管理資訊安全管理系統的運作；(7)取得實行所需資源及管制方法，在偵測出安全事件時提出警示及對重大安全事件做出回應。

㈦主管追縱與成果確認

如表6中，選定須評估的風險項目為資訊資產電腦設備「失竊」，失竊右方則為各種造成該風險項目發生之原因，然後探討該風險會對資產造成何種影響，同時標明目前預防該風險的措施（目前預防管制），以及目前的偵測方式，最後將嚴重性和發生機率及可偵測度三項乘積為風險值，超過150者，則採取矯正措施，以降低其風險值至可接受範圍內，並標示執行結果於表中，而主管是否鄉愿般的處理態度，將影響作業成效。

綜合整體FMEA之作業模式，經由討論來制定FMEA表單，有效分析高風險要項，提出有效之矯正措施，其最後一道防線即是「主管追縱與成果確認」，主要在使監控過程的有效性最大化，另為確保系統的完整性及有效性，組織應達成(1)執行監控、審查程序及其他控管；(2)著手對資訊安全管理系統有效性的定期審查（包含達成資訊安全管理系統政策及目標、安全管制的審查），需考量到安全性稽核、安全性事件的結果、量測有效性的結果及所有利益相關團體的建議及回饋；(3)測量控管項目的有效性以驗證安全需求是否符合；(4)在一定的期間內要審查風險評估、殘餘風險及可接受之風險程度；(5)在預計期間內執行內部資訊安全管理系統稽核；(6)以規律的方式進行資訊安全管理系統管理審查，以確保範圍持續適當；(7)更新安全計畫，並將監控及審查活動發現列入考量；(8)針對影響資訊安全管理系統之有效性及績效造成衝擊之行動與事件，應予以記錄。

㈧風險評估差異比較

透過上述之分析，「FMEA風險評估法」及「威脅弱點評估表」之比較，前者較能系統化整體考量一項資訊資產之風險與管理，並建立「預防矯正措施與持續改善作為」，加諸「主管追縱與成果確認」（如表7），可提供資訊安全管理工作之成果與有效性，然「威脅弱點評估表」於表7之第(6)及(7)部分無法整體呈現於單一文件中，欠缺系統化之管理思維。

伍、結論與建議

任何組織或企業要導入ISO27001資訊安全管理系統之際，必然須針對該單位之資訊資產進行風險評估與預防，並於年度「內部稽核」與「管理審查」時進行有效的檢視與討論。而本研究運用FMEA方法進行資訊安全管理風險評估與預防作業，分析國防事務之潛在資訊安全問題及造成的風險可能，指

表7　FMEA風險評估法與威脅弱點評估法之比較分析表

FMEA風險評估法	威脅弱點評估表
(1)成立跨功能小組。	(1)成立跨功能小組。
(2)決定驗證範圍與FMEA評估議題。	(2)決定驗證範圍與威脅弱點評估議題。
(3)討論與確認FMEA（失效模式對效應的影響、找出嚴重性評價、造成失效模式原因探討、造成失效模式發的機率高低、目前管制方式與能力探討，以及系統或現行作爲能偵測出失效原因的能力）。	(3)討論與確認威脅及弱點之等級。
(4)計算風險優先指數(RPN)。	(4)計算風險值(RN)，若超過單位之要求RN值以上，再訂定不同管制措施或辦法。
(5)找出高潛在風險因子。	
(6)預防矯正措施與持續改善。	
(7)主管追縱與成果確認。	

註：「威脅弱點評估法」並不採此7步驟，本研究就其精神與內涵進行區分與比較。

出所有偵測問題之方法及應對方式，以落實資訊安全的問題解決或改善之文件化作業。筆者提出此FMEA方法論，除改善現行一般組織申請「ISO27001」認證之「威脅弱點評估表」之作法，期能喚起國軍資訊安全管理議題，使業管單位能集思廣益，針對國軍相關資訊安全作為，提出具備風險評估與預防矯正作為之方法；經此方法論，將一系列可預測之國防事務可能發生的資訊安全問題，及其可能造成之影響作出評估，透過發現、改善與防治資訊安全問題之方法，更有效落實資訊安全作業。本研究之主要貢獻：

一、建立一套資訊安全管理系統FMEA風險管理啟發方法

㈠成立跨功能小組；

㈡決定驗證範圍與FMEA評估議題；

㈢討論與確認FMEA；

㈣計算風險優先指數；

㈤找出高潛在風險因子；

㈥預防矯正措施與持續改善；

㈦主管追縱與成果確認。

二、落實組織資訊安全管理系統之全面品質管理

發起ISO27001系統導入之專案活動包括：(1)申請認證單位及其利害關係人之組織、地點、資產及技術，為資訊安全管理系統之範圍；(2)由管理階層核准及界定資訊安全管理系統政策、目標；藉由ISO27001系統之一、二、三及四階文件，提供證據以證明其建立、實行、操作、監控、審查、維持及改善資訊安全管理系統之承諾；並透過文件化管理，有效性建立防範技術，落實於全校師生，得到客觀性建議與實施對象的指導與整合，以此建立資訊安全管理系統可靠度；(3)提供申請ISO27001資訊安全管理系統認證，亦或系統化評估資產風險者，將ISO27001國際標準，應用FMEA標準作業模式進行風險評估，建立文件並作單單位成員之參考依據。

最後，在應用FMEA方法以進行國軍各

單位或部隊之ISO27001資訊安全管理系統風險評估時，多位專家學者成立跨功能小組以執行「評估指標」之評分機制甚為重要，由於人為的評估其準確度仍受質疑，可行的話，定期聘任外部專業人員（如顧問公司）或內部專業資訊管理幹部，隨時吸收新知並改進不適用之防治方法等措施，不可或缺，且FMEA表之記錄或文件，應經由資訊安管理者，定期稽核與檢視，有效的內部稽核或偵測方式，以減少風險項目確保FMEA內容與改善方案能與時俱進。

收件：100年05月09日
修正：100年07月19日
接受：100年08月09日

作者簡介

韓慧林博士，海軍備役上校，中正理工學院造船系75年班、國防管理學院資源管理研究所管理科學組碩士、國立交通大學工業工程與管理學系博士；通過品質工程師、可靠度工程師、ISO9001：2008品質稽核系統主任稽核員、ISO14000環境稽核系統管理主任稽核員、AFAQ-AFNOR GPMS-HSPM及綠色供應鏈管理師、QC080000有害物質管理系統主任稽核員、IPMA/TPMA D-Level專案管理講師、ISO27001資訊安全管理系統主任稽核員；現任職於實踐大學高雄校區資訊管理系助理教授。

王貴民博士，海軍備役上校，海軍官校70年班、美國海軍工程研究院（加州蒙特瑞市）作業研究碩士、淡江大學資訊工程博士；曾任國防部整合評估室淨評估處及模式模擬處主管；現任職於實踐大學高雄校區資訊管理系助理教授。

王振陽、劉庭維、鄭曳庭，現為實踐大學高雄校區資訊管理系四年級學生。