資訊安全法制化初探之一：根基於美國聯邦資訊安全管理法

樊國楨[1]、林惠芳[2]、黃健誠[3]

[1]國立交通大學資訊管理研究所

[2]新竹市稅務局

[3] 國立臺灣大學資訊管理學研究所

中華民國一○○年十月二十九日

摘要：

「法規合為事而定」，自2002年起，美國聯邦資訊安全管理法(Federal Information Security Management Act，簡稱FISMA)及其實作計畫，已樹立：「建立(Build)資訊安全以確立(Establish)資訊安全管理系統(Information Security Management System，簡稱ISMS)的ISMS新典範。」「他山之石，可以攻玉」，本文闡明FISMA與FISMA實作計畫的脈絡，以為我國資訊安全法制化作業之參考。

關鍵詞：

1. 廣度防禦(Defense in Breadth)。
2. 深度防禦(Defense in Depth)。
3. 實作計畫(Implementation Project)。
4. 資訊保證(Information Assurance)。
5. 聯邦資訊安全管理法(Federal Information Security Management Act)。
6. 法制化(Legal Institutionalization)。

一、前言：

美國資訊安全之法規可以上溯到1929年之聯邦紀錄法(Federal Records Act)，1942年的聯邦報告法(Federal Records Act)更闡明資訊資源管理(Information Resources Management，簡稱IRM)由白宮之「管理與預算辦公室(office of Management and Budget，簡稱OMB)」之前身「預算局(Bureau of Budget)」主責；為因應1952年起，美國「國家安全局(National Security Agency，簡稱NSA)」對「機密性」的要求與規範，1985年12月24日，OMB以A-130公告(Circular)的附件(Appendix)III正式啟動資訊安全管理法制化的工作項目[1]。

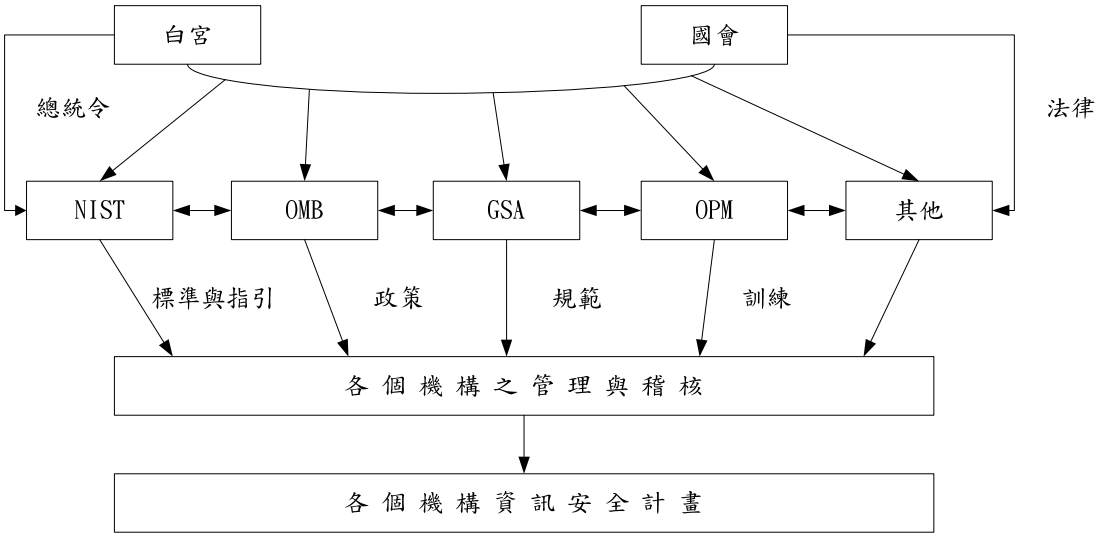
隨著資訊化之日益普及，面對多面向的網路威脅議題，1998年5月22日，柯林頓總統之第63號總統決策令(Presidential Decision Directive，簡稱PDD)將美國根基於「機密性」的電腦系統安全(Computer System Security)擴增至要求「機密性」、「完整性」與「可用性」之資訊安全(Information Security)，在「政府以身作則」的方針下，2002年12月17日美國頒布了「聯邦資訊安全管理法(Federal Information Security Management Act，簡稱FISMA)」，FISMA是「電子政府法(E-Government Act)」之第三篇(Title III)

，以立法的形式規範美國聯邦政府對資訊安全管理之要求，並進行FISMA實作計畫[1~7]，期能奠定美國資訊安全管理的基石。

FISMA是美國資訊安全管理之大事，在2002年以後，經由要求的遵循與績效之審計，FISMA實作計畫已於2007~2010年間開花結果並開展FISMA 2.0的計畫實作中[7]；根基於此，在第2節與第3節，本文分別闡明FISMA及其實作計畫；第4節，是本文的結論。

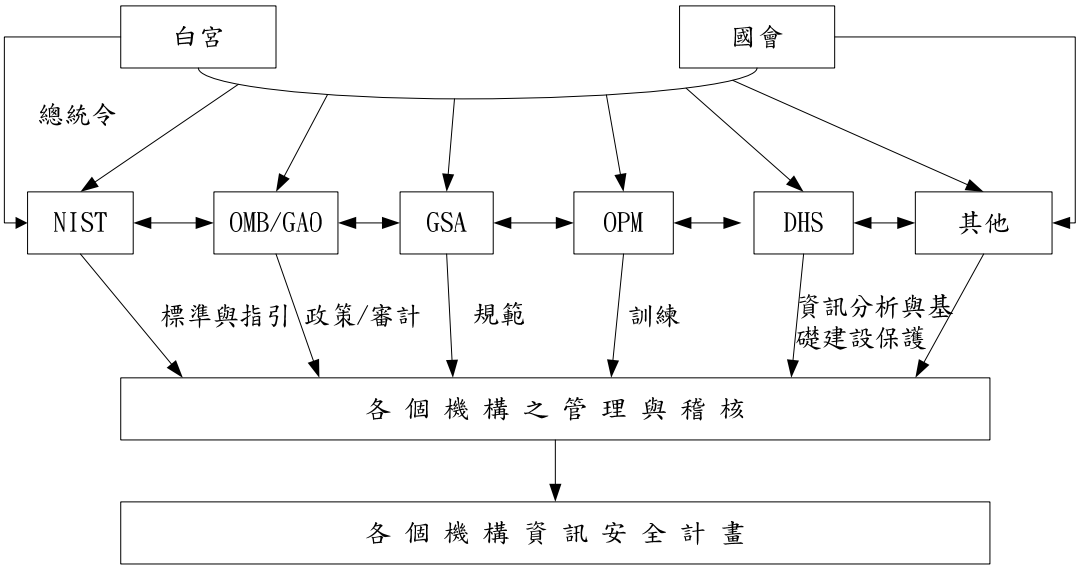
二、美國2002年聯邦資訊安全法初探：

隨著資訊化之日益普及，資訊安全管理已成為建立與完善資訊安全法律制度及明確社會各個面向資訊安全保證(Assurance)的責任以及義務之基石。根基於柯林頓總統1998年5月22日提出的：「政府以身作則」之決策[1~5]，根基於自1985年12月24日起，經由OMB A-130行政規則已建立的如圖2.1與圖2.2所示之機制；2002年12月17日，定位於：「提供確保能夠實現有效的資訊安全控制措施之聯邦運作及其資產中的資訊資源之綜整性框架。」的規範美國聯邦政府各個部門資訊安全責任與部署囿限於聯邦政府範圍內，強化資訊安全行動規劃之FISMA正式頒布。FISMA 分成：1.資訊安全(301節)、2.資訊技術之管理(302節)、3.國家標準與技術研究院(National Institute of Standards and Technology，簡稱NIST)(303節)、4.資訊安全與隱私諮詢(Advisory)委員會(304節)、技術與遵循(Conforming)之修正(Amendments)(305節)，共5節9條款，惟第2~5節均在修定諸如NIST法等；前述FISMA涉及諸如電腦安全法(Computer Security Act)中條款的廢止等與本文主旨較無關連，故此不贅。



說明：
1.NIST：National Institute of Standards and Technology
2.OMB：Office of Management and Budget
3.GSA：General Services Administration
4.OPM：Office of Personal Management

圖2.1：美國通資訊系統安全推動計畫機制示意



說明：

1. NIST：National Institute of Standards and Technology
2. OMB：Office of Management and Budget
3. GAO：Government Accountability Office
4. GSA：General Services Administration
5. OPM：Office of Personal Management
6. DHS：Department of Homeland Security

圖2.2：美國國土安全部成立之後的通資訊系統安全推動計畫機制示意

FISMA之主要內容包括：1.資訊安全與國家安全系統的定義、2.聯邦各個機關之責任、3.資訊安全的年度評估(Evaluation)、4.NIST之定位、5.NIST法的修正，簡述於後：

2.1 定義：

資訊安全管理之標的指定為：「資訊與資訊系統」，同時將資訊安全管理的目標指定為：「保護資訊及資訊系統以避免未經授權之存取、使用、洩漏、破壞、修改或銷毀以確保資訊的機密性、完整性及可用性」。其中，機密性是指對保護個人隱私與私有資訊之資訊存取及揭露的授權限制；完整性是指防止不恰當之資訊的鑑別性、可歸責性及不可否認性；可用性是指對資訊之及時以及可靠的存取與利用。

遵循慣例，國家安全系統指定為：涉及情報工作、與國家安全相關之密碼工作、軍隊的指揮及控制、武器或武器系統之裝備、國防或外交作業中的涉密資訊等，主責FISMA法實作之OMB主管的責任囿限於非國家安全系統。

2.2 責任：

2.2.1：OMB之責任在於：制定資訊安全政策、標準與指南，並監督其實作；要求聯邦各個機關/構確立並建置資訊安全保證措施；監督聯邦各個機關/構之資訊安全計畫；向國會提出聯邦各個機關/構的資訊安全工作之基本狀況；監督聯邦資訊安全事故中心的合規。

2.2.2：聯邦各個機關/構之責任在於：評鑑本單位之資訊安全風險，確定其等級，並提供與其資訊系統相稱的資訊安全防護；部署資訊安全之負責專人，展開資訊安全工作；遵循有關政策的規定，並將資訊安全工作融入其機關/構之策略與規劃運作的過程中。

2.3 資訊安全管理實作評鑑：

FISMA要求各個機關/構在每一年再確定之時間前，完成對其資訊安全計畫與實作之工作結果進行一次獨立評鑑，並將評鑑報告送交OMB，OMB將前述評鑑報告結合從其他通路獲得之資訊編製年度FISMA實作報告提交國會審查，並據以判斷前述實作計畫之效果；此面向，FISMA建立了一項具操作性的資訊安全治理之有效工具。

前述評鑑報告中，FISMA要求：所有聯邦機關/構所使用之資訊與資訊系統必須分類，在針對相應的風險等級提供適當之資訊安全防護；每一類資訊及資訊系統均應滿足最低的資訊安全要求；所有資訊系統在運行前必須進行驗證與認證(Certification and Accreditation，簡稱C&A)，通過C&A後方投入運行。前述安全計畫之查證、執行資訊系統的C&A以及測試等，如表2.1所示，是OMB提交國會審查之FISMA年度實作報告的績效指標[3~7]。

表2.1：美國聯邦政府FY2002~FY2009資訊安全概觀暨進展

目＼年 錄	FY02	FY03	FY04	FY05	FY06	FY07	FY08	FY09
1.已被總檢查長(Inspector General)查證之POA&M之聯邦部會的數目與百分比	未蒐集資料	12 50%	18 75%	19 76%	19 76%	19 76%	21 84%	24 96%
2.已執行驗證與認證(C&A)之系統數目及百分比	47%	62%	77%	85%	88%	92%	96%	95%
3.已完成應變計畫測試	35%	48%	57%	61%	88%	86%	92%	86%
4.已完成安全控制措施測試	60%	64%	76%	72%	77%	95%	93%	90%
5.資訊系統報告總數	7,957	7,998	8,623	10,289	10,595	10,304	10,679	12,930

說明：

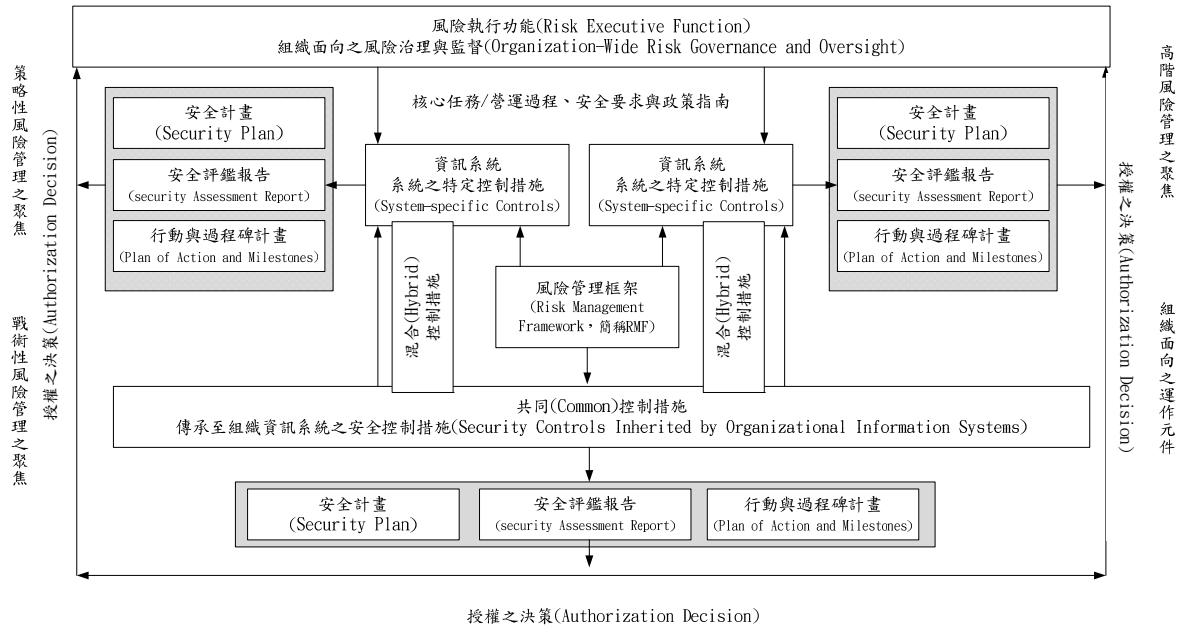
1. 行動與里程計畫(Plan of Action and Milestone，簡稱POA＆M)。
2. 驗證與認證(Certification and Accreditation，簡稱C&A)。
3. 資料來源：Office of Management and Budget, (2010), FY 2009 Report to

Congress on Implementation of The Federal Information security Management Act(FISMA) of 2002；與本研究。

2.4 NIST之定位：

FISMA責成NIST必須為前述資訊安全管理的定義、政策與評鑑等作業制定標準及指南並精進之，以達成資訊安全管理的目標。此項標準化作業已在2009年完成第1階段工作，FISMA實作計畫自2010年起已正式進入FISMA2.0[7]。

根基於FY2002~FY2009之FISMA的實作，在2010年NIST已正式提出如圖2.3所示之根基於風險管理的ISMS之框架，表2.2是其對ISMS稽核的規範舉隅。



資料來源：NIST Special Publication 800-37, Figyre2-4, P. 17, february 2010.

圖2.3：資訊安全控制配置

表 2.2：FISMA 實作計畫安全評鑑(Security Assessment)中組態控制之驗證服務要求舉隅－根基於評鑑小組(Assessment Team)

1. 知識(Knowledge)面向： 1.1 NIST Special Publication 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers. 1.2 ISAP (Information Security Automation Program) 與 SCAP (Scurity Content Automation Protocol) 1.3 OMB (Office of Management and Budget)之 M-07-11 號備忘錄(Memoranda)：2007-06-22。 2. 技能(Skill)面向： 2.1 調查(Examine)：安全組態設定之檢查(Checking)。

2.2 測試(Test)：安全組態設定之測試(Testing)。

3. 才藝(Ability)面向：
   3.1 OMB 之 M-07-11 號備忘錄：2007-06-22 的處理過程與執行程序及實作情境。
   3.2 SCAP 於資訊安全威脅、脆弱性、事故之對策應用情境。
   3.3 SCAP 於安全架構與組態設計中之應用情境。
4. 資料來源：Johnson A. and P. Toth (2007) Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal Information Systems (Initial Public Draft) September 2007.
5. 備考：2010 年，美國根基於資訊安全管理運作之要求，擴增 SCAP 至 EMAP (Event Management Automation Protocol)，期能規範稽核存底(Audit logs)的事實標準。

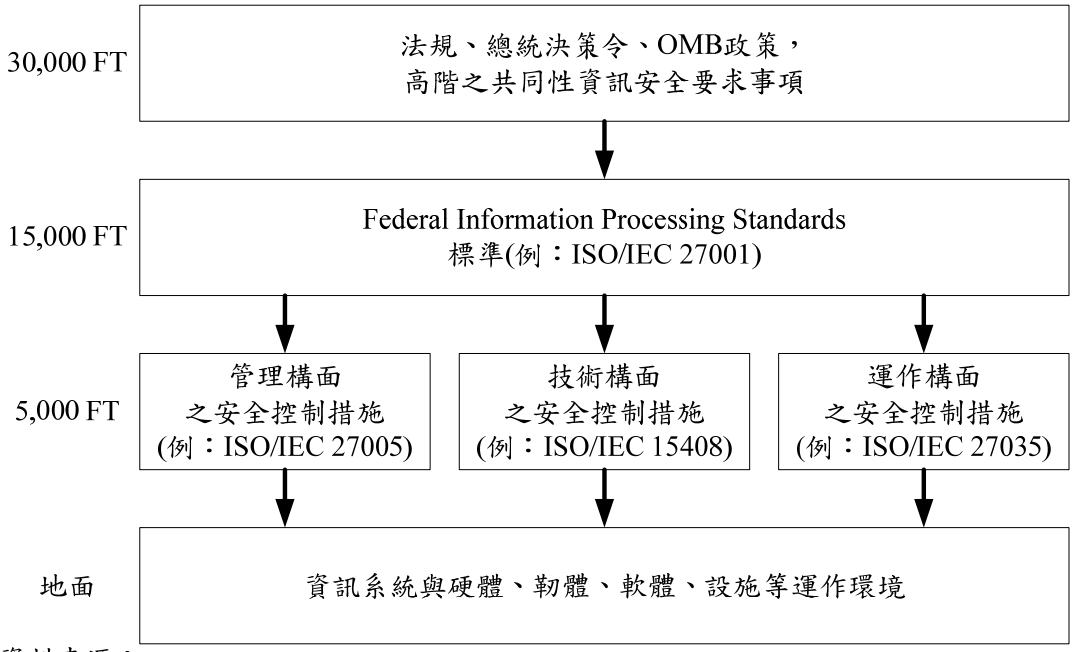
2.5 NIST法之修正：

將NIST法中之「電腦系統安全(Computer System Security)與隱私諮詢委員會(Privacy Advisory Board)」改名為：「資訊安全(Information Security)與隱私諮詢委員會」、電腦或通訊(Telecommunication)技術(Technology)及裝置(Device)均改名為資訊技術、電腦系統改名為資訊系統、電腦或通訊改名為資訊技術、電腦系統安全改為資訊安全。

FISMA可以借鑑處甚多，囿於篇幅，難以計列，「法規合為事而定」，2.1節~2.5節之闡述應可做為我國資訊安全法制化的參考。

三、FISMA實作計畫：

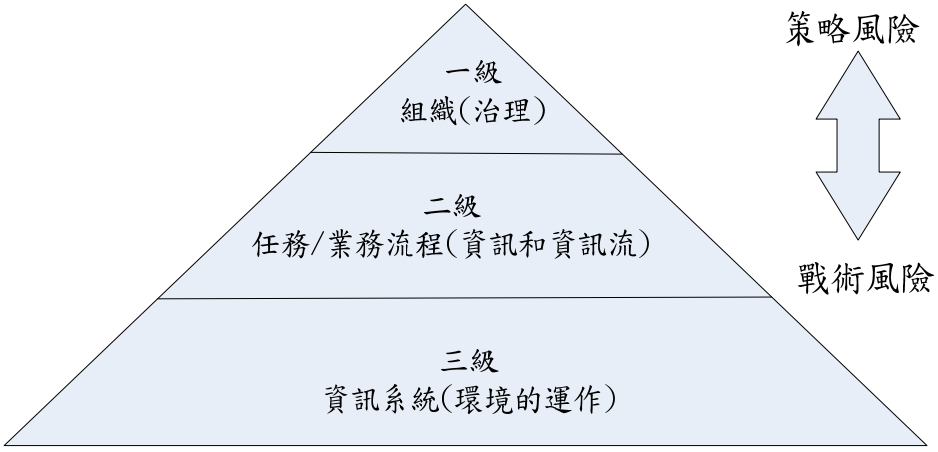
「徒法不足以自行」，FISMA實作計畫自2002年起於FISMA規範之「撥款(2002~2007)」與「時間線」進行「資訊安全管理」的「標準化」及「制度化」之工作項目；其目的在於「發展美國公(Public)與私(Private)領域(Sector)組織提供資訊安全管理系統(Information Security Management System，簡稱ISMS)安全評鑑(Security Assessment)驗證服務」，FISMA實作計畫為確保前述目的之有效性，在2002~2010間成功的塑建經由標準格式之安全資料分享的資訊系統安全控制措施自動畫之「安全內容自動化協定(Security Content Automation Protocol，簡稱SCAP)，提供執行其資訊安全自動化計畫(Information Security Automation Program，簡稱ISAP)的可操作性[8]。經由制定美國ISMS系列標準與發展SCAP並融入ISMS之作業ISAP作業，同時修訂前述標準的FISMA實作計畫[8]之第1階段工作(2003~2010)；於確立如圖3.1、圖3.2及圖3.3所示的根基於風險管理之建立ISMS規範後，進行ISMS安全評鑑的試運行，表2.1是其對ISMS稽核小組之能力要求簡述(2007~2010)以及ISAP試運行計畫的FISMA實作計畫之第2/3階段工作；2010年起，FISMA實作計畫經由如圖3.4之政策執行，正式要求進行如圖3.5所示的資訊系統組態管理之自動化作業，以落實資訊保證的工作目標[8]。



資料來源：

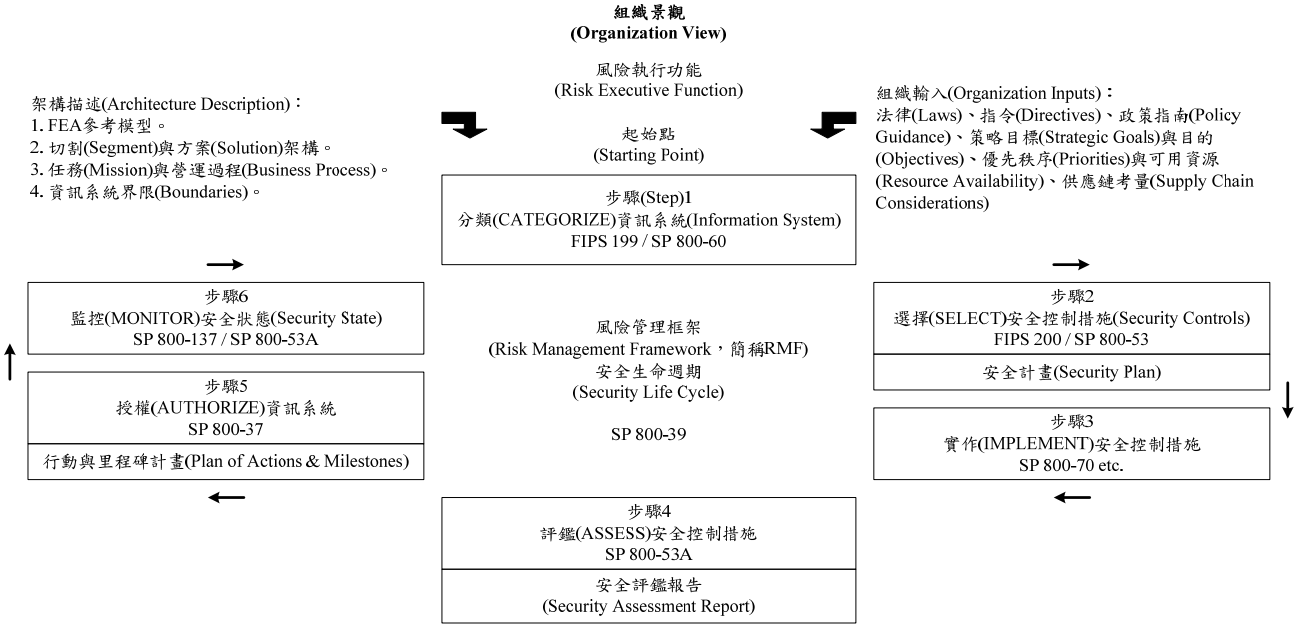
1. Ross R. (2010) Defending the United States in tHe Digital Age, Information Security Transformation for the Federal Government, NIST ICS Security Workshop, September 24, 2010。
2. 本研究
3. 說明：FT(英呎)。

圖 3.1：資訊安全管理系統要求事項之追溯性框架－美國的觀點



資料來源：Ross, R. eT al. (2010)Guide for Applying the Risk Management Framework to Federal Information Systems：A Security Life Cycle Approach, NIST Special Publication 800-37, Revision 1, February 2010.

圖 3.2：層次化風險管理取徑(Tiered Risk Management Approach)



說明：
1. FEA：聯邦企業架構(Federal Enterprise Architecture)。
2. ISMS：資訊安全管理系統(Information Security Management System)。
3. NIST：國家標準與技術研究院(National Institute of Standards & Technology)。

步驟說明：美國 FISMA 風險管理框架步驟說明

步驟 1：分類資訊系統 (Categorize Information Systems)

參考利用 FIPS 199 與 SP 800-60 標準，決定所使用之資訊系統與其處理、儲存、傳輸之資訊的重要性與敏感性類別。此工作對決定組織之資訊系統，及其採用適當保護組織任務與營運之安全控制措施的等級，與其優先順序有關。對特定資訊系統所採用之安全控制措施的等級，應與在失去機密性、完整性與可用性時對組織運作與資產、員工之潛在衝擊的大小相對應。

步驟 2：選擇安全控制措施(Select Security Controls)

參考利用 FIPS 200 與 SP 800-53 標準，識別與規劃資訊系統之適當安全控制措施。對組織之任務與營運而言，選擇安全控制措施與支援此控制措施之資訊系統是減輕風險的行動。

步驟 3：實作安全控制措施(Implement Security Controls)

參考利用 SP 800-70 標準，單位組織架構、系統發展生命週期 (System Development Life Cycle，簡稱 SDLC)等，指引組織內資訊系統之安全控制措施。對組織之任務與營運而言，選擇安全控制措施與支援此控制措施的實作。

步驟 4：評鑑安全控制措施(Assess Security Controls)

參考利用 SP 800-53A 標準，評估資訊系統之安全控制措施的有效性。使用適當方法與程序，決定是否安全控制被正確地實作、依設計運作、及產生預期的輸出，以符合資訊系統之安全目的與需求。

步驟 5：授權資訊系統(Authorize Information System)

參考利用 SP 800-37 標準，了解授權已實作安全控制措施之資訊系統，對組織運作、組織資產、組織員工與其他組織等所產生之風險，並清楚地決定接受此風險。

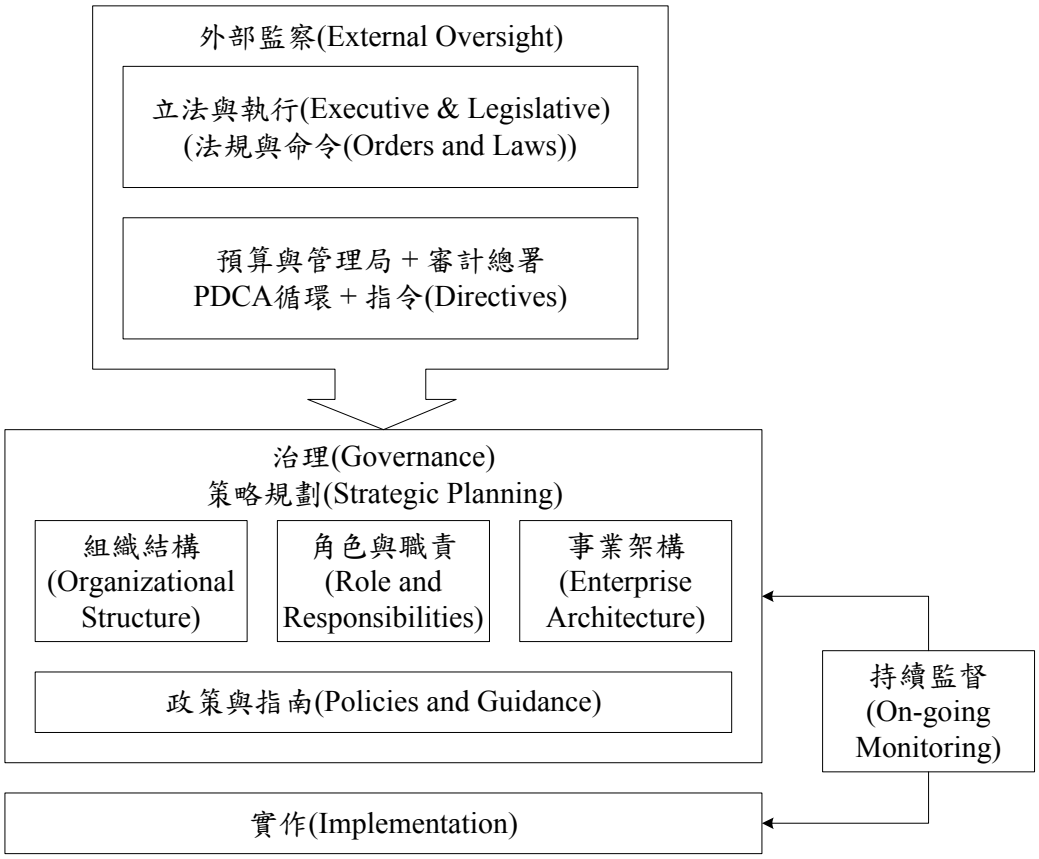
步驟 6：監控安全狀態(Monitor Security State)

1.1 參考利用 SP 800-137 與 SP 800-53A 標準，了解資訊系統作業環境之威脅與弱點是會不斷地變動，安全防護技術與其設計也需隨之更新。持續地執行安全控制措施之評鑑(assessment)與評估(evaluation)，提供對安全控制措施

之監視(oversight)與監控(monitoring)，以保證資訊系統能持續有效地運作下去。

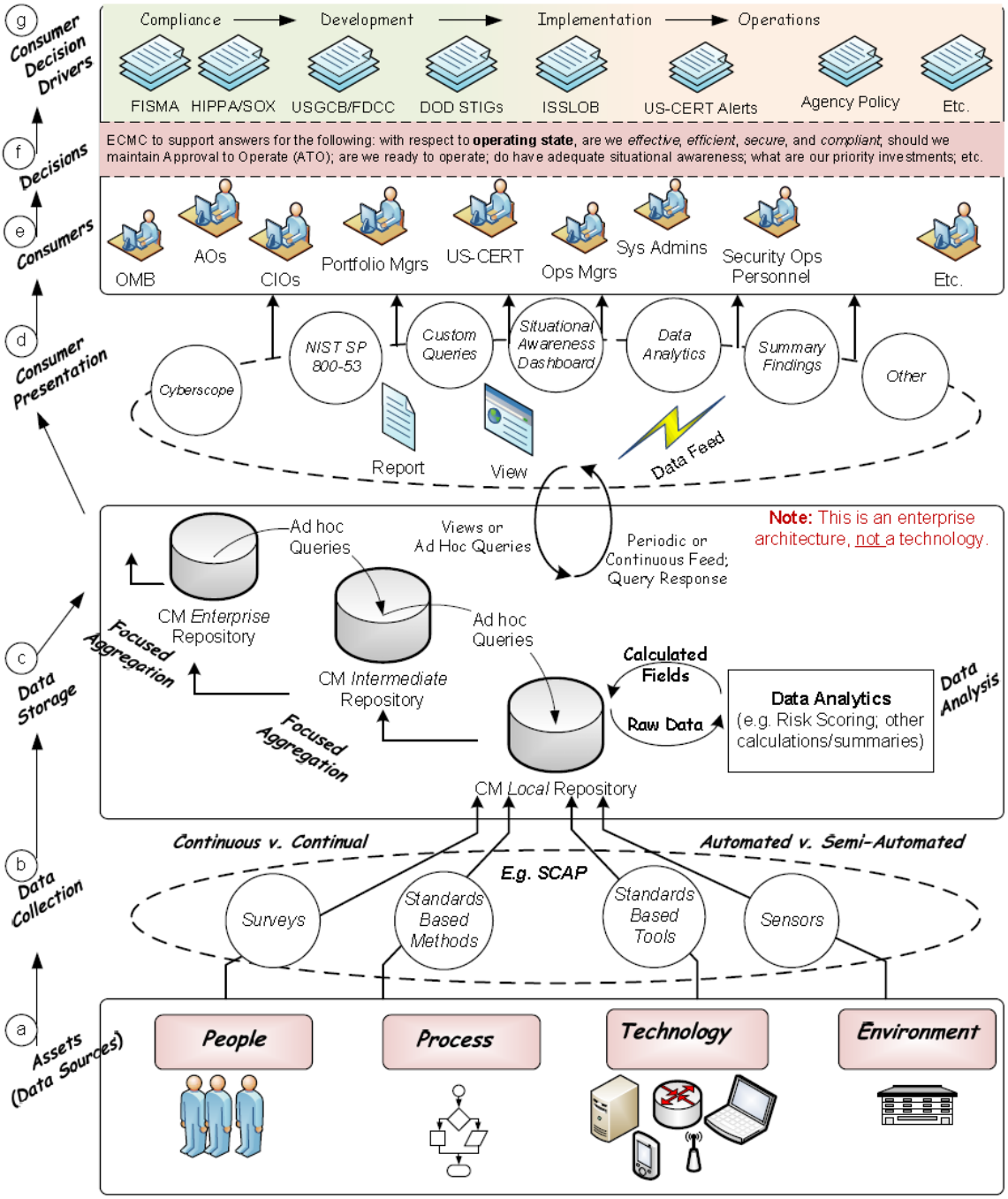
1.2 在資訊系統中，持續地監控與評鑑所選擇之安全控制措施，這包含記錄系統之改變、並對此改變做安全衝擊分析、與定期回報系統安全狀況給負責安全之組織主管。

圖 3.3：使用連續性監視之美國 FISMA 計畫資訊安全風險管理框架



資料來源：Bowen, P. et al. (2006) Information Security Handbook: A Guide for Managers, NIST Special Publication 800-100, Figure 2.2, p.5。

圖 3.4：美國聯邦政府資訊安全管理之框架與組件



Source: NIST Interagency Report 7756 (Draft), CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture, February 2011.

圖 3.5：連續性風險評鑑(Continuous Asset Evaluation Situational Awareness, and Risk Scoring，簡稱 CAESARS)之參考架構(Reference Architecture View)

於連續性稽核之準備工作告一段落，2008年10月1日，美國參議院國土安全與政務委員會(Senate Homeland Security and Governmental Affairs Committee)通過支持2002年FISMA(以下簡稱FISMA 2002)實作之名為FISMA 2008(FISMA of 2008)的議案(Bill)；2009年4月29日，美國參議院內再提出與FISMA 2008相似，惟增加網路安全研發條款的「加強網路安全法案(Information and Communications Enhancement Act of 2009)」，惟均未成功，FISMA 2008其對FISMA 2002主要的變更如後：

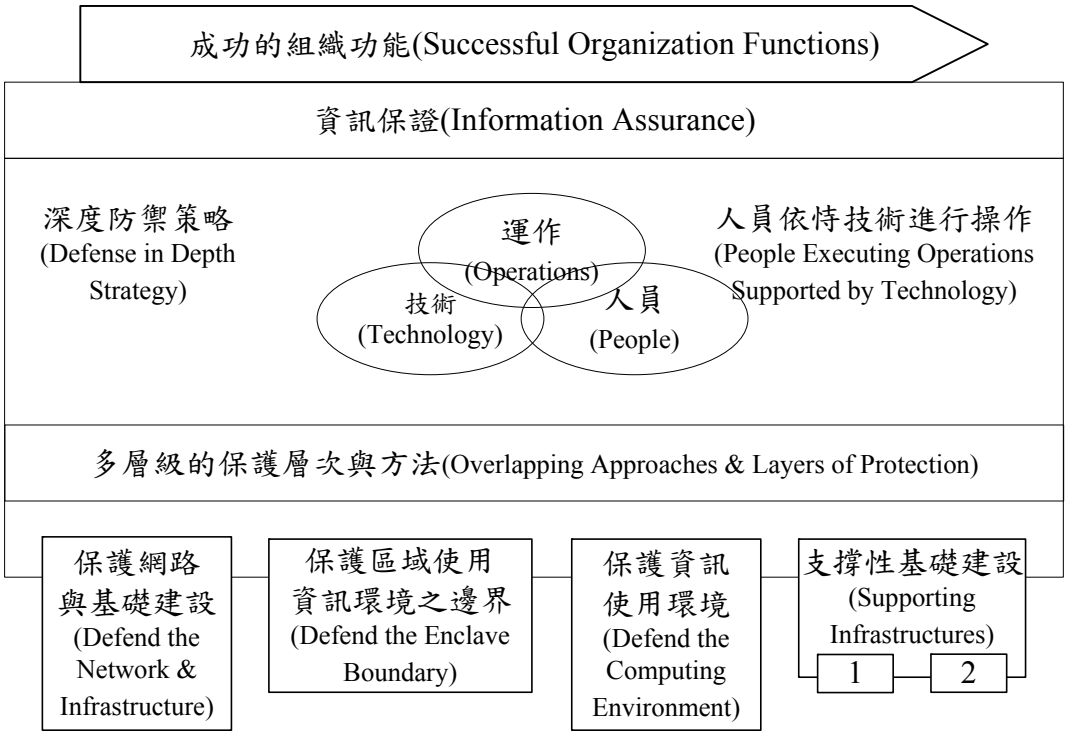
1. 創立資訊安全長(Chief Information Security Officer，簡稱CISO)之角色，賦予CISO執行資訊安全與遵循FISMA的權利。
2. 建立由美國電腦緊急整備小組(US Computer Emergency Readiness Team，簡稱US-CERT)、情報委員會事故反應中心(Intelligence Community Incident Response Center)、國土安全部(Department of Homeland Security，簡稱DHS)、國家數位安全中心(National Cyber Security Center)、國防部、國家情報總監辦公室(Office of the Director of National Intelligence，簡稱ODNI)、民營機構(Civilian Agencies)、管理與預算辦公室(Office of Management and Budget，簡稱OMB)等(但不限於)之全職資深員工組成CISO委員會，其中的民營機構為關鍵基礎建設之承包商(Contractors)。
3. CISO委員會執行增進連續性監控過程(Continuous monitoring process)的自動化機制、年度獨立稽核、資訊系統驗證與認證、風險管理之聚焦、資訊安全最佳實務的資訊分享等工作項目。
4. 責成OMB制定並公布關於資訊系統安全之正確與有效性，包含個人可識別資訊的蒐集及傳送，以及資訊安全事故之事件的程序之法規等的要求等。
5. 責成DHS於每年3月1日提交聯邦資訊安全情勢之詳細闡明的年度報告。

期能增進FISMA之可操作性與有效性。

「工欲善其事，必先利其器」，10年歲月，FISMA應已完成其制度化之標的，FISMA實作計畫亦邁向FISMA 2.0[7~9]；FISMA 2.0 提出之「建立(Build)資訊安全以確立(Establish)ISMS」，已成為ISMS工作項目的新典範。

四、結論：

借用先賢名句，「不信資安(青春)喚不回，不容管理(青史)盡成灰；低迴海上慶功時，萬里江山書一卷（酒一杯）。」雖是否能如美國所願，在FISMA 2.0中，成功整合資訊安全供應鏈風險管理之標準化作業[10]，FISMA實作計畫於2010年應已完成其里程碑，立下如圖4.1所示的「人員依恃技術進行操作」之ISMS的豐碑，並將圖4.1之深度防禦(Defense in Depth，簡稱DiD)擴增至：「尋求在系統、網路或生命週期(系統、網路或產品設計與開發、製造、系統整合、配送、營運、維護及汰除)的每一階段，識別、管理並降低可利用脆弱性之風險的一系列預先規畫、系統化之各種學科訓練活動」之供應鏈風險管理的廣度防禦(Defense in Breadth，簡稱DiB)，DiD之定義亦修正為：「整合人員技術與營運能力，以跨越組織之多層次及為度建立各種屏障的資訊安全策略」。根基於FISMA之有效性，如表4.1所示，擴及民間的數位安全法(Cybersecurity Act)於2010-03-24已通過美國參議院商務、科學與運輸委員會之審查，表4.2是其與FISMA的比較。



說明：

1. 公開金鑰基礎建設(Public Key Infrastructure，簡稱PKI)/
   金鑰管理基礎建設(Key Management Infrastructure，簡稱KMI)。
2. 偵測(Detect)與回應(Respond)。
3. 資料來源：IATF(Information Assurance Technical Framework)Release3.1,2002-09,
   Figure1- 8,Page1-14

圖 4.1：深度防禦示意說明

表 4.1：進行中之「數位安全法(Cybersecurity Act)」簡析

1. 緣起：
   - 1.1 2009-04：由約翰・洛克菲勒(John Rockefeller)與奧林匹亞・史諾(Olympia Snowe)參議員提出草案。
   - 1.2 2010-03-24：美國參議院商務、科學與運輸委員會全票通過共分 4 章 25 節之「數位安全法案」，隨後進入參議全院表決程序。
   - 1.3 2010-03-24：提出增列尼爾森(Nelson)、貝絲(Bayh)與米谷史基(Mikulski)參議員共同提出之新版。
2. 要點舉隅：
   - 2.1 將 2002-12「聯邦資訊安全管理法」之標的擴增至關鍵基礎建設的資訊系統。
   - 2.2 提出如何確定關鍵基礎建設資訊系統之過程。
   - 2.3 擴增國家標準與技術研究院(National Institute Standards and Technology，簡稱NIST)之職責至對民營機關(構)落實資訊安全標準的要求。
   - 2.4 規範由 GSA (Government Service Administration)主責美國聯邦政府資訊與通信採購之資訊安全要求的規範，制定統一之涵蓋產品及服務的 RFI (Request for Information)以及 RFP (Request for Proposal)之格式。
   - 2.5 建立數位安全緊急狀態啟動事件(允許使用軍事實力反擊)與一般性之緊急應變及回復工作的機制。
   - 2.6 制定民營機關(構)存取數位空間資訊安全國家機密之機制。
   - 2.7 建置關鍵基礎建設資訊系統(安全)人才培育與驗證之機制。

3. 資料來源：Cybersecurity Act (in the Senate of the Unite States)，2010-12-17。

表 4.2：美國聯邦資訊安全管理法與數位安全法之比較

	組織權責 (Organization Responsibility)	遵循與可歸責性 (Compliance & Accountability)	資料課責與識別竊取 (Data Accountability & Identity Theft)	教育、認知與研究及發展 (Education ,Awareness and R&D)	關鍵基礎建設與電力 (Critical Infrastructure & Electric-Power)	國際合作與數位犯罪 (International & Cyber Crime)	採購、獲取、供應鏈完整性 (Procurement , Acquisition Supply chain Integrity)
資訊安全管理法(2002)	✓	✓					
數位安全法	✓	✓		✓	✓	✓	✓

說明：

1. 備考：分類參考美國國會闡明數位安全(Cybersecurity)法案之方法。
2. 參考資料：
   2.1 Melissa E.Hathaway (2010)Cybersecurity：The U.S. Legislative Agenda, 2010-05-14。
   2.2 Melissa E.Hathaway (2010)Cybersecurity：The U.S. Legislative Agenda, Part2 2010-11。
   3.數位安全法根基於 2010-03-24 美國參議院商務、科學與運輸委員會通過知版本。

「制度化」是代表資訊安全管理工作成熟階段之指標，FISMA及其實作計畫可以借鑑處甚多，囿於篇幅，難以計列，「法規合為事而定」，第2節與第3節的闡述與正進行中之數位安全法等的進程，應可做為我國資訊安全管理法制化之參考。

參考文獻：

[1] Critical Infrastructure Assurance Office (2000) Practices for Security Critical Information Assets, Janural 2000。
[2] White House (1998) Critical Infrastructure Protection, PDD(Presidential Decision Directive)63, May 22,1998。
[3] OMB(Office of Management and Budget) (1985) Management of Federal Resources, Appendix III, OMB circualar No.A-130,December 24,1985。
[4] United State Congress (2002) Public Law 107-347-Dec. 17,2002。
[5] OMB (2000) Circular No.A130, Revised, Nov.30,2000。
[6] OMB (2003) Reporting Instructions for the Federal Information Security Management Act and Update Guidance on Quarterly IT Security Reporting, M-03-19,Aug. 6,2003。
[7] Ross, R. (2011) FISMA to FISMA 2.0：Myths and Realities(Prsentation),1105 Media Group Seminar,2011-01-12。
[8] http://www.csrc.nist.gov(2011-10-31)。

[9] 樊國楨 (2011) 資訊安全管理實作初探－根基於美國聯邦資訊安全管理法實作計畫與中國大陸等級保護之發展歷程(未發表)，2011-09。(備考：本文相關內容已完成 5 篇資訊安全護理之系列報導，其中之一刊登於資訊安全通訊，第 16 卷第 1 期，頁 4~25，2010-01；之二刊登於資訊安全通訊，第 16 卷第 2 期，頁 1~18，2010-04；之三刊登於資訊安全通訊，第 17 卷第 2 期，頁 3~26，2011-04；之四(上)刊登於資訊安全通訊，第 17 卷第 3 期，頁 3~20)；之四(下)刊登於資訊安全通訊，第 17 卷第 4 期，頁 1~22，2011-10。

[10] 樊國楨、林惠芳、黃健誠 (2012) 美國資訊安全策略與標準化初探－根基於 2011-05-16 之「數位空間策略」中的供應鏈風險管理標準化進程(已接受)，將刊登於標準與鑑驗月刊。