資訊安全治理(ISG)與資訊安全管理系統(ISMS)實作初探：根基於ISG框架之策略校準(下)

參照 ISO 已正式公布進行資訊安全治理之 ISO/IEC 27014 Information technology – Security techniques – Information security governance framework 的標準制定計畫，圖 3.3 與表 3.4 分別是其提出之框架概念的示意說明[2,9]，圖 3.4 是 ISMS 標準系列實作之應用框架的示意說明[10]，ISG 與 ISMS 之過程模型最大差異在於 ISG 強調規劃(Plan)、執行(Do)、檢查(Check)、改進(Improve)，而不是行動(Action)的 ISMS 之 PDCA 及 ISG 工作項目以及 ISMS 要求之條款的對照。

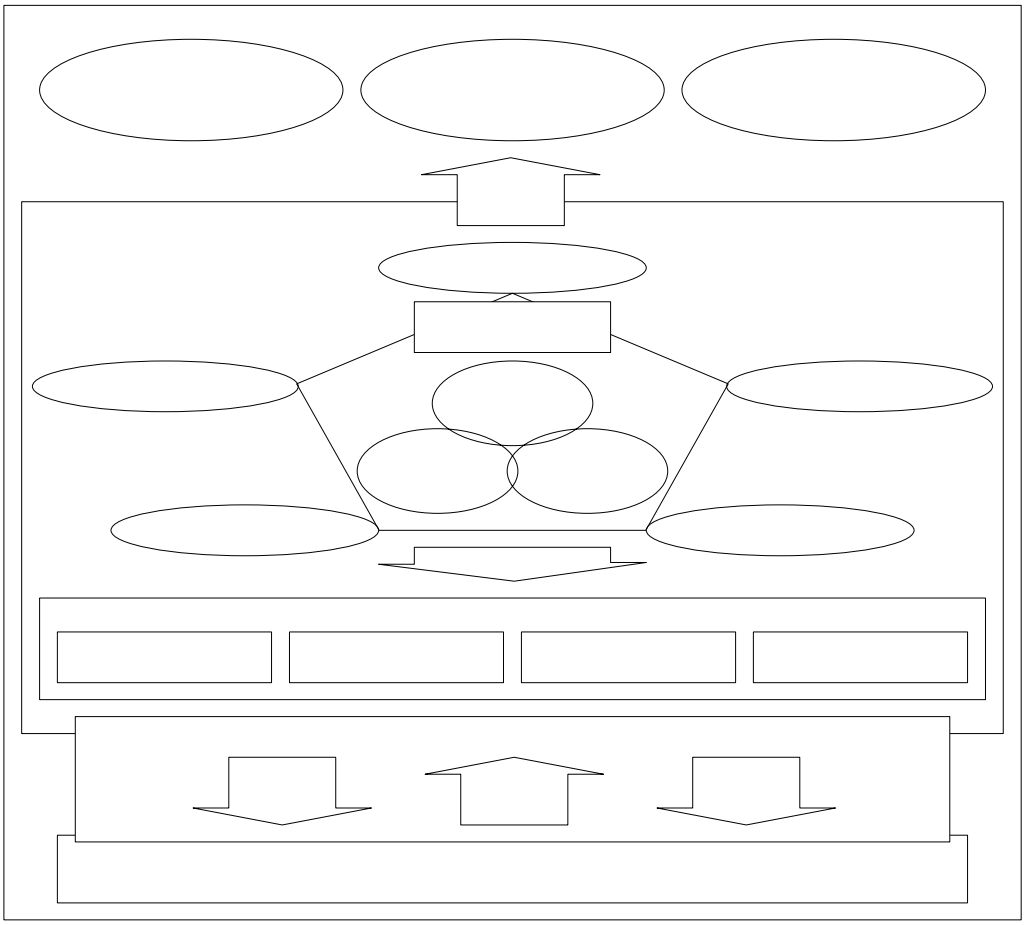


圖 3.3　資訊安全治理框架之概念

表 3.4　資訊安全治理工作項目(Tasks)與 CNS(ISO/IEC 27001:2005-10-15)條款對照

1.　領導(Direct)
5.1 a) 建立一份 ISMS 政策。
5.1 c) 建立資訊安全之各種角色與責任。
5.1 d) 向組織傳達符合各項資訊安全目標、符合資訊安全政策及法律規範下之組織責任，以及持續改進之需求等的重要性。
5.1 e) 提供充分資源以建立、實作、運作、監視、審查、維持與改進 ISMS(參照

第 5.2.1 節)。

5.1 f) 決定接受風險的準則與可接受風險等級的準則。

2. 監督(Monitor)

5.1 b) 確保建立 ISMS 各項目標及計畫。

5.1 d) 向組織傳達符合各項資訊安全目標、符合資訊安全政策及法律規範下之組織責任，以及持續改進之需求等的重要性。

5.1 h) 施行 ISMS 之管理階層審查。

3. 評估(Evaluate)

5.1 d) 向組織傳達符合各項資訊安全目標、符合資訊安全政策及法律規範下之組織責任，以及持續改進之需求等的重要性。

5.1 h) 施行 ISMS 之管理階層審查。

4. 報告(Report)

5.1 d) 向組織傳達符合各項資訊安全目標、符合資訊安全政策及法律規範下之組織責任，以及持續改進之需求等的重要性。

5. 督導(Oversee)

5.1 g) 確保施行內部 ISMS 稽核。

5.1 h) 施行 ISMS 之管理階層審查。

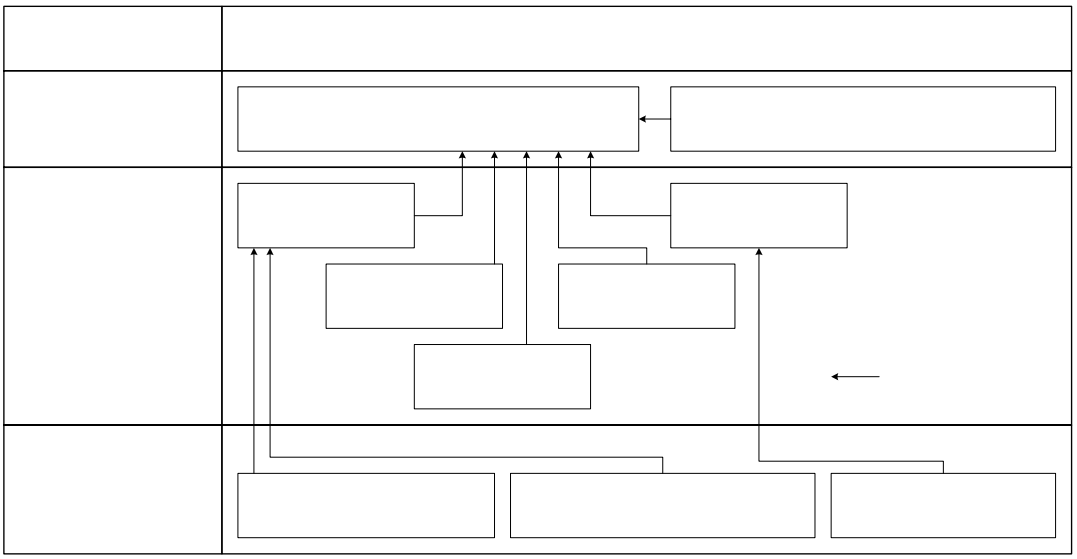


圖 3.4 資訊安全管理系統(Information Security Management System，簡稱 ISMS)標準系列(ISO/IEC 27001 屬別(Family))框架

2009 年 1 月新竹市稅務局正式宣布遵循如圖 3.4 所示之標準系列與新竹市政府「爲民服務」的治理原則，以「退稅業務」及自行撰寫所有 ISMS 文件之目標建置 ISMS，並於接受 12 個人/天的稽核後，在 2009 年 12 月通過驗證；2009 年 2 月 16 日行政院主計處電子資料處理中心中審字第 0980021063 號函要求處理 ISMS 的營運持續計畫[11]；囿於經費僅定期執行備分資料存放在台中市稅務局之作業若遵循前述行政規則建置熱機備援將大幅增加預算，另一方案則是依據我國憲法第 111 條(中央與地方權限分配)立法意旨的目標與原則，請財政部財稅資料

中心主責。經初步溝通，財政部財稅資料中心業管組長等均口頭回覆，係屬地方政府之業務中央不處理。於分析後，若全國 25 個地方稅務局之異地備援由中央政府統籌處理，其需求理論值是 $\sqrt{25}=5$ 個地方稅務局之需求[12]，則超過(>)5 個地方稅務局同時面臨 921 大地震時南投稅務局之情境，前述異地備援的理論值方不敷使用；假設每個地方稅務局在異地備援的規劃係面對巨災(Catastrophe)亦即每年發生之可能性小於(<)0.01 的重大資訊安全事故，其風險(Risk，簡稱 R)值應小於 1.5042E-7 (備考： $R \le \sum_{n=6}^{25}\binom{25}{n}(0.01)^n(0.99)^{25-n}$)；在另一方面，行政院研究發展考核委員會正推動如圖 3.5 所示之電子化政府的「資訊改造發展進程與核心工作」中。根基於此，新竹市稅務局將前述異地備援請中央政府統籌經由圖 3.3 中的「策略校準」、「風險管理」、「效能管理」、「價值交付」與「資源管理」之 ISG 分析[2,6,9]，於「效能管理」面向，如表 3.5 所示，財政部財稅資料中心已通過採購軟體品質管理制度[13]，理論上較地方政府稅務局具有效性，在「風險管理」與「資源管理」面向亦同，「策略校準」及「價值交付」面向，如圖 3.1 以及圖 3.5 所示，財政部與各個縣市政府均宜遵循；新竹市稅務局資訊安全長綜前所述，制定如表 3.6 所示的實作模型並納入 ISMS 政策。

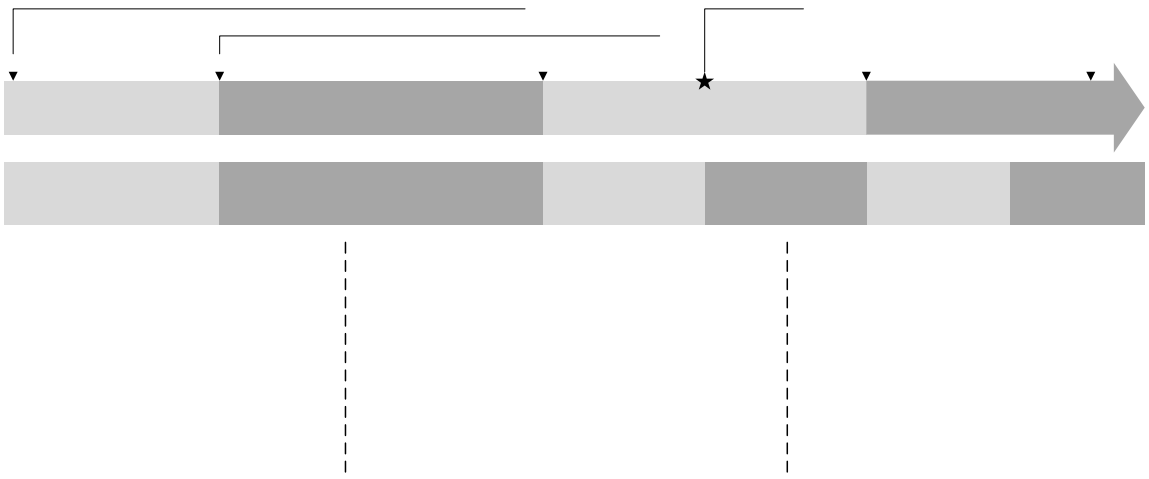


圖 3.5　電子化政府資訊改造發展進程與核心工作

表 3.5　CMMI (Capability Maturity Model Integration) ACQ (Acquisition)模式彙整

成熟度等級 / 類別	流程管理 Process Management	籌獲 Acquisition	專案管理 Project Management	支援 Support
等級 5 最佳化	• OID 組織創新和推展	—	—	• CAR 原因分析和解析方案

等級 4 量化管理	• OPP 組織流程績效	—	• QPM 量化專案管理	—
等級 3 定義	• OPF 組織流程專注 • OPD 組織流程定義 • OT 組織訓練	• ATM 籌獲技術管理 • AVER 籌獲驗證 • AVAL 籌獲確認	• IPM 整合性專案管理 • RSKM 風險管理	• DAR 決策分析和解決方案
等級 2 管理	—	• ARD 籌獲需求發展 • AM 協議管理 • SSAD 邀商與合約發展	• PP 專案管理 • PMC 專案監控 • REQM 需求管理	• MA 度量與分析 • PPQA 流程與產品品質保證 • CM 型態管理
資料來源：財政部財稅資料中心，2009 年 11 月。				

表 3.6　新竹市稅務局資訊安全治理之 ISMS 風險處理計畫「異地備援」工作項目實作模型說明

ISO/IEC 2nd WD 27014 實作項目	工作說明
過程/量度	分向財政部賦稅署與財稅資料中心爭取，並向行政院研究發展考核委員會資訊管理處反應，爭取納入電子化政府第三階段之優質化網路服務中「高效能共享集中管理與應變」的工作項目；同時提供由財政部財稅資料中心統籌各地方稅務局異地備援工作項目之成本與效益的綜效分析資料。
組織/角色與職責	資訊安全長主責，資訊安全官負責提供分析報告並向相關單位闡明之。
安全架構	併入「地方稅資訊平台整合應用計畫」。
投資管理	理論上可以節省 50%以上成本，並納入「地方稅資訊平台」分擔成本項下編列預算，應可精簡行政作業。

經過 6 個月左右之努力，並由新竹市稅務局石明紫局長在第 16 次全國賦稅會報中正式提案，財政部賦稅署於 2009 年 11 月 4 日財稅字第 09822003350 號函之「地方稅資訊平台整合應用計畫」中將「異地備援」正式劃歸「財政部財稅資料中心」主責，預定於 2013 年完成。

肆、結論

資訊化的浪潮席捲全球，一種全新先進技術之出現，把人類的生活帶引至知識經濟之數位社會。資訊技術的應用，催化人們工作方式、生活環境與思維觀念之巨大變化，大步地推動著人類社會的發展及世界文明的進步，把人類帶入新時代。然而，人們在享受數位社會帶來之巨大利益的同時，也面臨著資訊安全問題之嚴峻考驗。

當今時代，資訊已成爲一個國家最重要的資源之一，隨著資訊安全內涵的不斷延伸，經由新竹市稅務局之實作，本文如表 4.1 所示，將資訊安全治理的聚焦範疇融入 ISMS 之中並遵循表 4.2 的實作框架與圖 4.1 電子化政府之資訊安全治理框架以爲落實 ISMS 的基石[8]。

表 4.1　資訊安全治理框架(ISO/IEC 2nd WD 27014:2009-12-01)之聚焦範疇與資訊安全管理系統－要求事項(ISO/IEC 27001:2005-10-15)本文第 4~8 節的對映框架

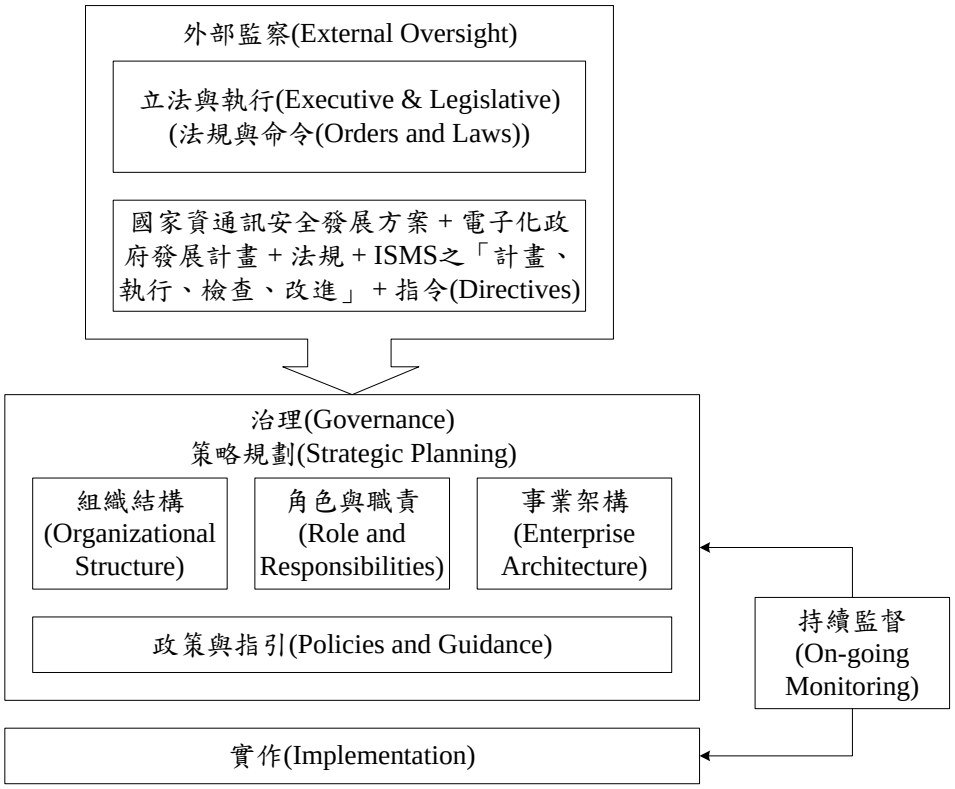
資訊安全治理之聚焦範疇(Foucs Areas)	CNS 27001 (ISO/IEC 27001:2005-10-15)條款節碼
策略校準	第 4.2.1 節(b)
風險管理	第 4.2.1 節(c)
效能管理	第 4.2.2 節(d)與 4.2.3 節(c)
價值交付	第 5.1 節(c)
資源管理	第 5.2 節與 8.1 節
備考：ISO/IEC 27014 闡明資訊安全治理之框架及其聚焦範疇與實作原則。	

表 4.2　資訊安全治理(Governance)實作框架

	目標與原則 (Objectives & Principles)	過程/量度 (Process/Metrics)	組織/角色與職責 (Organization/R&R)	安全架構 (Security Architecture)
策略校準 (Strategic Alignment)	P	P	P	P
價值交付 (Value Delivery)		P	P	P
風險管理 (Risk Management)		S	S	P
資源管理 (Resource Management)		S	S	S
效能測量 (Performance Measurement)	P	P	S	S
說明： 1、P：主要致能(Primary enabler)。 2、S：次要致能(Secondary enabler)。 3、資料來源： 3.1 COBIT 4.1，頁 26，圖 24。 3.2 ISO/IEC JTC1/SC27/WG1 (2009) Text for ISO/IEC 1st WD 27014: Information security				

governance framework, ISO/IEC JTC1/SC27/WG1 N17820:2009-05-08。

3.3 本研究



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與本研究。

圖 4.1：資訊安全治理之框架與組件示意說明

在 ISMS 標準化之過程中，實作「標準」是需要「同情」與「推理」的能力，「同情」是與制定「標準」之人有相同之情，那麼體驗的「標準」自然是立體、多元的。「同情」加上「推理」，則「標準」是活的，每一項「標準」之頒布是因或果，是一個趨勢的契機或是成績，「標準」是無數之偶然形成，但是亦絕非偶然，「標準」從長遠的角度來看，便可以體察出是有一股流勢，有無法阻擋的推移之力；ISMS 的「標準」更需整合自然科學及社會科學之脈絡來解讀、推理，方能融入文化與數位台灣渾然爲一體，如何遵循 ISO/IEC 38500 與 ISO/IEC 1st WD 27014 提出之框架，塑建「由上而下」的資安治理行動方案並融入 ISMS 實作中，宜展開更深入之探討，本文僅是作者對「資安治理推動方案」提出的一分學習心得，尚望先進宏達不吝指正。當 ISMS 標準化之過程已顯現「香蕉皮話語(Banana – peel words)」且無人指責時，如何正視 ISMS 標準化的議題，並建立相關機構之「組織管理能力(Organizational Management Capability)」與「安全評鑑能力(Security Assessment Capability)」的治理機制，據以養成相關人員應具備之知識(Knowledge)、技能(Skills)及才藝(Abilities)等能力已是必須面對之現象。ISMS 品質文化的淪落，最後終將使得社會對其驗證失去基本信任，我們不應只陷入「通過驗證」之泥淖，在那裏被僅見標識在外，無視標準要求的「金手銬症候群(Golden handcuffs syndrome)」之情境搞成混沌一片，更重要的是如何重建 ISMS 標準化之基本價值，恢復大家對 ISMS 驗證合格的信心，方是國家資訊安全標準發展之首務。隨著前述第 3 期的「國家資

通訊安全發展方案」公布之「推動資安治理」的行動方案，因爲形塑 ISMS 之決策與機制的行動者之本質是複雜且相互影響的多層級治理議題[14]，所以意味著 ISMS 標準化之進程已邁向資訊安全管理體系知識的境界[1,6~10,25]，如何善用此契機，應是我國 ISMS 標準化改進之關鍵行動方案的議題之一。

參考文獻：

[1] 國家資通安全會報 (2009) 國家資通訊安全發展方案(98~101 年)，行政院資安發字第 0980100055 號函，2009 年 2 月 5 日。

[2] 經濟部標準檢驗局 (2007) 資訊技術－安全技術－資訊安全管理系統－要求事項，CNS 27001:2007-10-24。

[3] 行政院院授主速審字第 096000567 號函，2007-08-23。

[4] http://www.moj.gov.tw/ (2009-11-27)。

[5] ISO (2008) Health informatics – Information security management in health using ISO/IEC 27002, ISO 27799:2008-07-01.

[6] ISO (2008) Corporate governance of information technology, ISO/IEC 38500:2008-06-01.

[7] http://nvd.nist.gov/ (2009-07-31).

[8] Bowen, P. (2006) Information Security Handbook: A Guide for Managers, NIST SP 800-100, 2006-10.

[9] ISO (2009) Information technology – Security techniques – Information security governance framework, ISO/IEC 2nd WD 27014:2009-12-01, ISO/IEC JTC1/SC7 N8244.

[10] ISO (2009) Information technology –Security techniques – Information security management systems – Overview, ISO/IEC 27000:2009(E).

[11] 行政院主計處電子資料處理中心中審字第 0980021063 號函，2009-02-26。

[12] Heyman, D.P. and M.J. Sobel (1982) Stochastic Models in Operation Research, Vol. I and Vol. II, McGraw-Hill.

[13] iThome (2009) e 政府，No. 2，2009 年 11 月 30 日。

[14] Bache, I. and M. Flinders eds. (2004) Multi-level Governance, Oxford Press.

[15] Back, A. et al. (2005) Putting Knowledge Networks into Action, Springer.

（本文由國立交通大學資訊管理研究所/樊國楨、新竹市稅務局/謝麗珠.廖菊芳.翁敏鈺、國立臺灣大學資訊管理學研究所/黃健誠、澳門科技大學研究生院/王演芳、真理大學資訊商務學系/林國水提供）