論述 》專論 · 評述

我國推動資安治理之建議

我國「國家資通訊安全發展方案（98 年至 101 年）」之行動方案—推動資安治理（Information Security Governance, ISG）的績效指標，已明確列示各級機關逐年度需完成導入資安治理之比例，以及組織應落實資安計畫等。本文就資安治理基礎框架與定義之要求—高階主管之承諾與參與，在資安治理框架（ISG Framework）中加入資安治理高階主管績效評估（S1）、資安治理「督導」（S2）的元件活動，以利作為未來我國推動資安治理之參考模式。

● 作者近照

蕭瑞祥（淡江大學資訊管理學系副教授）

壹、前言

資安治理（Information Security Governance, ISG）爲「國家資通訊安全發展方案（98 年至 101 年）」的 30 項行動方案之一，其執行要點與績效指標如下頁表 1 所示。依據「推動資安治理」之績效指標規範於民國 100 年與 101 年應分別 100% 完成 A 級與 B 級機關之資安治理的導入。然而，由表 1 之執行要點觀察，機關完成導入前後會有什麼明顯差異？除每年資安治理成熟度評估之外，應如何稽核導入之績效？本文以文獻探討方式，由 ISG 談起，建議由 ISG 框架中之「報告（Report）」利害關係人的內容、「督導（Oversee）」之遵循管理（Compliance management）與作業管理（Operational management）架構，以及對高階主管之資安治理績效的要求等，以做爲未來我國推動資安治理與績效評估之參考。

貳、資安治理框架

每次在參與協助組織推動資安治理訓練時，最常被問到的一個問題是：「組織已經導入 ISMS（Information Security Management System），爲什麼還要推動資安治理？有什麼不同？」首先，ISMS 的第一個重要的步驟爲定義資安管理範圍，換言之，導入 ISMS 可以自訂範圍，不一定是組織全面性的，根據 ISMS International User Group 的統計資料顯示全球導入 ISMS 機構的導入範圍統計以產品與服務別爲最多；臺灣導入 ISMS 機構的導入範圍統計以部門別爲最多。反觀資安治理是爲建立與維護提供資訊安全策略與組織目標一致，並符合相關法律規章的架構。資安治理的組成是由管理階層的承諾和領導能力、組織結構、使用者的認知和遵循、政策、程序、流程、技術和遵守執行機制等，以確保組織資訊資產隨時保有機密性、完整

表 1　「推動資安治理」行動方案之執行要點與績效指標

行動方案	執行要點	績效指標	主（協）辦單位
推動資安治理	(1) 由副首長擔任 CISO （Chief Information Security Officer）。 (2) 強化資安組織功能。 (3) 明確資安預算。 (4) 強化政風聯繫協調機制，發揮資安稽核人員功能。 (5) 定期評估與陳報執行成效 a. 評估資安治理成熟度。 b. 研訂具體改進措施。 c. 分級訂定資安治理績效評估準則，擇績效良好單位給予獎勵。 (6) 依機關資安等級分期推動實施。 備註：導入資安治理參考原則： (1) 由 CISO 每年主導進行一次資安治理成熟度評估，與資安處理小組共同檢視資安計畫成果，並向首長陳報績效。 (2) 組織應落實資安計畫，包含： a. 將資訊資產風險評估視為整體風險管理專案之一部分，定期加以評估，並根據評估結果制定資安政策與程序，且據以實施。 b. 建構內部資安管理架構，明確賦予每個人相對應的權責。 c. 將資安視為系統正常運作要素，針對網路、設施、系統、資訊等發展資安保護行動計畫，建立業務持續運作計畫、事件回應程序，並進行演練。 d. 對員工進行資安認知宣導與教育訓練。 e. 定期測試與評估資安政策與程序之有效性，並針對資安缺失提出矯正措施。 (3) 採用最佳資安實務指引（如 ISO 27002 （CNS 27002））衡量資安成果。	(1) A 級機關導入資安治理比例：98 年達 30 %；99 年 70 %；100 年 100%。 (2) B 級機關導入資安治理比例：99 年達 30%；100 年 70 %；101 年 100%。 (3) 資安治理成熟度提升比率。（導入機關自訂） (4) 資安演練防禦成功率上升比率。	行政院科技顧問組（行政院研考會、行政院主計處、各機關）

資料來源：行政院國家資通安全會報，「國家資通訊安全發展方案（98 年至 101 年）」，民國 98 年 1 月。

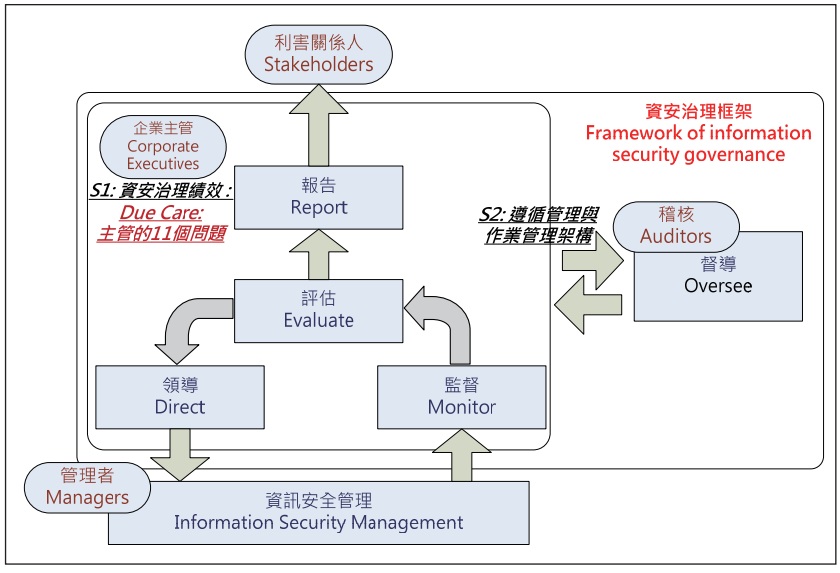
論述 》專論 · 評述

性和可用性。因此，資安治理是屬組織全面性的，並且要有管理階層的承諾的。

Ohki 等人（2009）所提出之資安治理框架（Information Security Governance Framework）（附圖）可以作爲本文建議未來我國推動資安治理之基礎。此模型是以 ISO 38500: Corporate Governance of Information Technology 標準爲基礎擴展加入兩個新組成元件，分別爲「督導」和「報告」，並由附圖顯示是以組織 ISMS 爲基礎，亦即資安治理的功能架構應該能夠包括現有的資訊安全管理和控制機制，如資訊安全管理體系等。有關附圖之各項重要元件說明如下：

- 領導：是要統領管理階層用組織目標與風險管理的角度推動資安治理。包括當面對資訊安全事件時，需要快速作決策，減少企業的損失或資訊資產的虧損、確保決策者和管理人員能有良好的互動去推行 ISMS、定義 ISM 範圍與制訂風險分析，並提供充分的資源。
- 監督：確保管理活動是可被量化衡量的指標，以利監督。包括監督 ISMS 的 PDCA（Plan-Do-Check-Act）循環現況、資訊安全事件及意外的監控，且動態或同步監控。
- 評估：從「監督」的過程去收集資料，分析和衡量達到目標的程度，若有必要則採取糾正行動。資安治理需要即時作決策，以減少安全事件造成的損失。此外，評估是要能向利害關係人報告，以利讓他們了解組織資訊安全之現況。
- 報告：將報告公開披露給組織的利害相關人，由報告實際的資訊安全活動，宣布企業有履行社會責任與組織責任，並以能提高組織價值的觀點，作資訊安全活動的報導，因爲這些活動可提供合作夥伴及客戶（或民眾）的信心，進而建立長久合作的夥伴關係，與客戶忠誠度

附圖　資安治理框架與建議



資料來源：Ohki et al.（2009）。

（或民眾信賴度、滿意度）。而組織公開的項目應包括：資訊安全政策、風險評估、風險和應對控制措施、管理制度。雖然對組織的利害相關人而言，在選擇與組織互動或作爲商業夥伴或投資目標時，也會將資訊安全治理活動納入考慮，但利害相關人並不包含在資訊安全治理的框架中，因爲他們是不可控制的。

- 督導：是一種稽核功能，由第三方的觀點檢查和驗證組織決策者資訊安全的相關活動。而資安治理框架將組織的稽核人員，獨立於管理人員，能較容易進行資訊安全相關的稽核。

本文建議我國推動資安治理除在如上頁表 1 所列之成熟度評估、評估後之資安計畫研擬與執行，對應上頁附圖之資安治理框架的「領導」、「監督」、「評估」等元件與活動之外，應再加上「報告」（S3）、「督導」（S2），以及對高階主管之資安治理績效要求（S1）等之活動，以力求推動資安治理之完整性。

參、資安治理高階主管績效評估（S1）

由於資安治理是要管理階層之承諾，因此資安治理績效評估除了要求成熟度評估與資安計畫落實之外，尚要求高階主管需要對資安治理具有應有的責任心（Due care）。Von Sloms 等人（2006）研究指出要如何看出是否有落實資安治理，在這裡強調的是如何做到落實 Due Care 而不僅是盡職審查（Due Diligence）。Due Diligence 大概意味的是盡到應盡的職責，就是當資訊安全政策制定及實行的時候，必須確保實施是持續每天都在進行的活動，不能偶爾做做樣子。Due Care 要做到的是盡到應盡的關注與重視，找出任何可能的風險，透過任何可能改善風險的方法，將風險降低，也就是在熟知與資訊安全相關的法令和準則下，再定奪攸關決策時將其考慮進去。

Von Sloms 等人（2006）認爲董事會和高階主管是組織福祉的最終負責人，因此需要採用 Due Care 的來保護公司有價值的資訊資產，若沒有採用 Due Care 保護資訊資產，可能會導致法律上的疏失。Von Sloms 等人提出了 11 個「問」董事會與高階主管的 Due Care 問題，而每一個問題都是有先後順序的，必須落實了第一個問題所描述的，方可進入檢測第二個問題。有關 11 個有關董事會與高階主管的 Due Care 問題如下：

一、資訊是否爲組織的重要資產？
二、是否有找出並確定有哪些關鍵的風險？
三、是否有建立方法或政策以降低風險？
四、組織的資安標準是否有考慮識別風險的存在？
五、組織是否有提供足夠的資

源，以落實組織的資安標準計畫？

六、組織資安作業程序是否有被適當的確認和實施？

七、組織的資安標準作業是否爲有效的（可以透過第三方做外部驗證）？

八、組織的所有員工是否了解公司的資安政策及指導方針？

九、組織的資安標準是否有定期的進行更新？

十、組織的資安管控措施是否有持續地監測？

十一、所有資安相關的內部控制（包括作業控制）爲正常的運作而被稽核？

藉由上述 11 個董事會與高階主管需瞭解之組織推動資安治理相關問題，組織之董事會與高階主管將更能達到對組織推動資安治理的承諾，因此，本文建議將組織高階主管對此 11 問題之認知、回饋、承諾程度等，增加作爲評估組織資安治理機指標之一，以利實踐推動資安治理之具體評估。

肆、資安治理「督導」（S2）

Von Sloms（2005）提出資訊安全之遵循管理（Compliance Management）與作業管理（Operational Management）架構，強調組織執行遵循管理的相關部門應依據作業管理部門所提供之日常設施運作情形的資訊，以評估組織資訊資產風險，並回報高層主管，亦可以對應到附圖中「督導」元件。Von Sloms 定義的資安治理 8 大作業管理規範準則如下：

一、邏輯存取控制管理：例如：對存取控制的清單進行新增、更改或刪除等的動作。

二、識別與認證管理：例如：針對使用者ＩＤ資料庫與密碼的檔案進行新增、更改或刪除等的動作。

三、防火牆的管理：針對防火牆、工作站連接到ＬＡＮ以及連上全球資訊網等的設定的權限。

四、病毒與惡意軟體管理：例如：進行安裝與更新防毒軟體。

五、防毒與資安事故的相關類型的掌控。

六、設置與更新工作站及伺服器的各項安全設定和組態。

七、確保ＵＰＳ系統的可用性。

八、確保正確備份及備份儲存裝置的安全。

Von Sloms 並指出現今企業對 IT 系統的嚴重依賴，已經無法只做一年一度的內部 IT 稽核報告，所以每日的遵循衡量與執行活動是相當重要。因此，Von Sloms 認爲一般資訊安全遵循管理應該包括下列規範準則與目標：

一、先前辨識出 IT 的風險的程度是要被管理和操控。

二、使用者資訊安全認知的程度

三、有助益的程序和標準，那些完整與整體的資安政策。

四、遵循政策、程序與標準的

程度。

五、企業中如果政策沒有被執行時，IT 風險對企業影響的位置。

六、管理上、法律與法令上的需求遵循

七、軟體授權問題

八、其他

本文彙總 Von Sloms 與 ISO 27006 之要求，針對 Von Sloms（2005）所倡導的資訊安全遵循管理與作業管理概念，深入分析與對應 ISO 27006 資訊安全控制標準，找出完整的對應實施表，以利協助組織資安治理之遵循管理部門自動化監控作業管理部門之日常運作資訊，以利風險爲基礎之資安治理的實踐。本文就文獻面進行分析比對後，整理出 Von Sloms 資訊安全的遵循管理準則對應 ISO 27006 標準的可施行彙總對應表。整理如表 2 所示。

再則，經本文分析比對後所整理出 Von Sloms 資訊安全的作業管理對應 ISO 27006 標

表 2　Von Solms 遵循管理對應 27001 控制目標之可施行彙總對應

項次	遵循管理規範準則（Von Solms）	27001 主要對應控制目標
1	先前辨識出 IT 的風險的程度是要被管理和操控	4.1 評鑑安全風險 4.2 處理安全風險
2	使用者資訊安全認知的程度	8.2 聘僱期間
3	有助益的程序和標準與整體的資安政策	5.1 資訊安全政策 6.1 內部組織
4	遵循政策、程序與標準的程度	6.1 內部組織 13.2 資訊安全事故與改進的管理 15.2 安全政策與標準的遵循性以及技術遵循性
5	企業中如果政策沒有被執行時，IT 風險對企業影響的位置	14.1 營運持續管理的資訊安全層面
6	管理上、法律與法令上的需求遵循	15.1 遵循適法性要求
7	軟體授權問題	15.1 遵循適法性要求
8	其他	其他

表 3　Von Solms 作業管理對應 27001 控制措施之可施行彙總

項次	作業管理規範準則（Von Solms）	27001 主要對應控制措施
1	邏輯存取控制管理	11.2.1 使用者註冊 11.2.2 特權管理
2	識別與認證管理	11.2.3 使用者通行碼管理 11.3.1 通行碼的使用
3	防火牆管理的權限設置 連接工作站至區域網路和網際網路	11.4.5 網路區隔 11.4.4 遠端診斷與組態埠保護 11.4.6 網路連線控制
4	病毒與惡意軟體管理	10.4.1 對抗惡意碼的控制措施
5	處理防毒相關類型的安全事故	13.2.1 責任與程序 13.2.2 從資訊安全事故中學習
6	設置與更新工作站或伺服器的安全設定和組態	11.5.1 保全登入程序 11.5.4 系統公用程式的使用 12.6.1 技術脆弱性控制
7	確保 UPS 系統的可用性	9.2.2 支援的公用設施 9.2.4 設備維護
8	確保備份和儲存裝置的安全	10.5.1 資訊備份

準的可施行彙總對應表，整理如上頁表 3 所示。由於相關對應的控制措施可能因組織型態、組織規模、組織業務範圍及組織資安治理成熟度等因素而有所差異，故本文只整理選出較具主要功能與代表性的項目，以增加實踐的明確度與可執行度。

本文建議應依據針對 Von Sloms （2005）所倡導的資訊安全遵循管理與作業管理概念，在附圖資安治理框架中之「督導」元件加入「S1：遵循管理與作業管理」，並依據本文所提出遵循與作業管理對應 27001 控制措施之可施行彙總表（表 2 與表 3），採用自動化與系統化之技術性檢測工具，以提供組織落實實施資訊安全遵循管理與作業管理的參考，以利協助組織資安治理之遵循管理部門自動化監控作業管理部門之日常運作資訊，以利風險爲基礎之資安治理的實踐。

伍、結論

本文主要是依據資安治理基礎定義與範疇，建議我國未來推動資安治理之架構應在「國家資通訊安全發展方案（98 年至 101 年）」之行動方案：推動資安治理的執行要點中，再加上資安治理高階主管績效評估（S1）、資安治理「督導」（S2）等兩項元件活動。其中，資安治理高階主管績效評估（S1）是以高階主管對於組織推動資安治理之 Due Care 爲出發點，以 11 個問高階主管之資安治理推動的問題，作爲確保高階主管承諾之基礎。有關資安治理「督導」（S2）的工作內容是以遵循管理與作業管理之架構，強調組織執行遵循管理的相關部門應依據作業管理部門所提供之日常設施運作情形的資訊，以評估組織資訊資產風險，並回報高層主管。本文並建議遵循管理與作業管理對應 27001 主要控制措施之相關自動化、系統化的技術性檢測工具等，以利日常作業快速與正確地執行及收集相關資訊呈報。

參考文獻

1. 行政院國家資通安全會報，國家資通訊安全發展方案（98 年至 101 年），民國 98 年 1 月。
2. Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T, & Kagaya, T.（2009）. Information security governance framework, WISG '09 Proceedings of the first ACM workshop on Information security governance, ACM New York, NY, USA, 1-6.
3. Von Solms, R.（2006）. Information security governance: Due care, Computers & Security, 25, 494–497.
4. Von Solms, S.H.（2005）. Information Security Governance -Compliance management vs operational management, Computers & Security, 24, 44–447.❖