清流月刊中華民國九十八年十月號

導入ISMS是為了保護政府機關的資訊安全，資訊安全的目標是設定機關內如何持續運作的資安管理目標與相關機制。

政府機關為何要導入ISMS

◎ 黃小玲

壹、前言

很久以前有一段相機底片的廣告詞曾提到：「我說…人活得好好的，他為什麼要拍照？」廣告詞的結尾則說：「我的天啊！什麼軟片這麼好啊？…一次OK」。

許多資安負責人員的疑問是，如果我的現行運作機制維運良好，為什麼要導入資訊安全管理系統(Information Security ManagementSystem, ISMS)？而且導入ISMS後，機關是否等同服用萬靈丹，就可以藥到病除，一次OK？

底片很神奇，ISMS是否也一樣神奇？

貳、導入前的評估作業

政府機關若導入ISMS，涉及的範圍與衝擊對內部影響甚為重大，應審慎評估需求。導入ISMS包括的預算編列，必需考量項目，如輔導費用、控制措施調整或建置費用及後續驗證費用等，更遑論所投入之人力與時間成本。導入ISMS可以是一項非常耗費資源的工作，因此如何確保所投入成本之效益回收，需經由下述評估作業後，建議各政府機關依照所定義之策略目標與評量準則，進行是否需要導入ISMS之作業分析。

一、法律或規範的要求

1. 行政規範：政府機關導入ISMS有不同的需求來源，大部分的原因為自願性導入，認定機關確實存在著資安管理制度之需求，才決定導入ISMS；至於部分非自願性的考量則為行政規範的要求。從89年開始每期4年的資通安全機制計畫，主要針對重要的政府機關建立一套完整的資通安全整體防護體系，包括資安專業人員的訓練、應變機制等防護；而該機制計畫亦包括重要政府機關(構)逐年通過資訊安全管理系統的驗證。政府若能從各機關先落實，再推向民間產業，共同建立完備的資安防護體系，並列入政府機關持續推動資安業務的範疇，則資安管理效益不言可喻。行政規範的符合通常是導入ISMS的主要考量，又因配合著機制計畫或是資通訊安全發展方案，施行計畫期程的設定，所以導入需求的急迫性與必要性反而容易被忽略。
2. 法律或合約要求：從法律的觀點來看，組織要考量的保護範圍是從個人資料至機關隱私，不論是內部管理或外部法律規範的要求，組織都應呈現積極的態度保護所擁有的資訊並建置完善管理的流程及相關的技術防護，以因應法律或合約的要求。資訊安全管理系統在其條文中亦提及與法律規範條文的符合性；對所有政府機關來說，如何避免違反任何法律、法令、法規或契約義務，皆可列入導入ISMS的評量要點。

二、業務持續重要性與安全目標

導入ISMS是為了保護政府機關的資訊安全，而資訊安全的目標是設定機關內如何持續運作的資安管理目標與相關機制。

資訊安全的定義是考量維持資訊的機密性、完整性及可用性；同時還可以包括資訊的鑑別性、可歸責性、不可否認性及可靠性等方向。

資訊安全是讓組織在有限的資源(包括時間、人力及預算)內，確保政府機關可以維持服務不中斷，達成業務服務水準的協議，並取得下列三項基本安全要素的平衡點。

1. 機密性：確保只有被授權的人可以存取資訊。政府機關內部列入機敏性資訊分級者，皆應列入保護。
2. 完整性：確保資訊從產生開始、處置、存放及廢止時，處理方式的正確性與完整性。例如，如何確保網站資訊不被篡改與誤用。
3. 可用性：確保資訊在被授權人有需要時可以存取。例如：使用者在預先定義的時間或權限上是否可以存取。

圖1：資訊安全目標示意圖

政府機關可以考量其所執掌的業務若是突然停頓或中斷、對國家、社會或民眾的衝擊分析或是所設定之安全目標後，再決定是否需要導入ISMS。

三、組織風險考量

政府機關應考量所可能面臨之風險，面對這些風險來源時，是否已設定可接受之風險等級(Risk Acceptance Level)；如果風險為不可接受時，可考量ISMS所建議的最佳實作規範與控制措施是否為最佳的解決方案。

政府機關的風險來源可概分為以下幾種：

1. 資料外洩：因為業務流程相關資訊安全部分控管不佳，造成非授權人士可以存取。例如，某醫院曾傳出名人病歷外傳的事故，造成病人隱私受損並間接影響醫院名聲。
2. 內部員工的疏失或惡意行為：印出的業務報表任意擺放或是使用懶人密碼等等。例如，公務人員利用職務之便，任意出賣民眾資料以牟利。
3. 駭客威脅：系統上的弱點，可能吸引來自全球的駭客攻擊；包括針對一般使用者的社交工程手法，與鎖定特定機關的目標式攻擊手法。例如，電子郵件社交工程的受害者，可能造成使用者成為無意的加害者。
4. 資訊交換風險：政府機關若與法人組織或民間團體進行資訊交換時，亦應考量資訊交換上可能產生的風險。例如，醫療單位與健保相關單位進行資料傳輸或交換時的安全防護。
5. 公務家辦的風險：隨著一些儲存媒體的方便使用，公務家辦的趨勢與隨之而來的風險也逐漸增加。

政府機關需要考量不同的風險來源，分析現行的控制措施是否具備資訊安全管理的架構。當現行控制措施不足以降低風險等級時，或因現行控制措施缺乏一套管理機制時，亦可以列為導入ISMS的要素。

四、導入預期效益分析

政府機關雖然不像民營機構需要自負盈虧，但導入ISMS前的評估作業，應包括預期的效益分析；到底導入此管理系統，對機關的效益在那裏，而且是否值得這大量資源的投入。

下表為建議之預期效益分析：

表1：ISMS導入前後預期效益分析

比較項目	ISMS導入前	ISMS導入後
清楚設定安全目標	未明確設定	可衡量指標
了解風險來源	被動回應	積極回應
業務所承擔之風險	風險高	風險降至可接受之等級
使用者操作信心	信心不足	信心高
使用者資安滿意度	滿意度低	滿意度高
資訊安全管理難度	分散式的資安管理	系統式的資安管理
資安事件回應速度	事件處理人力未有效管理	建立事件回應機制
資訊作業效率	人員經驗分享，效率低	定義標準作業程序書，效率高
內部稽核能力	缺乏專業人力	具規劃與實務能力

資訊安全管理系統的導入，如果事先未充分溝通清楚，容易產生管理階層或使用者對ISMS有過高的期待，以為資訊安全管理系統可以解決所有的資安事件，同時消弭所有可能之風險。導入前之效益評估與溝通，可以讓所有人對ISMS的效益有一致性的認知，如此方不會產生預期性之落差。

參、結論

當政府機關考量所有上述的情況後，可以在進行導入ＩＳＭＳ之前，列出評估項目與檢視表，以確認真正的需求是否已被清楚辨識。ISO(International Organization for Standardization, 國際標準化組織)相關的管理系統在國內組織環境內，若未進行實質的效益評估與內部資安需求的確認，則容易流於形式。如果政府機關只是為了導入而導入，為了驗證而驗證，逐漸地，資訊安全管理系統將淪為只是少數人負責維護的錯誤認知；縱使累積許多的資安政策與管理程序，卻未必能見到實質效益。因此ISMS導入前之評估，實在應謹慎為之。

參考文獻

- [1] ISO 27001：2005
- [2] ISO 27002：2005
- [3] 國家資通安全會報94至97年「建立我國通資訊基礎建設安全機制計畫」
- [4] 國家資通訊安全發展方案(98年至101年)

▲Top

資訊管理系統通過ISO27001標準的驗證，不應被視為最終目的，而應視為只是建置過程中的流程。

ISMS導入經驗分享

◎黃小玲

壹、前言

資訊安全長在管理會議上說：我聽說A機關已經通過驗證，花很多錢請國內知名的顧問公司輔導。會計主任說：我昨天參加一個研討會時，有個機關的資訊人員提到：因為他們沒有太多預算，但因同儕機關已通過驗證，所以打算跟他們複製資訊安全管理系統 (ISMS)的文件範本，試著自己導入看看。資訊處處長說：我已先編列預算，讓同仁先去受訓，回來再好好規劃，看看如何進行。

如果政府機關已決定導入ＩＳＭＳ，所面臨的第一個問題將是：我該從那裏開始？編預算交給顧問公司或是自己執行？導入的範圍該怎麼規劃？期程要多久才能通過驗證？

貳、差異性評估分析與範圍確認

導入專案一開始的差異性分析是為了評估現行之資安管理制度與防護技術，才可以確認機關的資安目標與導入範圍。差異性分析可先期評估現有人力，包括日後的推動小組人選與能力是否充裕、人員是否具備足夠能力足以執行後續專案工作，並在ISO 27001驗證標準與資安現況落差評估完成後，可以協助專案人員了解執行時間、投入資源及後續效益之結果。

一般在導入決定範圍時，會有一個迷思：範圍越小，越容易通過驗證；或是找資訊機房等範圍來通過驗證，如此對機關的衝擊才不致過大。因此在確認範圍時，應先進行業務衝擊分析(Business ImpactAnalysis, BIA)，了解在所有業務範疇內，依業務的重要性來決定導入的範圍。

參、可能面臨的困難與挑戰

每個機關由於業務與內部文化的不同，其所面臨的困難與挑戰也不同。茲列出以下幾種可能面臨的問題點。

一、預算不足

首先，應先列出可能需要的費用，再依據需求決定投入的資源。預算編列包括輔導、人員訓練、風險處理措施(例如基礎設施調整、防護技術工具購置) 及驗證費用，可能產生的費用還包括風險評鑑或是專案管理工具採購等等。

二、人員能力不夠

導入ISMS需要有專業人力，包括資訊安全長、管理委員會、資安推動小組、資訊人員及稽核等成員組成一個完整的管理組織。機關應評估適當人員與具備相關管理權責人員，以利導入ISMS後續主導與執行動作等。若發現相關人員需要專業訓練時，應即早規劃，才能執行專業管理分工的工作。

三、流程的變更與文化衝擊

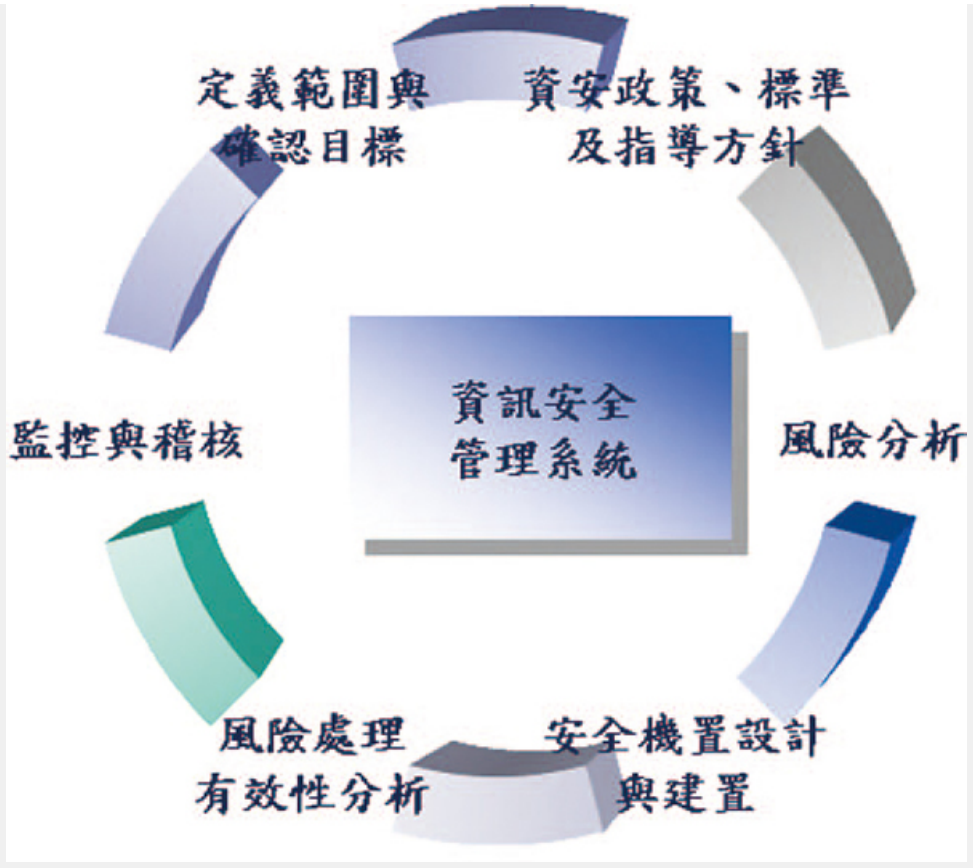
新制度的導入，往往帶來內部文化的衝擊。當原本熟悉的流程，在ISMS導入時，得進行變更。內部同仁一般會產生「領土被侵略」的感覺，進而排斥ISMS的導入。而這種排斥的心理，有時如同一種傳染病，會在瞬間蔓延。針對流程變更，同仁不適應或排斥的心理，得在一開始評估內部文化時，分析可能造成的衝擊。往往組織在導入ISMS時，會先以教育訓練為內化技巧，凝聚內部同仁資訊安全管理意識與對ISMS導入效益的認同感。

肆、導入階段

ISMS建置專案可分為兩大階段，包括資訊安全管理系統建置與驗證稽核階段。

一、ISMS建置

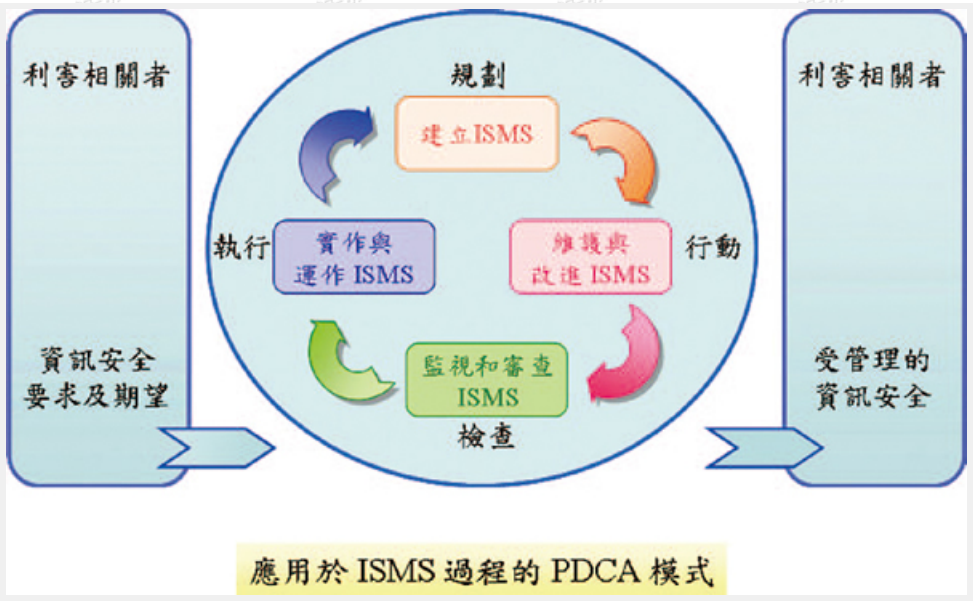
1. 專案執行規劃：確認專案效益、目的及目標。
2. 業務衝擊分析與風險評鑑：流程分析與風險分析。
3. 管理架構設計與建置：發展資訊安全管理相關程序。
4. 維護監控：產生管理紀錄、管理審查會議及內部稽核。
5. 認證準備階段：流程與程序最後確認、記錄確實追蹤審查及內部稽核結果缺失改善。



ISMS建置流程圖(自行整理)

二、驗證稽核階段

1. 驗證預評
2. 第一階段－書面審查
3. 畫面審查缺失改善
4. 第二階段－實地審查
5. 實地審查缺失改善
6. 建議或推薦發證



PDCA循環(資料來源：ISO 27001:2005)

伍、PDCA循環流程

資訊安全管理系統探討流程的運用與導入，在ISO27001標準提到應先考量組織所有利害相關者的資訊安全與期望之後，導入PDCA(P:Plan計畫；D:Do執行；C:Check檢查；A:Action處置)管理循環，以建置一個良善的管理資訊安全制度。PDCA管理循環也代表著持續改善的概念，於過程中因內部與外在環境的改變，而不斷調整管理方向評估與提出改善方案，以維護ISMS的有效性。

陸、成功關鍵因素分析

建置一個成功的資訊安全管理系統需要全體人員的充分配合與投入，才能設計與建置一個符合組織的客製且適用的管理制度。而在整個過程中又以風險管理最為耗時費力，若不能精準地分析機關的風險來源，則無法有效降低風險。以下列出幾種導入ISMS的成功關鍵因素。

一、資訊安全責任的正確歸屬

所有管理制度有一個共通點，若要實施成功，首推管理階層的支持與承諾。許多人誤解資安是資訊或是稽核人員的責任，正確的觀念是資安需要所有人的認知與配合，而最終的歸屬責任則在管理階層。管理階層若只是口頭承諾支持建置資安管理系統，卻未見任何實質的指導與配合行動，則將出現縱使驗證通過，但資安成效依然不彰的情況。

二、資訊安全管理不是技術導向

由於大部分的資訊處理、管理及維護皆落在資訊部門，所以普遍認為今日若要推動資訊安全管理制度，就應先從資訊部門開始。當資訊人員在建置相關的防護技術後，其餘的部分就是將ＩＳＯ四階文件補齊，就等著通過驗證。惟片面的資訊技術導向，無法健全整個管理制度，仍要配合管理機制的導入，在技術與管理相輔相成下，方可成就健全的管理制度。

三、管理制度的落實與符合

資訊安全管理制度文件數量的多寡，不是導入成功與否的重點。少數錯誤的想法是文件越多，代表管理得越謹慎，則風險也會相對地比較少，因此常見明明是不同業務性質的組織寫出來的管理制度文件，其相似度卻高得令人咋舌。如何產生量身訂做或是制定適用的管理制度，並確保其落實與符合程度，才是成功推動的關鍵要素。

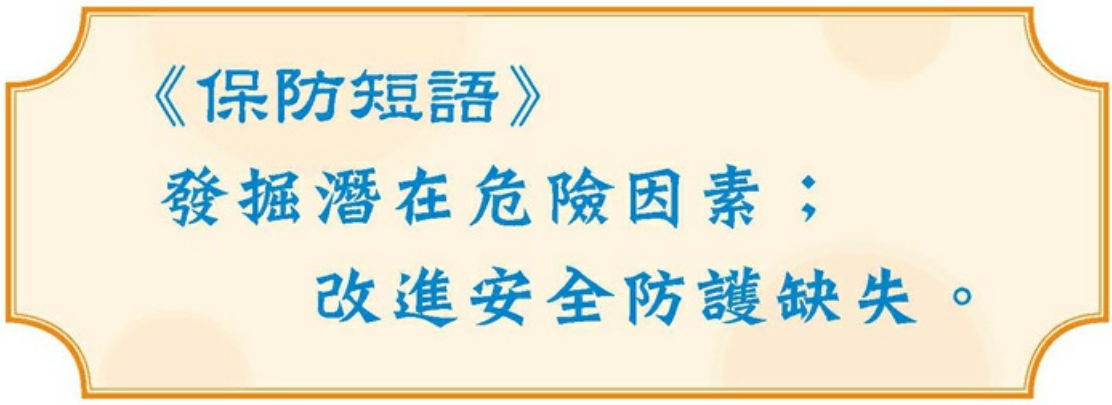
四、稽核廣度與強度的運用

稽核人員的作用在確認所建置之制度與標準的要求是否有落差，因此必須要求稽核人員有一定程度的專業能力與稽核經驗。資訊安全管理系統因為涉及資訊技術，所以稽核人員除應具備稽核經驗外，尚需兼具資訊技術能力，亦即必須涵蓋管理與技術，並能提出對機關真正具效益的改善方向與建議，同時驗證管理制度的有效性。

柒、結論

資訊安全管理系統通過ＩＳＯ27001標準的驗證，不應被視為最終目的，而應視為只是建置過程中的流程，畢竟後續的持續管理與維護工作，有時更具挑戰與困難。

（作者是行政院國家資通安全會報技術服務中心組長）



▲Top