中小企業資安認證導入實例

四大訣竅ISO27001認證勢在必得

文／江敏霞

本文作者將以自身企業導入通過ISO27001的經驗說明，即使是中小企業，只要掌握四大要領，一樣可以順利拿到ISO27001的認證。

資安管理認證ISO27001全名ISO/IEC 27001:2005 - Information Security Management Systems Certification，為資訊安全管理系統(ISMS)之認證標準，國內對應標準為CNS27001，並為「行政院及所屬各機關資訊安全管理要點」、「行政院及所屬各機關資訊安全管理規範」等國家法規所採用。自2005年起政府積極推動資訊安全以來，所有政府A級單位皆陸續取得驗證。ISO系列國際標準，都是藉由經過認證的驗證公司，以公正客觀的方式，確認導入單位是否落實標準所規範的框架與流程、並符合所有準則。

根據ISO27001認證網站指出，目前全球通過ISMS認證的機構有5,822個，其中台灣占331個，排名全球第四，其中通過認證的331個機構中，有超過半數是政府單位。拜政府機關為因應法規皆需導入ISMS之賜，這套管理系統在資訊與資安業界中頗為知名。分析民間企業的認證需求，除了國外客戶要求、大型ISP業者與少數跨國企業外，自主性地建置資訊安全管理系統的企業尚在少數，但以現今企業運作高度倚賴資訊應用環境下，資安也漸受重視，像ISMS這樣一套有效的資訊安全控管措施，其實不分企業規模與類別都十分適合導入。以下我們將就自身的導入經驗，提出4大訣竅以供讀者參考

訣竅1：導入安全政策先從觀念著手

要安全，限制與管控的手段就會多，可以預期使用者端多少會認為不便而反彈。但是只要透過生動的教育訓練與相關配套措施的結合，就會有事半功倍的效果！比如說：利用被駭入侵的新聞事件、駭客手法示演，讓同仁體會並思考資安漏洞與駭客入侵事件，對於個人與公司會造成多大的損害，大家就能理解資安規範背後的目的。

訣竅2：從大架構與核心精神出發，以簡馭繁

ISO27001總計有133個控制要項，可歸納為安全政策、資產管理、風險管理、事故管理…等十二大系統框架（見圖1）。

▶將相關項目批次進行

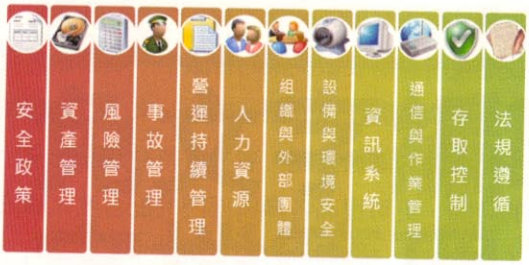

圖1　ISMS 12大系統框架。

要查核的雖有一百多項，其實執行時可將同主題或相關的項目，利用框架的結構及ISO規範內容分階段批次進行，例如：為了分析組織內較高的風險在哪裡，須先進行資產盤點、再依盤點結果為每個資產標定機密、完整、可用性的分數，然後再進行資產的威脅、弱點評估，列出高風險項目請高層主管協助評定後，先進行改善；至此即完成了資產管理、風險管理及部分的安全政策擬定。針對衝擊性大但發生機率不高的弱點或威脅，可規劃緊急處理與復原作業，進一步完成完整的營運持續計劃。由於在ISMS當中，「人員」也是重要的資產，因此不論是徵才、教育訓練或離職、交接等作業，也可藉由ISO27001提供的相關控制要項檢視現行作業是否已顧及資訊安全的層面。

▶確認PDCA的主要執行精神

ISO27001雖有百餘條項目，但事實上條文不會告訴你要做到什麼程度，才會獲得單項的滿分；而是要你拿出證據（政策文件、表單紀錄），證明你可以確保這個項目有做好安全控管。評量方式如此設計是因為每個機構的規模、人力、財力等狀況不同，很難用齊一的標準規範大家，ISO只要確認最主要的執行精神：P（計畫）、D（執行）、C（查核）、A（行動）已落實在組織中，當組織運用這套循環式的流程管理模式，即可自行調校做不好的

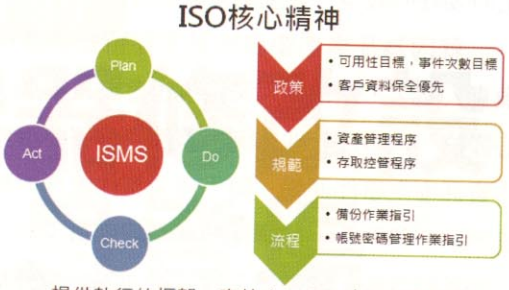

圖2　ISO核心精神-PDCA。

地方、自我療癒與進化。也因此導入過ISMS資訊安全管理系統的組織就知道，在這個管理系統裡沒有如聖旨般不可修改的文件、也沒有不會填寫的表單，當然也不保證零事故發生…因為只要不足、不適當、有失誤，就將PDCA從頭來一遍，這樣組織就有能力自行調校出最切合實用的資安政策與作法。

訣竅3：養成凡事紀錄、文件化的好習慣

ISMS對於必備的文件類型已訂立好規範，共分為四大類：

- 政策與原則（一階文件）
- 各領域的操作程序（二階文件）
- 操作程序之作業指引（三階文件）
- 執行時之表單紀錄（四階文件）

▶透過文件化促使日常工作謹慎

通常從組織有意取得ISO27001認證開始，文件撰寫以及導入文件控管制度會是一大重頭戲。據統計，導入ISMS會需要至少六十份以上的文件產出與發行作業。ISMS要求所有決策、輸入輸出、異動，都要有文字紀錄與負責人簽核。紀錄可以是紙本表單當然也可以是文管系統。如果想要做的事情，文件上沒有，或是文件表單已不符時宜，都可以修改，只是變

更時要註明版本，並記載變更的理由。

就因為凡事都要白紙黑字存留紀錄並由負責人簽字，連帶的大家做事也會變得更加小心謹慎。以事件管理為例：事件發生需要填寫「資通安全事件通報」與「資通事件處理與矯正預防紀錄單」：依事件的嚴重程度有不同的上報簽核等級，除陳述失誤狀況並進一步分析根本原因之外，還要追蹤事件是否矯正完畢。所以，用「凡走過必留下痕跡」這句話來形容ISMS的文件管理，實在再貼切也不過了！

▶從紀錄中發現問題

滴水不漏的事件紀錄，其實還可以幫助組織進一步發現長久以來問題狀況的趨勢；只要將事件統計表做成每季、每半年的匯整，再依時間序與類別進行分析，就有機會抓出問題狀況的趨勢。例如：從統計發現某台主機，每一兩個月不定期就會當機一次，再次檢視經常性的當機事件，換個角度思考也許會有新的發現；問題的癥結也許不在於得多花精神監控這台機器，也許只是因為機器老舊，只要將其下線更換新機就不會再反覆當機。但若未將事件統整歸納出來，靜心思考問題的根本原因，恐怕平日也只能專注在問題發生時，忙著救火而已！

訣竅4：高層支持全員配合是成功的關鍵

想要加快導入的時程，讓整個資安制度進展順利，最有效的做法就是高層的帶頭參與。再次強調ISMS只是一個架構，至於要怎麼符合133個控制要項，組織需要很多的討論、決策、分工、領導與執行。如果導入工作只有專注在少數人如網管人員身上，對於推行至全公司的事務，肯定窒礙難行。建議的作法是：邀請具有決定權的高層，加入ISMS任務編組，或是在所有需要做決策的會議中，邀請他們直接參與決策與任務分派，如此一來，可大幅減少部門間的溝通問題、省去等待高層審閱裁示的時間，更可提高各參與部門的配合度。資安工作的推動，高層的實際支持非常重要，有了他們的一聲令下，政策通常都能快速的落實到各個部門。

ISO27001對企業的好處

取得ISO27001認證是個榮譽，而且對於私人企業更有莫大的好處：

1. 透過國際資訊安全證照的背書，從今以後站在第一線的業務與客服人員更容易說服客戶、讓客戶放心企業在資料交換、保管以及個資的處理上的做法是保證安全的。
2. 經由嚴謹的資安理論架構，可徹底釐清組織在資訊安全上不足之處，並在有限的時間內儘快做補強措施，不啻為企業資安體質大整頓的好機會。
3. 也是最直接的獲益，就是強化了企業的競爭力。在導入的過程中，經由事件控管，降低了事件發生的次數。而其他的ISMS活動：如資產管理、帳號密碼控管、備份作業、營運持續計畫、事故演習、人員安全觀念提升等措施，不但同時健全了企業的內在體質也必然提升對外的競爭力！

責任編輯／陳啟川