JCIC「全組織一次通過」ISO 27001資安驗證經驗分享

潘萬年、陳進棋／金融聯合徵信中心資訊部

現今網路安全設備技術及效能日新月異，儘管如此，資訊安全事件仍是層出不窮，「員工」的疏忽往往是其中的關鍵，而ISO 27001的核心就是建立資訊安全管理體系（Information Security Management System, ISMS），提供一個資訊安全作業準則的平台，避免人為因素所造成資訊安全事件；ISMS以資訊資產（Asset）為出發點，評估定義的資產，決定出那些風險是無法容忍並針對無法容忍的風險作好控管，進而謹慎考量政策或流程以管理殘餘風險，即所謂風險管理。

驗證專案之起始

風險管理分成兩個部份，第一部份是風險評鑑（Risk Assessment），根據資訊安全管理系統範圍內的資產，評鑑其風險等級；第二部份是針對高風險資產作風險處理（Risk Treatment），以降低其風險，使其一但發生風險時，仍然在可以接受的範圍內。

透過適當的風險評鑑和風險處理，聯徵中心各個單位透過完整的資訊資產風險評估，將工作上的資訊資產分門別類管理，並使剩餘風險（Residual Risk）皆控制在可接受的範圍內，藉以達到效益和成本的最佳平衡，並完成資訊安全的三個最主要目標：機密性（Confidentiality）、完整性（Integrity）、可用性（Availability），這三個最主要的目標。

聯徵中心以ISO 27001國際標準為基礎，最佳化資訊安全管理體系，並與現行之內部控制制度及員工手冊進行整合，依據ISO 27001標準之要求，ISMS共分為11個控制面向（包含相對應的133 個控制措施），涵蓋資訊相關的所有層面，諸如政策、組織、人員、資產管理、實體環境、作業管理、存取控制、資訊系

統開發及維護、危機處理、營運持續管理，及法律等等，以有效達成資訊安全的目的，並落實整體資訊環境安全。

驗證專案執行過程

進行ISO 27001資安驗證前，最重要的工作即是決定要驗證之範圍；聯徵中心在原始規劃驗證範圍時，擬採「部門組織」別方式，計劃分二階段完成全組織通過驗證，第一階段僅針對資訊部及風險研究組、第二階段再擴及其他部室組；經多次研商及全盤考量後，決定採納專案輔導顧問之建議，一次全組織進行驗證。

當驗證範圍決定之後，接下來最重要的工作，就是由顧問輔導團隊與聯徵中心全體同仁合作，對驗證範圍內之聯徵中心現有資訊安全管理體系（ISMS）開始進行檢視、差異分析、風險評鑑、改善及強化、落實執行等活動，其間不斷進行所有ISO國際標準管理系統皆強調之「計劃、執行、檢查、行動」（Plan-Do-Check-Act, PDCA）之持續改進過程，直到正式驗證方歇。

對驗證活動本身而言，除了決定驗證範圍外，另外第二項重要工作即是完成「適用性聲明書」（Statement of Applicability, SOA）之內容，亦即確認ISO 27001各項條文是否「適用」或是可以「排除」。「適用」的意義表示，當外部驗證機構之稽核員進行查核活動時，稽核員就要從該條文之要求，確認組織活動是否符合。當然確定SOA之內容，對於條文要有一定熟悉之程度，此時就要大力借助專案輔導顧問之協助，與驗證機構稽核員進行溝通，重點在於確認組織認定之「不適用」條文是否真的就是可以被排除。

接下來即是要選擇所謂之驗證機構，選擇之考量因素，如：業界名聲、驗證費用、驗證通過難易度等，各組織應會就其需求，對上述各點作出最佳選擇。以聯徵中心而言，產業屬性應歸類為金融服務產業，以目前國內資安驗證通過現況（參考網站 www.iso27001certificates.com資訊），金融業幾乎都是選擇英國標準協會（British Standard Institute, BSI）為第三方驗證機構；同時聯徵中心之主管機關行政院金融監督管理委員會（以下簡稱金管會）銀行局之週邊機構，如：財金資訊公司、聯合信用卡中心，或是金管會證期局之週邊機構，如：證券交易所、櫃檯買賣中心、期貨交易所、集保結算所，亦全是由BSI驗證，因此，聯徵中心也選擇BSI擔任第三方驗證機構。

為了確定「考試通過」即「驗證通過」，被驗證機構幾乎都會安排「預評」，就是所謂之「模擬考」，同時為了使預評更加擬真，進行預評之稽核員也會選擇正式驗證機構派出之稽核員擔任；惟預評是需要費用的，如果組織預算不是相當拮据，那麼為了使考試順利通過，還是建議參加「模擬考」。

通常預評大都安排為一個「人日」，為了讓稽核員有充足時間看更多，避免正式審查時

有任何「意外」，不妨考慮貴組織之實際狀況增加稽核人日，以聯徵中心之實際經驗，預評是兩個人日。

最後就是「正審」了，驗證機構會依據驗證範圍內之員工人數，決定所需之稽核人日，並排定「Stage 1 書面審查」及「Stage 2 實地審查」之日期，屆時就會派稽核員到組織進行驗證審查之工作。如稽核人員查核結果未發現「不符合事項」（Non-Conformity），在Stage 2 實地審查之結束會議的會上，大家就會得知驗證機構稽核組長作「建議發證」之答案。

驗證專案經驗分享

雖然「通過第三方驗證」是本專案成功與否的重要且同時必定要達成之目標，但是整個ISMS制度之建立及落實運作，才是專案之終極目標，因為，唯有整個「ISMS管理之PDCA」持續運作，才是確保組織資訊安全成功之唯一要素，以下乃落實本專案過程中獲取之重要經驗，茲提供同業先進參考。

（一）成立常設性工作小組

由於驗證範圍是全組織，如何讓全體員工共同參與，必然是專案推行之重點。所以一開始，先確立整個資安管理系統之組織，由各部室（組）代表組成「資安推行小組」，其性質為「常設性」之跨部門工作小組，作為組織內任何資安問題討論之窗口，藉著小組之持續且正常運作，使得ISMS制度能真正契合組織資安之需求，不致有過鬆或窒礙難行情況。同時全體員工之一般性資安教育訓練，也是增進全體員工資安意識認知（Awareness）最重要之方法。

（二）組織「資安委員會」

任何ISO管理系統，都會要求管理階層之支持，因此，為確保高階主管對於任何資安問題能確實掌握，有效之溝通是基本的成功要素；所以也會設置「資安委員會」，由各部室（組）之一級主管組成，定時召開委員會會議，作為全組織最高資訊安全政策決定單位，協調資訊安全控制措施之落實情況，以合理之責任分配和有效之資源管理，並得到管理階層之實際支援，促進組織內部安全。

（三）謹慎進行文件整合

由於ISO 27001條文對於制度面有其文件化之要求，而這方面通常是組織需要輔導顧問協助著墨之處。但是過去很多實際案例，為了使專案順利完成，以及為確保組織手上具有能滿足ISO 27001驗證通過所需之文件，因此，顧問通常會依據過去輔導驗證成功之經驗帶入一套所謂「標準版」之ISMS制度文件，再根據組織個別差異進行內容調整，這種方法對於現有相關程序文件不齊備之組織，不失為一種快速建立及有效學習之方法；但對於組織內已有相關程序文件者，將衍生組織內會有多套文件之後遺症。

試想，倘如組織內部為ISO 9000品質系統已有一套文件，而員工執行日常業務另有其一套SOP（Standard Operation Procedure），之

後為ISO 27001又「生出」一套資安文件。如此一來只會讓員工混淆，不知如何遵循；更甚者，會造成「上有政策、下有對策」之心態，認為這一套文件只是為了ISO 27001外部稽核驗證而虛設的。長此以往，對組織文化一定會有負面之影響，更遑論資安工作是否能夠有效落實。因此，如果組織內已有相關程序文件，甚至「多套」者，「文件整合」之問題，一定要嚴肅面對；切莫為了專案速成及通過驗證，而又「生出」一套程序文件出來。

（四）切忌削足適履

對於程序文件問題，另外值得思考及注意的一點是，有些輔導顧問因為滿腔熱血，或是過去成功之經驗，甚至想帶入「業界最佳實務」（Best Practice）範本，但是往往未能真正考量組織之現實狀況，如：組織之部門架構、員工人數、作業習慣等「組織文化面」之因素；程序文件內容本身絕對是無懈可擊，但是對組織卻可能造成無法真正執行之困境，等到真正被稽核的時候，又產生「說、寫、做」不一致的缺失項目。因此，組織在面對資安程序文件內容時，切莫好高騖遠，以為採用Best Practice就一定沒有問題；但實際上訂出適合自己組織的，就是Good Practice。每一步腳踏實地站穩，循序漸進，落實PDCA之機制，自然而然就會達到Best Practice才是王道。

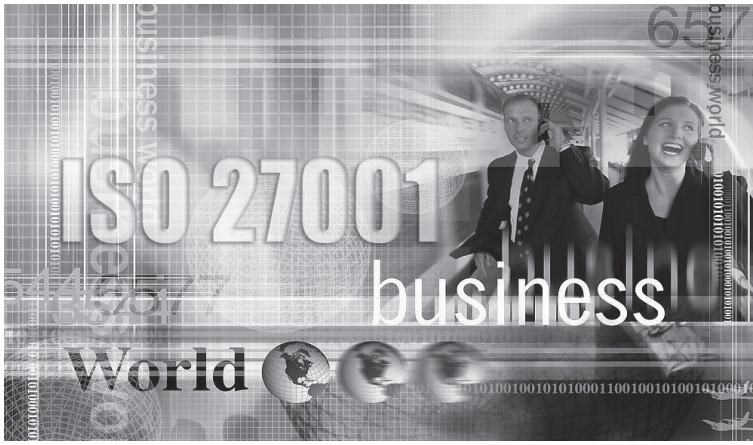
（五）精確辨識資訊資產

除了訂出資安程序文件是重點外，另外一項ISO 27001驗證重點就是「風險評鑑」，這方面對許多組織而言，都不是核心能力，所以勢必仰賴輔導顧問；而「風險評鑑」的成功基本要素，絕對在於「資訊資產之辨識」。根據歷史經驗，輔導顧問能力再高強，也不容易在短時間內，幫組織找出所有之資訊資產，因此，這方面的責任一定是組織內部要承擔，切勿全部倚賴輔導顧問。顧問可以幫忙的地方，在於釐清某項資訊資產是屬於什麼種類、是否該納入、或是可以忽略等。但是，如果內部沒有人告訴顧問，他們也無從提供意見及建議。就如同資訊界之Old Saying－Garbage In, Garbage Out，如果資訊資產無法正確地被辨識出來或被刻意的忽略，風險評鑑之結果可想而知；表面上作出來的結果是「天下太平」，但實際上卻是「暗潮洶湧」，組織或許已承擔過多之風險卻不自知。

此外，需要提醒的是，不是把會計系統中之資產帳拿出來，或是找一個人去弄出張清單就算了，而是各個部門都一定要確實參與，因為，唯有自己部門才最清楚瞭解自己之業務，也才知道哪些才是要被辨識出的資訊資產，否則武功再高及滿腔熱血的輔導顧問，也是巧婦難為無米之炊，作出來的風險評鑑結果，自然一定無法反映組織真實的狀況。

就如之前提過，最早聯徵中心之規劃，是分二階段完成全組織通過驗證，後來決定採納專案輔導顧問之建議，一次全組織進行驗證，其最主要原因是考慮如何保持全組織進行資安驗證專案之Momentum（推進力、動力、氣勢），是進行這種類型專案執行時必須考

量的重點。原則上還是建議，輔導至實際驗證時間不宜過長，以保持凝聚組織內部及輔導顧問之動力，雖不敢說可以「事半功倍」，但至少可以避免「事倍功半」，讓大家保持焦點，一鼓作氣完成，而不要如齊人「再而衰，三而竭」。



驗證專案完成後之實際效益

導入資訊安全管理制度並取得ISO 27001認證，可協助確保客戶資料的機密性、保護資訊資產之完整性，以及提升資訊資源之可用性；聯徵中心全體員工除落實「資訊安全，人人有責。」的觀念外，以展現保護客戶資料之決心與承諾，完成驗證專案後之實際效益如下：

（一）凝聚內部資安共識

透過教育訓練與專案的推動將加深聯徵中心同仁之資訊安全認知、凝聚內部資安共識、共同參與及維持資訊安全制度的運作。透過資訊安全管理體系的建置，確保資訊的機密性、完整性、可用性，使資訊能安全地、正確地、適當地及可靠地被運用。

（二）辨識資訊資產，降低營運風險

藉由良好的風險控管程序，可使聯徵中心能有效地掌握營運中所面臨的風險，並進一步有效的控管及處理相關的風險。

（三）建立可行方案與制度

於日常作業中落實風險管理，建立可行適用制度，使各部室人員願意遵行，並樂於遵行，所有風險管理措施才能真正落實。透過同仁從日常流程了解現行作業，從主管需求中萃煉出可行方案，使資訊風險管理真正在聯徵中心生根。

（四）透過嚴謹資安制度，確保民眾隱私

民眾及法人之相關資料實屬「電腦處理個人資料保護法」及相關隱私權法令所保障的個人資料範圍內，ISO 27001國際資訊安全驗證程序過程嚴謹，共分為預評、文件審查與實地審查三階段，其驗證之專業性及權威性獲得全球一致的肯定，確保有效地加強對個人資料的保護，向國際資訊安全標準接軌。

（五）強化民眾與會員使用電子平台信心

聯徵中心推行電子化服務，透過電子平台提供會員更快速正確之服務，因此，需要一個安全可信賴，且接受國際驗證的平台，以大幅強化民眾與會員使用電子平台的信心。