ISO 27001資訊安全標準及驗證流程簡介

沈柏村／金融聯合徵信中心資訊部

ISO 27001資訊安全標準

國際標準組織（International Organization for Standardization, ISO）於2005年10月15日公佈ISO 27001資訊安全標準（全名是ISO/IEC 27001：2005 - Information Security Management Systems Certification），是一種國際認可的資訊安全管理體系（Information Security Management Systems）驗證標準；ISO 27001資訊安全標準是從英國標準協會（British Standards Institution）提出之BS7799-2 標準（全名是BS7799 Information technology-Security techniques-Information security management systems-Requirements），延伸整合而成的國際資訊安全標準，其演進過程如下：

1995年：英國公佈BS7799 Part I

1998年：英國公佈BS7799 Part II

1999年：英國公佈新版BS7799 Part I、Part II

2000年：ISO通過成為ISO/IEC 17799 Part I

2002年：BS7799：2-2002，成為資訊安全管理系統驗證規範

2005年：ISO/IEC 17799：2005

2005年：BS7799：2-2005，2005年10月15日成為國際標準 ISO27001

ISO 27001資訊安全標準的規範要求，是一般性且可廣泛應用的，適用於任何型式的組織，並不限制組織規模大小和營業性質；因此，只要組織在經營策略上有必須取得ISO 27001資訊安全標準認證，皆可參考及依照ISO 27001資訊安全標準的規範，訂定欲取得認證的範圍，制定符合且適當的資訊安全制度文件及控制措施，運用「計劃、執行、檢查、行動」（Plan-Do-Check-Act, PDCA）持續改進模式運作，在整體資訊安全管理制度落實後，即可請驗證單位（例如：BSI、SGS、DNV）進行ISO 27001資訊安全標準驗證作業。

通過驗證之效益

通過ISO 27001資訊安全標準驗證，對於組織（企業）而言，至少可以產生以下三點效益：

（一）確保企業核心競爭力，保護營業機密，防止資訊之濫用；

（二）保護客戶財產，對提供作為使用或組合成為產品之顧客財產（包括智慧財產），可予以識別、查證、保護及安全防護；

（三）確保企業生產力，防止資訊之誤用與意外災害，確保業務永續運作。

ISO 27001資訊安全標準驗證流程簡介

組織於確認驗證範圍、並建立及實施ISO 27001資訊安全管理制度三個月後，即可申請取得ISO 27001資訊安全標準認證，申請驗證必須要通過驗證單位（例如：BSI）的稽核驗證，由驗證單位向發證單位（例如：UKAS）提出建議發證申請，最後由發證單位決定發證並頒發ISO 27001證書。

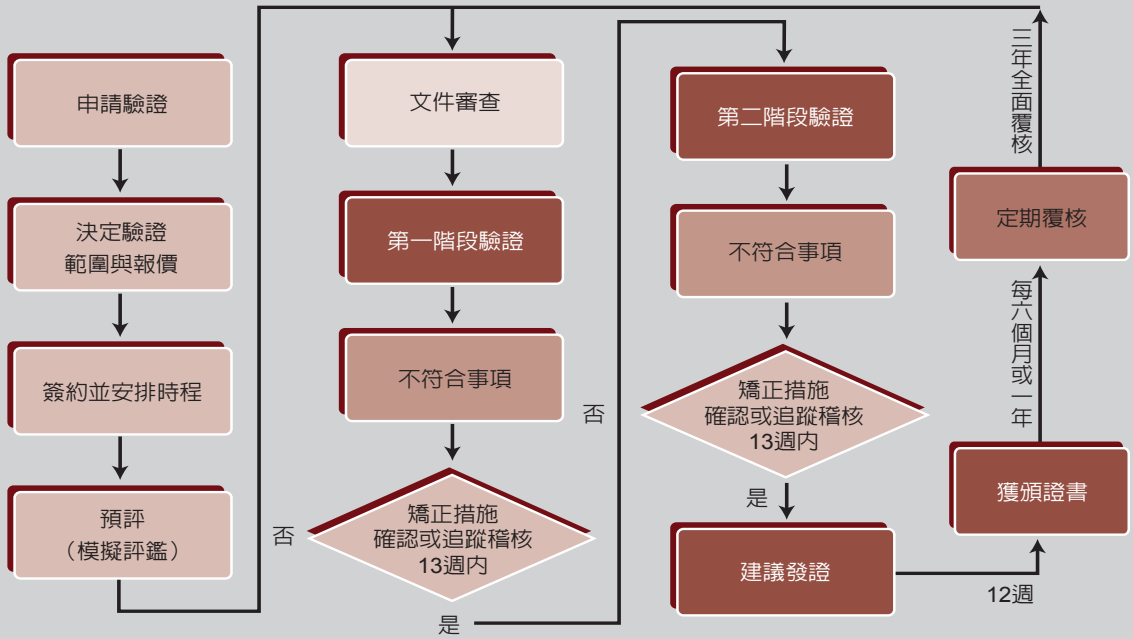
ISO 27001驗證流程，可以分成三個程序：

(一) 申請驗證前應注意事項

第一個程序為驗證前的準備，組織開始向驗證單位申請驗證前需注意下面條件要準備完成：

1. 系統文件完成且符合標準要求，並符合相關法規要求；
2. 全員認知公司之政策、目標、承諾；
3. 所有關鍵人員依訓練需求及計畫接受訓練；

ISO 27001 驗證流程圖



4. 管理系統程序執行中， 且有完整之管理循環及三個月執行紀錄；
5. 已執行過系統稽核， 並舉行獨立審查。

然後決定驗證範圍，並與驗證單位確認實際驗證工作人天數與價格，雙方簽約並安排時程進行驗證作業，一般為早期發現正式驗證可能會有的問題，並使正式驗證能順利進行，於正式驗證前會安排預評作業，就是模擬正式驗證的作業，在預評作業完成後，再進行下一階段。

(二) 文件審查作業

第二個程序為正式驗證作業之第一階段驗證（Initial Audit Step 1, IA1），即文件審查作業，主要驗證重點如下:

1. 驗證範圍與適用性聲明是否適當；
2. 確認管理系統的運作型態和文件化程度；
3. 管理系統是否依風險評估結果所建立；
4. 審查及驗證是否可信賴；

在此階段如果沒有「不符合事項」，則不需矯正措施確認或追蹤稽核。

(三) 實地審查作業

第三個程序為正式驗證作業之第二階段驗證(Initial Audit Step 2, IA2），即實地審查作業，主要驗證重點如下:

1. 文件化的管理系統是否符合相關標準；
2. 管理程序是否確實執行；
3. 管理系統方面是否能達到持續改善及法規遵循。

在此階段如果沒有「不符合事項」，則不需矯正措施確認或追蹤稽核，驗證單位會建議發證，並頒發ISO 27001證書。