論　述

行政院主計處電子處理資料中心導入「資訊安全管理制度」歷程

行政院主計處電子處理資料中心向來以資訊安全為重，為強化資訊安全制度，提供可信賴的資訊服務，及配合推動國家資通安全會報頒布之「國家資通訊安全發展方案（98年至101年）」，遂於98年4月導入「資訊安全管理制度（ISMS）」，以全中心之資訊處理活動為導入及驗證範圍，並於11月通過英國標準協會（BSi）驗證，99年元月取得ISO 27001：2005及我國CNS 27001：2006兩張證書。

◉ **黃慶裕**（行政院主計處電子處理資料中心管理師）

壹、前言

行政院於民國90年成立「國家資通安全會報」，以建立國家資訊與通訊安全機制為目的，將政府機關資訊安全責任等級分為A、B、C、D四個等級，並於98年1月發布「國家資通訊安全發展方案（98年至101年）」，制定「政府機關（構）資訊安全責任等級分級作業施行計畫」，明定A級機關應於民國98年，B級機關應於民國100年前通過「資訊安全管理制度（Information Security Management System）」（以下簡稱ISMS）第三方驗證。

行政院主計處係屬B級機關，爰於98年規劃導入ISMS，並以電子處理資料中心（以下簡稱本中心）為導入及驗證範圍。本中心設置審查輔導、分析設計、研究訓練、資料處理

等4個業務組及秘書、會計、人事、政風等4個行政室。負責推動政府機關業務電腦化、辦理政府機關資訊計畫審議及安全稽核服務、建置共通性軟體系統、辦理公務人員資訊訓練、推動中文交換共通平台機制、建立各類資訊網，發揮網路應用功能等業務。本次導入及驗證範圍涵蓋全中心（含行政單位）之資訊處理活動，規模範圍較其他政府機關更為完整。

貳、ISMS制度導入

本制度之導入係依循ISO 27001國際資訊安全管理系統標準之11大控制領域、39項控制目標、133項控制措施等規範指引，以風險管理為基礎，維護資訊資產的機密性、完整性及可用性為目標，並在建立、實作與運作、監視與審查、維持與改進之PDCA（Plan-Do-Check-Act）管理循環架構下，適切調整與反映制度的可用性與有效性，建構出符合本中心組織目標及業務特性之資安防護體系與管理制度。

導入期間每月由本中心主任親自召開工作會議，除管控專案進度與品質外，並與各組室協調相關事務及取得各階層主管全力支持，俾以順利推行ISMS各項活動。茲將建置過程中，重點工作項目作一概述。

一、組織現況分析

主要目的在診斷本中心資訊安全現況，藉由高階主管訪談，以瞭解全中心資訊安全運作概況，並透過主要業務訪談、文件審查及實體環境勘查的方式，瞭解本中心業務實際運作情形、現行的資訊安全架構及相關文件、表單等，並將調查結果與ISO 27001標準要求進行差異性分析，以評估中心作業與標準要求之落差，進而訂定相關措施。

二、制定資訊安全政策

「資訊安全政策」，係衡酌本中心業務需求所訂之政策，明訂資訊安全管理目標、對象、範疇及各階層人員應有的資訊安全責任。另為符合ISO 27001標準要求，並制定「資訊安全管理制度（ISMS）政策」，使同仁了解ISMS制度相關程序及規範，特將本制度的框架、程序、運作管理、監督審查、維持改善、文件化要求、管理階層責任及審查、稽核及改進等制定成策，作為參考指引。

三、成立資訊安全組織

為有效推動與辦理本中心資訊安全各項工作，特成立「資訊安全推動小組」。推動小組置召集人、副召集人及執行秘書各一人，並以中心主管為成員。負責擬訂本中心資訊安全之目標、策略及管理程序，促進資訊安全管理制度執行之有效性。其下設資訊安全分組，負責規劃及執行各項資訊安全作業；緊急處理分組，負

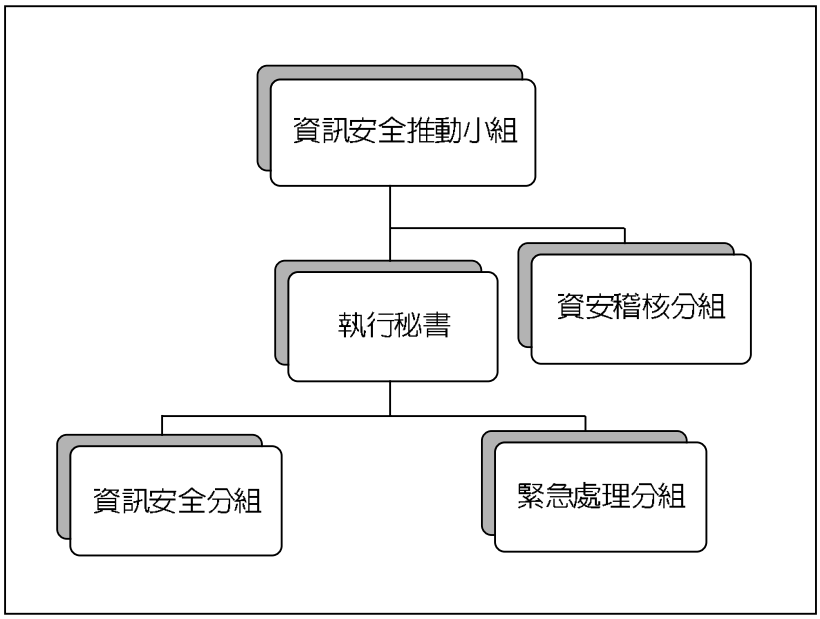
責重大資安事件之通報及改善處理之追踪；資安稽核分組，負責資訊安全之稽核、矯正預防處理之追踪。組織架構如圖1。

四、建立文件架構體系

制度的文件化，是ISMS的重要工作項目，也是ISO 27001的要求。文件架構體系（如圖2）是ISMS整個框架，包含政策、目標、管理程序、作業規範及表單紀錄等。所有文件內容先針對本中心業務特性設計範本，再由資安組織成員及相關業務同仁進行密集的討論，並整合現行相關資訊安全文件，持繼不斷的修正，以確認制度的符合性及可行性，甚至在文件發行後仍持續更新版本，足見本中心對文件規範之重視。

文件制修訂完成需經管理階層核准後發行，並立即由文件管制人員透過電子郵件通告同仁週知，並同步更新ISMS網站之文件版本，確保同仁取得最新資訊。對於文件產製、修訂、調閱、保存、廢止之生命週期及安全等級，皆有適當的程序管控，以確保其機密性、完整性及可用性。本中心將文件依其屬性分爲四階，第一階爲資訊安全最高指導原則；第二階爲各項作業之管理原則與程序；第三階爲各項流程之標準作業細節；第四階爲ISMS產出之資料及紀錄，共計81份。

圖1　資訊安全組織架構

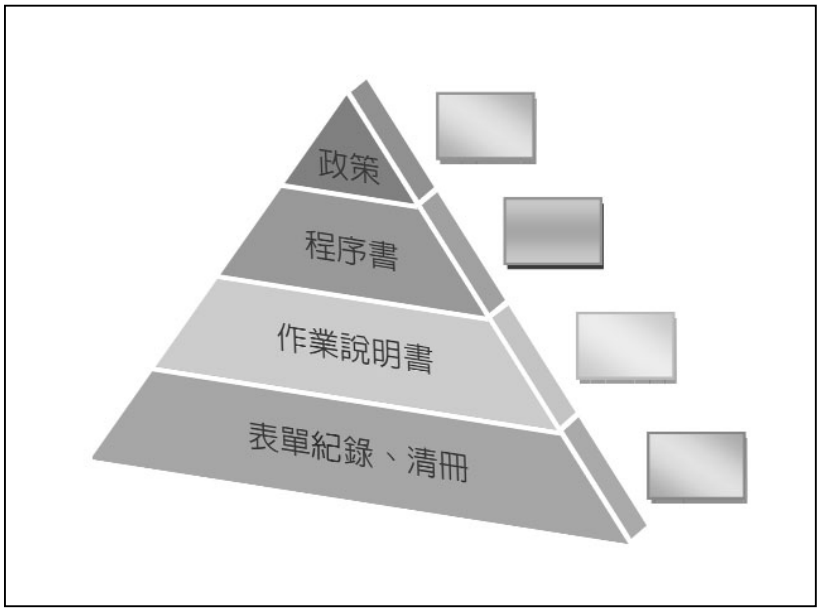


五、實施資產與風險管理

要達到百分之百的資訊安全是一種過高的期望，資訊安全管理的目標是透過控制措施，把資訊風險降低到可接受的程度內，因此，藉由資訊資產及風險管理，鑑別出重要資訊資產及所面臨的高風險，適時適切的投入人力與經費等資源，以降低風險帶來的衝擊。以下簡述風險管理過程：

（一）建立資訊資產與風險管理程序

圖2　四階文件架構



資訊資產管理程序是將資產的分類（本中心分爲人員、文件、軟體、通訊、硬體、資料及環境等7類）、編號、標示、異動管理及評價準則等建立程序，俾利同仁清查資產，建立清冊及評鑑資產價值；風險管理程序則是定義風險之建立全景、識別、估計、評估、處理、審查及接受等相關活動的準則與方法，使風險評鑑的結果可比較與可再產生，降低同仁對風險評鑑產生的偏差。

（二）風險評鑑

「風險是特定的威脅利用單一或一群資產之弱點，造成資產損失或損壞之潛在可能性」。執行風險評鑑，首要之務是資訊資產的盤點、群組化並造冊，次依各類資產的機密性（Confidentiality）、完整性（Integrity）及可用性（Availability）三個面向之定性或定量評估準則，鑑別出資產價值，再參酌工作流程、稽核結果、內外部資安全事件或相關標準（如ISO 13335 、27005）等面向，鑑別出本中心可能面臨的外來威脅與資產本身弱點，經由估計威脅等級（發生機率）與弱點等級（被威脅利用的程度），並考量現有控制措施，評估出每一資產之風險值（估算方式爲：資產價值x威脅等級x弱點等級）。

（三）風險處理

風險評鑑活動結束後，參酌資訊資產類別與數量統計及綜合風險值數量統計結果，並考量本中心人力、資源、組織環境及作業之安全需求，進行可接受風險值之訂定，經評估若無法接受、避免或轉移高於此值之風險，則制訂風險處理計畫，選擇適當之控制措施，以降低風險帶來的衝擊，並提陳管理階層審查，決定所需資源之分配。

六、發展營運持續管理

根據風險評鑑結果，由核心業務負責人進行業務流程或系統之營運衝擊分析（Business Impact Analysis，BIA），評估當各業務服務中斷時所造成之

衝擊程度，據以訂定最大可容忍中斷時間、目標回復時間及最低營運水準等指標，再彙總各核心業務BIA後，排定回復之優先順序及投入之資源。

完成BIA後，開始發展和實施營運持續計畫（Business Continuity Planning，BCP），制定營運持續策略之啓動時機、方式、備援措施、回復作業及場所等共同原則，且由各核心業務負責人依其業務特性規劃不同之營運持續子計畫，並進行測試演練以驗證計畫之可行性及有效性，期能於發生業務服務中斷時，在最短時間內將之回復至最低營運水準，降低事件所造成之損失。本中心每年至少演練一項營運持續子計畫，3年內演練完所有子計畫，自ISMS導入至今，已經完成防火牆、行政知識網（AKM）、內部核心網路、IBM大型主機及全國主計網(eBAS)應用系統等計畫之演練。

七、資訊安全內部稽核

內部稽核是對ISMS的成果初步檢驗，期望在第三方驗證前，透過內部自我稽核活動，找出不符規範之事項，即早矯正預防。本中心在9月由政風室主任率稽核分組同仁及協同一位外部稽核人員，進行對全中心與安全相關之業務抽樣檢查，稽核結果共發現6項次要缺失、7項觀察事項，均迅速改善完成。

八、管理審查會議

管理審查會議是管理階層對ISMS活動的審核與指導，本中心於10月召開會議，針對內部稽核及有效性量測結果、矯正及預防措施處理、利害關係團體（Stakeholder）對ISMS之建議、CCTV監控設備及程式原始碼檢測工具等資安產品之評估、風險評鑑的適切性、IBM大型主機之汰換等議題進行討論，並對ISMS有效性及控制措施量測方法之改進、風險評鑑與風險處理計畫之更新、對可能影響ISMS之內外部事件所作程序之修訂、資源需求等議題作出結論。在資安推動小組所有成員熱烈討論下，對本中心ISMS各項活動的支持與承諾更加明確。

九、教育訓練

教育訓練是推行ISMS的成功關鍵要素之一，惟有不斷的宣導與訓練，使所有同仁迅速熟悉規範與制度，方能理論與實務並進，在邊作邊學的模式下，有利掌控建置時程及品質。本中心依主官管、資安、資訊及一般使用者等不同角色，舉辦12場次講習，在密集的訓練下，有效宣達ISMS建置的理念與目標，提高同仁對制度的了解及配合度，對推行各項ISMS活動獲益良多。

參、ISMS符合性驗證

歷經7個月（4至10月）建置的辛苦歷程後，本中心委由英國標準協會（BSi）前來進行ISMS第三方驗證，由於以

全中心爲驗證範圍，受驗證人數較多，到場稽核共需8人天方能完成，稽核之嚴密可想而知，本中心同仁無不嚴陣以待。

ISMS驗證概分爲預評及正評兩階段，預評階段主要審閱本中心ISMS制度及運作情形，查核有無重大不符合事項，此項活動在10月21日完成，共發現1項次要缺失，13項觀察事項，並無主要缺失，故可進入第2階段正評審查。正評又分爲書面審查及實地審查兩步驟，書面審查在確認ISMS相關程序及紀錄的完整性及符合性，此項活動於11月5日完成，發現4項觀察事項；而在11月18、19日全面進行系統、作業程序實地抽樣檢查、人員訪談、資安事件通報與應變處理情形、營運持續管理稽核等，共發現3項次要缺失及8項觀察事項、1項改善機會。

針對稽核發現，皆由本中心稽核組長召開矯正預防檢討會議，確實尋求各缺失之根因，並分派人員進行矯正預防處理之追踪，迅速將改善方案及處理情形提交驗證公司審核，審核通過後於12月1日取得建議發證，99年元月3日取得證書，11日進行頒證儀式，自此，本中心之資訊安全邁入另一個里程碑。

圖3　ISO 27001：2005及CNS 27001：2006證書

肆、未來展望

在長官的支持、同仁的配合及顧問的輔導下，本制度如期如質達成目標，並獲致顯著效益，如資安政策及目標明確化、資安制度與紀錄文件化、資訊資產與風險管理化、作業流程與標準一致化，使本中心之資安控管更臻完備與落實。

資訊安全不是一種產品，而是一項流程，ISMS的落實亦非一次到位，展望未來，仍應秉持PDCA精神，持續不斷的落實與改善，調適出最符組織的執行方案，並將資訊安全活動融入每位同仁的日常業務及習慣中，形成組織的文化，確保本中心資通安全及業務持續營運。❖