國中小資通安全管理系統實施原則說明

劉志銘 顧問

Time:13:30~16:30

Date:2011年09月06日(五)

Out Line

- 背景說明
- 教育體系資通安全管理規範介紹
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    - 網路安全
    - 系統安全
    - 實體安全
    - 人員安全
    - 法令遵循
- 結語

- 背景說明

背景說明

- 行政院成立「國家資通安全會報」以協助建立政府機關及重要民間業者建立安全之資通訊及網路系統。
- 政府為了滿足各行政單位之需求，民國88年制定了「行政院及所屬各機關資訊安全管理規範」。

背景說明(續)

- 由於學術單位與政府機關的屬性不同， 雖然行政院已有頒布可依循之規範，但無法適用於教育體系，因此有必要研擬一套專屬的資通安全管理規範。
- 教育部於 96 年 6 月 11 日發函各機關學校公布推動「教育體系資通安全管理規範」及「國中小學資通安全管理系統實施原則」為教育體系 ISMS 建置參考。
- 可於校園資訊安全服務網http://cissnet.edu.tw/下載

教育體系資通安全管理規範設計原則

- 施行單位規模
- 施行單位之業務內容
- 施行單位可運用之資源
- 施行單位之執行能力
- 施行單位於資訊安全控管上的需求
- 成本效益原則

背景說明(續)

行政院國家資通安全會報資通安全責任分級

作業名稱 / 等級	防護縱深	ISMS推動作業(註一)	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者(註二))	專業證照(註四)	檢測機關網站安全弱點
A級	NSOC直接防護/SOC自建或委外、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少2次內稽	1. 每年至少(3、6、18、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定(註三)	維持至少2張資安專業證照	每年2次
B級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少1次內稽	1. 每年至少(3、6、16、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定(註三)	維持至少1張資安專業證照	每年1次
C級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2、6、12、3小時)	資安專業訓練	每年1次
D級	防火牆、防毒、郵件過濾裝置	推動ISMS觀念宣導	自我檢視	每年至少(1、4、8、2小時)	資安專業訓練	每年1次

背景說明(續)

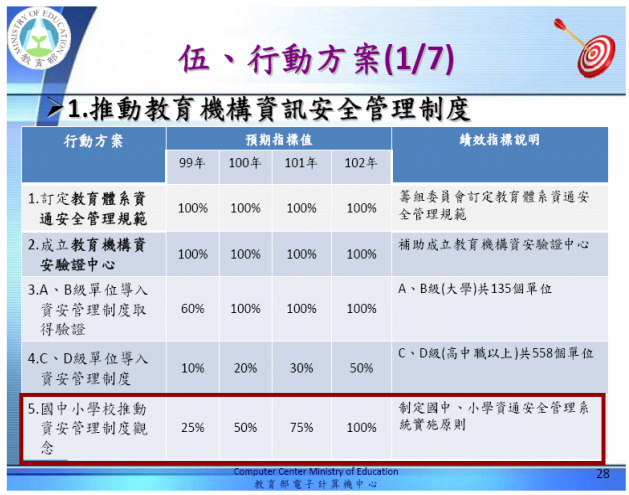
- 教育部針對資訊安全責任分級，規劃教育體系機關學校共分為A、B、C、D四級。

背景說明(續)

學研機關（構）資安等級區分表

類別	內容
A 級 重要核心	● 教育政策主管機關（教育部） ● 教學醫院（台大醫院、成大醫院）
B 級 核心	● 5 所入學考試常設機構 ● 102 所大學 ● 12 個 TANet 區網中心 ● 25 個縣/市網中心 ● 陽明大學附設醫院 【註：承辦入學考試業務機關學校比照 B 級單位】
C 級 重要	● 49 所技術學院及 15 所專科學校 ● 24 個部屬館所
D 級 一般	● 503 所高中職學校 ● 3,412 所國中小學

背景說明(續)



伍、行動方案(1/7)

➢1.推動教育機構資訊安全管理制度

行動方案	預期指標值				績效指標說明
	99年	100年	101年	102年	
1.訂定教育體系資通安全管理規範	100%	100%	100%	100%	籌組委員會訂定教育體系資通安全管理規範
2.成立教育機構資安驗證中心	100%	100%	100%	100%	補助成立教育機構資安驗證中心
3.A、B級單位導入資安管理制度取得驗證	60%	100%	100%	100%	A、B級(大學)共135個單位
4.C、D級單位導入資安管理制度	10%	20%	30%	50%	C、D級(高中職以上)共558個單位
5.國中小學校推動資安管理制度觀念	25%	50%	75%	100%	制定國中、小學資通安全管理系統實施原則

Computer Center Ministry of Education 教育部電子計算機中心 28

資料來源：

教育部民國99~102年教育體系資通安全發展策略及行動方案

- 教育體系資通安全管理規範介紹

教育體系資通安全管理規範發展背景

- 為協助教育體系各級單位，以有限的成本與時間，達到資訊安全之目標，95年度由成功大學賴溪松教授、NII 團隊共同草擬，並邀請產官學研界專家共同檢視與修正。
  - 參考 CNS_ISO 27001、CNS_ISO 27002與我國政府規範等法令標準，訂定出適用於教育體系之資訊安全管理規範。
  - 使各級學校與教育網路中心能以最低成本與時間，建構嚴謹且合適之資訊安全管理系統。
  - 配合教育部規劃之「**教育體系資訊安全管理驗證機制**」，建構國內專屬之第三方驗證標準。

規範設計之準則

- 將CNS_ISO 27001中不適用各連線單位之項目予以調整；並將語義不清或不適用之文字進行修改。
- 參酌CNS_ISO 27002控制措施之最佳實務說明進行實作建議。
- 參酌行政院及所屬各機關資訊安全管理規範為稽核項目範本，並刪除其中不適用之項目。

適用範圍

- 本標準適用於教育部電算中心、部屬館所、縣市網中心、大專院校以及高中職資訊管理單位等資訊業務相關單位（或其他管理單位認為應加入ISMS規範範圍之部門）。
- 依單位層級區分二群
- 第一群：教育部電算中心、部屬館所、縣市網中心、公私立大專院校（計網中心及校務行政）等。
- 第二群：公私立高中職學校為主要。
- 依業務分為「學術網路系統」與「行政資訊系統」。

ISO 27001與教育體系資通安全管理規範

規範名稱	章節數	控制目標	控制項
ISO 27001:2005	11	39	133項

規範名稱	章節數	控制目標	控制項
教育體系資通安全管理規範	11	36	適用大專院校 100項 適用高中職以下 69項

Information Security Management System (ISMS)

規範內容 – 整體架構

- 資訊安全管理制度建置步驟
  - ISMS之建立(Plan)
  - ISMS之實施與操作(Do)
  - ISMS之監控及審查(Check)
  - ISMS之維持及改進(Act)
- 資訊安全管理系統 (ISMS)建置需求
  - 文件要求
  - 管理階層責任
  - 管理階層審查

規範內容 – 整體架構(續)

- 控制項 - 共11個領域(1/2)
  - 資訊安全政策訂定與評估 (A.5)
  - 資訊安全組織 (A.6)
  - 資訊資產分類與管制 (A.7)
  - 人員安全管理與教育訓練 (A.8)
  - 實體與環境安全 (A.9)
  - 通訊與作業安全管理 (A.10)

規範內容 – 整體架構(續)

- 控制項 - 共11個領域(2/2)
  - 存取控制安全 (A.11)
  - 系統開發與維護之安全 (A.12)
  - 資訊安全事件之反應及處理(A.13)
  - 業務永續運作管理 (A.14)
  - 相關法規與施行單位政策之符合性 (A.15)

資訊安全管理制度建置步驟

- ISMS之建立
  - 依據該單位之類型、規模、資源、業務性質等特性，定義 ISMS 範圍；考慮相關法律、法規，以及合約之要求，於適度評估風險及應對措施後，訂出經由管理階層核准之ISMS政策，並擬定一份適用性聲明書文件。

- ISMS之實施與操作
  - 施行單位應確實實施控制措施，以符合控管的目標，並執行訓練與認知計畫，確保偵測安全事件的能力，以及迅速回應和應對處理的時效。

資訊安全管理制度建置步驟（續）

- ISMS之監控及審查
  - 施行單位應針對ISMS進行監控程序與其他控制措施，即時鑑別資安事件的發生、處理順序與解決方法；定期審查ISMS有效性（建議一學年至少一次），並將相關有顯著影響之活動與事件記錄下來。

- ISMS之維持及改進
  - 施行單位應定期實行改進活動，採取適當的矯正與預防措施，並得到管理階層之同意，並確保各項措施達到預期目標。

資訊安全管理制度建置步驟（續）

- 文件要求
  - 關於ISMS文件化（電子檔案或紙本），必須包含安全政策、安全目標、ISMS範圍、適用性聲明、資安事件紀錄，以及其他有助於提升ISMS成效之文件；上述之文件需接受保護與管制，並定期的審查及更新，確保文件之最新版本；任何過期文件需保留或銷毀，應予以適當的鑑別。

- 管理階層責任
  - 管理階層最為重要的是給予承諾及實際的支持，並適度的提供資源以助ISMS程序進行，必要時審查 ISMS 的控制措施與有效性；另外，確保於ISMS範圍內之員工具備足夠之能力及認知，並定期進行教育訓練。

資訊安全管理制度建置步驟（續）

- 管理階層審查
  - 管理階層應在規劃期間內，審查該單位的ISMS與適用範圍，確保其持續的適用性、適切性及有效性；其中應審查包含變更需求與改進時機，並將其結果確實文件化。

- ISMS之改進
  - ISMS的改進是持續的，必須藉由各資安事件與審查結果，做出適度的反應與改進，持續系統之有效性；另外，對應的矯正措施以及防範未然的預防措施，亦須予以制定並文件化。

教育部推動現況

- 推動機制
  - 成立並營運教育體系資安推動組織。
  - 建立教育體系「第三者驗證」機制，大多數區、縣網中心皆已通過教育體系資通安全管理規範之驗證。
  - 已成立教育體系資安通報處理程序與通報應變網站。

教育部推動現況(續)

- ISMS推動
  - TANet 區/縣市網中心ISMS建置，已得教育體系第三者驗證。
  - 公私立大學（B級）導入資安管理制度，原則由各校自行推動導入。
  - 依教育體系資通安全管理規範進行ISMS導入及驗證，並輔導C、D級單位。

教育部推動現況(續)

- 教育訓練
  - 規劃辦理教育體系人員資安證照訓練課程。
  - 針對教育體系主管、資訊技術人員的認知與教育訓練。
  - 國中小學生的資安認知推廣活動。

- 國中、小學資通安全管理系統實施原則

- 國中、小學資通安全管理系統實施原則
  - 文件目標

文件目標

- 提供國中、小學資通安全管理實施原則指引。

- 國中、小學資通安全管理系統實施原則
  - 適用範圍

適用範圍

- 國中、小學資訊系統及其相關處理設施之管理。

- 國中、小學資通安全管理系統實施原則
  - 實施原則
    - 網路安全

實施原則 – 網路安全

- 網路控制措施
  - 學校與外界連線，宜僅經由縣網中心，以符合一致性與單一性之安全控管要求。
  - 學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）宜區隔於網路之外；當有必要透過網路傳輸資料時，應有安全的控管機制如（加密、VPN、SSL 等）。
  - 禁止以電話線連結至電腦主機或網路設備。

實施原則 – 網路安全(續)

- 網路安全管理服務委外廠商合約之安全要求
  - 委外開發或維護廠商必須簽訂安全保密切結書。

Out Line

- 國中、小學資通安全管理系統實施原則
  - 實施原則
    - 系統安全

實施原則- 系統安全

- 集中式管理
  - 學校的行政系統主機（例如財務、人事、公文系統等）電腦，宜由各個 縣（市）教育網路中心或教育局等單位統籌管理。
  - 學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由各個縣（市）教育網路中心或教育局等單位**統籌管理**。

實施原則- 系統安全(續)

- 對抗惡意軟體、隱密通道及特洛依木馬程式
  - 學校內的個人電腦應：
    - 安裝防毒軟體，並定期更新病毒碼。
    - 定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞。
- 不得使用非法軟體。
- 新系統啟用前，應經過掃毒與更新系統密碼，以防範可能隱藏的病毒或後門程式。
- 學校對外提供之網頁服務應防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查。

實施原則- 系統安全(續)

- 資料備份
  - 學校重要系統（例如系統檔案、應用系統、資料庫等）應定期進行資料備份；建議週期為每週進行一次。

實施原則- 系統安全(續)

- 操作員日誌
  - 敏感度高、或包含特殊資訊的電腦系統應進行檢查、維護、更新等活動，並將這些活動填寫日誌予以記錄，以供查考。
  - 日誌內容應包含以下各項：
    - 系統例行檢查、維護、更新活動的起始時間。
    - 系統錯誤內容和採取的改正措施。
    - 操作人員簽名。

實施原則- 系統安全(續)

- 資訊存取限制
  - 學校宜針對個人隱私資料相關資訊之使用、傳輸與管理，訂定安全的管理規定。
  - 學校內之多人共用的電腦應以特定功能為目的，並設定安全管控機制（例如限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。

實施原則- 系統安全(續)

- 使用者註冊
  - 學校應制定電腦系統使用者註冊及註銷程序，並透過該註冊及註銷程序來管理使用者存取權限，該作業應包括以下內容：
    - 每位使用者皆有各自的識別碼（ID）。
    - 保存一份包含所有識別碼註冊的紀錄。
    - 使用者調職或離職(留職停薪)後，應調整或移除其存取權限。
    - 定期（建議每學期1 次）檢查使用者之帳號及權限，若有未經授權的帳號產生或不適當之權限設定，應立即調整或取消帳號權限。帳號檢查活動應留存紀錄。
    - 若上述帳號異常狀況研判為駭客入侵應依通報程序處理（參照本文件2.10 段落）。

實施原則- 系統安全(續)

- 特權管理
  - 學校的電腦與網路系統具有最高權限之帳號應建立使用人員清單。
  - 應開啟電腦系統稽核紀錄功能，留存最高權限的使用活動電腦稽核紀錄(log)。 。

實施原則- 系統安全(續)

- 密碼之使用
  - 管制使用者第一次登入系統時，必須立即更改預設密碼。
  - 資訊系統與服務應避免多人使用共同帳號及密碼。
  - 學校應制定及發佈密碼（Password）使用規則[參考優質密碼設定原則與使用原則，附件A-3]，內容應包含以下各項：
    - 使用者應該對其個人所持有密碼盡保密責任
    - 要求使用者的密碼設定，避免使用易於猜測之數字或文字，例如生日、名字、鍵盤上聯繫的字母與數字（如12345678 或 asdfghjk），以及過多的重複字元等。或建議密碼應該包含英文字大小寫、數字、特殊符號等四種設定中的三種。

實施原則- 系統安全(續)

實施原則- 系統安全(續)

- 原始程式庫之存取控制
  - 應用程式之原始碼存取行為應加以控管。

實施原則- 系統安全(續)

- 通報安全事件與處理：
  - 資訊安全事件包括：任何來自網路的駭客攻擊、病毒感染、資料或網頁遭竄改、以及通訊中斷等。
  - 學校應建立資訊安全事件通報程序，其程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。
  - 當遭遇重大或學校內部無法處理之資通安全事件，應通報其所屬縣市網路中心。
  - 所訂出之資訊安全事件通報程序應公佈於校園內使用電腦與網路之場所，提供使用者瞭解。原始程式庫之存取控制。

- 實施原則
  - 實體安全

實施原則- 實體安全

- 設備安置及保護
  - 學校重要的資訊設備應置於安全地點（如主機機房）並設有空調設施。
  - 學校設置大量資訊設備之地點，如：主機機房、電腦教室區域，應設置滅火設備，並避免堆積易燃物或在區域內飲食。
  - 學校設置大量資訊設備之地點：如主機機房、電腦教室區域內的電源線插頭應有接地的連結或有避雷針等裝置，避免如雷擊事件造成損害情況。
  - 學校設置大量資訊設備之地點，如：主機機房、電腦教室區域，應於入出口處加裝門鎖或其他安全措施。

實施原則- 實體安全(續)

- 電源供應
  - 學校重要的資訊設備應有適當的電力支援設施，例如UPS、電源保護措施，以免斷電或超過負載而造成損失。
- 纜線安全
  - 學校主機機房、電腦教室區域內應使用符合安全要求之纜線並綑綁整齊，必要時以管線包覆。
- 設備與儲存媒體之安全報廢或再使用
  - 所有包括儲存媒體的設備，在報廢或再使用前應先確保已將任何敏感資料和授權軟體刪除或覆寫。設備安置及保護。

實施原則- 實體安全(續)

- 設備維護
  - 設備委託廠商維護時應與廠商建立維護合約，並將安全條款納於合約中。
  - 廠商受託維護設備或執行任務而接觸學校重要或敏感資訊時，須先請其簽訂全保密切結書。
- 財產攜出
  - 財產之攜出應依教育部或學校既有之相關規定處理。包含：
    - 未經授權不得將學校的資訊設備、資訊/資料或軟體攜出校園以外。
    - 財產攜出應予登記並追蹤歸還情形。

實施原則- 實體安全(續)

- 桌面淨空與螢幕淨空政策
  - 學校教職員工於工作結束時，應將其所經辦或使用具有機密或敏感特性的資料（例如公文、學籍資料等）及資料的儲存媒體（如USB 隨身碟、磁碟片、光碟等），妥善存放。
  - 學校提供教職員工或學生使用的電腦應採取適當的安全措施，如鎖匙、登入密碼驗證及設定螢幕保護程式。

- 人員安全

實施原則- 人員安全

- 將安全列入工作執掌中
  - 應將資訊安全要求納入教職員手冊說明中，以強化工作上之資訊安全意識。
- 資訊安全教育與訓練
  - 學校資訊系統管理人員應定期參與資訊安全專業訓練，確保有足夠能力執行任務。
  - 學校應安排全體教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。

– 實施原則

  • 法令遵循

實施原則- 法令遵循

- 法規之遵守：
  - 學校全體教職員應對以下法令有基礎認知，以免誤觸法令。
- 智慧財產權：
  - 應實作適當程序，以確保所使用的資料可能涉及智慧財產權與所使用的專屬軟體產品，可遵循法律、法規及契約的要求。
  - 個人資訊的資料保護及隱私：應如同相關法令，法規及若適用的契約條文所要求的，確保資料保護與隱私。

簡報完畢
敬請指教