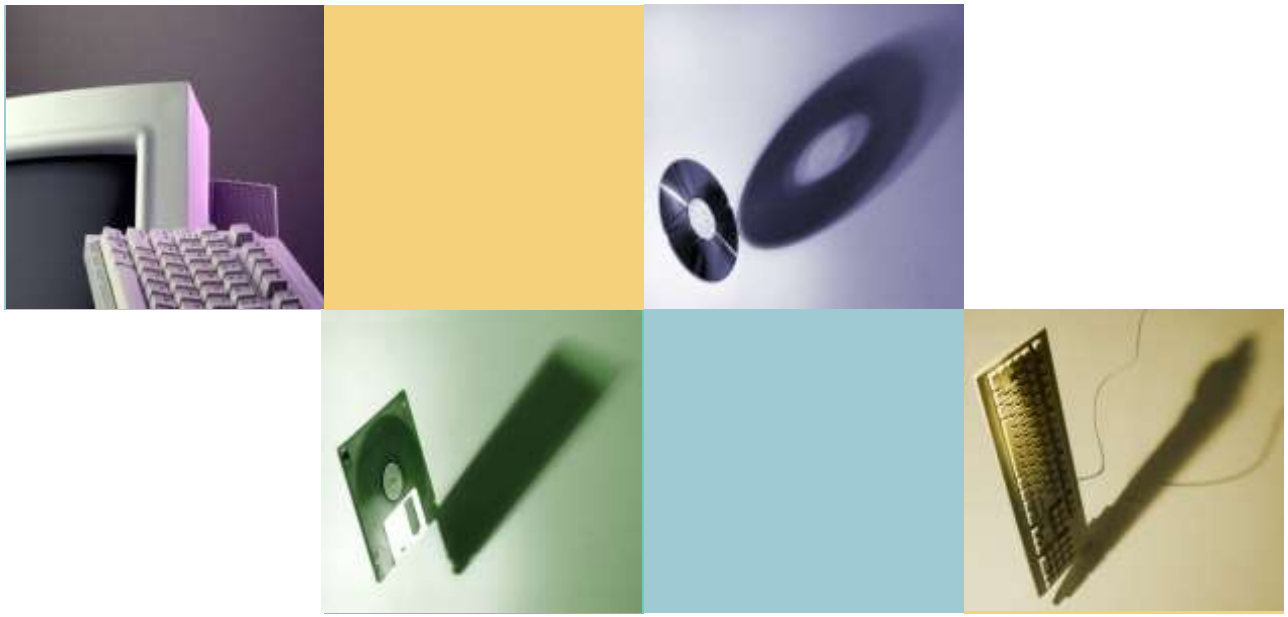
教育體系資通安全管理規範簡介



國立宜蘭大學圖書資訊館

網路組　曾國旭

Wednesday, Mar 12 2014

- 資訊安全之概念說明
- 教育體系資通安全管理要求
- 附錄A 控制目標與控制項說明



重要詞彙說明

- 何謂資產？
  - 對組織有價值的任何事物。
- 何謂資訊？
  - 資訊是一種資產，對於組織營運不可或缺。
  - 資訊存在形式有許多種，可以列印或書寫於紙本，可以電子形式儲存，或交談口述等，無論資訊形式為何，以何種方式分享或儲存，均應加以適當保護。



資產特色

- 不只侷限於電腦科技的產物
- 對組織有用的資訊都屬於資訊資產
- 無所不在

資料庫

資訊安全管理制度

- 資訊安全管理制度(Information Security Management System, ISMS)
  - 整體管理系統的一部份，以營運風險方案為基礎，用以建立、實施、操作、監督、審查、維持及改進資訊安全。



資訊安全管理重點


資安
處理技術
資安
控管流程
人員資安知
識與能力
Manageable Secure Infrastructure
DATA

資訊安全三大原則

- 機密性(Confidentiality)：
  確保只有經授權的人才可以取得資訊，避免資訊洩露。
- 完整性(Integrity)：
  確保資訊不受未經授權的竄改與資訊處理方法的正確性。
- 可用性(Availability)：
  確保經授權的使用者，在需要時可以取得資訊，並使用相關資產。

ISMS目的在於保護資訊資產的機密性、可用性與完整性。



學校單位的資訊安全需求

- 為什麼學校單位需要資訊安全
  - 學生學籍資料
  - 成績資訊
  - 強化資訊網路防護能力
  - 建立機制、程序與PDCA流程管理
- 學校單位所擁有的資訊特色
  - 非機密性
  - 敏感性且涉及隱私及個人資料保護法相關規定



- 資訊安全之概念說明
- 教育體系資通安全管理要求
- 附錄A 控制目標與控制項說明



教育體系資通安全管理要求

- 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。



規範設計之準則

- 將ISO 27001:2005(E)中不適用各連線單位之項目予以刪除或合併（刪除項目請參閱刪除之規範與控制項）；並將語義不清或不適用之文字進行修改。
- 參考行政院及所屬各機關資訊安全管理規範為稽核項目之範本，並刪除其中不適用之項目，並調整其中的內容。



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。
- 依業務分為「學術網路系統」與「行政資訊系統」。



規範內容－ 整體架構

- 資訊安全管理制度建置步驟
  - ISMS之建立、ISMS之實施與操作、ISMS之監控及審查、ISMS之維持及改進
- 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
- 控制項（共11個領域）
  - 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)
  - 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。



資訊安全管理系統建置需求

- 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。

資訊安全管理系統建置需求（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。



- 資訊安全之概念說明
- 教育體系資通安全管理要求
- 附錄A 控制目標與控制項說明



A.5 資訊安全政策訂定與評估

- 資訊安全政策訂定與評估(A.5)
  - 資訊安全政策乃是管理階層對施行單位資訊安全的指示以及支持的表徵，藉此引導相關人員認知、遵循規範條則，並具備完善之資安觀念。
- 資訊安全政策訂定與評估(A.5.1)
  - 資訊安全政策制定(A.5.1.1)
  - 資訊安全政策評估(A.5.1.2)



A.6 資訊安全組織

- 資訊安全組織(A.6)
  - 施行單位之應指定適當權責之高層主管人員，負責推動資訊安全組織，召開資安會報、訂定權責分屬、主導評估建置等相關活動，除了解各項需求外，籌備必要資源，確保資安措施正常運作，建立起一完善、安全之環境，降低組織資安威脅的機率。
- 資訊安全組織推動與權責(A.6.1)
  - 資訊安全組織推動以及權責之分配(A.6.1.1)
  - 資訊設施使用之授權(A.6.1.2)
  - 保密條款之簽訂(A.6.1.3)
  - 跨單位合作及協調(A.6.1.4)
  - 資訊安全諮詢與顧問(A.6.1.5)
  - 資訊安全政策的獨立檢視(A.6.1.6)
- 施行單位外部人員存取安全管理(A.6.2)
  - 施行單位外部人員存取之安全掌控(A.6.2.1)

A.7 資訊資產分類與管制

- 資訊資產分類與管制(A.7)
  - 為確保施行單位資產獲得適切的保護，明確的資產分類與保護層級，將有助於資產保管的執行效率，降低受危害的可能。
- 資訊資產分類與責任分屬(A.7.1)
  - 資訊資產目錄建立(A.7.1.1)
  - 資訊資產之安全等級分類(A.7.1.2)



A.8 人員安全管理與教育訓練

- 人員安全管理與教育訓練(A.8)
  - 施行單位所屬相關人員需針對其擔負的資安責任，進行管理與教育訓練，確保其在職位上能執行各項相關資安措施，降低可能的資安風險。
- 聘任前(A.8.1)
  - 所屬角色與責任(A.8.1.1)
- 聘用中(A.8.2)
  - 資訊安全教育訓練(A.8.2.1)
  - 違反規定之處理(A.8.2.2)
- 結束聘任或改變職務(A.8.3)
  - 結束聘用(A.8.3.1)
  - 資產繳回(A.8.3.2)
  - 存取權移除(A.8.3.3)

A.9 實體與環境安全(1/2)

- 實體與環境安全(A.9)
  - 為保護資訊處理設施以及所在位置的安全，除環境的管制保護措施外，軟硬體的防護措施也需徹底實行，有效降低資安事件發生的機率。
- 區域之安全(A.9.1)
  - 實體環境安全(A.9.1.1)
  - 人員進出控制(A.9.1.2)
  - 資訊處理設施安全(A.9.1.3)



A.9 實體與環境安全(2/2)

- 設備之安全(A.9.2)
  - 設備安置地點之保護措施(A.9.2.1)
  - 電源供應(A.9.2.2)
  - 電纜線安全防護(A.9.2.3)
  - 設備之維護(A.9.2.4)
  - 設備報廢與再使用(9.2.5)
  - 預防未經授權之移動(A.9.2.6)



A.10 通訊與作業安全管理(1/5)

- 通訊與作業安全管理(A.10)
  - 為確保正確以及安全的操作資訊處理設施，降低各種可能的風險與損害，維護資訊處理與通訊服務之完整性及可用性，應設立通訊與作業安全之管理措施。
- 作業程序與責任(A.10.1)
  - 作業程序文件化(A.10.1.1)
  - 作業變更之管理(A.10.1.2)
  - 資訊安全責任之分散(A.10.1.3)
  - 系統發展、測試及實務作業之分散(A.10.1.4)

A.10 通訊與作業安全管理(2/5)

- 資訊作業委外服務之安全管理(A.10.2)
  - 資訊作業服務之管控(A.10.2.1)
  - 服務之監控與審查(A.10.2.2)
  - 廠商服務異動(A.10.2.3)
- 系統規劃與驗收(A.10.3)
  - 系統作業容量之規劃(A.10.3.1)
  - 新系統上線作業之安全評估(A.10.3.2)



A.10 通訊與作業安全管理(3/5)

- 電腦病毒、惡意軟體(A.10.4)
  - 電腦病毒及惡意軟體之控制(A.10.4.1)
- 備份作業之管控(A.10.5)
  - 資料備份(A.10.5.1)
- 網路安全管理(A.10.6)—適用於學術網路系統
  - 網路安全規劃與管理(A.10.6.1)
  - 網路服務之安全控制(A.10.6.2)



A.10 通訊與作業安全管理(4/5)

- 儲存媒體的處理與安全(A.10.7)
  - 電腦媒體之安全管理(A.10.7.1)
  - 電腦媒體處理之安全(A.10.7.2)
  - 資料檔案之保護(A.10.7.3)
  - 系統文件之安全(A.10.7.4)
- 資訊與軟體交換(A.10.8)
  - 資訊與軟體交換安全政策與協定(A.10.8.1)
  - 電子郵件安全管理(A.10.8.2)
  - 電子辦公系統安全(A.10.8.3)
  - 對外公告資訊之管理(A.10.8.4)

A.10 通訊與作業安全管理(5/5)

- 系統存取及應用之監督(A.10.9)
  - 事件記錄(A.10.9.1)
  - 系統使用之監控(A.10.9.2)
  - 記錄的保護(A.10.9.3)
  - 系統管理者與作業人員之記錄(A.10.9.4)
  - 系統錯誤事項之紀錄(A.10.9.5)
  - 系統時鐘應予同步，確保紀錄的正確(A.10.9.6)



A.11 存取控制安全(1/4)

- 存取控制安全(A.11)
  - 施行單位應鑑別(Identify，該資料機密等級與存取動作)與文件化相關之存取行為，建立存取控制政策的內容及範圍。
- 使用者存取控制(A.11.1)
  - 使用者註冊管理(A.11.1.1)
  - 系統存取特別權限管理(A.11.1.2)
  - 一般通行碼之控管(A.11.1.3)
  - 系統存取權限之評估(A.11.1.4)



A.11 存取控制安全(2/3)

- 使用者責任(A.11.2)
  - 辦公桌面之安全管理(A.11.2.1)
- 網路存取控制措施(A.11.3)
  - 網路服務之限制(A.11.3.1)
  - 遠端使用者身份鑑別(A.11.3.2)
  - 診斷埠(Diagnostic Ports)存取控制(A.11.3.3)
  - 網路分隔控制(A.11.3.4)—較適用於第一~二群
  - 網路連線控制(A.11.3.5)—較適用於第一~二群
  - 網路路由控制(A.11.3.6)—較適用於第一~二群



A.11 存取控制安全(3/3)

- 作業系統存取控制(A.11.4)
  - 系統登入程序(A.11.4.1)
  - 使用者通行碼管理(A.11.4.2)
  - 系統公用程式管理(A.11.4.3)
  - 連線作業時間之控制(A.11.4.4)
- 應用系統的存取控制(A.11.5)—較適用於行政資訊系統
  - 資訊存取限制(A.11.5.1)
  - 機密及敏感性系統之獨立作業(A.11.5.2)
- 行動式電腦作業與遠距工作管理(A.11.6)
  - 行動式電腦作業控制(A.11.6.1)
  - 遠距工作管理(A.11.6.2)—較較適用於第一~二群



A.12 系統開發與維護之安全(1/3)

- 系統開發與維護之安全(A.12)
  - 系統開發與維護應納入資安方面的考量，針對可能的危機與錯誤採取相對的措施，並符合施行單位的要求。
- 系統安全要求(A.12.1)─較適用於行政資訊系統
  - 安全需求分析及規格訂定(A.12.1.1)
- 應用系統安全(A.12.2)─較適用於行政資訊系統
  - 資料輸入之驗證(A.12.2.1)
  - 系統內部作業處理之驗證(A.12.2.2)
  - 訊息真確性之鑑別(A.12.2.3)─較適用於第一~二群
  - 資料輸出控管(A.12.2.4)

A.12 系統開發與維護之安全(2/3)

- 加密控制措施(A.12.3)
  - 資料加密(A.12.3.1)—較適用於第一~二群
  - 憑證機構之技術安全(A.12.3.2)—較適用於第一~二群
- 系統檔案安全(A.12.4)
  - 作業軟體控制(A.12.4.1)
  - 系統測試資料之保護(A.12.4.2)—較適用於第一~二群
  - 原始程式庫(Source Library)資源之存取控制(A.12.4.3)—較適用於第一~二群

A.12 系統開發與維護之安全(3/3)

- 開發與支援作業的控制(A.12.5)
  - 變更作業之控制程序(A.12.5.1)—較適用於第一~二群
  - 作業系統變更之技術評估(A.12.5.2)—較適用於第一~二群
  - 套裝軟體變更限制(A.12.5.3)
  - 資訊洩漏控制(A.12.5.4)—較適用於第一~二群
  - 軟體委外開發(A.12.5.5)—較適用於第一~二群
- 系統弱點管理(A.12.6)—較適用於第一~二群
  - 系統弱點控制(A.12.6.1)

A.13 資訊安全事件之反應及處理

- 資訊安全事件之反應及處理(A.13)
  - 針對安全事件的發生，應即刻進行反應，並採取適當的處理措施，降低損害的擴大，並作為改進的參考。
- 資訊安全事件與弱點之通報(A.13.1)
  - 資訊安全事件與弱點通報(A.13.1.1)
- 資訊安全事件之管理(A.13.2)
  - 資安事件處理責任與程序建立(A.13.2.1)
  - 從資安事件中學習(A.13.2.2)
  - 資安事件證據之收集(A.13.2.3)

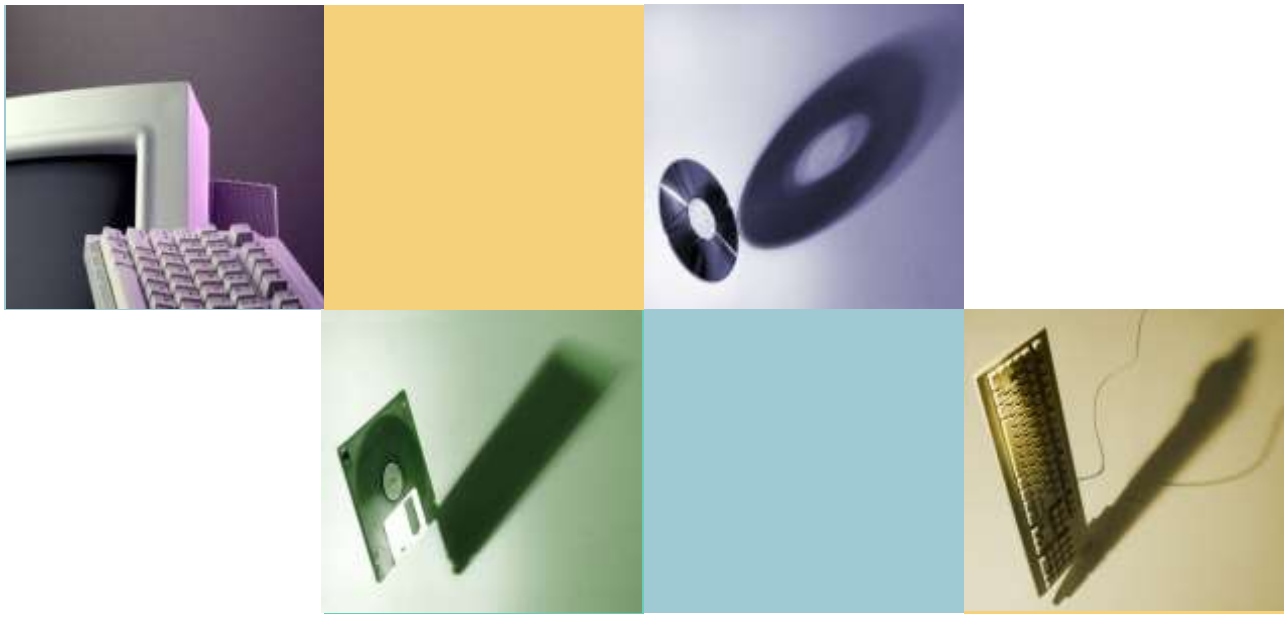
A.14 業務永續運作管理

- 業務永續運作管理(A.14)—較適用於第一~二群
  - 為維持施行單位業務的永續運作，應進行相關的規劃及檢測，達到業務進行不中斷之目的。
- 永續運作管理之規劃(A.14.1)
  - 業務永續運作之規劃程序(A.14.1.1)
  - 業務永續運作計畫之測試及更新(A.14.1.2)

A.15 相關法規與施行單位政策之符合性

- 相關法規與施行單位政策之符合性(A.15)
  - 確保施行單位之執行業務及資訊處理設施，能符合相關法規以及資安政策。
- 法規之遵守(A.15.1)
  - 適用法規之鑑別(A.15.1.1)
  - 適用法規之遵循(A.15.1.2)
- 安全政策與技術符合性之檢驗(A.15.2)
  - 確保遵守安全政策與規範(A.15.2.1)
  - 資訊系統符合性審查(A.15.2.2)
- 系統稽核的考量(A.15.3)
  - 系統稽核控制(A.15.3.1)
  - 系統稽核工具之保護(A.15.3.2)

Q and A



THANKS !