以風險評估方式建置資安架構

成大計網中心
楊峻榮
yang@mail.ncku.edu.tw
2004/08/23

大綱

- 資安概念
- ISMS資安管理系統
- 風險評估
- 校園資訊安全機制

資訊安全目標

- 機密性(Confidentiality)
  確保資訊的存取或作業是經許可被授權。
- 完整性(Integrity)
  確保資訊和流程方法的準確和完善。
- 可用性(Availability)
  確保被授權的人需要時可以獲取資訊和相關的資產。

各組織依業務型態及其系統別，對於CIA之比重與要求有所不同，因此風險評估的著眼點也不同。

資訊安全概念

- 資訊安全，人人有責。
- 看不見問題，並不代表沒有問題。
- 資訊安全是一個持續性的工作，而其防護措施也沒有極限。
- 資訊安全領域不只是網路安全而已（駭客，病毒）。
- 安全設備非萬能，也沒有100%安全的系統。
- 便利性和安全性總是相衝突的，實施的控制措施應該是在合理的平衡點(成本與效益)。
- 了解真正問題點(弱點)，並施以正確的控制措施。
- 資安措施的實施，在於降低至可接受之風險程度。

企業及學術機構資安之差異性

	企　　業	學術機構
營運方針	以商業行為為導向	以服務為導向
管理模式	中央控管	支援
管理機制	著重組織管理機制	著重設備機制
組織人員定位	明確	混淆(學生)

校園資安弱點

- 系統漏洞
- 人為疏失
- 服務需要或過於注重便利性
- 無危機意識（該防未防）
- 無所謂（發生問題不覺得有影響）
- 無專人負責之系統
- 實體環境不良
- 軟體之安全機制不足
- 角色定義不明

校園資安威脅

- 病毒
- 入侵及跳板
- 阻絕服務(DoS, DDoS)
- 垃圾郵件
- 資料或實體竊取
- 資料竄改
- 操作不當
- 系統失效(硬體系統、作業系統、應用系統、網路系統)
- 溫濕度因素或電源供應不良
- 火、水災或地震等天然災害

資訊安全機制(系統)之建立

- ISMS導入 ： Top-Down，先由政策定義、定義資產、風險評估、選用控制措施……。著重於整個組織制度及管理
- 由控制措施著手：Bottom-Up，先由各別系統之控制措施著手。著重於技術層面
- 雙管齊下:考慮到現階段之環境與急迫性之考量，在管理及技術層面以組織文化及環境為背景，建立起組織之資訊安全系統

資訊安全機制考慮之因素

- 管理制度，IT技術,與各業務考量的結合
- 要有一套系統性的管理及控制的制度(或方法)
- 各子系統或控制措施必須整合(不互相抵觸或干擾)

ISMS PDCA Process Model

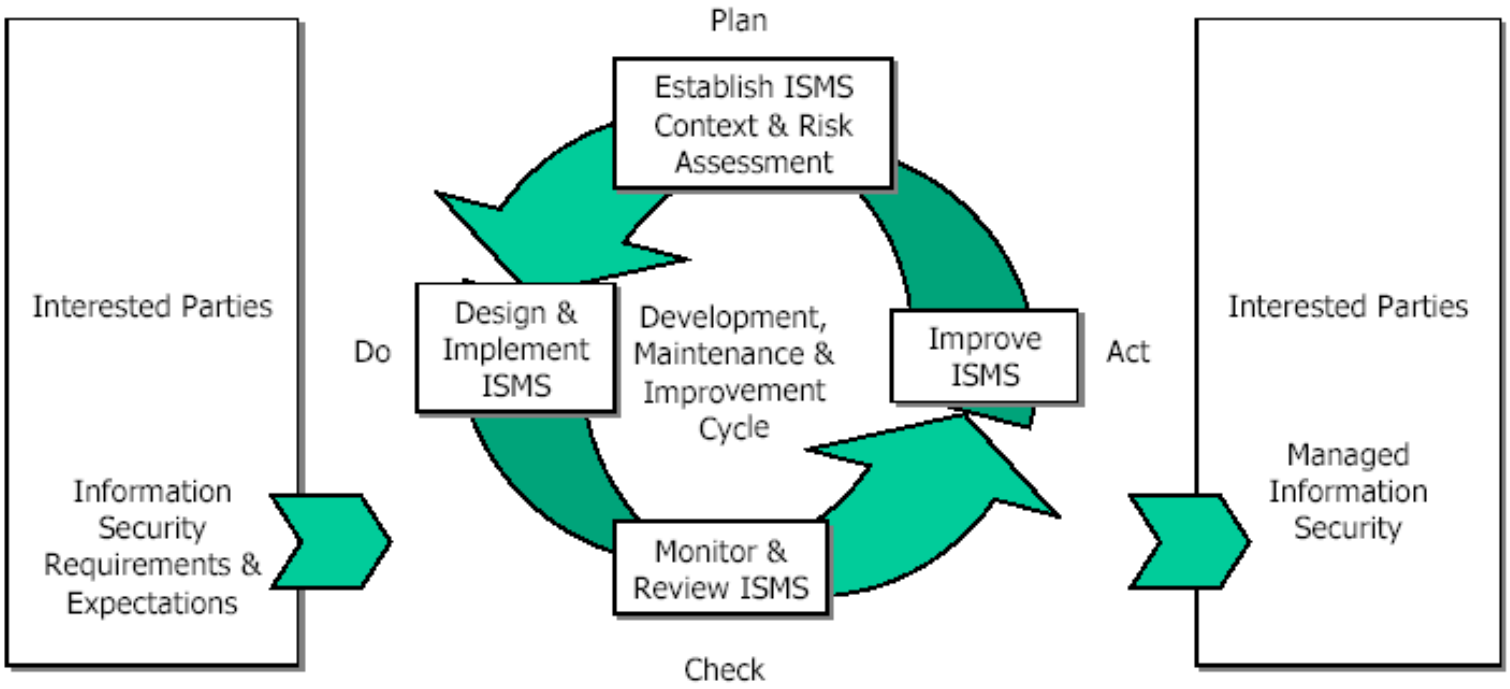


Figure 1 PDCA Process Model

計劃（建立ISMS）

建立安全政策、目標、標的、過程及相關程序以管理風險及改進資訊安全，使結果與組織整體政策與目標相一致。

- ISMS的範圍(組織部門別，流程別)
- 資訊安全政策，目標
- 風險鑑別與評估
- 風險處理計劃

執行（實施與操作ISMS）

安全政策，控制措施，過程與流程之實施與操作

檢查（監控與審查ISMS）

依據安全政策、目標與實際經驗，以評鑑及測量(適當時)過程績效，並將結果回報給管理階層加以審查。

- 例行檢查
- 自我督導程序
- 從事件中學習
- 稽核
- 管理階層審查

行動（維持與改進ISMS）

依據管理階層審查結果採取矯正與預防措施，以達成持續改進資訊安全管理系統。

- 不符合事項
- 矯正及預防措施

BS7799 控制措施

- １０項控制條款
- ３６個控制目標
- １２７條控制措施

資通安全外部稽查核(自我評審)表，以BS7799之控制措施為基礎，訂定233項查核項目

BS7799 控制條款

A.3安全政策
A.4安全組織
A.5資產分類與控制
A.6 人員安全
A.7 實體與環境安全
A.8 通訊與作業管理
A.9 存取控制
A.10 系統開發及維護
A.11 營運持續管理
A.12符合性

風險評估

- 安全的要求是經由有條理的安全風險評估予以定義
- 風險評估的方式可應用在整個組織或部份，不但單獨的資訊系統，特定的系統的一部份均可以應用
- 可了解組織內之資安潛在威脅，及系統之風險值，以進而施以有效益之控制措施
- 在有限的資源下（施以控制措施之成本），優先針對具重要性及時效性之衝擊施以控制措施，其餘者接受或轉移風險
- 針對ISMS PDCA Process Model，週期性的進行風險評估，並考量現有之控制措施，以期持續改善
- 風險評估沒有標準程序及評定之標準

名詞解釋

- 資訊資產：對組織有價值之事物
- 衝擊：事件產生造成之結果
- 安全風險：威脅事件對資產造成潛在傷害或損失之程度
- 控制項目：降低安全風險所需之程序規則或機制
- 威脅：事件之潛在影響程度，將對資訊系統造成傷害
- 弱點：一項資產的弱點，會被威脅事件加以利用而造成衝擊

風險評估之考量因素

- 資訊系統之特質
- 系統或流程之範圍
- 服務之目地及範圍
- 資訊系統使用及操作之環境
- 現有控制措施所提供之保護措施

風險評估及程序

1. 定義資產價值及範圍
2. 弱點評估
3. 威脅評估
4. 確認已存在之控制措施
5. 風險評量
6. 選擇控制措施
7. 定義風險接受程度

定義資產價值及範圍

- 資產範圍：作業流程、系統服務、主機
- 資產項目：資料、軟硬體、人員、服務
- 衝擊及性質：系統重置之成本、直接損失、服務中斷之時間、組織形象、法令規章、敏感度
- 評比階度：定量（10等）或定性（重要、普通、不重要）
- 計算方式：資產＝項目 x 範圍 x 衝擊度

弱點評估

- 針對一項資產評估其弱點項目
- 每一弱點之階度依可導致威脅的容易度及頻率給予定義該弱點之階度(Ex 1-5)
- 其弱點範圍：實體設備之環境、人員及行政管制制度、軟硬體及網路設備
- 實際作法：弱點可由威脅反推，也可不理會弱點階度

威脅評估

- 針對每一弱點，列出威脅項目，並針對威脅發生之頻率與嚴重程度，定義不同之威脅等級(1-5)
- 每一弱點可能有多個威脅項目（例如存取控制不當可導致資料遭竊取及遭置後門程式當跳板之威脅），且同一威脅項目可能針對不同的弱點（例如病毒威脅針對系統漏洞及防毒軟體失效之弱點起作用）

確認已存在之控制措施

- 當弱點及威脅評估完成後，確認針對該威脅之現有控制措施
- 控制措施主要針對弱點進行補強，進而達到抑制威脅之目的
- 在弱點及威脅評估階段，尚不需將現有之控制措施考量在內

風險評量

- 任何風險評估工具或方法皆可運用
- 風險評估值是由資產價值及弱點威脅所組成
- 組織內需用同一評比標準，以免不同資產風險值之定義與實際相差太大
- 各資產之風險值會隨著時間及環境而變化 ,固需持續週期性之重新評估(ex 半年一次)
- 風險評估之方式，範圍及評比標準需文件化，以利將來重新評估之依據

風險評量表

資產項目	資產價值 (1-10)	弱點	威脅	威脅階度 (1-5)	現有控制措施	控制措施	風險值
Web server	7	OS存取管控不良	非法存取	3	關閉網芳功能		21
			帳號破解	2		以高安全度設定密碼	14
		電源不穩定	硬體Down	3		裝設UPS	21
			資料毀損	5		資料備份	35
電腦教室PC	3	未設通行碼	非法存取	2			6
			亂發廣告信	3	現有filewall 阻擋		9
		實體管制環境不良	遭竊	4		加裝監視器	12

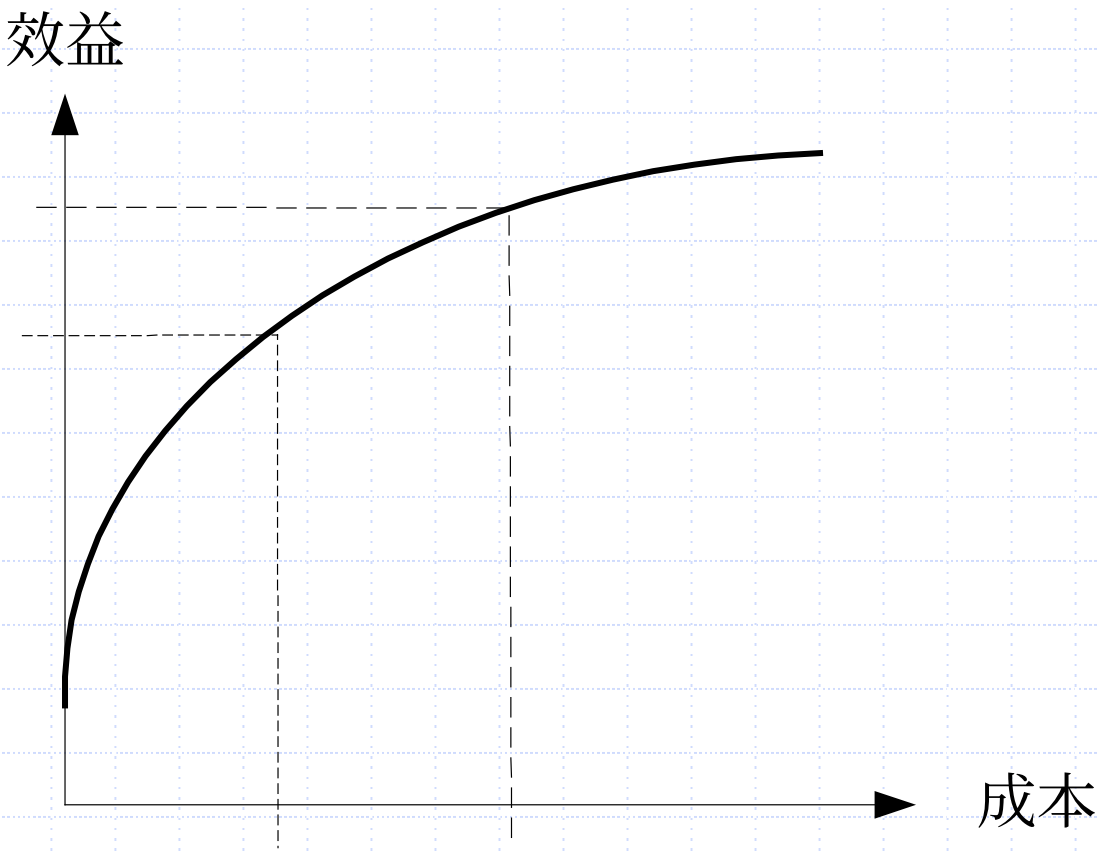
選擇控制措施考量因素

- 經費
- 措施範圍:同一控制措施可針對多個資產
- 效益:同一控制措施可針對多個威脅弱點
- 管理權限:該措施是否為組織內之權限
- 技術可行性及合理性

風險處理

- 定一基準線，基準線以上為必須施以控制措施項目或轉移風險
- 基準線以下則為可接受之風險
- 施以控制措施可以由風險值之大小設定優先次序
- 可就整體，例如每部PC裝設軟體及裝設防毒牆，可就以管理之效益或成本擇一，或是為增加安全係數兩者皆施行

資安投資之成本效益



簡易評估方式

- 以較簡易方式先行建立評估概念
- 以IT設備或系統為主要著眼點給予分級，再依其級別給予不同之控制措施
- 適合校園之單純使用環境與需求，及一系統多應用的狀況
- 施以一段時間後，進階至以風險評估方式施行
- 需有政策之訂定發佈與高層之支援

系統別分級表

主機系統範圍資訊	IP_address： 功能： 範圍：			
項目＼分級	高	中	低	無
有形資產值				
系統之影響範圍				
服務範圍				
作業之重要性				
作業敏感性				
主機系統（總結）				

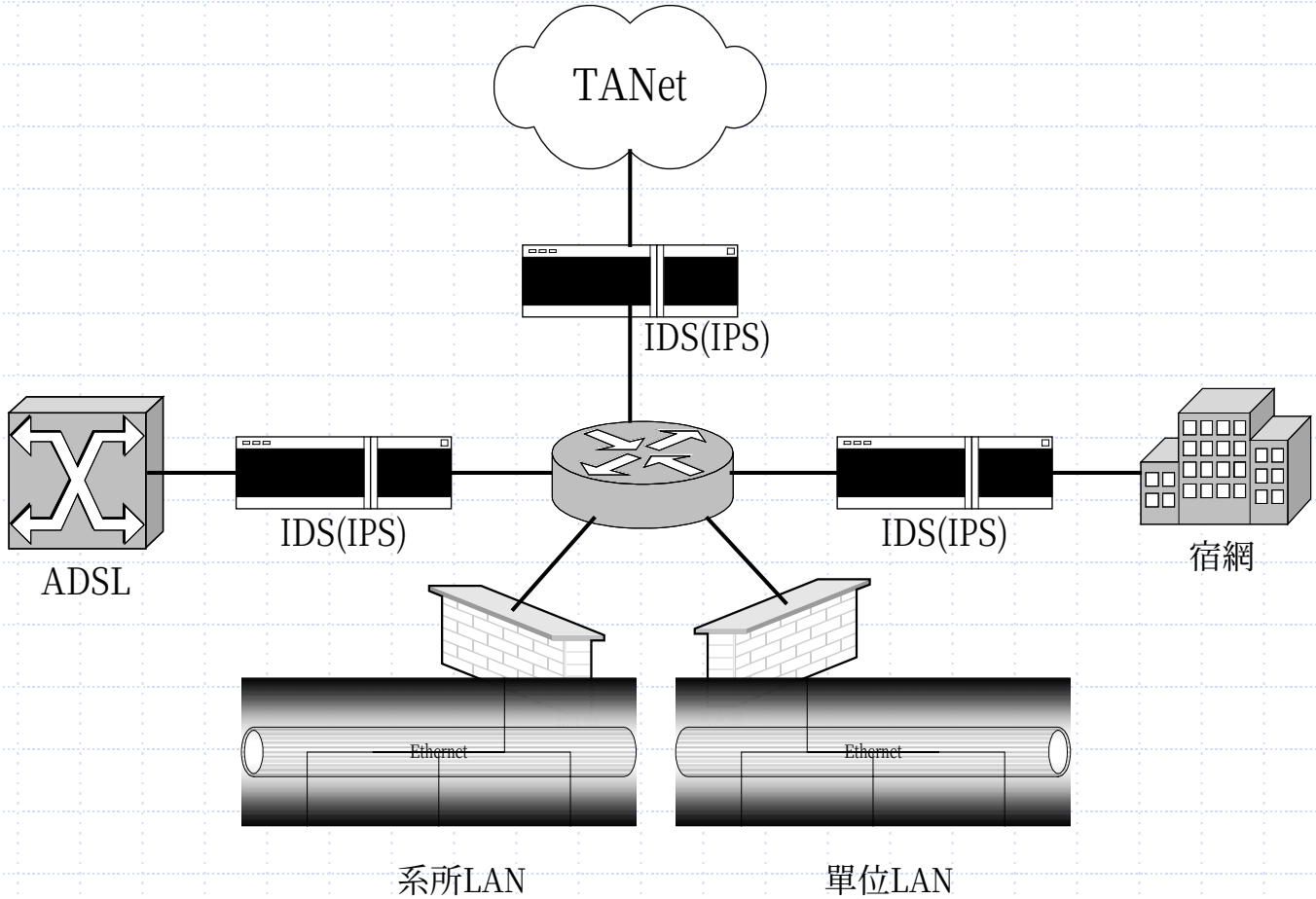
系統別分級表說明

- 以主機系統之有形資產值：範圍有主機、server、網路設備、PC，並含其週邊設備與傳輸媒介。完全以資產值來評估其等級，最單純以採購價格來評估。而軟體成本也可加入考量。
- 以系統之影響範圍分級：當此系統Down時，對於作業之影響層面之多寡而定。例如計網中心之core router肩負所有對外之傳輸，故屬最高等級。
- 以服務範圍分級：例應用系統及遠端登入、E_mail之個人帳號之數量。
- 以作業之重要性：舉例而言，計網中心之網路設備肩負全校及台南區所有學校之連接，故以範圍而言應屬最高等級；醫院之醫療系統若系統Down，則整個醫院作業也將停罷，故亦屬最高等級。
- 以作業敏感性分級：主要針對資料機密性分級。

學校資訊部門之資安措施

- 防毒機制
- 垃圾郵件防制
- 流量監控
- IP控管
- 防火牆
- 弱點掃描
- 入侵偵測(防禦)系統IDS(IPS)
- 系統備援(針對組織內所有或重要資訊系統)
- 事件通報及訊息通告(雙向)
- 事件處理小組
- 資安稽核
- 教育訓練(管理階層,IT部門,一般業務負責人,業務服務對象)

校園網路安全設備配置示意圖



防火牆機制

- 是組織(或單位)內資源存取控制，包含範圍與服務種類及程度控制
- 由單位內之網路服務政策來規劃存取控制措施
- 建立一個外部與內部網路間的管制界面，或是單位內各主機（伺服器or PC）各自建立存取管制界面
- 所採用之措施不一定得架設實體防火牆閘道，但得考量單位存取控制管理的效率性

防火牆功能

- 隔絕或位址轉換 (Network Address Translation NAT)
- 封包過濾(IP, PORT)
- 應用層代理(Application Porxy)
- 狀態檢驗
- 虛擬私人網路(Virtual Private Network VPN)
- 即時監控及警報

建置防火牆考量點

- 經濟成本(風險及成本)
- 位置及管制政策
- 網路型或主機型，硬體型或軟體型
- 效能（Throughput，port數量及速度）
- 功能（阻絕程度，管理界面，附加功能：anti-virus,IDS）
- 技術支援
- 可靠性

入侵偵測系統(IDS)

- 功能
  監測並分析使用者和系統的活動
  檢查系統配置和漏洞
  評估系統關鍵資源和資料檔案的完整性
  識別已知的攻擊行為
  統計分析異常行為
  作業系統日誌管理，並識別違反安全策略的用戶活動。
- 入侵偵測系統(IDS)&入侵防禦系統(IPS)
- 將IPS(IDS)及Firewall及Anti-Virus功能合而為一是目前的趨勢

防毒機制

- 中央控管式防毒軟體優點:
  確實裝設防毒軟體
  自動更新病毒碼
  掌握PC端之狀況
  管理方便
- 多層次防毒機制
  以電子郵件為例，mail server一層防毒，PC端另一層防毒

弱點掃瞄

- 充份了解組織內資訊系統設備之弱點
- 資安稽核工具(ISMS之測試與改進階段)
- 發送報表供該設備系統改進(例如安裝那個Patch或停掉那個service)
- 最大的挑戰是判斷的準確率(多種掃瞄軟體交叉比對)
- 受掃瞄端之設備系統需注意解決方式之有效性, 是否會與原有服務及安全性問題相抵觸

資安稽核列表例

1. IP列管：針對IP登記列表，包含負責人姓名、主機所在位置、作業系統、用途。
2. IP管制：針對非IP列管表中之主機，限制其使用。
3. 網路存取控管（防火牆）：針對外部網路對單位內之存取控制
4. 主機設備是否有專責負責人
5. 主機是否不需密碼之登入
6. 主機系統是否有不明之帳號
7. 檔案分享之控制機制：是否有檔案分享之存取控制
8. 螢幕淨空（screen lock有密碼保護）
9. 是否提供非必要之Service
10. 各重要主機或Server之備份機制
11. 各重要主機或Server之弱點及漏洞及修補（patch）
12. 防毒軟體之有效性：是否裝設防毒軟體及是否及時更新病毒碼

結論

- 少作多錯，多作少錯
- 各組織依組織文化，業務型態，作業流程，發展出適合組織的資安機制
- ISMS是一個規範性條款，而非指南，風險評估無固定之法則及程序
- 需高層之有形的支援與承諾
- 安全機制及其措施，著重有效性及合理性
- 針對組織成員適當的教育訓練及安全意識
- 資訊安全工作不只是事件處理，是常態工作
- 不論組織或系統大小，也需有安全政策及風險評估概念