資訊資產評估
暨風險管理與風險評鑑教育訓練

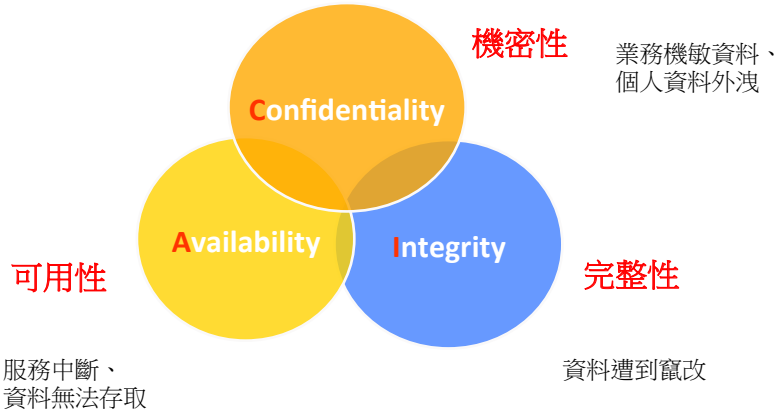
課程綱要

- 資訊資產管理概要
- 風險管理概論
- 風險評鑑作業
- 可接受風險與風險處理
- 實作討論

課程綱要

資訊安全與風險

- 資訊安全在保護單位的資訊資產，避免遭受各種威脅及降低可能危害



資訊資產分類

- 分類的好處
  - 協助識別資訊資產。
  - 將適當的弱點、威脅歸納至相關的資訊資產分類。
  - 將提供資訊安全保護的需求及優先考慮的事。
- 分類擬訂
  - 風險管理的範圍。
  - 組織的業務性質。
  - 個人的作業型態。

資產分類(範例)

- 資訊類資產
  - 資料庫，系統文件，訓練教材
- 軟體類資產
  - 應用軟體，公用程式
- 實體類資產
  - 電腦設備，媒體
- 服務類
  - 空調，電力
- 人員類
  - 資格與經驗
- 無形資產
  - 聲譽與形象

資產分級

- **SEC1**
  - 揭露於組織之外將不適切並造成不便
- **SEC2**
  - 揭露於組織內外部將造成組織重大利益損害
- **SEC3**
  - 揭露於組織內外部皆造成組織嚴重利益損害

資產價值相關考量

Asset	業務作業	經濟損失	聲譽	客戶損失	法令法規	平均值	業務衝擊
制度文件	3	2	5	6	1	3.40	L
客戶資料	5	5	4	5	5	4.80	H
加密技術	3	2	3	2	1	2.20	L

資訊資產清冊(欄位參考)

- 資產分類
- 資訊資產名稱-簡單易辨認
- 說明-填寫詳細的補充資訊，例如規格、版本等等
- 存放位置-實體、邏輯
- 擁有者-資訊資產的負責人
- 管理者-資訊資產的保管人
- 使用者(部門)
- 營運衝擊分析評分(資訊資產價值)
  - C-機密性
  - I-完整性
  - A-可用性
- 備註-補充資訊(數量)

資訊資產群組化

- 好處：
  - 降低風險評鑑負擔，減少弱點、威脅的重複識別。
- 原則：
  - 資訊資產價值相同。
  - 資訊資產性質相同，且數量較多。
  - 存在於相同的實體、邏輯環境。
  - 遭遇弱點、威脅相同。
  - 不需知道細部作業，即可進行風險鑑別。

資訊資產群組化範例

Windows 作業系統

個人電腦

合約、專案檔案文件

商用軟體

課程綱要

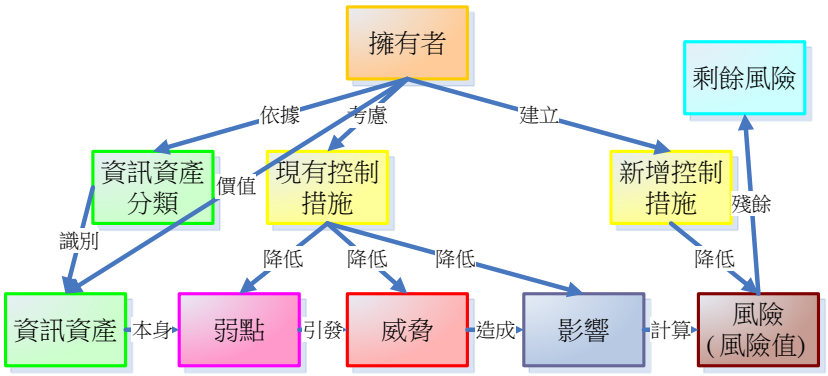
ISO 27001名稱彙總

- 資訊安全(Information Security)-保護資訊的機密性、完整性與可用性；另外也能涉及如鑑別性、 可歸責任性、 不可否認性與可靠性等特性。 [ISO/IEC 17799:2005]
- 資訊安全管理系統(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。
- 機密性(Confidentiality) -資訊不被未經授權的個人、實體或過程取得或揭露的特性。 [ISO/IEC 13335-1:2004]
- 完整性 (Integrity)-保護資產準確及完整的特性。
- 可用性(Availability)-獲得授權的實體要求時可以存取並使用的特性。 [ISO/IEC 13335-1:2004]
- 風險管理(Risk Management)-指導與控制組織有關風險的協調活動。
- 風險評鑑(Risk Assessment)-風險分析與風險評估的整體過程。
- 風險分析(Risk Analysis)-系統化的使用資訊以鑑別資源與估計風險。[ISO/IEC Guide 73:2002]
- 風險評估(Risk Evaluation)-將估計的風險與所訂的風險準則加以比較，以決定風險重要性的過程。
- 風險處理(Risk Treatment)-選擇與實施各項控制措施，以修正風險的過程。

風險管理名稱彙總

- 資訊資產(Asset)-是一種資源(實體或邏輯)，對組織是有價值的。
- 威脅(Threat)-是一種事件，可能會對系統或組織及其資產造成傷害，威脅必須利用資產的弱點才能對資產造成傷害。
- 威脅來源(Threat Agent)-引發潛在威脅的源頭。
- 暴露(Exposure)-弱點誘發威脅的情況。
- 弱點(Vulnerability)-指單一或一系列會讓威脅有機可趁而造成資產損害的狀況。資產的脆弱點本身並不會造成傷害。
- 控制措施(Safeguards) -降低潛在風險的機制。
- 風險(Risk)-有害事件發生的可能性。
- 剩餘風險(Residual Risk)-剩餘的部份風險。

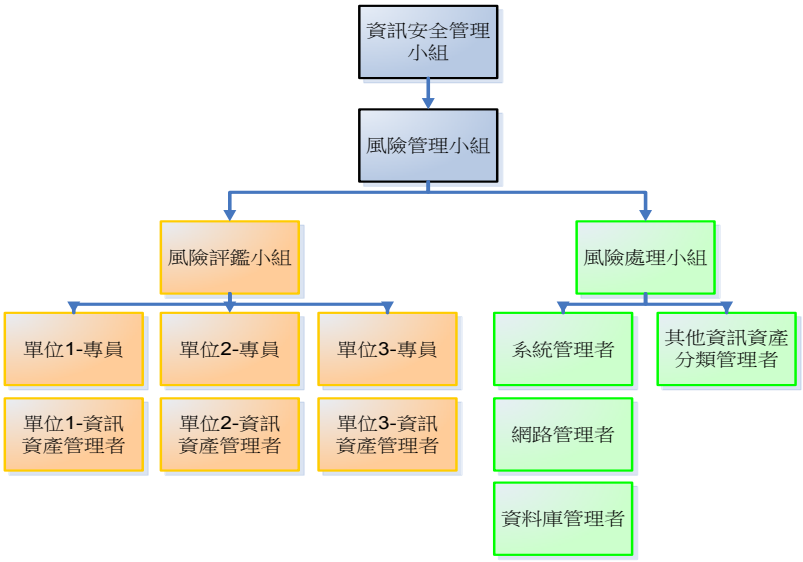
風險管理原則



風險評鑑的分析方式

- 定量分析
  - 試圖去分配獨立的數量化價值物件(例如財務價值)作為風險評鑑的要素及潛在損失的評估。
  - 當全部要素(資訊資產價值、影響、威脅頻率、防護效果、防護成本、不確定性及可能性)是定量化處理，則表示完全定量的考慮。
- 定性分析
  - 以情節為導向。
  - 資訊資產價值、弱點及威脅的重要等級。

風險管理組織架構(範例參考)



建立風險評鑑作業標準

基於資訊資產的比較性，故建立一致性的格式、分類及評分標準。如：

- 資訊資產分類
- 資訊資產清冊格式
- 風險評鑑工作底稿格式
- 風險評鑑公式計算
- 各項鑑別指標
  - 資訊資產價值
  - 弱點脆弱度
  - 威脅發生機率
  - 影響層面

課程綱要

資訊資產分級

- **以資產之C、I 、A設定評估等級標準。**
- **設定評估等級標準採定性化、定量化法則，如：**
  - 機密性(C)：此資訊資產所包含資訊為組織或法律所規範的機密資訊 。
  - 完整性(I) ：資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止。
  - 可用性(A) ：該資訊資產容許失效4小時內不用被修復或是尋找替代品。

資產價值鑑別(一)

- 權責單位應鑑別管轄內所有資訊資產之價值。
- 資產價值鑑別方式以除考量機密等級之外，尚需考量可用性及完整性，其評估標準如下：

機密性評估標準（範例）

評估標準	數值
一般：此資訊資產無特殊之機密性要求	1
限閱：此資訊資產含敏感資訊，但無特殊之機密性要求，且僅供組織內部人員或被授權之外部單位使用	2
敏感：此資訊資產僅供內部相關業務承辦人員存取	3
機密：此資訊資產所包含資訊為組織或法律所規範的機密資訊	4

資訊資產價值鑑別(二)

完整性評估標準（範例）

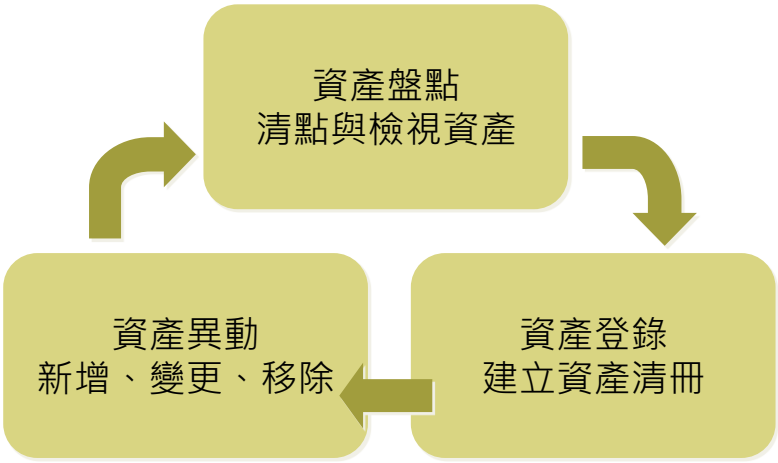
評估標準	數值
資產本身完整性要求極低	1
資產本身具有完整性要求，但是完整性被破壞不會對本會造成傷害	2
資產具有完整性要求，且完整性被破壞會對組織造成傷害，但不至於太嚴重	3
資產具有完整性要求，且完整性被破壞會對組織造成傷害，甚至會造成業務終止	4

資訊資產價值鑑別(三)

可用性評估標準（範例）

評估標準	數值
該資訊資產容許失效 3 天以上，不用被修復或是尋找替代品。	1
該資訊資產容許失效 8 小時以上，3 天以下，不用被修復或是尋找替代品。	2
該資訊資產容許失效 4 小時以上，8 小時以下，不用被修復或是尋找替代品。	3
該資訊資產容許失效 4 小時內不用被修復或是尋找替代品。	4

資產管理

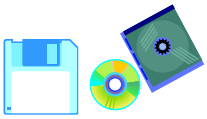


資產報廢

- 資訊資產之報廢（或銷毀）應視其機密等級，採取適當之方式進行銷毀。

文件

電腦設備



光碟、磁片

磁碟、硬碟

資訊資產之分級參考

- 定期檢討評估「機密」、「敏感」等級資訊資產的清冊內容，以確保重要資產受到適當的安全保護。
- 有關文件、紀錄、相關電子檔及儲存媒體控管原則及方式，應於文件管理程序文件規範。
- 有關人員之控管原則及方式，應於人員安全程序文件規範。

資訊風險的要素

- 外部威脅、內部弱點、需要保護的作業或資訊資產。
- 依據資產遭受威脅及弱點之影響做成衝擊分析(Impact Analysis)。
- 依管理目標與現實狀況所做之差異分析(Gap Analysis)及評估風險可能發生之機率。

安全威脅

- 利用資產的安全弱點，可能對資產造成損害
- 可分為意外的及蓄意的安全威脅
- 可能的安全威脅
  - 天然災害：颱風、地震、水災及停電等
    - 地震可能威脅到資訊資產的可用性及完整性
  - 人為因素：非法存取資料、偷竊及竄改資料等
    - 偷竊可能威脅到資訊資產的可用性及機密性
  - 技術因素：網路不通、網頁無法正常運作及硬體故障等
    - 硬體故障可能威脅到資訊資產的機密性、可用性及完整性

安全弱點

- 資產之安全漏洞
- 安全弱點如未妥善處理，將成為安全威脅，可能對資產造成損害
- 可能的安全弱點
  - 作業上的安全弱點
  - 有形的安全弱點
  - 人員上的安全弱點
  - 科技上的安全弱點

風險類別

- 人為：包含因人員有意或無意行為、人力資源管理不當所產生之風險。
- 文件/資料：包含資料、文件之建立、維護、控管、傳遞之不當所產生之風險。
- 軟體：包含系統設計、維護、操作之不當所產生之風險。
- 硬體：包含所有硬體設施之失效、損毀等可能風險。
- 通訊：包含資料、影像、聲音傳輸媒介失效等所可能產生之風險。
- 環境：包含天災、供水、用電、空調等，整體資訊環境，可能發生之風險。

風險評鑑作業

- 評鑑作業
  - 資產價值
  - 威脅利用弱點發生資安事件發生機率
  - 事件發生時對資產影響程度
  - 現有及規劃之資訊安全控管措施
- 評鑑方法
  - 確認資產之安全弱點：是否有安全問題、是否有遺漏之安全控管措施、目前保護機制是否有弱點。
  - 確認作業環境之安全弱點：應用技術、網路連線、實體安全、安全意識、是否遵守相關規定。

風險評鑑

- 威脅
  - 危害資訊資產機密性
  - 損害資訊資產完整性
  - 中斷資訊資產可用性
- 脆弱性
  - 能被一或多個威脅利用之資產或一群資產之弱點

風險評鑑(威脅)

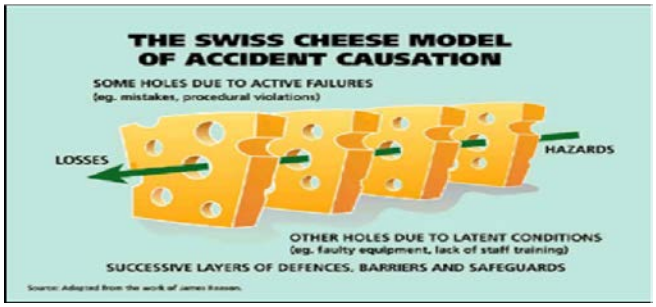
- 技術因素
  - 網路或系統失效
- 邏輯因素
  - 假冒，滲透
- 人為
  - 使用錯誤，故意損壞
- 環境
  - 電力中斷，火災，水災

風險評鑑(弱點)

- 技術因素
  - 未保護網路主機連線
- 邏輯因素
  - 錯誤使用密碼
- 人為
  - 缺乏安全訓練
- 環境
  - 缺乏不斷電系統

風險評鑑(影響之衝擊)

- 風險等級
  - 威脅損害資訊資產機率
- 衝擊
  - 造成業務損害與潛在連續發生可能性的程度



威脅、弱點、風險之間的關係

- 定義：威脅利用資訊資產弱點而對資產所造成的影響與可能性
- 風險= *f* (資產價值，影響程度，發生機率)
- 發生機率=威脅利用弱點對資產造成影響的機率
- 影響程度=威脅利用弱點對資產造成影響的程度

事件發生機率評估

- 依以下之標準評估各事件（威脅-弱點）發生機率。

事件發生機率/等級對應表範例

發生機率評估標準	機率	等級
每年發生一次之可能性	低	1
每季發生一次之可能性	中	2
每月發生一次之可能性	高	3
每週發生一次之可能性	極高	4

事件影響程度評估

- 依以下之標準評估各事件（威脅-弱點）對資產影響程度。

事件影響程度/等級對應表範例

影響程度	程度	等級
對資產價值造成 0 % ~ 25 % 的損失	低	1
對資產價值造成 26 % ~ 50 % 的損失	中	2
對資產價值造成 51 % ~ 75 % 的損失	高	3
對資產價值造成 76 % ~ 100 % 的損失	極高	4

風險值的計算

- 資產價值 = 機密性、完整性、可用性，取最大值
- 風險之定義與評估
  - 資產價值 * 事件影響程度 * 事件發生機率
- 風險值：1 ~ 64

事件風險權值對照表

資產價值	事件影響程度															
	事件發生機率															
	低(1)				中(2)				高(3)				極高(4)			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	1	2	3	4	2	4	6	8	3	6	9	12	4	8	12	16
2	2	4	6	8	4	8	12	16	6	12	18	24	8	16	24	32
3	3	6	9	12	6	12	18	24	9	18	27	36	12	24	36	48
4	4	8	12	16	8	16	24	32	12	24	36	48	16	32	48	64

風險控管原則與方法

- 風險值之高低可決定風險控管之優先順序。
- 高於可接受風險值者，優先選擇控管(處理)風險之方式。
- 選擇風險控管方式
  - 規避
  - 轉嫁
  - 降低
  - 接受
- 建立及執行風險改善計畫
- 執行風險再評鑑

課程綱要

風險處理程序

風險處理(Risk Treatment)-選擇與實施各項控制措施，以修正風險的過程。

可接受風險值的決定

↓

擬訂風險處理計畫

↓

執行風險處理計畫

↓

評估風險處理計畫執行成效

可接受風險值的決定

- 資源有限
- 決定因素
  - 風險嚴重(衝擊)程度(例如：財務、聲譽...)
  - 風險處理急迫性
  - 可分配的資源(例如：人力、時間、金錢)
- 決定方式
  - 80/20法則(排序百分比法)
  - 基本統計(平均數、中位數)
  - 高階統計分析(變異與標準差、常態分配)
  - 檢視法
  - .....等

可接受風險值的決定(續)

- 高於可接受風險值的資訊資產，應依據識別的弱點、威脅進行風險處理計畫的擬訂。
- 新增控制措施，降低弱點、威脅的發生機率。
- 將資訊資產的風險值降低至可接受風險值以下。
- 例外原則:擬訂風險處理計畫時，仍檢視可接受風險值下的資訊資產，是否仍有較高的潛在風險。

擬訂風險處理計畫

- 風險處理決策
  - 風險減緩：提供對策減少風險及加強資訊安全的情形。
  - 風險轉移：轉換風險予其它人，例如：保險。
  - 風險迴避：決定不持續相關活動及不支持風險發生的情形。
  - 風險承受：不論發生與否均接受風險及吸收相關成本。
- 依據風險處理策略，資訊資產管理者擬訂風險處理計畫。
- 風險處理計畫的風險處理措施，應根據ISO 27002(CNS 27002)對各項資訊安全的要求目標，擬訂適當的處理措施及相關執行資源。

風險處理建議及規劃(範本)

- **系統使用之資料或傳輸加解密技術存在弱點，遭利用造成資訊不當揭露**
- 預防性措施：
  - 制定委外服務安全管理程序，規範委外服務的安全管理方式。
  - 禁止服務提供者及其人員接觸任何與加解密有關的系統及傳輸之檔案。
  - 提出提升加解密安全性之需求。
  - 對委外廠商實施資訊安全宣導。
  - 制定委外服務廠商安全須知，並要求簽署。
  - 修定安全事件處理程序增加委外服務人員之安全事件處理準則，考量以下事項：
    - 證據保全
    - 合約及法律責任
    - 政風室及法務科的參與

風險處理建議及規劃(範本)續

- **系統使用之資料或傳輸加解密技術存在弱點，遭利用造成資訊不當揭露**
- 偵測性措施：
  - 建立資訊安全監控作業細則，規範安全監控項目及方式。
  - 將服務提供者及其人員對於系統的存取及操作列為安全監控項目。
  - 對於加解密系統的使用及相關檔案之存取列為安全監控項目。
- 矯正性措施：
  - 依照委外服務人員之安全事件處理準則，進行蒐證並通知政風室及法務科。

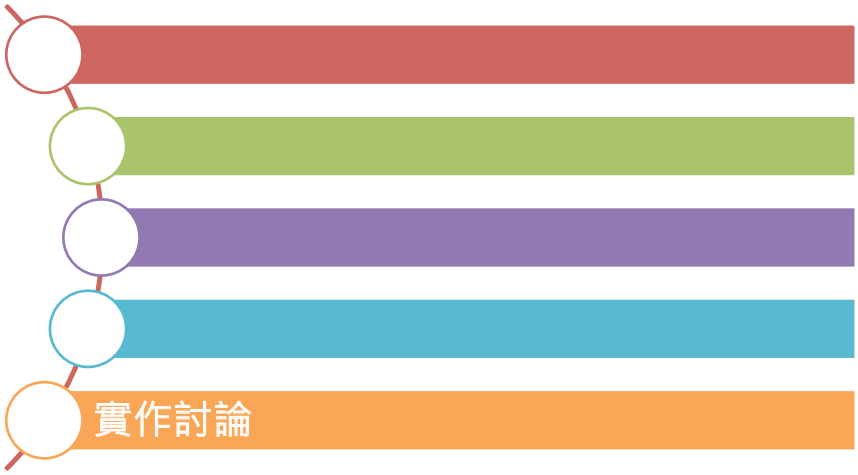
風險處理計畫表(範例參考)

資訊資產名稱：				風險處理計畫表			
弱點 / 威脅項目	新增的控制措施	脆弱度 / 發生機率		控制措施提案與執行			
		處理前	處理後	編號	提案人	經辦人	完成日期
風險值：			殘餘風險：				

風險管理之後

- 建立一套量測系統(例如：**KPI**指標)，協助控制目標的達成。
- 執行內部稽核，確保控制措施的有效性。
- 當有下列情況時，執行風險評鑑作業。
  - 每年定期執行
  - 營運組織變更
  - 作業流程改變
  - 資訊資產新增或變更
  - 發生重大資訊安全事件

課程綱要



Q&A 問題與討論