資訊資產盤點與管理教育訓練

講師：劉志銘 資深顧問

財團法人中華民國國家資訊基本建設產業發展協進會

課程大綱

1. 資訊資產概論
2. 資訊資產清單
3. 資產分類分級及管理
4. 資產價值識別
5. 資產管理作業
6. 資產報廢及處理規範

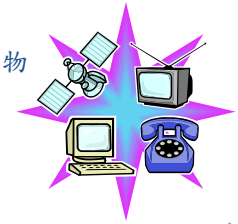
課程大綱

1. 資訊資產概論
2. 資訊資產清單
3. 資產分類分級及管理
4. 資產價值識別
5. 資產管理作業
6. 資產報廢及處理規範

資產的特色

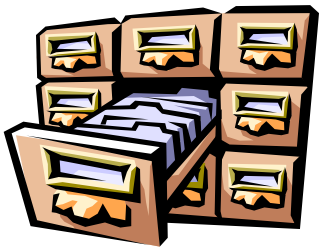
資訊資產→資訊→組織營運之命脈

即對組織有價值的任何事物



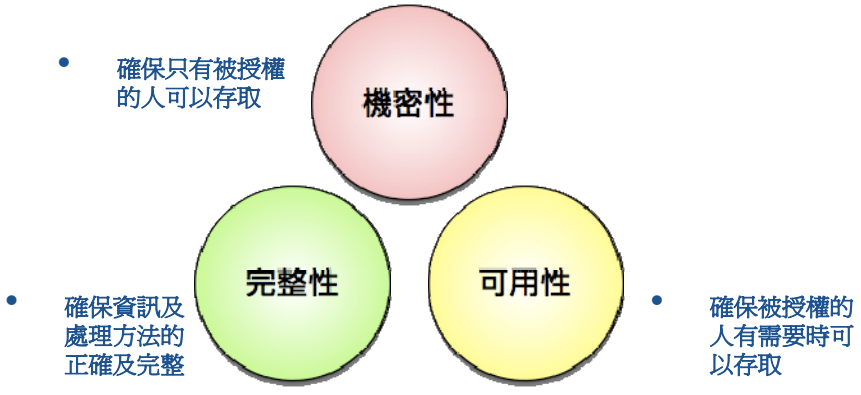
資產管理的目的

適切保護資訊資產→ 確保達成資訊安全之要求

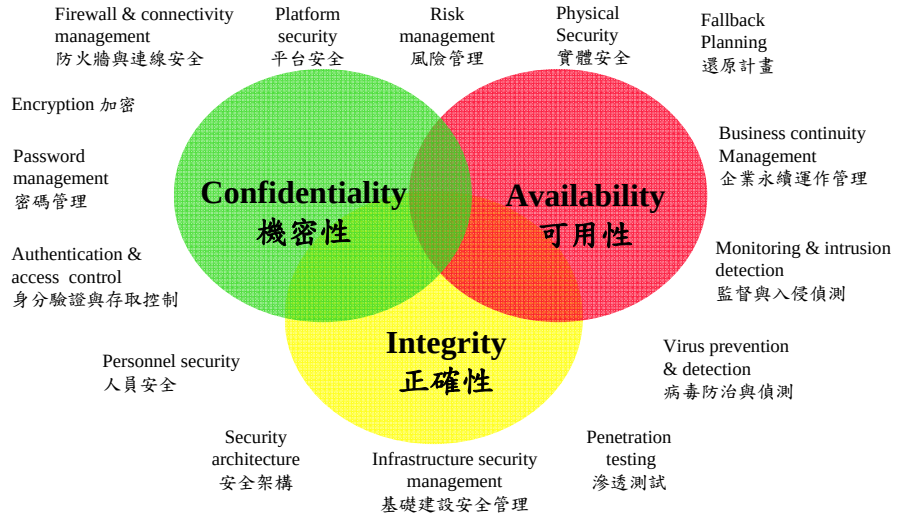


資訊安全三要素

ISO27001 ISMS 所強調的資訊安全包含了:
資訊的機密性(Confidentiality)、完整性(Integrity)、以及可用性(Availability)等三個要素。

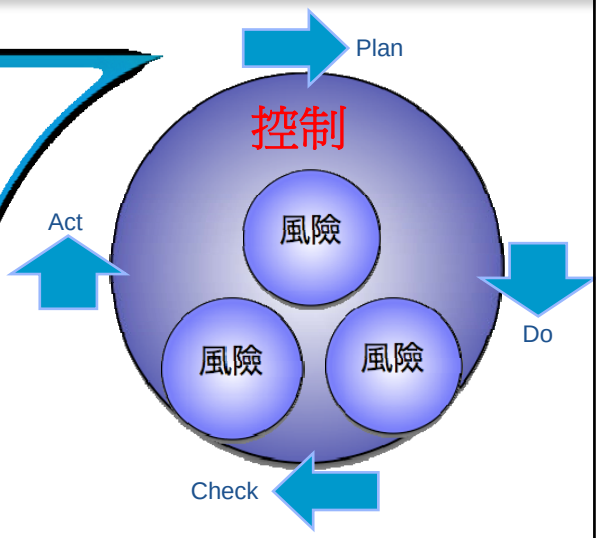


資訊安全三大原則



資訊安全管理制度如何實施?

- 辨識資訊風險
- 評估資訊風險
- 選擇控制措施
- 實行控制措施
- 監控安全狀況
- 處置安全事件
- 評估控制有效性
- 改善控制有效性



課程大綱

1. 資訊資產概論
2. 資訊資產清單
3. 資產分類分級
4. 資產價值鑑別
5. 資產管理作業
6. 資產報廢及處理規範

資產管理角色

- Owner 權責單位：

  由組織指定的資訊資產擁有單位。

  註：Owner指的是負有被認可管理責任個體，負責資產的生產、發展、維護、使用及安全；並非對該資產有任何實質的財產權。
- Keeper 保管單位：

  由組織指定的資訊資產保管單位。
- User 使用單位：

  由組織授權的資訊資產使用單位。

資產清單建立

- 權責單位應清點及鑑別所管轄之資訊資產，建立「資訊資產清單」
- 權責單位應定期更新與維護所管轄之資訊資產清單
- 由各權責單位彙整資訊資產清單，陳報至資訊安全小組予以統一控管，以確保資訊資產清單之完整性

資訊資產清單範例

文件編號：XXX-XX-ISMS-D-00X　　日期：98年03月17日

紀錄編號：098-001

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
XXXX-CM-001	CM	Core Router & Switch	Cisco 6509 Router 1部	計算機中心	網路組	網路組	2	3	4	4

資產清單範例

資訊資產清單

文件編號：XXXX-ISMS-D-00X　　日期：98年03月17日

紀錄編號：098-001

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
XXXX-CM-001	CM	Core Router & Switch	Cisco 6509 Router 1部	計算機中心	網路組	網路組	2	3	4	4

資產管理角色

權責單位	保管單位	使用單位
計算機中心	網路組	網路組

課程大綱

資訊資產鑑別

- What
  - 找出作業中具有價值之資訊資產。
- Why
  - 產生資訊資產清冊，以供後續風險評鑑作業使用。
- How
  - 透過資產管理系統或財產帳方式清查。
  - 由業務承辦人依據承辦業務與作業進行資訊資產清查與確認。

資訊資產鑑別(續)

- Tool
  - 資產管理系統(如:單位自行開發、smartIT、WinMatrix等)。
- Output
  - 資訊資產清冊
- **資訊資產**
  - 硬體、網路設備、實體環境及空調、消防設施
  - 硬體設備上的軟體(OS,AP,DB)等

資訊資產鑑別方式

- 點
  - 個人工作職掌或業務。
  - 主機、伺服器、個人電腦或NB等
- 線
  - 各作業流程(過程中相關資產)
  - 應用系統的資訊資產關連圖
- 面
  - 實體環境配置
  - 網路架構圖
  - 資產管理系統(硬體、軟體)

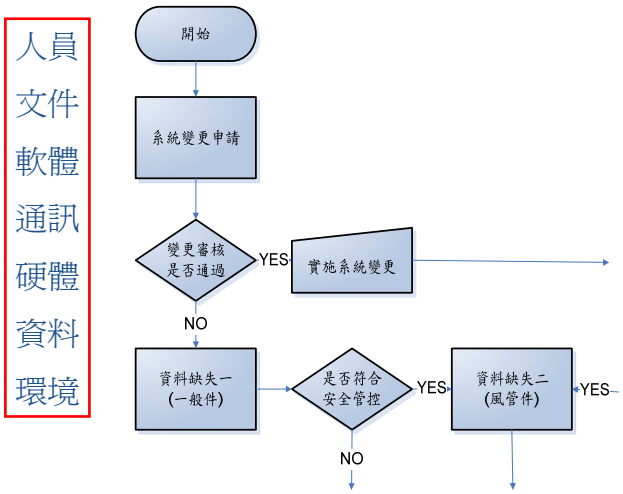
資訊資產鑑別-個人工作職掌

- 依據人員本身工作職掌鑑別資訊資產

姓名	職稱	工作職掌	地點
方大爲	系統開發組組長	1.綜理全組業務 2.系統之統籌規劃 3.督導及推展系統開發組業務	資訊大樓10樓
王大川	系統工程師	1.系統開發與設計 2.系統程式碼管理 3.系統安全檢測	資訊大樓10樓

資訊資產鑑別-作業流程面

人員
文件
軟體
通訊
硬體
資料
環境



什麼人在做？(內、外部人員)

人員怎麼作業？(紙本及電子文件)

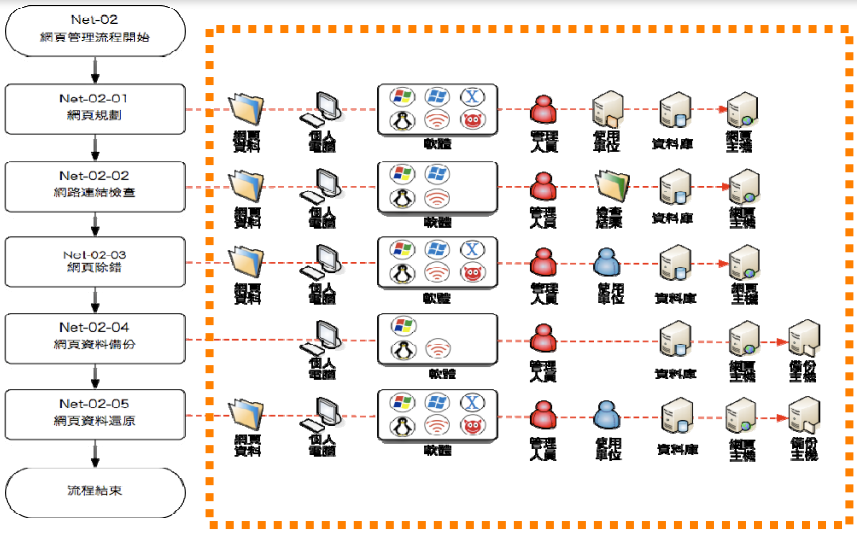
哪些作業原則？(紙本及電子文件)

使用相關什麼設備？(一般硬體)

產出資料(紙本及電子文件)

利用什麼傳送資料或訊息？(電訊，內、外部服務)

資訊資產鑑別-作業流程面(續)



資訊資產分類

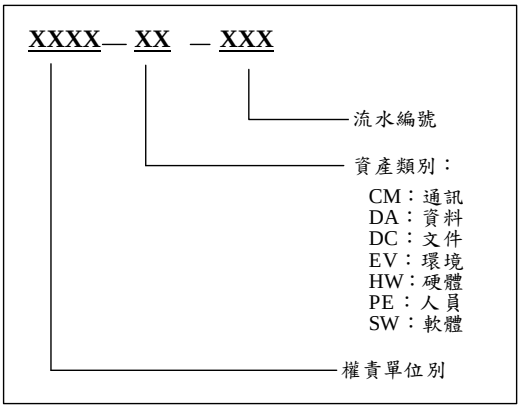
- 人員 (People)
  - 包含全體同仁，以及委外廠商。
- 文件 (Document)
  - 以紙本形式存在之文書資料、報表等相關資訊，包含公文、列印之報表、表單、計畫、合約等紙本文件。
- 軟體 (Software)
  - 作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼、資料庫等。

資訊資產分類

- 通訊 (Communication)
  - 網路設備、網路安全設備 、提供資訊傳輸、交換之線路或服務。
- 硬體 (Hardware)
  - 主機設備等相關硬體設施。
- 資料 (Data)
  - 儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
- 環境 (Environment)
  - 相關基礎設施及服務，包含辦公室實體、實體機房、電力、消防設施等。

資產編碼方式

- 除「文件」類之資訊資產外，資產編號之編碼方式，如右圖：
- 1~4碼為權責單位別
- 5~6碼為資產類別
- 7~9碼為資產流水編號



資訊資產編碼方式圖

資產群組

- 群組的好處
  - 降低風險評鑑負擔，減少威脅、弱點的重複識別
- 群組做法
  - 先依據識別出之資訊資產進行分類，再從分類中群組化資產，以避免遺漏重要資產
  - 針對群組化之資訊資產進行風險評鑑
- 群組原則
  - 同性質之資產且數量大
  - 相同控管措施
  - 存在於相同的實體、邏輯環境
  - 資產價值相同

資產群組範例

Windows 作業系統

個人電腦

合約、系統文件

商用軟體

資產清單範例

資訊資產清單

文件編號：XXXX-ISMS-D-00X　　日期：99年11月11

紀錄編號：099-001

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性
XXXX-CM-001	CM	Core Router & Switch	Cisco 6509 Router 1部	計算機中心	網路組	網路組	2	3	4

群組資產名稱

資產基本資料

資產編號	資產類別	資產名稱	資產說明
XXXX-CM-001	CM	Core Router & Switch	Cisco 6509 Router 1部

資訊資產分級

- 以資產之C、I、A特性對組織之價值進行評估
- 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)：容許該資訊資產失效的時間長短。

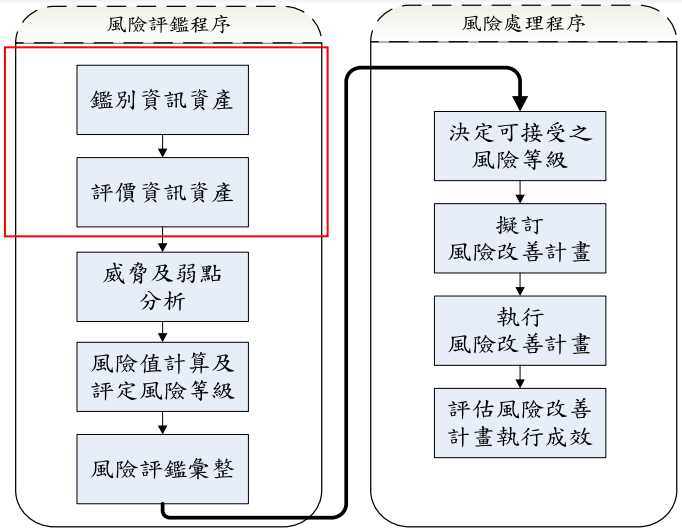
為何做資訊資產分級?

資產分級的好處?

- 清楚分辨資產等級的不同，配合資產類別給予適當的控管措施(如原始碼、資料庫等)。
- 單位能確定哪些資產是對組織是有價值或重要性的。
- 確立單位對資訊資產保護之方式與政策。

課程大綱

風險評鑑與管理



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：此資訊資產僅供組織內部人員或被授權之單位及人員使用	2
敏感：此資訊資產僅供組織內部相關業務承辦人員及其主管，或被授權之單位及人員使用	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

資產價值鑑別（二）

– 完整性評估標準（範例）

評估標準	數值
該資訊資產本身完整性要求極低	1
該資訊資產本身具有完整性要求，當完整性遭受破壞時，不會對組織造成傷害	2
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，但不至於太嚴重	3
該資訊資產具有完整性要求，當完整性遭受破壞時會對組織造成傷害，甚至造成業務終止	4

資產價值鑑別（三）

– 可用性評估標準（範例）

評估標準	數值
該資訊資產可容許失效 3 工作天以上	1
該資訊資產可容許失效 8 工作小時以上，3 工作天以下	2
該資訊資產僅容許失效 4 工作小時以上，8 工作小時以下	3
該資訊資產僅容許失效 4 工作小時以下	4

資產價值鑑別（四）

- 評估資訊資產之機密性、完整性及可用性後，取三者之**最大值**，為資訊資產之價值

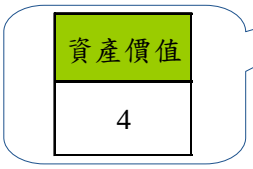
資產價值=MAX (C, I, A)

資訊資產清單

文件編號：XXXX-ISMS-D-00X　　日期：98年03月17日

紀錄編號：098-001

資產編號	資產類別	資產名稱	資產說明	權責單位	保管單位	使用單位	機密性	完整性	可用性	資產價值
XXXX-CM-001	CM	Core Router & Switch	Cisco 6509 Router 1部	計算機中心	網路組	網路組	2	3	4	4



資訊資產清單之價值確認

- 資訊資產權責單位應依據資訊資產清單之機密性、可用性、完整性之評估標準，確認資產價值。
- 資訊資產清單及價值評估結果，應陳報至資訊安全委員會審議 。

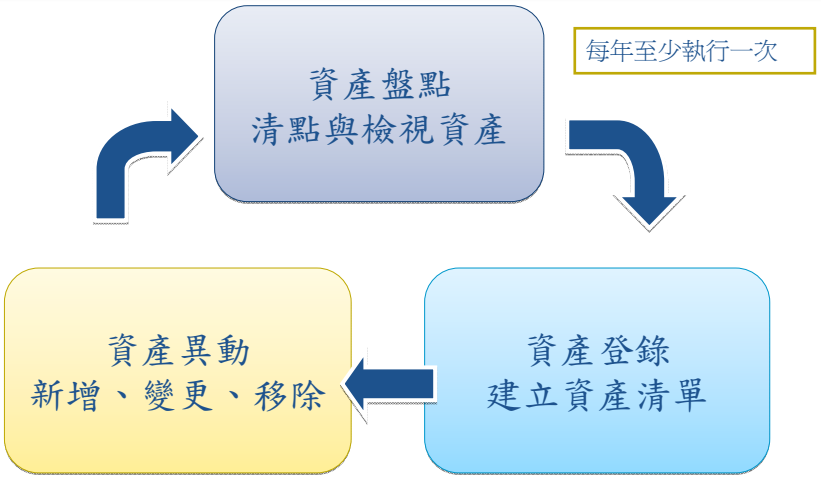
課程大綱

1. 資訊資產概論
2. 資訊資產清單
3. 資產分類分級
4. 資產價值鑑別
5. 資產管理作業
6. 資產報廢及處理規範

資產管理-ISO27001要求

- A.7.1 資產責任
  - ✓A.7.1.1 資產清冊
  - ✓A.7.1.2 資產的擁有權
  - ✓A.7.1.3 資產之可被接受的使用
    （組織員工、廠商及第三方使用資產的限制）
- A.7.2 資訊分類
  - ✓A.7.2.1 分類指導綱要
  - ✓A.7.2.2 資訊標示與處置

資產管理



資產標示

- 機密等級分類的資訊資產及系統之輸出資料，應明確標示，避免其機密性遭破壞
- 重要等級標示方式：
  - 不同顏色標籤區分，並註明財產編號與財產名稱。
    - 資產價值 X 為藍色標籤(依單位需求調整)
    - 資產價值 X 為黃色標籤(依單位需求調整)
    - 資產價值 X 為綠色標籤 (依單位需求調整)

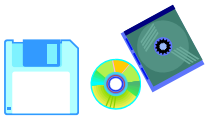
資產清單檢視

- 權責單位每年至少進行一次資產盤點與資產清單覆核，以更新及確保資產清單的正確性及完整性
- 當範圍內有以下的狀況發生之時，則實施不定期的覆核，以更新及確保資產清單的正確性及完整性
  - 有新增、變更或移除資訊資產；
  - 系統有重大異動；
  - 作業環境改變。

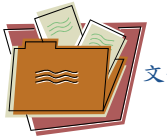
課程大綱

資產報廢

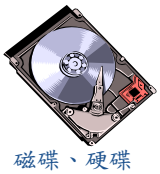
- 資訊資產之報廢應循單位資產報廢程序辦理，並依資產類別相關管理程序作業原則與資訊資產之機密等級，採取適當之方式進行銷毀。



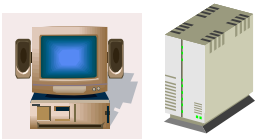
光碟、磁片



文件



磁碟、硬碟



電腦設備

硬體及通訊資產報廢

- 硬體及通訊資訊資產需報廢或移作它用，硬體及通訊資產之相關設定與儲存媒體之資料必須清除。
- 硬體及通訊資訊資產報廢時，資訊資產權責單位應填寫具相關申請單，並留存紀錄備查。經權責單位審核並確認資料清除後，方可進行資訊資產報廢程序。
- 資訊資產保管單位依據填具之申請單，經審核後，辦理更新「資訊資產清單」，可重複使用之資料儲存媒體，於不再繼續使用時，應將儲存之內容完全消除，內含機敏資料之資訊資產必須確認資料清除後無法還原其內容。

儲存媒體報廢

- 儲存媒體如要報廢或移作他用時，儲存媒體上之資料必須確定不再使用後，方可清除。
- 當儲存媒體須報廢或移作他用時，應採用以下任一種合宜之措施進行銷毀：
  - A.硬碟
    利用專業資料清除軟體工具或實體破壞方式，清除硬碟資料。
  - B.光碟
    光碟一律將反光層抹除、刀片割損或折斷銷毀。
  - C.磁帶或磁片
    磁帶或磁片應以工具進行實體之破壞，使其無法使用。

軟體版權管理及文件報廢

- 軟體版權到期與移除
  - 當軟體版權到期而需移除時，由資訊資產權責單位填寫相關申請單，陳報主管核准後，方可通知使用者並確認其執行移除。
  - 資訊資產保管單位依據單位資訊資產管理程序審核後，辦理更新「資訊資產清單」。
    - 分享軟體
    - 免費軟體
- 文件報廢
  - 當資訊安全管理制度相關文件報廢時，依照單位文件管理程序辦理。

問題與討論

&