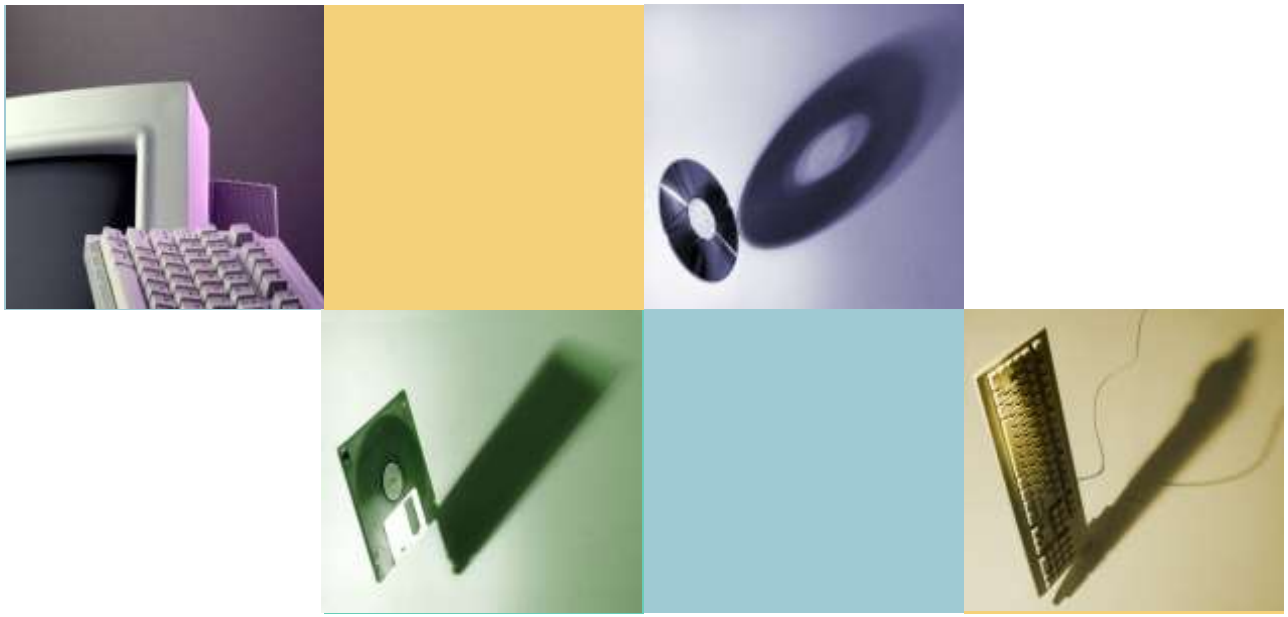
資訊資產評估與風險評鑑



國立宜蘭大學圖書資訊館

網路組 曾國旭

Wednesday, Mar 05 2014

大綱

- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - 風險識別作業
  - 風險評鑑方法
  - 風險控管方式



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。



- 資訊資產評估
  - 資訊資產概論
  - **資訊資產清單**
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - 風險識別作業
  - 風險評鑑方法
  - 風險控管方式



資產管理角色

- 權責單位(Owner)：
  - 由組織指定的資訊資產擁有單位。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。
- 保管單位(Keeper)：
  - 由組織指定的資訊資產保管單位。
- 使用單位(User)：
  - 由組織授權的資訊資產使用單位。



建立資產清單

- **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。
- 資訊資產清單由各權責單位提供，資訊安全小組負責彙整，並**陳報至資訊安全委員會**，以確保清單之完整性。



資訊資產清單範例

資訊資產清單										
						機密等級：□一般 ■限閱 □敏感 □機密				
文件編號：	NIU-ISMS-D-009					版　　次：1.0				
紀錄編號：	098-001					填表日期：　98　年　03　月　25　日				
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
CCN-CM-001	CM	外網Core Router	骨幹 Cisco 6506、Cisco ONS 15454、Cisco 7609(2部)、Cisco 3750(2部)路由器共6部	網路組	網路組	網路組	1	2	3	3
CCN-CM-002	CM	內網Core Router	Extreme BD 6808路由器1部	網路組	網路組	網路組	1	2	3	3
CCN-CM-003	CM	區網Switch	Extreme 3802、Cisco 2960共2 部	網路組	網路組	網路組	1	2	3	3

資產管理角色



- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - **資產分類分級**
  - 資產價值鑑別
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - 風險識別作業
  - 風險評鑑方法
  - 風險控管方式



資訊資產分類

- 人員(People / PE)：包含全體同仁，以及委外廠商。
- 文件(Document / DC)：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、計畫等紙本文件。
- 軟體(Software / SW)：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。



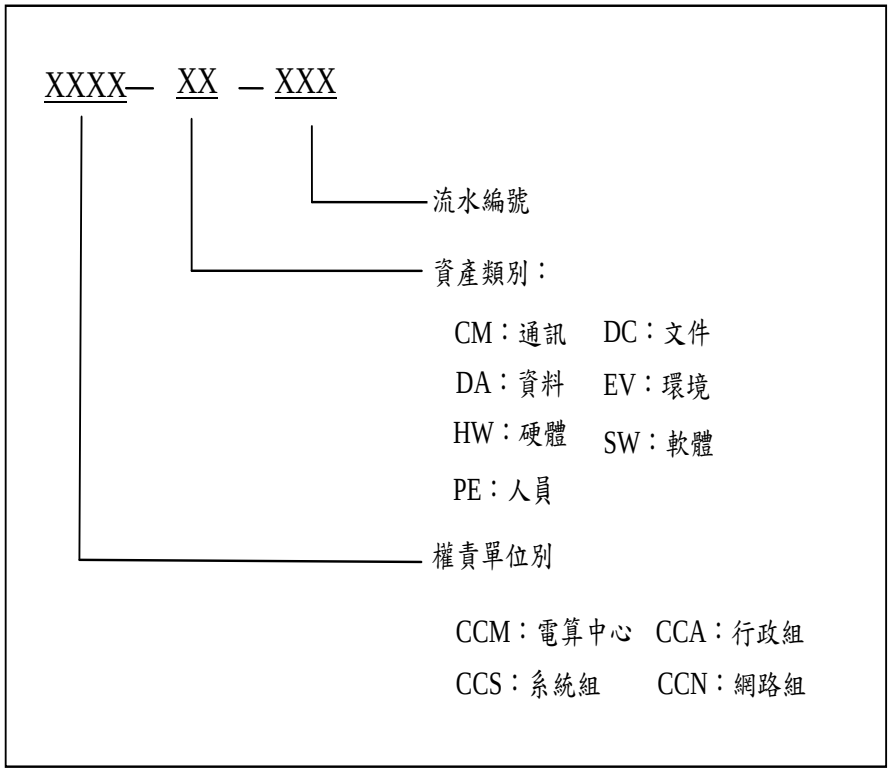
資訊資產分類(續)

- 通訊(Communication / CM)：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 / HW)：主機設備等相關硬體設施。
- 資料(Data / DA)：儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
- 環境(Environment / EV)：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。



資訊資產編碼方式

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



資訊資產編碼方式圖



資訊資產群組化

資訊資產群組化(續)

- 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。
  - 遭遇弱點、威脅相同。



資訊資產群組化(續)

資訊資產清單						機密等級：□一般 ■限閱 □敏感 □機密			
文件編號：	NIU-ISMS-D-009					版　　次：1.0			
紀錄編號：	098-001					填表日期：　98　年　03　月　25　日			
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
CCN-CM-001	CM	外網Core Router	骨幹 Cisco 6506、Cisco ONS 15454、Cisco 7609(2部)、Cisco 3750(2部)路由器共6部	網路組	網路組	網路組	1	2	3	3
CCN-CM-002	CM	內網Core Router	Extreme BD 6808路由器1部	網路組	網路組	網路組	1	2	3	3
CCN-CM-003	CM	區網Switch	Extreme 3802、Cisco 2960共2 部	網路組	網路組	網路組	1	2	3	3

資訊資產群組



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。
- 各類資訊資產機密等級分為4級：
  - 一般：無特殊之機密性要求，可對外公開之資訊。
  - 限閱：僅供組織內部人員或被授權之單位及人員使用。
  - 敏感：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。
  - 機密：為組織、主管機關或法律所規範之機密資訊。



- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - **資產價值鑑別**
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - 風險識別作業
  - 風險評鑑方法
  - 風險控管方式



資產價值鑑別

- 權責單位應鑑別其所管轄內所有資訊資產之價值。
- 資訊資產價值除考量資訊資產機密等級之外，尚需考量資訊資產之可用性及完整性，其評估標準如下：
  - 機密性評估標準

評估標準	數值
此資訊資產無特殊之機密性要求	0
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	1
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	2
此資訊資產所包含資訊為組織或法律所規範的機密資訊	3



資產價值鑑別(續)

- 完整性評估標準

評估標準	數值
該資訊資產本身完整性要求極低	0
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	1
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	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，甚至造成業務終止	3

- 可用性評估標準

評估標準	數值
該資訊資產可容許失效 3 工作天以上	0
該資訊資產可容許失效 8 工作小時以上，3 工作天以下	1
該資訊資產僅容許失效 4 工作小時以上，8 工作小時以下	2
該資訊資產僅容許失效 4 工作小時以下	3



資產價值鑑別(續)

- 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

機密等級：□一般 ■限閱 □敏感 □機密

文件編號：NIU-ISMS-D-009　　版　　次：1.0

紀錄編號：098-001　　填表日期：98 年 03 月 25 日

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
CCN-CM-001	CM	外網Core Router	骨幹 Cisco 6506、Cisco ONS 15454、Cisco 7609(2部)、Cisco 3750(2部)路由器共6部	網路組	網路組	網路組	1	2	3	3
CCN-CM-002	CM	內網Core Router	Extreme BD 6808路由器1部	網路組	網路組	網路組	1	2	3	3
CCN-CM-003	CM	區網Switch	Extreme 3802、Cisco 2960共2部	網路組	網路組	網路組	1	2	3	3

資訊資產價值



資訊資產清單之價值確認

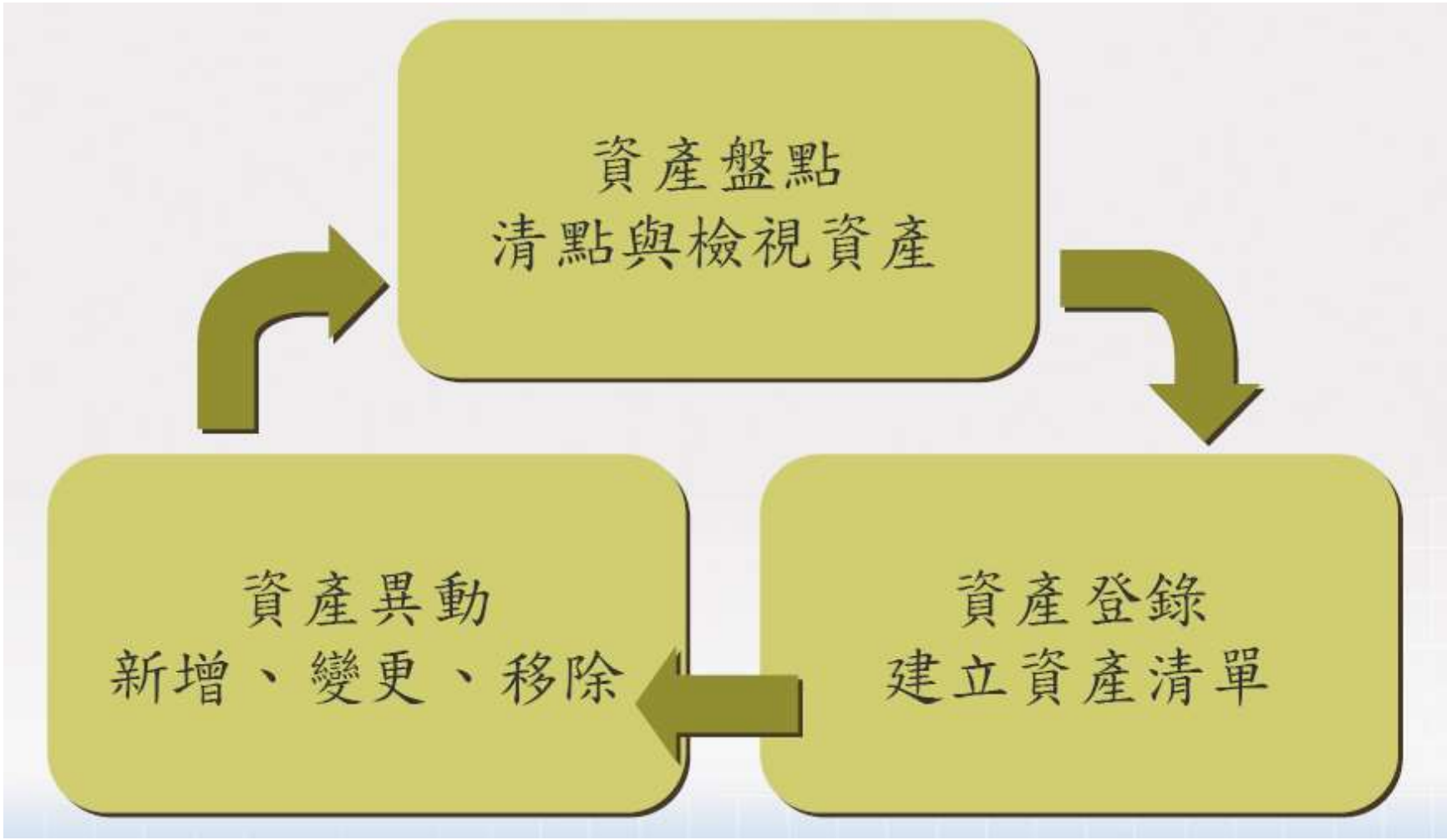
- 資訊資產權責單位應依據資訊資產清單之機密性、可用性及完整性之評估標準，確認資產價值。
- 資訊資產清單及價值評估結果，**應陳報至資訊安全委員會審議**。



- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - 資產價值鑑別
  - **資產管理作業**
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - 風險識別作業
  - 風險評鑑方法
  - 風險控管方式



資產管理



資產標示

- 已列入機密等級分類的資訊資產，應明確標示其機密等級，避免其機密性遭破壞。
- 實體設備之重要等級標示方式，應**以不同顏色標籤區分**：
  - 資產價值1為綠色標籤。
  - 資產價值2為黃色標籤。
  - 資產價值3為紅色標籤。



資產清單檢視

- 權責單位**每年至少進行1次資產盤點與資訊資產清單覆核**，以更新及確保資訊資產清單的正確性及完整性。
- 當範圍內有以下的狀況發生時，則實施不定期的覆核，以更新及確保資訊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。

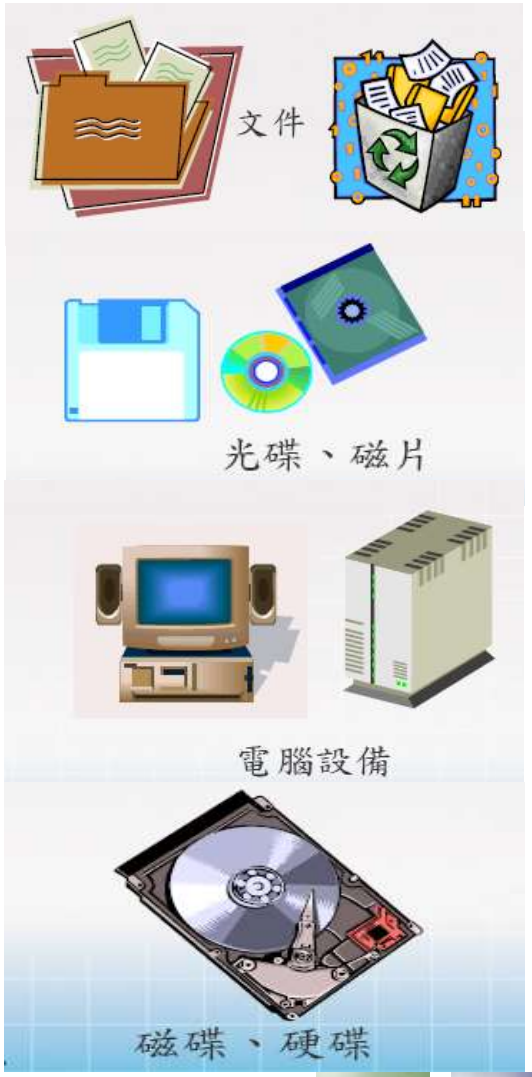


- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理作業
  - **資產報廢及處理**
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - 風險識別作業
  - 風險評鑑方法
  - 風險控管方式



資產報廢

- 資訊資產之報廢（或銷毀）應**依「資訊資產異動作業說明書」**之相關**規定**，採取適當之方式進行銷毀



資訊資產之處理規範

- 針對價值2或3之資訊資產，應加強安全保護及存取控制管控措施，以防止洩漏或不法及不當的使用。
- 價值2或3文件類資訊資產之安全處理應符合以下作業要求：
  - 紙類文件不再使用時，應銷毀處理。
  - 系統流程、作業流程、資料結構及授權程序等系統相關文件，應予適當保護，以防止不當利用。
  - 系統文件應指定專人管理，並鎖在安全的儲櫃或其他安全場所，且發送對象應以最低必要的人員為限。
  - 電腦產製的文件，應與其應用檔案分開存放，且應建立適當的存取保護措施。



資訊資產之處理規範(續)

- 針對價值2或3軟體類資訊資產之安全處理作業，請參閱「存取控制管理程序書」及「系統開發與維護程序書」之相關程序。
- 價值2或3硬體類資訊資產之安全處理作業，請參閱「實體安全管理程序書」中重要設備之相關程序。
- 應定期檢討價值2或3之資訊資產清單內容，以確保重要資產受到適當的安全保護。



資訊資產鑑別實作

- 請運用所提供之資訊資產清單範本，**各類試列舉出一項**資訊資產。
- 將所列資訊資產就機密性、完整性及可用性，試評出符合該資訊資產在組織內之價值。
- 將C、I、A之價值鑑別結果，取最大值，填入「資產價值」欄位。



- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - **風險概論**
  - 風險管理流程
  - 風險識別作業
  - 風險評鑑方法
  - 風險控管方式



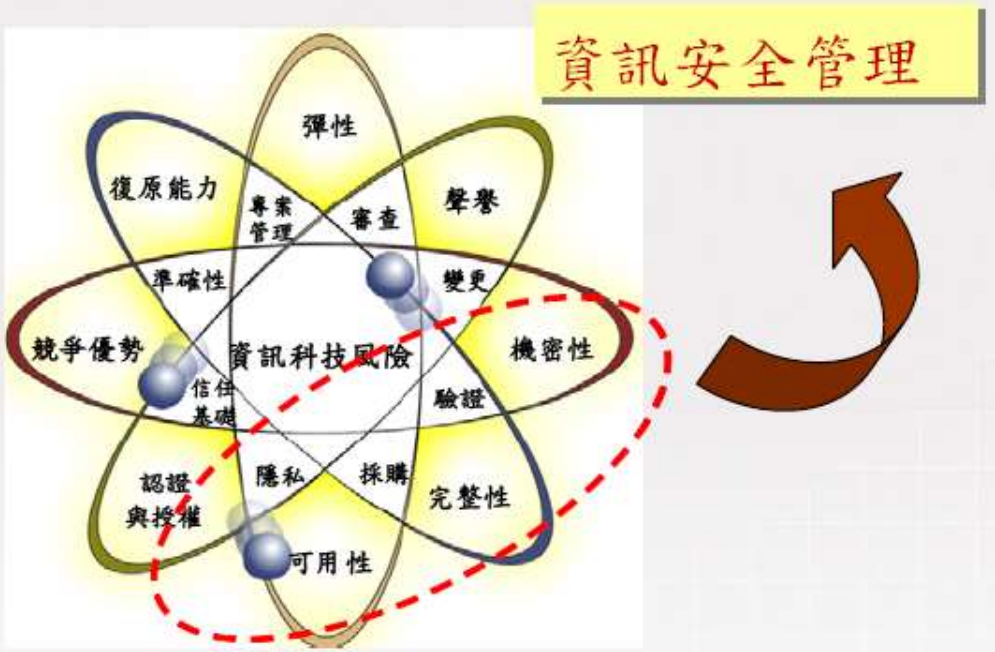
何謂風險

- 風險是具有破壞某種事物發生的可能性。
- 風險管理是識別、評估風險，並將這種風險減小到一個可以接受的程度。
  - 物理損壞。
  - 人為錯誤。
  - 設備故障。
  - 內部和外部攻擊。
  - 資訊誤用。
  - 資料遺失。
  - 應用程式出錯。



風險的種類

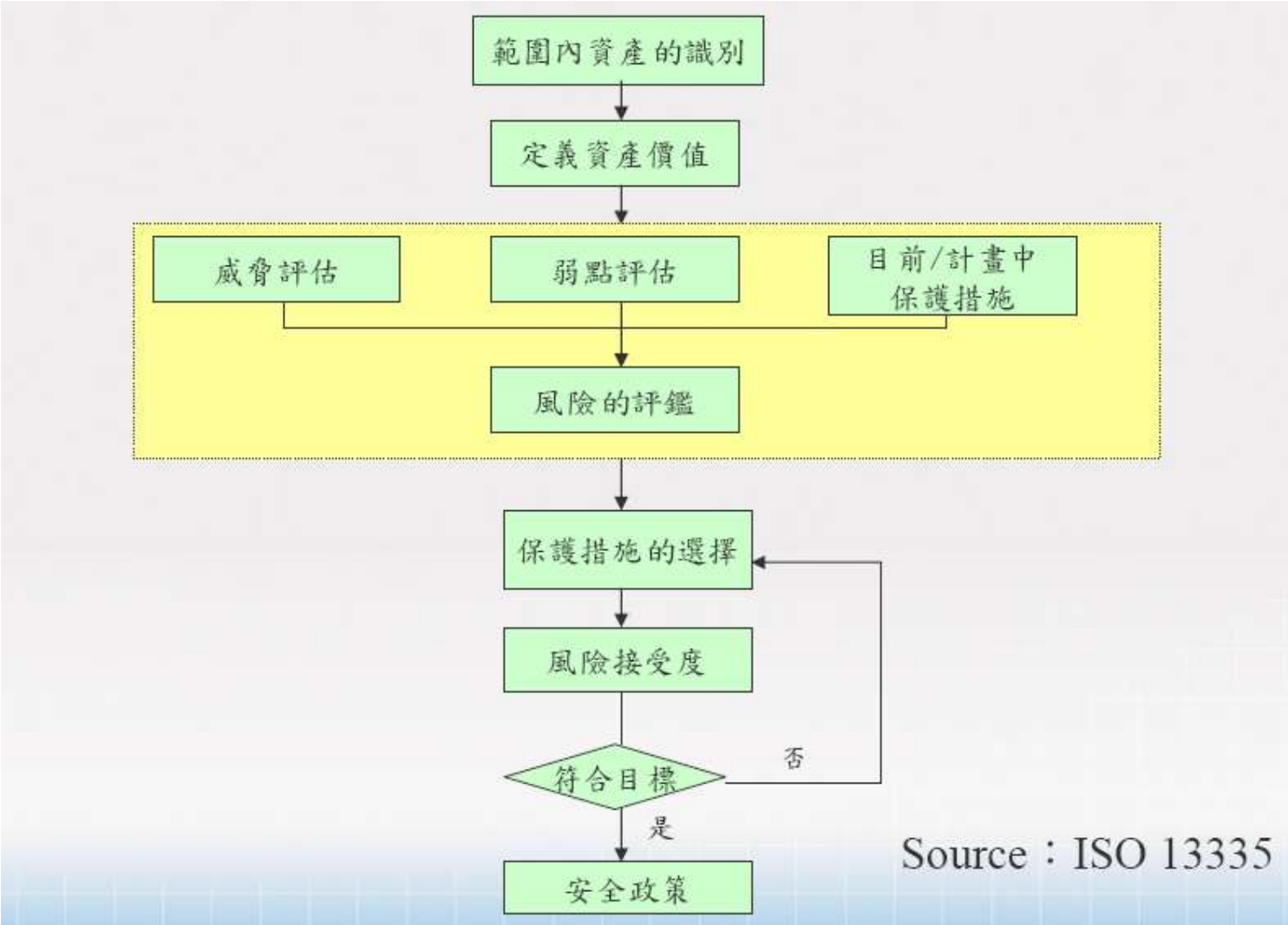

策略風險
營運風險
科技風險
財務風險
市場風險
作業風險


資訊安全管理
彈性
復原能力
專案管理
審查
擊潰
準確性
變更
競爭優勢
資訊科技風險
機密性
信任基礎
驗證
認證與授權
隱私
採購
完整性
可用性

- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - **風險管理流程**
  - 風險識別作業
  - 風險評鑑方法
  - 風險控管方式



風險管理流程


範圍內資產的識別
定義資產價值
威脅評估
弱點評估
目前/計畫中保護措施
風險的評鑑
保護措施的選擇
風險接受度
符合目標
否
是
安全政策
Source：ISO 13335

風險管理循環

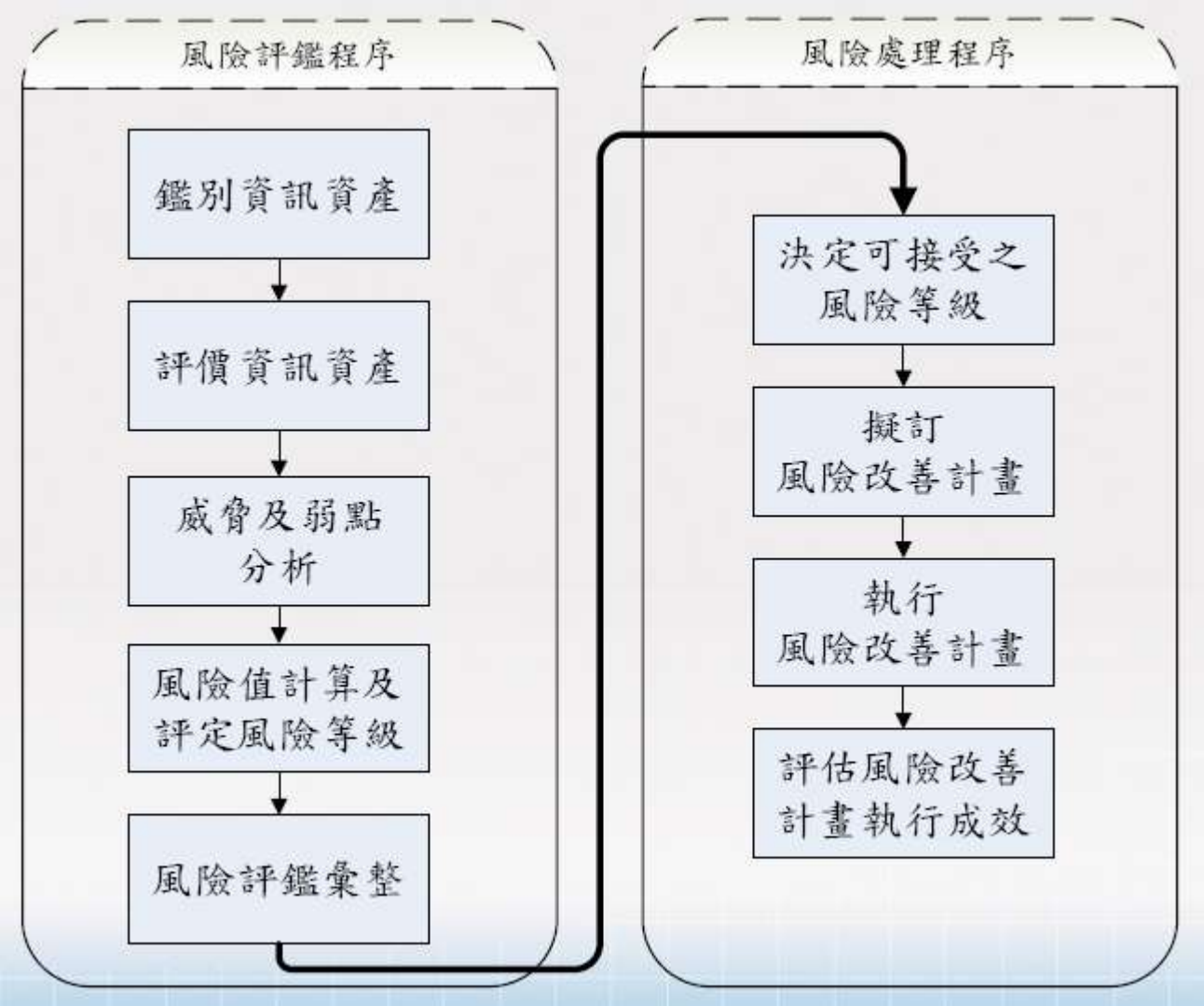

風險管理
選擇執行風險管理方式（避免、轉移、降低、接受）
辨識資產
由權責單位辨識重要資訊資產
風險評鑑
以ISO 27001與ISO 13335為基礎，辨識風險所在
定義價值
以機密性、完整性、可用性決定資訊資產之價值



- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - **風險識別作業**
  - 風險評鑑方法
  - 風險控管方式



風險評鑑與處理程序


風險評鑑程序
鑑別資訊資產
評價資訊資產
威脅及弱點分析
風險值計算及評定風險等級
風險評鑑彙整
風險處理程序
決定可接受之風險等級
擬訂風險改善計畫
執行風險改善計畫
評估風險改善計畫執行成效

威脅及弱點

- **威脅可能**對系統、組織或資產**造成一個有害的事件**。如
  - 天然災害：颱風、地震、水災及停電等，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，可能威脅到資訊資產的可用性及機密性。
- **弱點存在於資產本身，並不會造成傷害**。但如果沒有妥善管理，將促使威脅形成。如
  - 人員教育訓練不足。
  - 系統漏洞。



- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - 風險識別作業
  - **風險評鑑方法**
  - 風險控管方式



威脅、弱點與風險之間的關係

- 威脅利用弱點對資訊資產造成傷害。
- 風險= f【資產價值，威脅等級(發生之可能性)，弱點等級(受到威脅利用之容易度)】



威脅、弱點等級評估

- 依以下之標準評估各事件之威脅等級(發生之可能性)

評估標準	評估值
威脅發生之可能性為低	1
威脅發生之可能性為中	2
威脅發生之可能性為高	3

- 依以下之標準評估各事件之弱點等級(受到威脅利用之容易度)

評估標準	評估值
該弱點不容易被威脅利用	1
該弱點容易被威脅利用	2
該弱點非常容易被威脅利用	3



風險值的計算

- 資產價值=MAX (C，I，A)
  - 機密性、完整性、可用性，取最大值
- 風險之定義與評估
  - **風險值=(資訊資產價值x威脅等級x弱點等級)**
- 風險值：0~27



事件風險權值對照表

威脅等級 （發生之可能性）		低(1)			中(2)			高(3)		
弱點等級 （受到威脅利用之容易度）		低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	低(1)	中(2)	高(3)
資產價值	0	0	0	0	0	0	0	0	0	0
	1	1	2	3	2	4	6	3	6	9
	2	2	4	6	4	8	12	6	12	18
	3	3	6	9	6	12	18	9	18	27



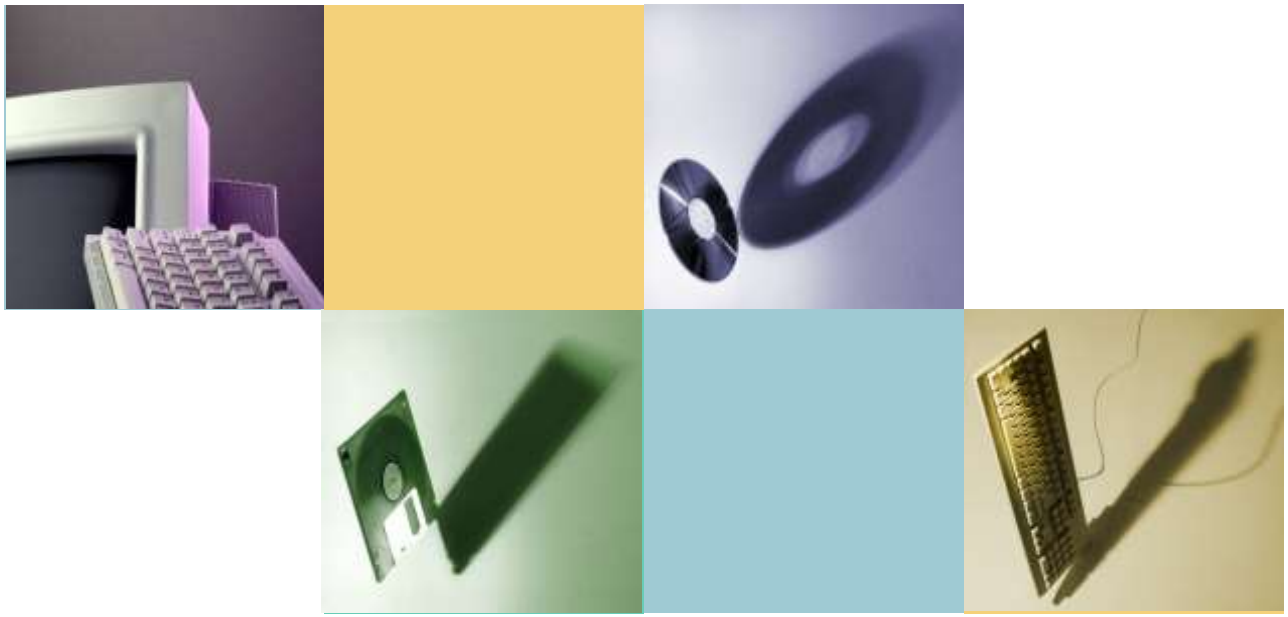
- 資訊資產評估
  - 資訊資產概論
  - 資訊資產清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理作業
  - 資產報廢及處理
- 風險評鑑
  - 風險概論
  - 風險管理流程
  - 風險識別作業
  - 風險評鑑方法
  - **風險控管方式**



風險控管原則與方法

- 辨識資產和它們面臨的威脅。
- 量化潛在威脅的影響。
- **計算風險**。
- 在風險影響和處理對策費用之間取得預算上的平衡，**決定組織可接受之風險值**。
- **高於可接受風險值者，優先控管或處理**。
- 選擇風險控管方式。
  - 避免。
  - 轉移。
  - 降低。
  - 接受。
- 建立及執行風險改善計畫。
- 建立適用性聲明書。
- 執行風險再評鑑。





THANKS !