資產盤點與風險管理

徐國鈞
崑山科技大學
HSU@ADM.KSU.EDU.TW

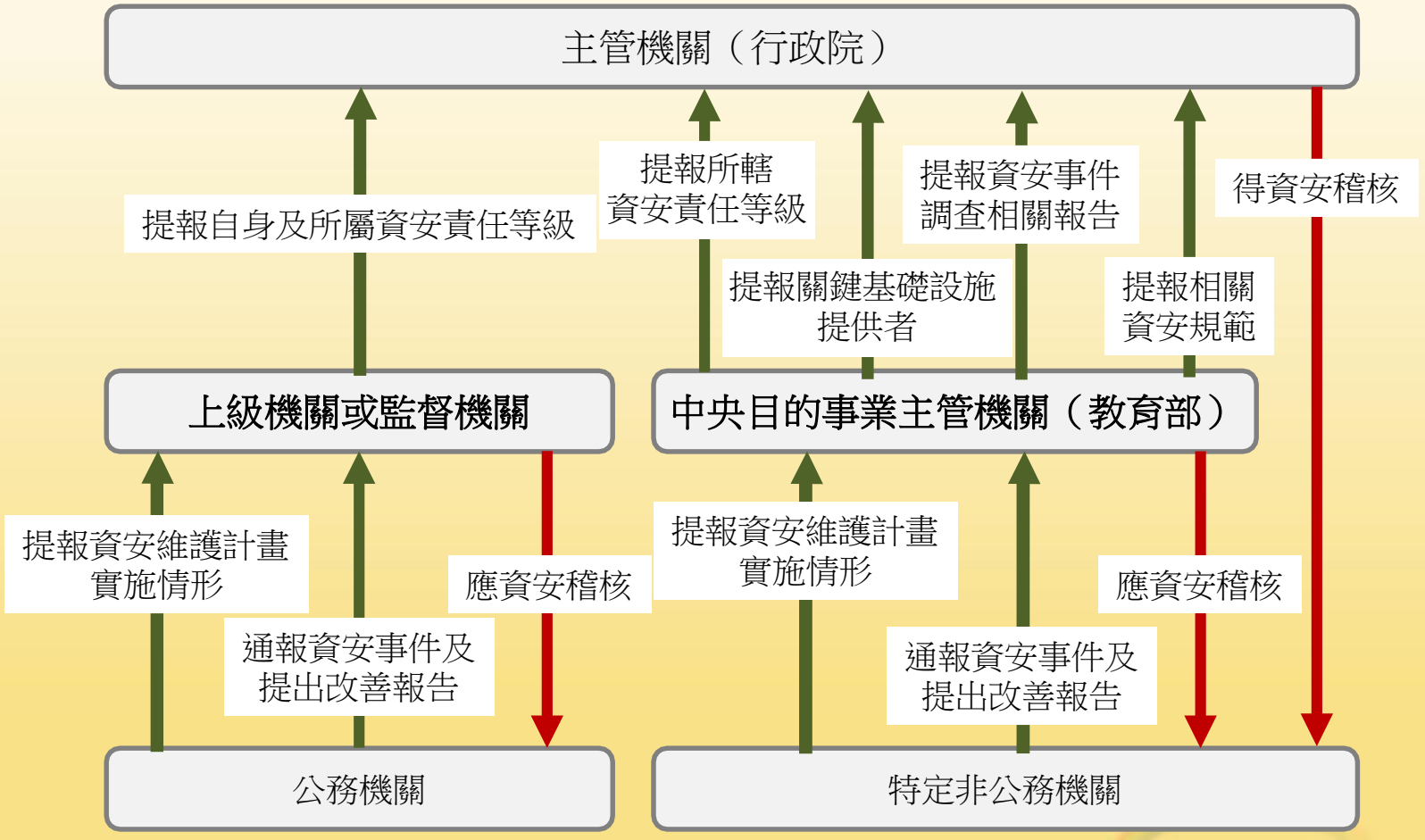
大綱

- 資訊資產盤點
- 資產清單與資產分類
- 資產價值識別
- 威脅、脆弱性與風險
- 風險識別
- 風險分析
- 風險評估
- 可接受風險與風險處理

法律規定

- 第 6 條
- 本法第十條、第十六條第二項及第十七條第一項所定資通安全維護計畫，應包括下列事項：
  - 六、資通系統及資訊之盤點，並標示核心資通系統及相關資產。
  - 七、資通安全風險評估。

角色與權責



- 設置資安長
- 訂定及實施資安維護計畫
- 訂定資安事件通報及應變機制

- 訂定及實施資安維護計畫
- 訂定資安事件通報及應變機制

5.

資訊資產盤點

- 資通安全維護計畫：
  - **柒、資訊及資通系統之盤點**
    - 至少包含資訊及資通系統之分類及盤點之程序，並應包含標示核心資通系統及相關資產之要求。
- 需清查盤點該資訊系統的所有資訊資產。
- 何謂資產？ 對組織有價值的任何事物。
- 資產受到破壞會影響業務進行、資訊系統運作，甚至造成中斷或癱瘓。
- 資產是單位的資源或產出，可以是有形或無形。

資訊資產蒐集與管理

將資訊資產依其特性
進行分類/群組

- 應維持資產清冊的正確性
- 設計資訊資產清冊的更新流程

依不同分類/群組進行不同管控
Ex ：核心重要設備必須建置備援
Ex：內部機密資料不得任意複製

資訊資產分類

8.

資產的分類

- 資訊資產分為**七大類**：
  - 人員（People / PE）：全體同仁、駐點人員、委外廠商及工讀生等。
  - 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。
  - 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。

資產的分類

- 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。

- 註：ISO 27002 7.1.1 資產分成實體資產、軟體資產、電子化資訊資產、書面文件、服務 及人員。

資訊資產清單

資產編號	資產種類	資產名稱	資產說明	權責單位	保管單位	風險擁有者	使用單位	存放位置	機密性	完整性	可用性	資訊資產價值

- 資產編號
- 資產種類
- 資產名稱
  - 簡單易辨認
- 資產說明
  - 簡單說明資產用途及相關資訊，例如規格、版本、數量等等
- 權責單位
- 保管單位
- 風險擁有者
- 使用單位
- 存放位置(機房、辦公室、異地)
- 營運衝擊分析
  - C　機密性
  - I　完整性
  - A　可用性
- 資產價值
  - 機密性、完整性及可用性三者中之最大值

資產管理角色

- **權責單位：**
  - 由組織指定的資訊資產擁有單位。
  - 註：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。
- **保管單位：**
  - 由組織指定的資訊資產保管單位。
- **風險擁有者：**
  - 由資訊資產負責人(單位主管)授權或擔任。
- **使用單位：**
  - 由組織授權的資訊資產使用單位。

資產清單-範例：全球資訊網

資產編號	資產種類	資產名稱	資產說明	權責單位	保管單位	風險擁有者	使用單位	存放位置
ISMS-HW-00001	硬體	全球資訊網伺服器	HP XXXXXXX	系統組	系統組	應總管	系統組	資訊機房
ISMS-HW-00002	硬體	NAS網路硬碟	IBM XXXXX	網路組	網路組	王管人	資訊處	資訊機房
ISMS-SW-00001	軟體	全球資訊網系統軟體	大大資訊網站系統	軟體組	軟體組	阮主管	全機關	軟體組
ISMS-SW-00002	軟體	MS SQL 資料庫系統	MS SQL 2012	軟體組	軟體組	阮主管	資訊處	軟體組
ISMS-PE-00001	人員	全球資訊網管理人員	負責管理全球資訊網	網路組	網路組	王管人	網路組	網路組
ISMS-PE-00002	人員	全球資訊網系統維護廠商	大大資訊	軟體組	軟體組	章主管	軟體組	大大資訊
ISMS-PE-00003	人員	NAS管理人員	負責管理NAS	網路組	網路組	王管人	網路組	網路組
ISMS-DA-00001	資料	全球資訊網網頁內容	全球資訊網網頁內容	軟體組	軟體組	阮主管	全機關	資訊機房
ISMS-DA-00002	資料	網站管理辦法	網站管理辦法107.11.11通過	軟體組	軟體組	阮主管	全機關	軟體組
ISMS-DA-00003	資料	網站原始程式	網站原始程式1.1版	軟體組	軟體組	阮主管	軟體組	軟體組

資產價值(營運衝擊分析評估)

- 將資產衝擊(價值）以機密性、完整性、可用性三個層面評估判斷
  - C(機密性)-資訊資產分級、資訊資產洩露傷害程度、人員業務性質等
  - I(完整性)-不完整造成損失影響的範圍、正確性及完整性的要求程度 、利害關係人權益影響的範圍等
  - A(可用性)-可忍受服務中斷時間長度、仰賴系統程度、仰賴員工程度等
- 評分標準
  - **資訊資產價值評估標準**
- 工具
  - **資訊資產清冊**

資產價值評估範例-人員類

人員類資訊資產-機密性評估標準

評估標準	數值
工作內容及處理之資料為公開之資訊。	1
工作內容及處理之資料為內部使用資訊，洩漏會對組織造成有形或無形的損害，此損害為組織可承受之範圍。	2
工作內容及處理之資料為限制使用資訊，洩漏後可能使組織安全或形象遭受明顯損害者。	3
工作內容及處理之資料為敏感或密級的資訊，洩漏後將引起組織安全或形象遭受重大的損失者。	4

人員類資訊資產-完整性評估標準

評估標準	數值
人員無法執行其工作職掌，不會對系統業務造成影響。	1
人員無法執行其工作職掌，影響單一系統業務運作。	2
人員無法執行其工作職掌，影響二個系統業務運作。	3
人員無法執行其工作職掌，影響三個(含)以上全部系統業務運作，甚至會造成業務終止。	4

人員類資訊資產-可用性評估標準

評估標準	數值
資訊資產容許 3 個工作天(含)以上未處理業務。	1
資訊資產容許 8 個工作小時(含)以上，未達 3 個工作天未處理業務。	2
資訊資產容許 4 個工作小時(含)以上，未達 8 個工作小時未處理業務。	3
資訊資產容許未達 4 個工作小時未處理業務。	4

資產價值評估範例-文件類、軟體類、通訊類、硬體類、資料類

文件類、軟體類、通訊類、硬體類、資料類資訊資產-機密性評估標準

評估標準	數值
資訊資產無特殊之機密性要求，可對外公開之資訊。	1
資訊資產僅供組織內部人員，或被授權之單位及人員使用，內容若洩漏會對組織造成有形或無形的損害，此損害為組織可承受之範圍。	2
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，內容若洩漏會影響組織聲譽或相關人員權益。	3
資訊資產為組織、主管機關或法律所規範之密級資訊，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，內容若洩漏會嚴重影響組織聲譽或相關人員權益。	4

文件類、軟體類、通訊類、硬體類、資料類資訊資產-完整性評估標準

評估標準	數值
資訊資產遭受未經授權的破壞或設定被竄改，不會對系統業務造成影響。	1
資訊資產遭受未經授權的破壞或設定被竄改，影響單一系統業務運作。	2
資訊資產遭受未經授權的破壞或設定被竄改，影響二個系統業務運作。	3
資訊資產遭受未經授權的破壞或設定被竄改，影響三個(含)以上業務運作，甚至會造成業務終止。	4

文件類、軟體類、通訊類、硬體類、資料類資訊資產-可用性評估標準

評估標準	數值
資訊資產容許失效 3 個工作天(含)以上。	1
資訊資產容許失效 8 個工作小時(含)以上，未達 3 個工作天。	2
資訊資產容許失效 4 個工作小時(含)以上，未達 8 個工作小時。	3
資訊資產容許失效未達 4 個工作小時。	4

資產價值評估範例-環境類

環境類資訊資產-機密性評估標準

評估標準	數值
資訊資產為可公開設施。	1
資訊資產僅供組織內部人員，或被授權之單位及人員使用，公開會對組織造成有形或無形的損害，此損害為組織可承受之範圍。	2
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，公開可能使組織安全或形象遭受明顯損害者。	3
資訊資產為組織、主管機關或法律所規範之機密資訊，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，公開將引起組織安全或形象遭受重大的損失者。	4

環境類資訊資產-完整性評估標準

評估標準	數值
資訊資產遭受損害或破壞後，不會對系統業務造成影響。	1
資訊資產遭受損害或破壞後，影響單一系統業務運作。	2
資訊資產遭受損害或破壞後，影響二個系統業務運作。	3

環境類資訊資產-可用性評估標準

評估標準	數值
資訊資產容許 3 個工作天(含)以上無法使用。	1
資訊資產容許 8 個工作小時(含)以上，未達 3 個工作天無法使用。	2
資訊資產容許 4 個工作小時(含)以上，未達 8 個工作小時無法使用。	3
資訊資產容許未達 4 個工作小時無法使用。	4

資產價值-範例：全球資訊網

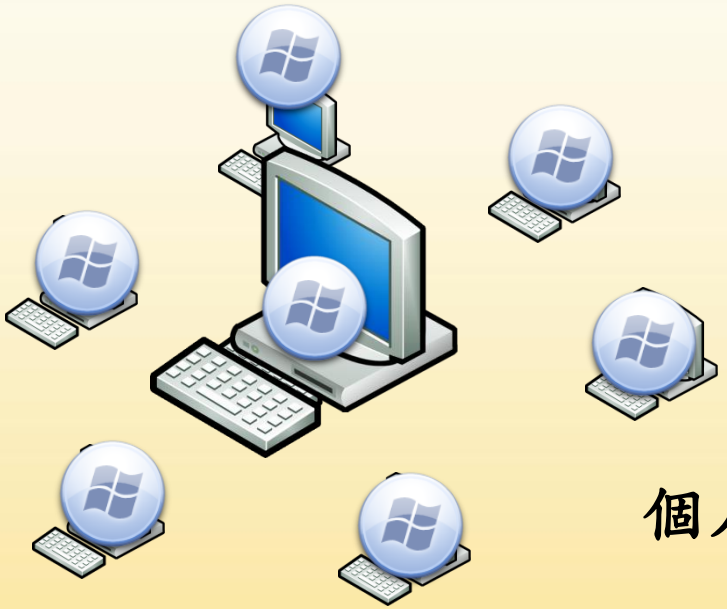
資產編號	資產種類	資產名稱	資產說明	機密性	完整性	可用性	資訊資產價值
ISMS-HW-00001	硬體	全球資訊網伺服器	HP XXXXXXX	1	3	3	3
ISMS-HW-00002	硬體	NAS網路硬碟	IBM XXXXX	3	3	3	3
ISMS-SW-00001	軟體	全球資訊網系統軟體	大大資訊網站系統	1	3	3	3
ISMS-SW-00002	軟體	MS SQL 資料庫系統	MS SQL 2012	1	2	2	2
ISMS-PE-00001	人員	全球資訊網管理人員	負責管理全球資訊網	1	3	2	3
ISMS-PE-00002	人員	全球資訊網系統維護廠商	大大資訊	1	3	1	3
ISMS-PE-00003	人員	NAS管理人員	負責管理NAS	3	3	3	3
ISMS-DA-00001	資料	全球資訊網網頁內容	全球資訊網網頁內容	1	3	3	3
ISMS-DA-00002	資料	網站管理辦法	網站管理辦法107.11.11通過	1	1	1	1
ISMS-DA-00003	資料	網站原始程式	網站原始程式1.1版	2	3	3	3

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。
- 群組原因
  - 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避免遺漏重要資產。
  - **針對群組資訊資產進行風險評鑑。**
- 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。
- 資產群組及命名原則
  - **資訊資產群組及命名原則**
- 工具
  - **資訊資產清冊**

資訊資產群組化範例

Windows 10 作業系統



個人電腦

合約、專案檔案文件

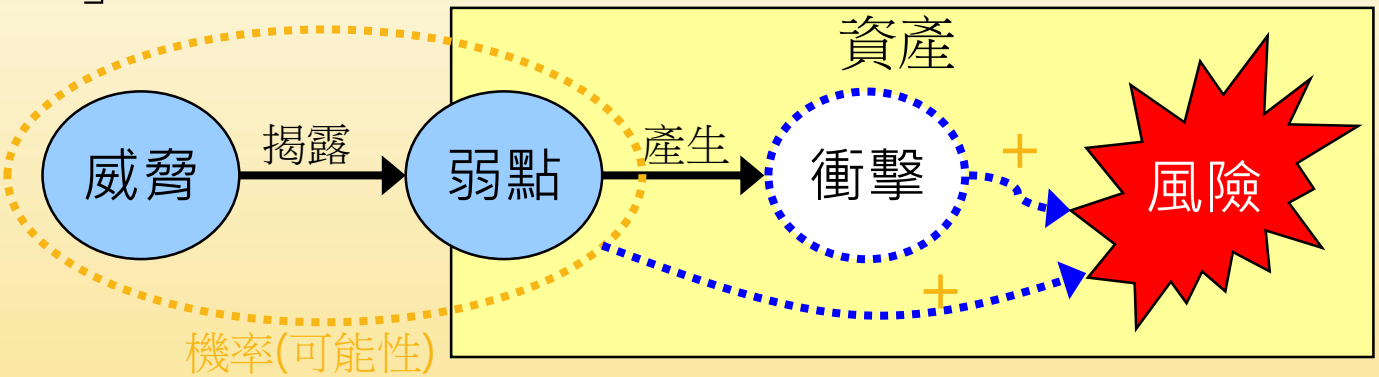
辦公室商用軟體

威脅、脆弱性與風險

- 資產
  - 識別資產並鑑定其價值。
- 威脅
  - 利用資產存在的弱點，對資產造成傷害。
- 弱點
  - 包括能夠被利用並可導致不預期結果的系統脆弱性（它們可能會讓威脅造成傷害的機會）
- 衝擊(風險)程度
  - 依據資產對潛在攻擊者的誘因如何、威脅發生的可能性、以及弱點可被利用的容易度而定。

風險的定義

- 所謂「風險」是指「威脅」利用其相對應「脆弱性」直接或間接造成組織一個或一群「資訊資產」受到「衝擊(Impact)」的「可能性」

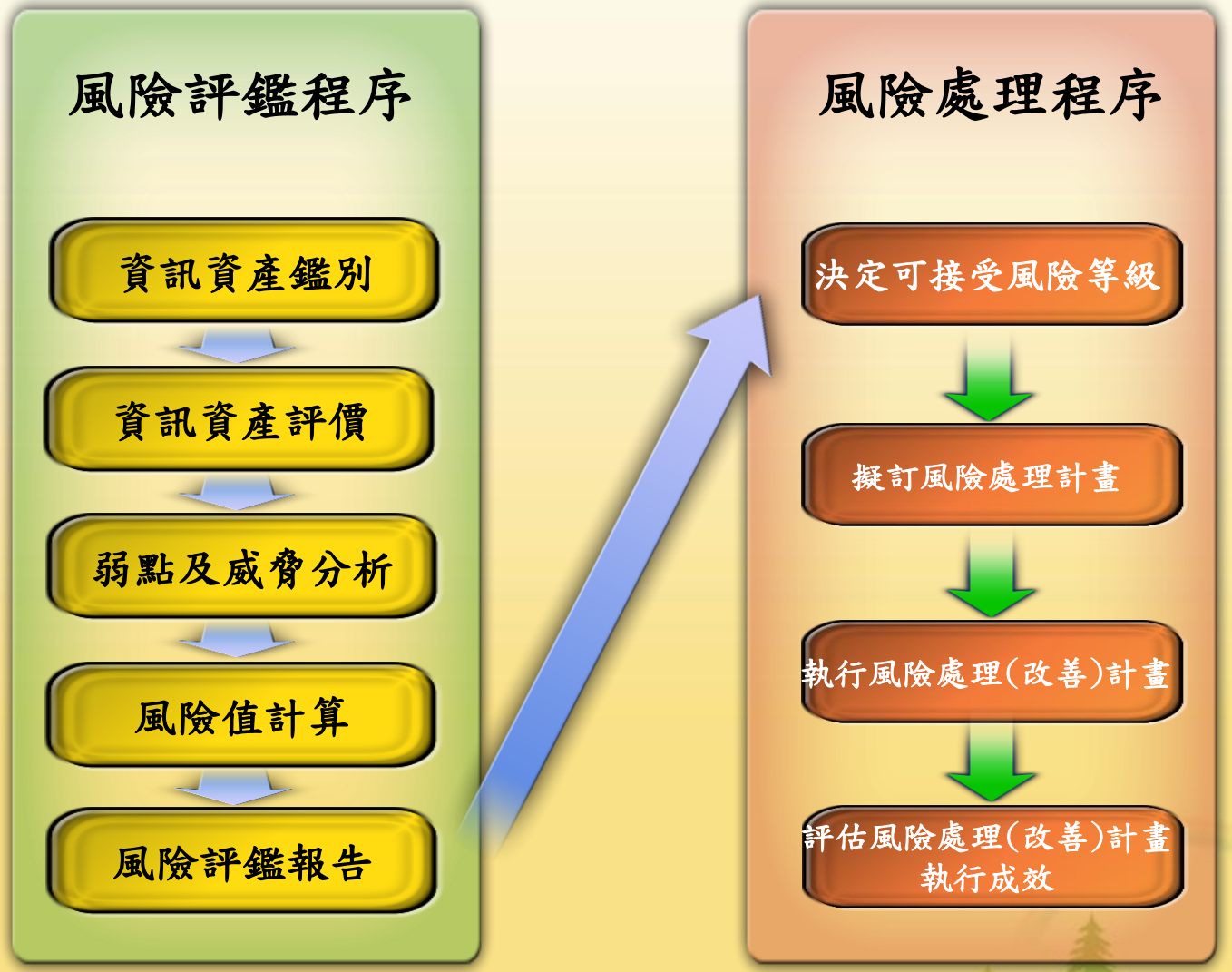


- 風險透過「衝擊」與其「可能性」兩個因素的結合來定義其影響程度或損害程度
- 風險管理的目標
  - 在最低的防護成本投入下獲得最優化的安全性(最優化非最強固，而是最合適)

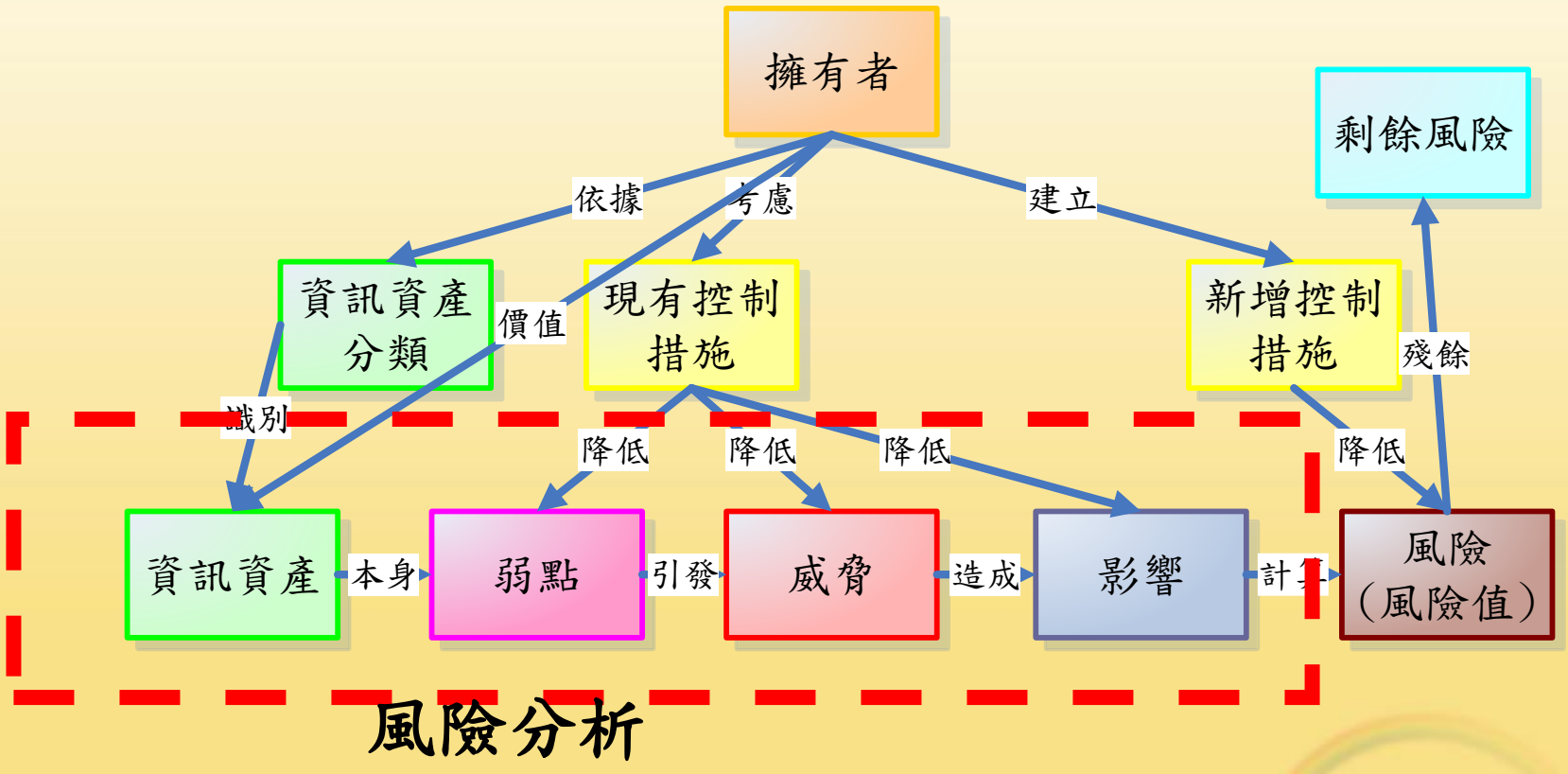
威脅、脆弱性與風險-範例

- **小陳沒有上鎖的習慣，每次出門只是將門帶上，造成家裡遭小偷光顧，總共損失珠寶、美金共計168萬元。**
  - 風險=珠寶、現金(台幣、美金)遭竊
  - 資產=珠寶、現金(台幣、美金)
  - 威脅=小偷光顧
  - 弱點=沒有上鎖的習慣
  - 影響=生活、家人....

風險管理程序


風險評鑑程序
資訊資產鑑別
資訊資產評價
弱點及威脅分析
風險值計算
風險評鑑報告
風險處理程序
決定可接受風險等級
擬訂風險處理計畫
執行風險處理(改善)計畫
評估風險處理(改善)計畫執行成效

風險分析


擁有者
剩餘風險
依據
考慮
建立
資訊資產分類
價值
現有控制措施
新增控制措施
殘餘
識別
降低
降低
降低
降低
資訊資產
本身
弱點
引發
威脅
造成
影響
計算
風險（風險值）
風險分析

風險分析的方式

- **組織執行的方式(以ISO27001:2013)**
  - 由評鑑人員進行專業判斷(主觀判斷)。
  - 以會議的方式進行討論(較為客觀)。
- **外單位常用的方式：**
  - 觀察-觀察實體環境、作業流程。
  - 訪談-詢問資訊資產負責人或管理人。
  - 檢視-相關文件(安全事件的報告、系統稽核及安全檢查的結果)、網路架構圖。
  - 測試及驗證-針對控制或作業的程序及結果進行正確性確認。
  - 問卷-透過問卷瞭解眾人的意向。
  - 其他-外部安全事故的經驗、資訊安全事件通報、資訊安全相關論壇。

風險分析流程

- 風險分析(Risk Analysis)-系統化的使用資訊以鑑別資源與估計風險。

鑑別資訊資產(分類或群組)的弱點

↓

鑑別資訊資產(分類或群組)因弱點而引起的威脅

↓

評估該項威脅發生時對資訊資產(分類或群組)影響的層面

風險分析結果

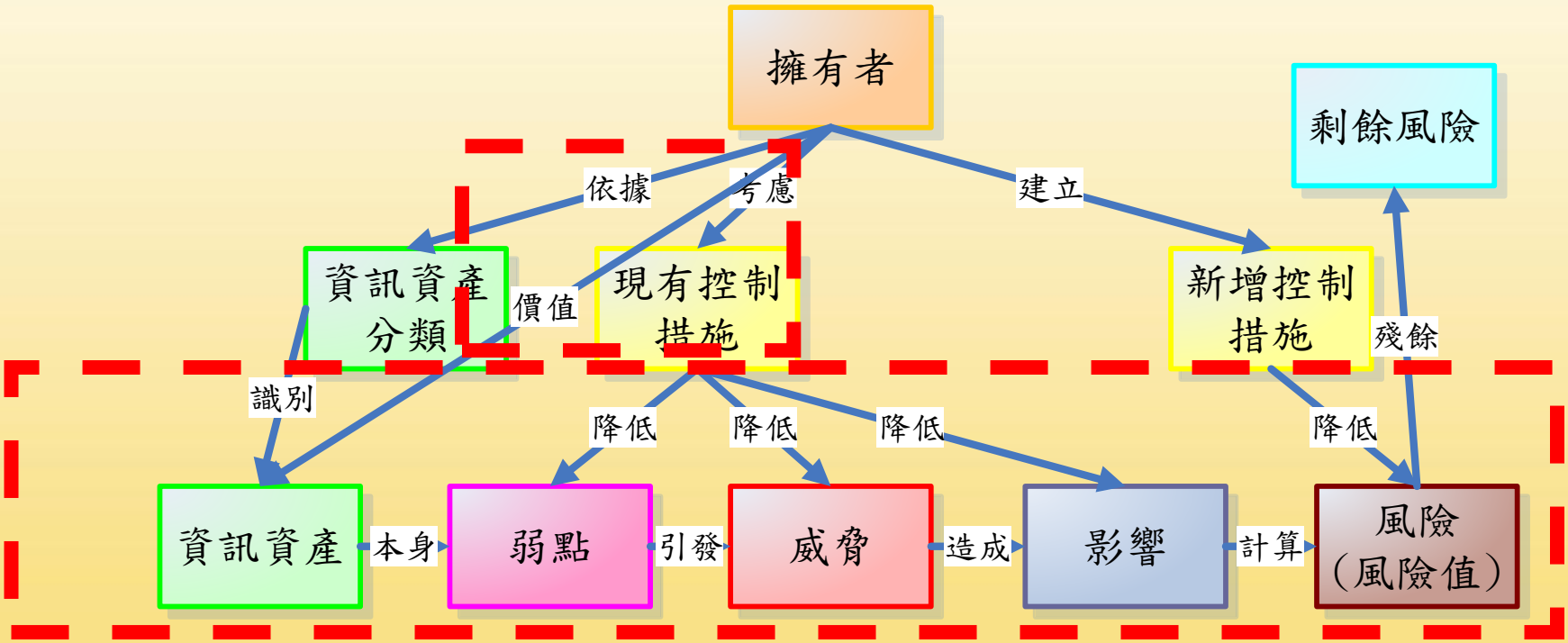
[redacted]

威脅及弱點評估表

文件編號：	[redacted]	發行日期：		版		機密等級：□公開 ■一般 □限閱 □敏感					
資產名稱：		資產編號：		價值：		C		I		A	
權責單位：		保管單位/保管人：		使用單位/使用者：							
資產類別：	環境(EV)	資產說明：									

威脅	弱點	威脅等級				弱點等級				風險值
		低(1)	中(2)	高(3)	不適用	低(1)	中(2)	高(3)	不適用	
風險類別:環境										
火災	人員安全訓練不足									
	缺乏建築物、門、窗等物質的保護									
	儲存易燃物									
	環境控制系統失效									
失竊	建築物、房間的物質進出控制的不足或不小心使用									
	缺乏安全警覺									
	缺乏建築物、門、窗等物質的保護									
	識別與認證機制的不足									
地震	缺乏建築物、門、窗等物質的保護									
[redacted]	[redacted]									

風險評估


擁有者
剩餘風險
依據
考慮
建立
資訊資產分類
價值
現有控制措施
新增控制措施
殘餘
識別
降低
降低
降低
降低
資訊資產
本身
弱點
引發
威脅
造成
影響
計算
風險（風險值）

風險評估

風險評估流程

- 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

評估弱點發生的脆弱度(被威脅利用的機率)
【考量現有管理機制】

↓

評估威脅發生的機率
【考量現有控制措施】

↓

計算資訊資產的風險值

資訊資產弱點

- 定義
  - 資訊安全的漏洞（弱點），其本身不會造成傷害，但是可能造成一種或多種威脅來利用，對資產造成影響
- 評分標準
  - 弱點的等級對應表
- 工具
  - 威脅及弱點評估表

弱點遭利用等級評分-範例

- 評估弱點被威脅所利用的程度

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

弱點等級對應表

資訊資產威脅

- 定義
  - 可能會對系統或組織及其資訊資產造成傷害的事件，資產通常都會面臨許多不同的威脅：威脅必須利用資產的弱點才能對資產造成傷害
- 評分標準
  - 威脅的等級對應表
- 工具
  - 威脅及弱點評估表

威脅發生機率評分-範例

- **判斷該威脅發生的可能性**

評估標準	等級	評估值
威脅發生之可能性為低 例-每年發生 5 次以下或 0~5 次/年	低	1
威脅發生之可能性為中 例-每季發生 3 次以上或 12 次/年以上	中	2
威脅發生之可能性為高 例-每月發生 2 次以上或 24 次/年以上	高	3

事件發生機率/等級對應表

弱點與威脅的資訊來源

- 資訊資產的威脅及弱點可由下列項目得知：
  - 安全事件的報告
  - 系統稽核及安全檢查的結果
  - 觀察工作流程
  - 與資訊資產負責人或保管人訪談
  - 外部安全事件的經驗

風險計算公式-範例

- 風險值的計算
  - 評估事件發生機率及影響程度後，計算出風險值。
- 資產價值=**MAX (C, I, A)**
  - 機密性、完整性、可用性，取最大值
- 風險值=（**資訊資產價值×威脅等級×弱點等級**）
- 風險值：1~36
- 工具
  - 事件風險值對照表

事件風險權值對照表-範例

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	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
	4	4	8	12	8	16	24	12	24	36

資訊資產類別與數量統計-範例

資產類別/資產價值	1	2	3	4	總計
通訊	0	1	2	2	5
資料	6	5	6	4	21
文件	1	2	1	0	4
環境	0	5	2	3	10
硬體	0	5	14	16	35
人員	0	2	6	1	9
軟體	3	6	6	8	23
總計	10	26	37	34	107

資訊資產類別與數量統計表

資訊資產風險值分佈-範例

風險值	1	2	3	4	6	8	9	12	16	18	24	27	36	總計
通訊	0	1	1	1	1	1	0	0	0	0	0	0	0	5
資料	6	4	2	1	3	3	1	1	0	0	0	0	0	21
文件	0	3	1	0	0	0	0	0	0	0	0	0	0	4
環境	0	3	0	1	2	3	0	0	1	0	0	0	0	10
硬體	0	0	0	3	10	13	0	9	0	0	0	0	0	35
人員	0	1	6	1	0	1	0	0	0	0	0	0	0	9
軟體	3	3	2	5	3	6	0	1	0	0	0	0	0	23
總計	9	15	12	12	19	27	1	11	1	0	0	0	0	107

資訊資產綜合風險值統計表

資訊資產風險值檢查、確認

- 組織重要資產是否有被凸顯？
- 作業或流程重要資產是否有被凸顯？
- 機密性極高是否有被凸顯？
- 完整性極高是否有被凸顯？
- 可用性極高是否有被凸顯？
- 風險值極高？
- 風險值極低？

是否合理、可以解釋？

風險接受準則

- 用途
  - 用來判斷風險是否可以接受或必須要進行處理的原則，例如：
    - 可接受風險的評估原則
- 通常依據組織政策、目標及業務關係來定義可接受或不可接受的狀況與條件
- 可參考接受的原因
  - 風險處理成本高過損失
  - 有能力處理相關安全事故
  - 尚無有效處理風險的技術

- 可接受風險的評估原則：
  - 普級風險且衝擊類型非屬人員生命與法律規範相關
  - 中級風險且衝擊類型屬可用性之風險
  - 凡與人員生命相關之衝擊所產生之風險一律不得接受
  - 凡與法律與規範相關之衝擊類型一律不得接受

可接受風險值-範例

- 方法一： 資產價值、弱點及威脅之組合
  - 決定可接受風險值原因：(4x2x2，高價值資產不允許等級中等以上之弱點及威脅，即風險值為16) 。故風險評鑑作業之可接受風險值建議為12 。
- 方法二： 80/20法則
  - 決定可接受風險值原因：係以採80/20法則，本次取資訊資產風險值最高(16)前二十，故風險評鑑作業之可接受風險值建議為12 。
    - 風險值為12(不含)以上為高風險值。
    - 各項資訊資產風險值高於可接受風險值12以上者，將於「風險改善計畫表」中提出風險控管之建議方案。

高風險值資訊資產分佈-範例

風險值	16	18	24	27	36	總計
通訊	0	0	0	0	0	0
資料	0	0	0	0	0	0
文件	0	0	0	0	0	0
環境	1	0	0	0	0	1
硬體	0	0	0	0	0	0
人員	0	0	0	0	0	0
軟體	0	0	0	0	0	0
總計	1	0	0	0	0	1

資訊資產之風險值高於12（不包含12）

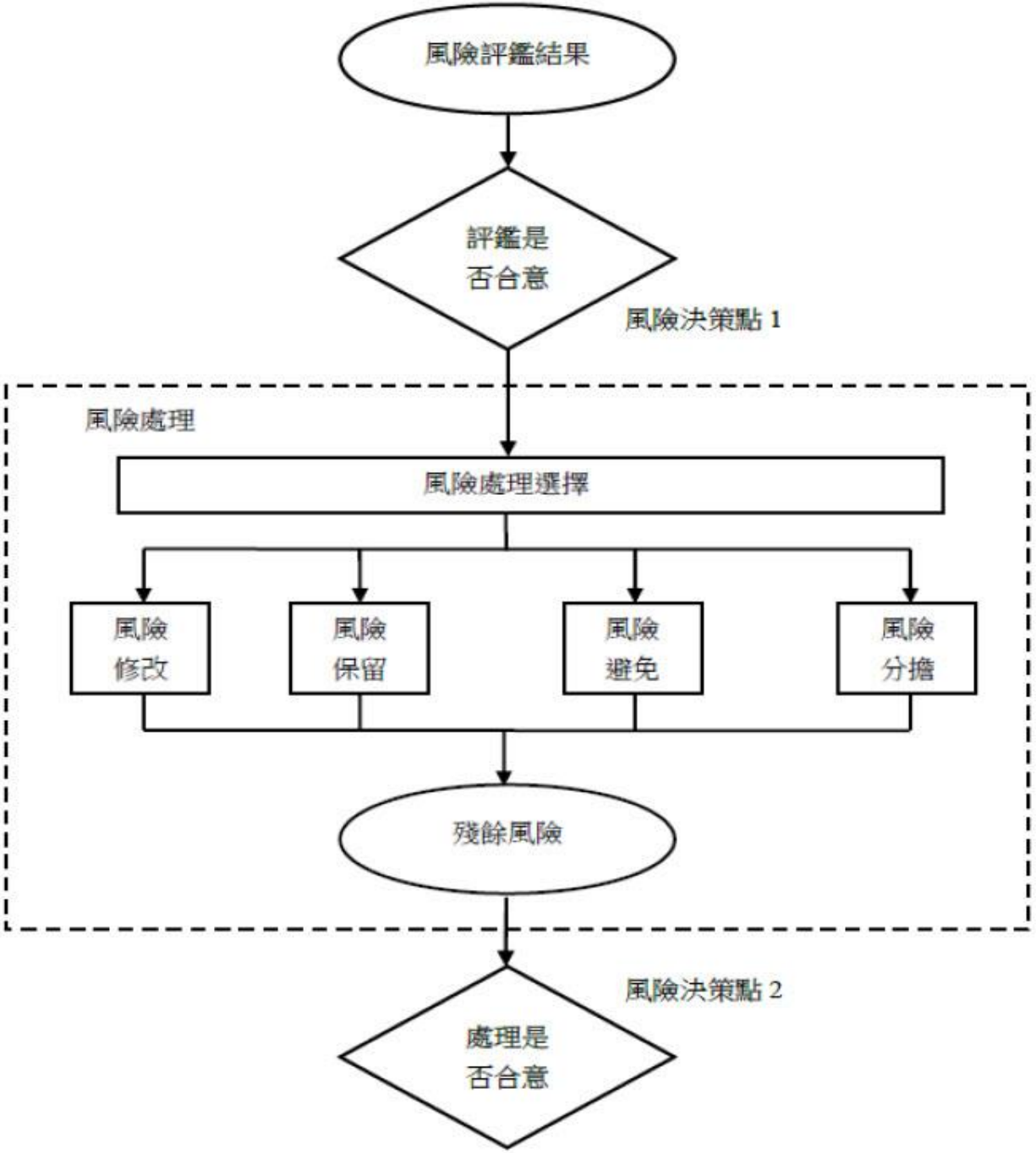
風險控管方法

- 選擇風險控管方式
  - 接受
  - 降低
  - 轉移
  - 避免

風險處理型式

- 接受風險
  - 符合組織的政策與風險接受準則，則知悉且客觀地接受風險。
- **降低風險**
  - **參考標準選擇適當之控制措施以降低風險。**
  - **藉由加強各項作業之內控以降低風險發生之機會。**
- 轉移風險
  - 轉移相關之營運風險至他者，例如：承保商、供應商。
- 避免風險
  - 修改作業方式或採用技術以避開風險。
  - 經由政策或標準以禁止從事高風險活動或使用高風險資訊資產。

風險處理活動


風險評鑑結果
評鑑是
否合意
風險決策點 1
風險處理
風險處理選擇
風險
修改
風險
保留
風險
避免
風險
分擔
殘餘風險
風險決策點 2
處理是
否合意

風險評鑑彙整表-範例

項次	資產編號	資產類別	資產名稱	資產說明	權責單位	資產價值	風險事件		風險值
							威脅	弱點	
1	ISMS-EV-00009	環境	資訊機房	網路與伺服器設備空間	網路組	4	火災	消防設施的不足或缺乏消防器材的保護	16

風險再評鑑				
資產價值	威脅等級	弱點等級	風險值	風險擁有者確認

風險改善計畫表-範例

- 依據資訊資產風險評估的結果，對於超出組織風險值可接受程度之風險，進行改善與處理。

教育體系資通安全暨個人資料管理規範或ISO 27001控制目標	現況說明	風險改善建議措施	教育體系資通安全暨個人資料管理規範或ISO 27001條文
A.11 實體及環境安全	目前資訊機房為手持滅火器，當火災或其他不可抗力因素發生時，無法即時處理。	建議規劃經費及安裝排程，增購消防設備，以降低其現況所產生之風險。	A11.1.4防範外部及環境威脅 A11.2.1設備安置及保護

建議權責單位	預計改善時間	實際完成時間	與高風險資產之風險評估彙整表對照	風險擁有者確認
網路組	108.12.31		1	

風險評鑑報告

- 風險評鑑處理程序
- 相關評量尺度
- 風險評鑑工作紀錄
- 可接受風險等級(值)

Thanks for your Attention

Thanks for your Attention

Thanks for your Attention

Thanks for your Attention

Q & A