資安風險管理
與
資產盤點探討

周冠吉

大綱

- **資產清查、評估與管理**
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

大綱

- **資產清查、評估與管理**
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

基礎觀念

- 甚麼是資產？
  - 對組織有價值的任何事物。
- 甚麼是資訊？
  - 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

- 不只局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

資訊安全4大原則

- 機密性（Confidentiality）：

  確保只有經授權的人才可以取得資訊，避免資訊洩漏。

- 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，並使用相關的資產。

- 適法性（Compliance）

  需遵循任何法律、法令、法規或契約義務，以及組織內部規章之要求。

ISMS目的在於保護資訊資產的機密性、完整性、可用性與適法性。（風險說明）

練習：

- 學校有哪些資產?

  建築物、電腦、伺服器、監視器、桌椅、校務系統、除草機、隨身碟、會議記錄、人員、家長

- 學校有哪些資訊?

  系統紀錄(電腦、伺服器)、監視器紀錄、備份檔案、教育訓練影片、錄音資料、家長的建議、會議記錄、簽到表、公告資料

大綱

- **資產清查、評估與管理**
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

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。

資產管理角色(續)

- 單位主管
  - 覆核該單位所編列整理屬於資訊安全管理系統範圍內之資訊資產項目。
  - 覆核風險評鑑結果之合理性。
- 資訊資產保管人
  - 保管人係指對於該資訊資產須盡保管、保護之義務與責任者。
  - 編列整理其使用、保管之資訊資產項目並鑑別其價值及安全需求。
  - 對所保管之資訊資產進行風險評鑑。
- 文件管理員
  - 負責資訊資產風險評鑑之相關表單彙整與保存。

建立資產清單

- 權責單位應清點及鑑別所管轄之資訊資產，並建立「資訊資產清單(冊)(或資訊資產評鑑表)」。
- 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(冊)由各權責單位提供，再由指定單位負責彙整，並陳報至「機關的資訊安全組織」，進行檢視與審查，以確保清單之完整性。
- 近期政府重點盤查中國大陸廠牌資通訊設備要列冊管理

資訊資產清單範例

文件安全等級：□一般 ■敏感 □機密　　流水號__110-001__

新北市 000000 國小
資訊資產評鑑表

單位：0000　　填表人：0000　　填表日期：110 年 01 月 03 日

業務流程	資訊資產名稱	數量	資訊資產類別	使用人（註一）	保管人（註二）	放置地點	機密性	完整性	可用性	適法性	資訊資產價值	資訊資產安全等級（註三）	潛在風險事件	發生機率	衝擊程度	總風險值	風險等級
網路系統連線服務	核心網路交換器	1	支援資產-實體設備類	王館仁	李寶瑄	資訊機房	2	2	3	2	9	高	組態設定錯誤	1	3	27	低
校務資訊系統作業	校務系統	1	支援資產-資訊系統類	開伐昇	李寶瑄	資訊機房	2	3	3	2	10	高	資料遭竄改	2	3	60	中

資產管理角色

大綱

- **資產清查、評估與管理**
  - 基礎觀念
  - 資產清查清單
  - **資產分類分級**
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- 風險評估、處理與管理
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

資訊資產分級

- 各類資訊資產機密等級(紀錄安全等級)分為3級：
  - 一般：無特殊之機密性要求，可對外公開之資訊。
  - 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。

建議：機關在自訂資訊資產分級時，不要同時存在【密】與【機密】!!

資訊資產分級(續)

資訊資產分級

新北市政府教育局

文件安全等級：□一般 ■敏感 □機密

資訊安全管理文件

流水號__110-001__

新北市政府教育局
資訊資產評鑑表

單位：0000　　填表人：0000　　填表日期：110 年 01 月 03 日

業務流程	資訊資產名稱	數量	資訊資產類別	使用人（註一）	保管人（註二）	放置地點	機密性	完整性	可用性	適法性	資訊資產價值	資訊資產安全等級（註三）	潛在風險事件	發生機率	衝擊程度	總風險值	風險等級
網路系統連線服務	核心網路交換器	1	支援資產-實體設備類	王館仁	李寶瑄	資訊機房	2	2	3	2	9	高	組態設定錯誤	1	3	27	低
校務資訊系統作業	校務系統	1	支援資產-資訊系統類	開伐昇	李寶瑄	資訊機房	2	3	3	2	10	高	資料遭竄改	2	3	60	中高

大綱

- **資產清查、評估與管理**
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - **資產價值鑑別**
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

資訊資產分類

- 主要資產
  - 業務流程與活動，例如：
    - ✓流程喪失或降低服務等級將使組織不能執行其任務
    - ✓包含機密流程或涉及私有技術的流程
    - ✓若修改流程將大幅影響組織任務的完成
    - ✓對組織遵循合約、法令法規要求是必要的流程
- 支援性資產
  - 實體設備類
  - 資訊系統(資訊紀錄)類
  - 人員類
  - 服務類
  - 工作區域類

資訊資產分類(續)

文件安全等級：□一般 ■敏感 □機密　　流水號__110-001__

新北市 000000 國小
資訊資產評鑑表

單位：0000　　填表人：0000　　填表日期：110 年 01 月 03 日

業務流程	資訊資產名稱	數量	資訊資產類別	使用人（註一）	保管人（註二）	放置地點	機密性	完整性	可用性	適法性	資訊資產價值	資訊資產安全等級（註三）	潛在風險事件	發生機率	衝擊程度	總風險值	風險等級
網路系統連線服務	核心網路交換器	1	支援資產-實體設備類	王館仁	李寶瑄	資訊機房	2	2	3	2	9	高	組態設定錯誤	1	3	27	低
校務資訊系統作業	校務系統	1	支援資產-資訊系統類	開伐昇	李寶瑄	資訊機房	2	3	3	2	10	高	資料遭竄改	2	3	60	中

資訊資產
類別

資訊資產價值鑑別

- 資訊資產之價值係藉由評估其**機密性**（Confidentiality）、**完整性**（Integrity）、**可用性**（Availability）及**適法性**（Compliance）遭受破壞對自身機關造成之衝擊來判定其價值。

資訊資產價值鑑別(續)

- 以資產之機密性(C)、完整性(I)、可用性(A)與適法性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。
  - 適法性(Com)：遵循法令規範要求。

資訊資產價值鑑別_定義判斷標準

評分 / 類型	0	1	2	3
機密性	無此特性或可公開。	僅供本局內部人員使用。	僅供業務相關人員存取。	具特殊權限人員方可存取。
完整性	無此特性或不影響本局運作。	將造成部份業務運作效率降低。	將造成部份業務運作停頓。	將造成全部業務運作停頓。
可用性	無此特性或最大可容忍中斷時間5天以上。	最大可容忍中斷時間3天以上，5天以下。	最大可容忍中斷時間1天以上，3天以下。	最大可容忍中斷時間1天以內。
適法性	無此特性或不影響本局運作。	須符合本局或市府內部規定的要求。	須符合行政法規（如：國家資通安全會報等）或外部合約規範的要求。	須符合國家法律（如：個人資料保護法、著作權法等）規範的要求。

資訊價值鑑別(續)

資訊資產
價值鑑別

文件安全等級：□一般 ■敏感 □機密　　流水號__110-001__

新北市 000000 國小
資訊資產評鑑表

單位：0000　　填表人：0000　　填表日期：110 年 01 月 03 日

業務流程	資訊資產名稱	數量	資訊資產類別	使用人（註一）	保管人（註二）	放置地點	機密性	完整性	可用性	適法性	資訊資產價值	資訊資產安全等級（註三）	潛在風險事件	發生機率	衝擊程度	總風險值	風險等級
網路系統連線服務	核心網路交換器	1	支援資產-實體設備類	王館仁	李寶瑄	資訊機房	2	2	3	2	9	高	組態設定錯誤	1	3	27	低
校務資訊系統作業	校務系統	1	支援資產-資訊系統類	開伐昇	李寶瑄	資訊機房	2	3	3	2	10	高	資料遭竄改	2	3	60	中

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。

資訊資產群組化(續)

- 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)

資訊資產群組

資訊資產
價值鑑別

密等：□一般 ■敏感 □機密

00 市 0000 國小中

資訊資產評鑑表 (Ctrl)

單位：0000　　填表人：0000　　填表日期：110 年 01 月 03 日

業務流程	資訊資產名稱	數量	資訊資產類別	使用人（註一）	保管人（註二）	放置地點	機密性	完整性	可用性	適法性	資訊資產價值	資訊資產安全等級（註三）	潛在風險事件	發生機率	衝擊程度	總風險值	風險等級
網路系統連線服務	(1) 核心網路交換器(C6509) (2) 網管軟體 (3) 邊際交換器(C2960)	1	支援資產-實體設備類、資訊系統類	王館仁	李寶瑄	(1) 資訊機房 (2) 網路機房	2	2	3	2	9	高	組態設定錯誤	1	3	27	低
													系統軟體操作錯誤	2	3	54	中
													設備失竊	1	3	27	低
校務資訊系統作業	(1) 校務系統資訊平台 (2) 資料庫(SQL) (3) 伺服器(hp DL380G9)	1	支援資產-資訊系統類、實體設備類	開伐昇	李寶瑄	資訊機房	2	3	3	2	10	高	資料遭竄改	2	3	60	中
													硬體故障	2	3	60	中
													人為操作設定不當	3	3	90	高

Q：思考一下，資訊資產群組化有沒有缺點?

資訊價值鑑別(續)

- 訂定機關適合的**資訊資產價值**的方法論
- 常見的計算方法論，如下：
  - CIA與適法性的值取最大值
  - CIA與適法性的值之總和
  - (C值*2+I值*3+A值*4+適法性值*1)/10
  - (CIA與適法性的值之總和)/4

資訊價值鑑別(續)

- 制訂一套適當之資訊資產保護管理制度，確保各等級之資訊資產均受到最妥適之處理
- 資訊資產價值之安全等級

資訊資產價值	安全等級
0～4	低
5～8	中
9～12	高

資訊價值鑑別(續)

- 評估資訊資產之機密性、完整性、可用性及適用性後，將四者加總後的值，為資訊資產之價值。
- 以下以【資產價值=C+I+A+適法性值】為例

資訊資產價值

文件安全等級：□一般 ■敏感 □機密　　流水號__110-001__

新北市 000000 國小
資訊資產評鑑表

單位：0000　　填表人：0000　　填表日期：110 年 01 月 03 日

業務流程	資訊資產名稱	數量	資訊資產類別	使用人（註一）	保管人（註二）	放置地點	機密性	完整性	可用性	適法性	資訊資產價值	資訊資產安全等級（註三）	潛在風險事件	發生機率	衝擊程度	總風險值	風險等級
網路系統連線服務	核心網路交換器	1	支援資產-實體設備類	王館仁	李寶瑄	資訊機房	2	2	3	2	9	高	組態設定錯誤	1	3	27	低
校務資訊系統作業	校務系統	1	支援資產-資訊系統類	開伐昇	李寶瑄	資訊機房	2	3	3	2	10	高	資料遭竄改	2	3	60	中

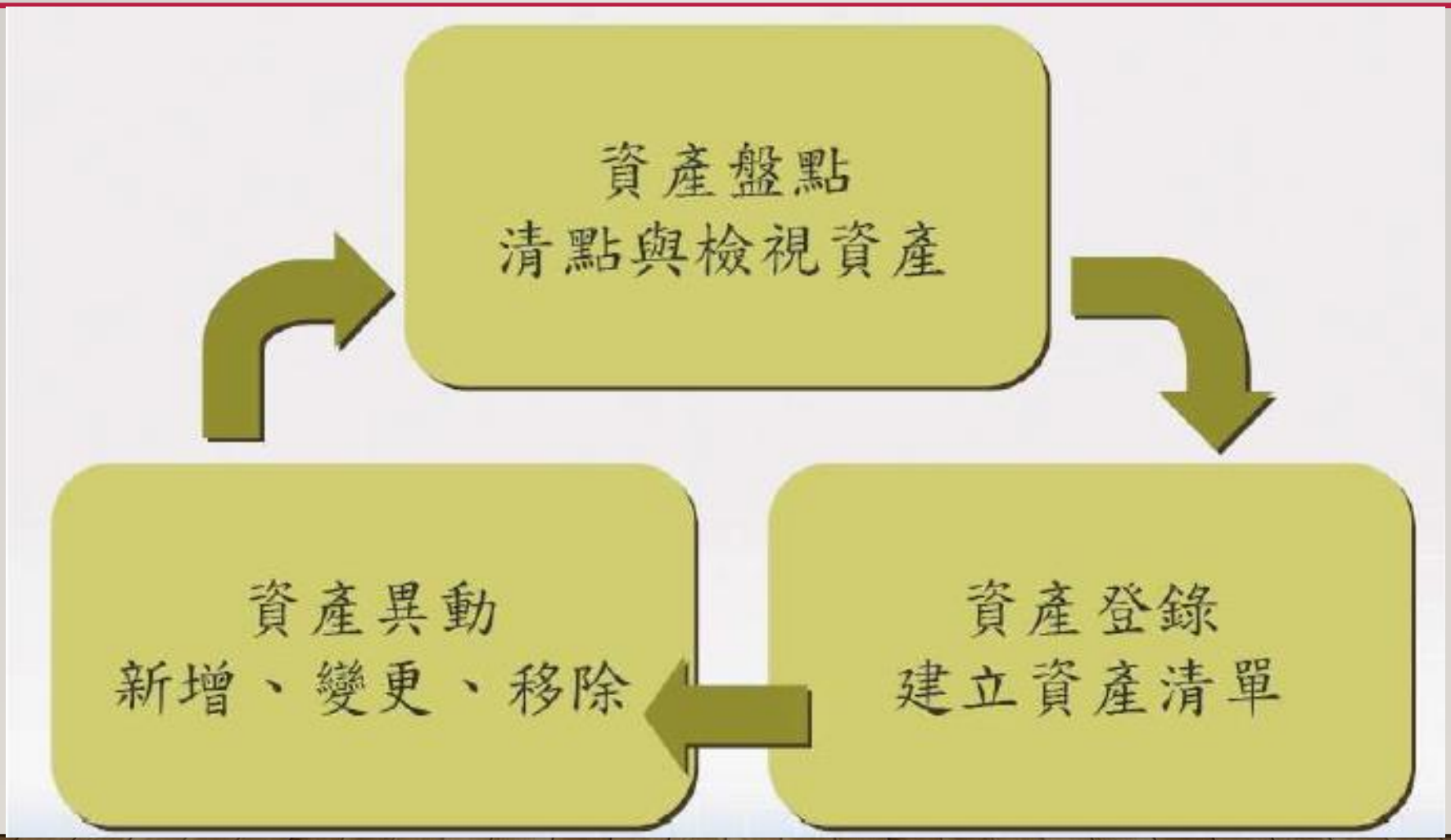
資訊資產清單之價值確認

- 資訊資產權責單位應依據資訊資產清單之機密性、可用性、完整性及適法性之評估標準，確認資產價值。
- 資訊資產清單及價值評估結果，應陳報至機關資通安全組織進行審議。

大綱

- **資產清查、評估與管理**
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - **資產管理與檢視**
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

資產管理



資產標示

- 已列入機密等級分類的資訊資產，可明確標示其機密等級，避免其機密性遭破壞。
- 實體設備之資訊資產安全等級標示方式，宜以不同顏色標籤區分，進行識別，如：
  - 資訊資產安全等級-低：綠色標籤
  - 資訊資產安全等級-中：藍色標籤
  - 資訊資產安全等級-高：黃色標籤

Q：將實體設備進行顏色標籤的標示識別，有何優點?

資產清單檢視

- 定期檢視
  - 機關每年至少進行 1 次資產盤點與資訊資產清單覆核
- 不定期檢視
  - 當有以下的狀況發生時：
    - ✓ 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
    - ✓ 組織架構調整

大綱

- **資產清查、評估與管理**
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- 風險評估、處理與管理
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

資產移除

- 資訊資產之報廢（或銷毀）應依機關所制定資訊資產異動作業相關說明書之規定，採取適當之方式進行銷毀、廢除
- 適切地進行風險評鑑資料的關聯性更新

資產移除_範例表單

□紀錄安全等級：□一般 □敏感 □機密　　流水號_____

新北市 00000 國小

資訊資產銷毀申請單

申請單位		申請人		申請日期	
資產名稱					
申請原因					
處理方式					

資訊資產之處理規範

- 針對安全等級較高的資訊資產，要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。
  - 資產安全等級較高文件類資訊資產之安全處理應符合以下作業要求：
    - ✓ 紙類文件不再使用並確認已逾保存期限時，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，要適當保護，以防止不當利用。
    - ✓ 系統文件要指定專人管理，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)

- 安全等級較高的軟體類資訊資產之安全處理作業
- 安全等級較高的硬體類資訊資產之安全處理作業
- 應定期檢討安全等級較高的資訊資產清單內容，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(C)、完整性(I)、 可用性(A)及適法性，試評出符合該資訊資產在組織內之價值。
- 將C、I、A與適法性之價值鑑別結果，加總後的值，填入「資產價值」欄位，並對應其資產安全等級。

大綱

- 資產清查、評估與管理
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

風險管理相關標準

- ISO/CNS 27001

  資訊安全管理系統-要求事項

- ISO/CNS 27005

  資訊安全風險管理

- ISO/CNS 31000

  風險管理-原則與指導綱要

- ISO/CNS 31010

  風險管理-風險評鑑技術

CNS 31010（REF.1）

風險評鑑方法

工具與技術	風險評鑑過程					註記
	風險識別	風險分析			風險評估	
		衝擊後果	發生可能性	風險等級		
腦力激盪	極適用	不適用	不適用	不適用	不適用	
結構或非結構化面談	極適用	不適用	不適用	不適用	不適用	
德爾菲(Delphi)	極適用	不適用	不適用	不適用	不適用	
查檢表	極適用	不適用	不適用	不適用	不適用	
初期危害分析(PHA)	極適用	不適用	不適用	不適用	不適用	
危害與可操作性研究（HAZOP）	極適用	極適用	適用	適用	適用	
危害分析與關鍵管制點（HACCP）	極適用	極適用	不適用	不適用	極適用	
環境風險評鑑	極適用	極適用	極適用	極適用	極適用	
結構化之"如果這樣會怎樣"(SWIFT)	極適用	極適用	極適用	極適用	極適用	
情境分析	極適用	極適用	適用	適用	適用	

資料來源：CNS 31010

CNS 31010（REF.2）

工具與技術	風險評鑑過程					註記
	風險識別	風險分析			風險評估	
		衝擊後果	發生可能性	風險等級		
企業衝擊分析(BIA)	適用	極適用	適用	適用	適用	●
根本原因分析(RCA)	不適用	極適用	極適用	極適用	極適用	
失效模式與效應分析(FMEA)	極適用	極適用	極適用	極適用	極適用	
失效(故障)樹分析(FTA)	適用	不適用	極適用	適用	適用	
事件樹分析（ETA）	適用	極適用	適用	適用	不適用	
因果分析	適用	極適用	極適用	適用	適用	
原因與效應分析	極適用	極適用	不適用	不適用	不適用	
保護層分析(LOPA)	適用	極適用	適用	適用	不適用	

資料來源：CNS 31010

CNS 31010 (REF.3)

工具與技術	風險評鑑過程					註記
	風險識別	風險分析			風險評估	
		衝擊後果	發生可能性	風險等級		
馬可夫(Markov)分析	適用	極適用	不適用	不適用	不適用	
蒙地卡羅模擬	不適用	不適用	不適用	不適用	極適用	
貝氏統計法(Bayesian statistics)與貝氏網路(Bayes Nets)	不適用	不適用	不適用	不適用	極適用	
FN 曲線	適用	極適用	極適用	適用	極適用	
風險指數	適用	極適用	極適用	適用	極適用	
後果/機率矩陣	極適用	極適用	極適用	極適用	適用	●
成本/效益分析(CBA)	適用	極適用	適用	適用	適用	
多準則決策分析(MDCA)	適用	極適用	適用	極適用	適用	
註記	CNS/ISO/IEC 27005:2011 建議之資訊安全風險評鑑風法： 高階風險評鑑法＝企業衝擊分析 詳細風險評鑑法＝後果/機率矩陣					

資料來源：CNS 31010

企業衝擊分析(BIA)_範例

企業(/業務)衝擊分析表(BIA)					
文件編號	ISMS-D-025	機密等級	內部使用	版次	2.0

製表日期：

備註：BIA(Business Impact Assessment，營運衝擊分析)、MTD(Maximum Tolerable Downtime，可以忍受的最大服務中斷時間)、RTO(Recovery Time Objective，系統回復時間)、RPO(Recovery Point Objective，資料回復點)

系統名稱	關鍵次序	MTD	RTO	RPO	衝擊說明	服務/關鍵作業時間	多重備援方案（設備可用性）例如 具HA、VM、異地備援、異地備份等	負責人

後果/機率矩陣_範例

影響 / 可能性	輕微	普通	嚴重/顯著
幾乎確定	中	高	高
可能	低	中	高
幾乎不可能	低	低	中

風險

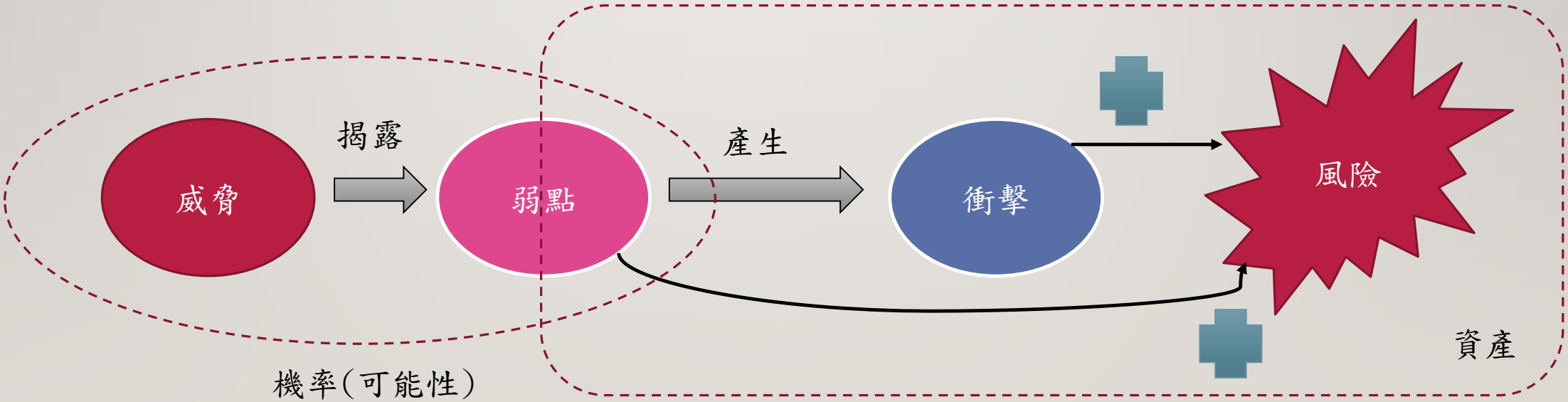
- 參考ISO/CNS 31000的定義

  對於組織目標之不確定影響

- 風險意指任何類型與大小的組織，為達成組織的目標，所面對內部及外部因素影響的**不確定性**，包含事件發生的改變程度與發生的**可能性**等。

甚麼是資訊安全風險?

- 當**威脅**利用其相對應**脆弱性**直接或間接造成組織資訊及資通系統資產的「機密性」、「完整性」、「可用性」及「適法性」受到漏失或損害的「可能性」



資安事件案例探討

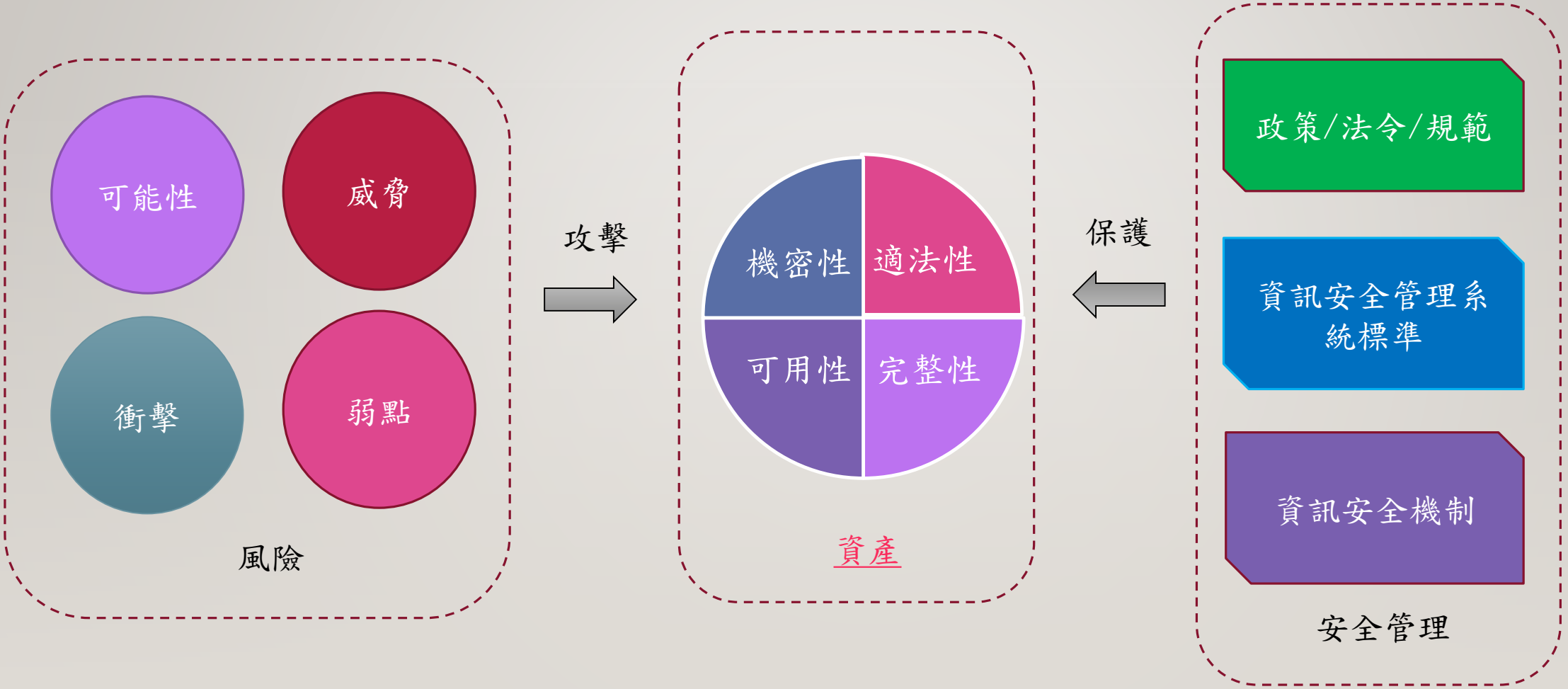
- 網頁搜尋可以找到某老師與校務資訊系統的帳號跟密碼資料
- 某老師寄錯班級學生連絡簿資料給其他非相關學生
- 網頁公告招生考試日期資訊標示錯誤
- 機電系統時常跳電，造成電子公文系統無法運作

以上案例的最大衝擊，分別屬於資訊安全3大原則（CIA）的哪一種？

安全問題的緣由

- 技術面
  - 資料外洩
  - Bug、未修補的Patch
  - 越權存取
  - 沒標準
  - 難以維持最新技術
- 流程面
  - 權責區分不明
  - 未考量安全性
  - 角色權責不清
  - 缺乏稽核追蹤機制
  - 權限授權模糊
- 人員面
  - 操作不當
  - 認知錯誤、不足
  - 輸入資訊錯誤
  - 聯繫溝通管道不佳
  - 內部管理不善

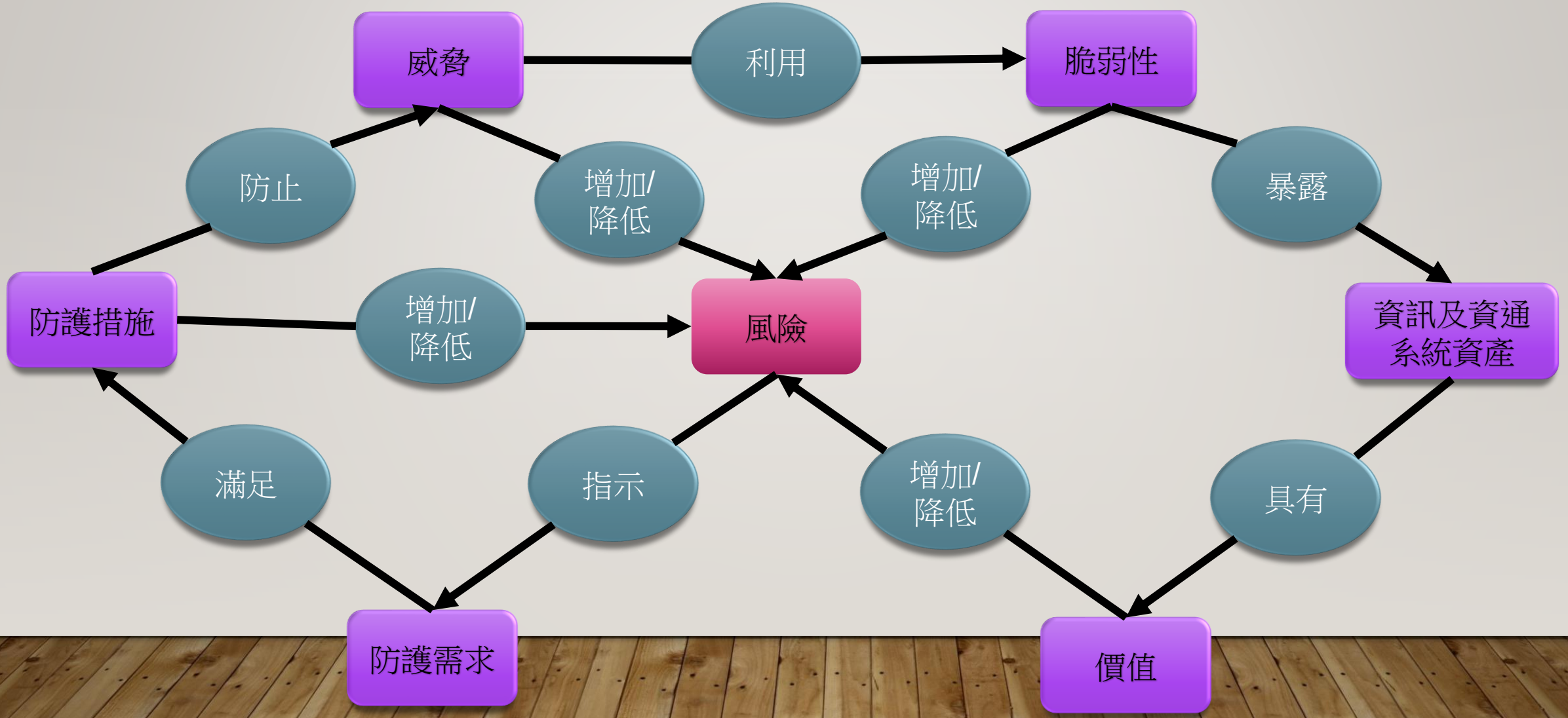
資訊安全概念圖


可能性
威脅
衝擊
弱點
風險
攻擊
機密性
適法性
可用性
完整性
資產
保護
政策/法令/規範
資訊安全管理系統標準
資訊安全機制
安全管理

大綱

- 資產清查、評估與管理
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - **風險管理過程**
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

風險管理關係圖


威脅
利用
脆弱性
防止
增加/
降低
增加/
降低
暴露
防護措施
增加/
降低
風險
資訊及資通
系統資產
滿足
指示
增加/
降低
具有
防護需求
價值

威脅

- 指可能利用或引發脆弱性的潛在方法
- 任一情況或事件，可能以破壞、洩漏、不當竄改資料及拒絕服務的形式，而危害資訊及資通系統資產均稱之
- 範例：
  - 落雷、洪水
  - 病毒
  - 順手牽羊者
  - 未預警停電
  - 不愉快的員工

脆弱性

- 指資產因設計不當、人為操作管理失誤或強度不足，可用於作為攻擊行動(威脅)利用的突破口之處
- 存在於實體環境、資通系統及其他組成元件(例如：系統安全程序、硬體設計及內部控制)本身
- 範例：
  - 輕巧筆記型電腦
  - 重要主機設備
  - 地勢低窪的產品製造廠房
  - 關鍵應用系統

威脅與脆弱性(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。

攻擊手法

- 使威脅可以利用資訊及資通系統資產脆弱性造成破壞其資訊資產的機密性、完整性及可用性之方法、工具、途徑、媒介及時序等總和稱之
- 範例：
  - 潛入工作場所
  - 淹沒廠房
  - 停止供電
  - 埋惡意程式碼
  - 透過email傳播

威脅、脆弱性及攻擊手法-範例

資產	威脅	脆弱點	攻擊手法
商業機密	商業間諜	未妥善保護	潛入工作場所
筆記型電腦	順手牽羊者	輕巧	趁其不備快速行動
關鍵應用系統	不愉快的員工	員工不忠誠	盜賣程式碼
生產廠房	洪水	位於地勢低窪地區	淹沒廠房
電腦系統	電腦病毒	缺乏警覺性的員工	透過email傳播

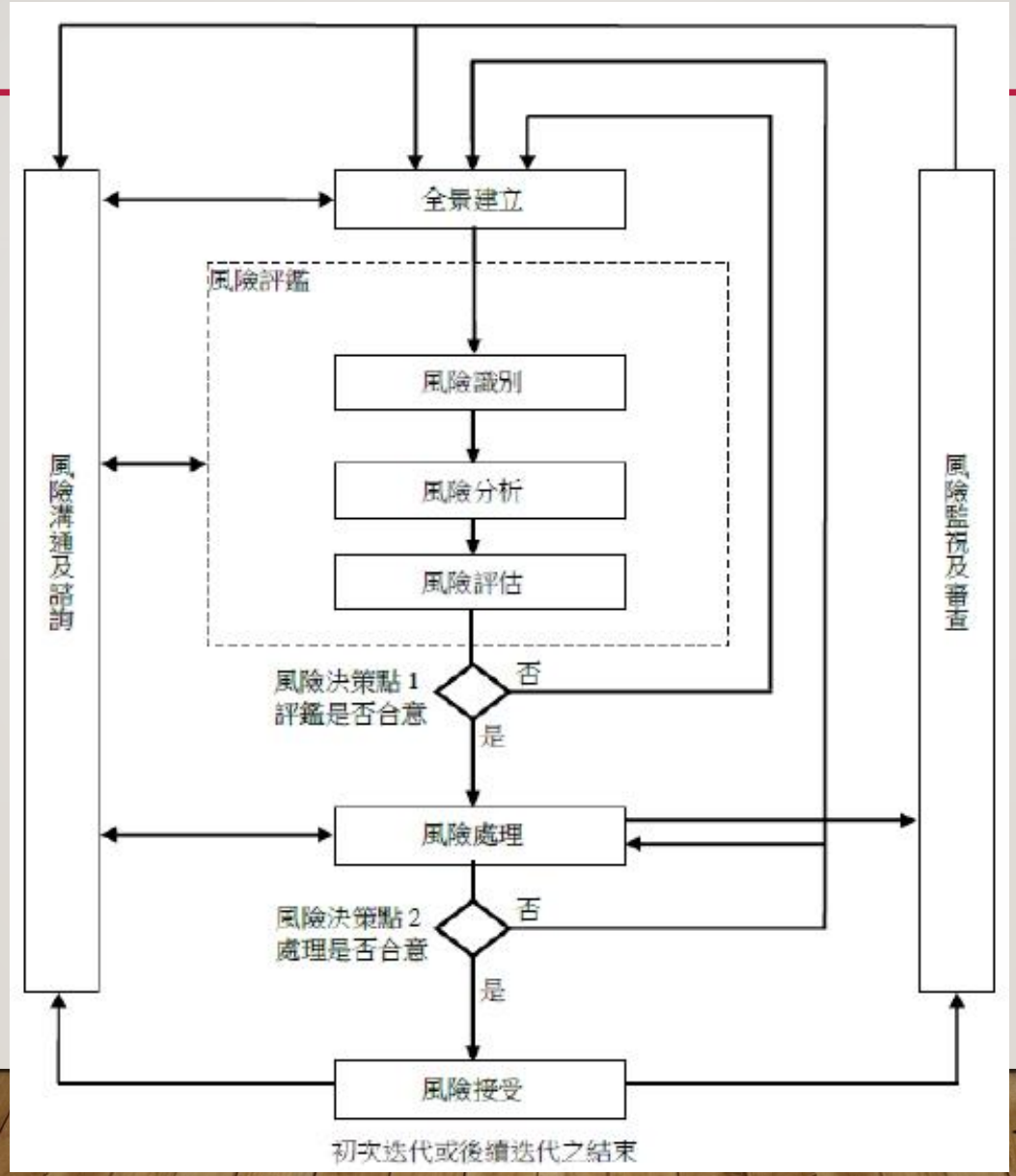
風險所造成的損害

重大	一般	輕微
• 火災 • 地震 • COVID-19 • 個資外洩 • 駭客入侵	• 主機中毒 • 主機故障	• 人員操作錯誤 • 個人電腦中毒

風險管理過程

資料來源：ISO 31000

風險管理過程(續)



資料來源：CNS 27005

風險評鑑

- 風險識別
  - 資產識別
  - 威脅及脆弱性識別
  - 現有控制措施識別
  - 後果識別

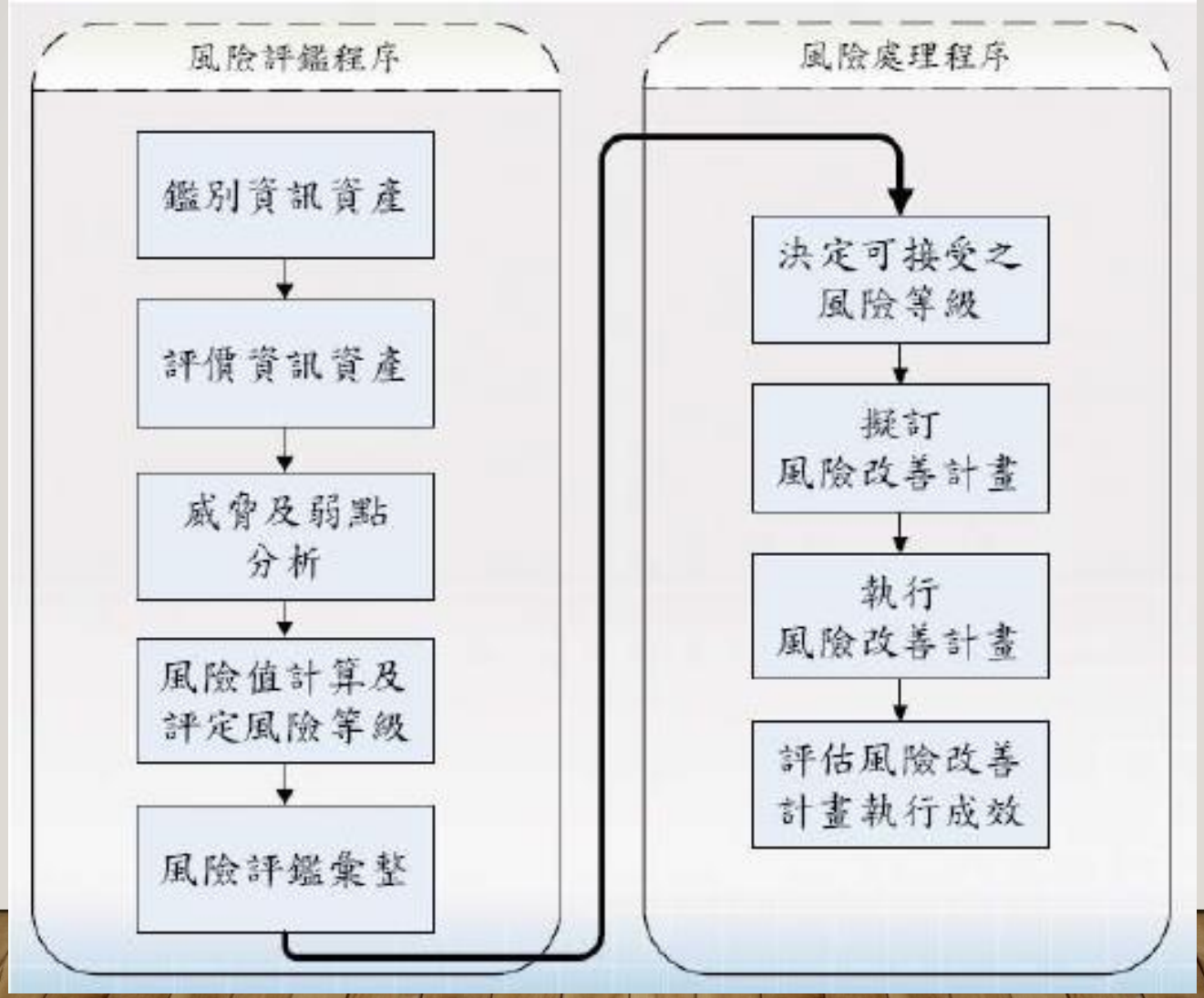
- 風險分析
  - 後果評鑑
  - 評鑑事件可能性
  - 評估風險等級

- 風險評估
  - 訂定風險等級
  - 決定風險可接受等級

大綱

- 資產清查、評估與管理
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - **風險評鑑與處理程序**
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

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

大綱

- 資產清查、評估與管理
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - **風險評估準則**
  - 風險控管作為
  - 風險監視與審查

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(受到威脅利用之衝擊程度)】

可能性、衝擊程度與風險之間的關係

- 威脅等級
  - 發生之可能性（Possibility）
  - 風險發生的機率
- 弱點等級
  - 對營運造成的衝擊性（Impact）
  - 衝擊程度

風險發生機率(發生的可能性)

- 以發生之機率估算
- 當實際有相對應之潛在風險事件發生時，需覆核該項資訊資產之風險發生機率值，以避免發生低估的情形

風險發生機率值	判斷依據
低	每年至多發生一次安全事件；相對應風險發生機率值等於 1
中	每年至多發生五次安全事件；相對應風險發生機率值等於 2
高	每年發生安全事件次數大於五次；相對應風險發生機率值等於 3

衝擊程度

- 依資訊安全事件或事故發生時，對機關營運造成之衝擊程度或影響程度為判斷(評估)之依據。

風險等級	判斷依據
低（衝擊程度值1）	不影響本機關之營運
中（衝擊程度值2）	將造成相關業務之運作效率降低
高（衝擊程度值3）	將造成本機關業務運作停頓

可能性、衝擊程度與風險之間的關係

- 訂定機關適合的風險值計算的方法論
- 常見的計算方法論，如下：
  - 資產價值*發生機率*衝擊程度
  - 資產價值*(發生機率+衝擊程度)
  - 資產價值+發生機率+衝擊程度
  - 資產價值*(發生機率+衝擊(或損害)程度*(構面1+構面2+構面3))

備註：
(1)發生機率 V.S 威脅等級
(2)衝擊程度 V.S 弱點等級

風險值的計算(以簡報範例為例)

- 資產價值=機密性+完整性+可用性+適法性
- 風險之定義與評估
  - 風險值=資訊資產價值*發生機率值*衝擊程度值
- 風險值：

總風險值	風險等級
0～36	低
37～72	中
73～108	高

風險等級(以簡報範例為例)

總風險值	風險等級	說明
0～36	低	該資訊資產的安全需求遭受破壞時，對業務之運作影響極少，於一定時間以內處理即可。
37～72	中	該資訊資產的安全需求遭受破壞時，會影響部分業務之運作或個人工作的進行，需及時處理。
73～108	高	該資訊資產的安全需求遭受破壞時，會影響整個機關或整個業務單位的營運，需要緊急處理。

資訊資產評鑑表

文件安全等級：□一般 ■敏感 □機密

00 市 0000 國小中

資訊資產評鑑表 (Ctrl)

單位：0000　　填表人：0000　　填表日期：110 年 01 月 03 日

業務流程	資訊資產名稱	數量	資訊資產類別	使用人（註一）	保管人（註二）	放置地點	機密性	完整性	可用性	適法性	資訊資產價值	資訊資產安全等級（註三）	潛在風險事件	發生機率	衝擊程度	總風險值	風險等級
網路系統連線服務	(1) 核心網路交換器(C6509) (2) 網管軟體 (3) 邊際交換器(C2960)	1	支援資產-實體設備類、資訊系統類	王館仁	李寶瑄	(1) 資訊機房 (2) 網路機房	2	2	3	2	9	高	組態設定錯誤	1	3	27	低
													系統軟體操作錯誤	2	3	54	中
													設備失竊	1	3	27	低
校務資訊系統作業	(1) 校務系統資訊平台 (2) 資料庫(SQL) (3) 伺服器(hp DL380G9)	1	支援資產-資訊系統類、實體設備類	開伐昇	李寶瑄	資訊機房	2	3	3	2	10	高	資料遭竄改	2	3	60	中
													硬體故障	2	3	60	中
													人為操作設定不當	3	3	90	高

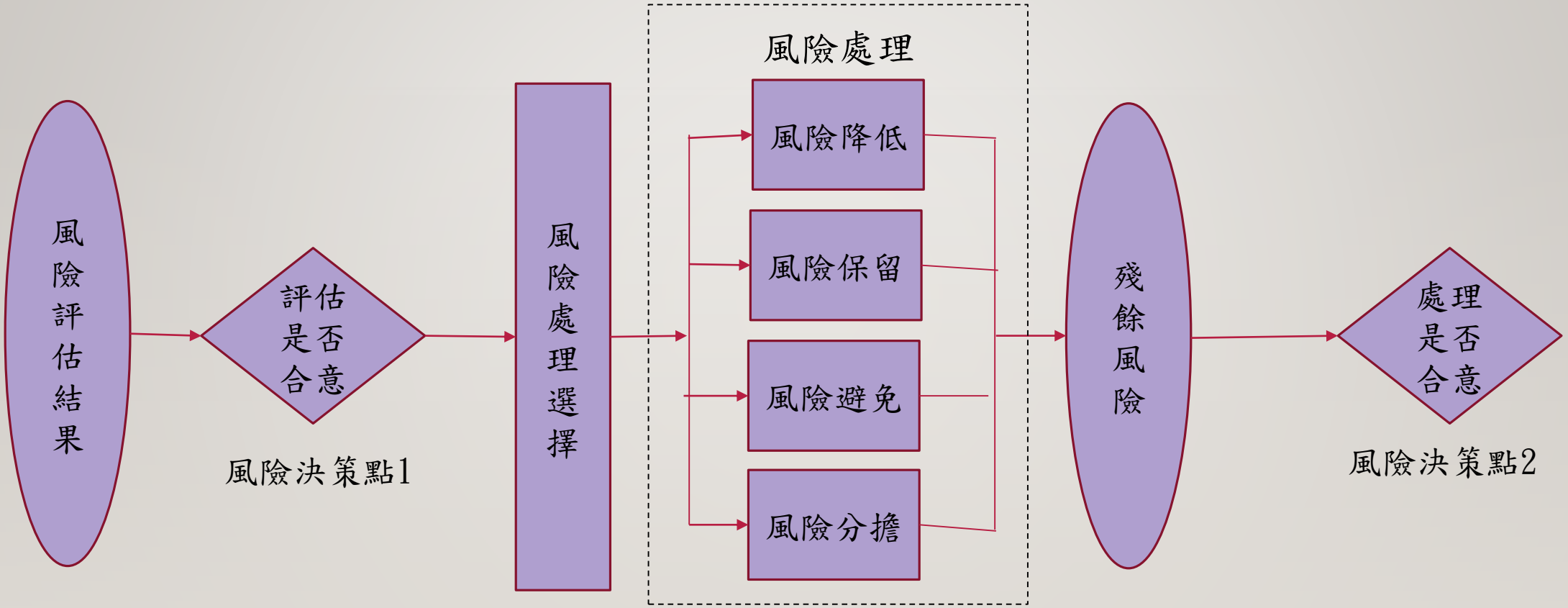
風險值與等級

潛在風險事件

大綱

- 資產清查、評估與管理
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - **風險控管作為**
  - 風險監視與審查

風險處理活動


風險評估結果
評估是否合意
風險決策點1
風險處理選擇
風險處理
風險降低
風險保留
風險避免
風險分擔
殘餘風險
處理是否合意
風險決策點2

風險控管原則與方法

- 辨識資產和它們面臨的潛在安全事件
- 量化事件發生的可能性與衝擊程度的影響
- 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，決定機關可接受之風險值
- 高於可接受風險值者(面臨不可接受風險的資訊資產)，優先控管或處理
- 建立及執行風險改善計畫(參考風險控制計畫)、針對高風險進行風險再評估(鑑)
- 選擇風險控管方式：

★風險避免	★風險降低
★風險分擔	★風險保留

- 對高風險的項目進行相關管控措施，並適切進行追蹤與列管
- 建立適用性聲明書(SOA)

可接受風險值

- 制定方式
  - 管理審查會議、00工作會議
  - 簽呈紀錄
- 制定方法論
  - 單一固定值
  - 80/20法則
  - 依各單位資源支援情形採客觀性的依據
  - …

選擇風險控管方式

- 風險避免　(規避風險)
- 風險分擔　(轉移風險)
- 風險降低
- 風險保留　(接受風險)

舉例：

(1)林先生因有出差到大陸的業務需求，但又擔心搭飛機會遇到機械故障，所以轉搭郵輪前往。 =>風險避免(規避風險)

(2)延續(1)，林先生另外再購買意外保險。 =>風險分擔(轉移風險)

(3)校園核心交換器目前只有一台，林先生擔心會有單點故障問題，於是在多購買一台交換器並建立HA機制。 =>風險降低

風險控制計畫_參考範本

新北市政府教育局

紀錄安全等級：□一般 □敏感 □機密

資訊安全管理文件
流水號_____

新北市政府教育局
風險控制計畫

填表日期：　年　月　日

資訊資產名稱	資訊資產類別	潛在風險事件			
計畫實施前	資訊資產價值	發生機率	衝擊程度	總風險值	風險等級

風險管理策略	控制項目	預計完成日期

控制措施

預估成本	預期效益

有效性量測方法

大綱

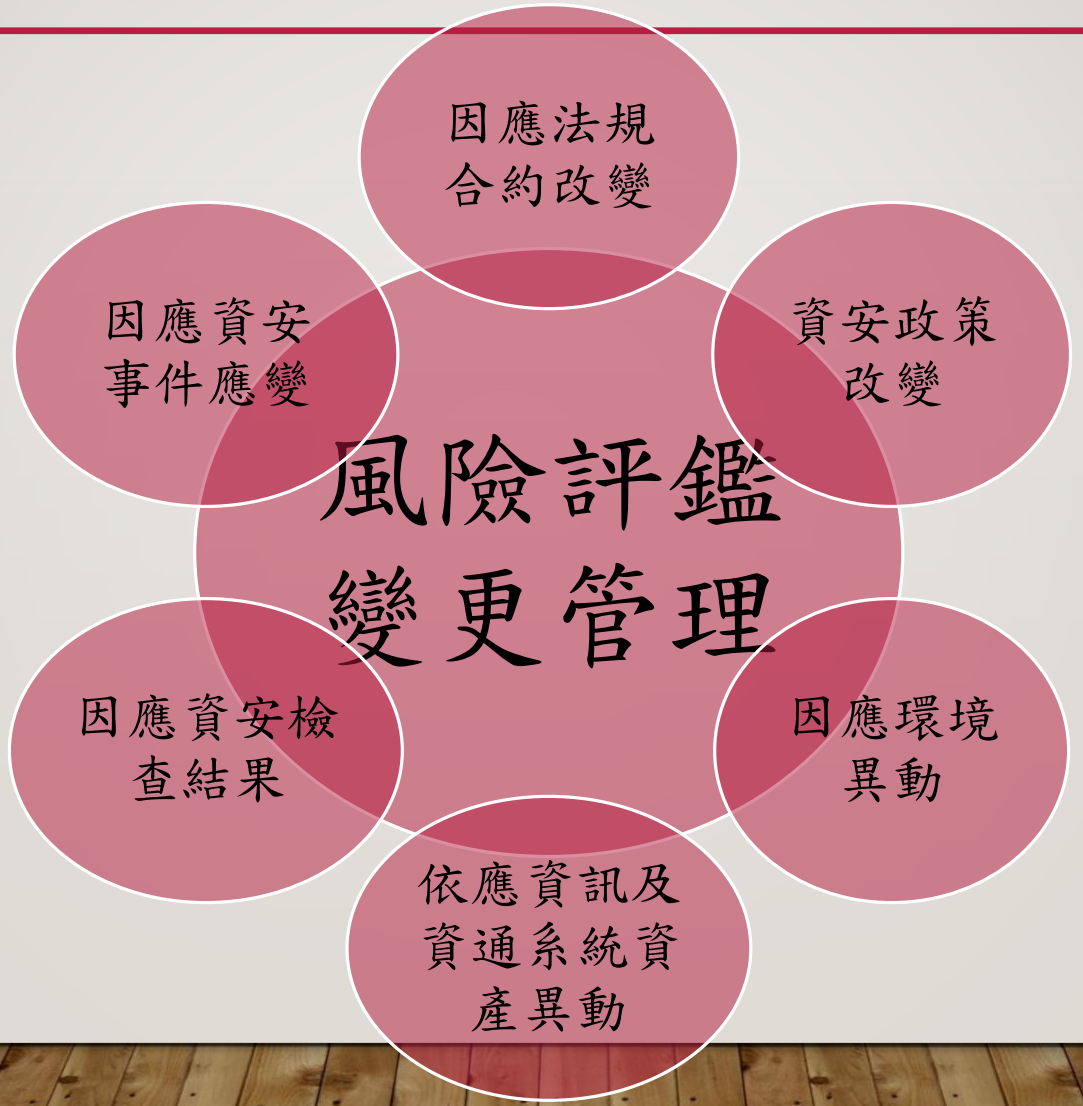
- 資產清查、評估與管理
  - 基礎觀念
  - 資產清查清單
  - 資產分類分級
  - 資產價值鑑別
  - 資產管理與檢視
  - 資產移除與處理
- **風險評估、處理與管理**
  - 風險基礎概念
  - 風險管理過程
  - 風險評鑑與處理程序
  - 風險評估準則
  - 風險控管作為
  - 風險監視與審查

風險因素之監視與審查

- 審查時機：
  - 定期審查
  - 不定期審查

    當環境與資通系統發生異動或改變時，須及時檢視與更新
- 確保風險評鑑報告成為「動態文件」
- 風險評鑑報告之變更管理是用來協助識別該資通系統是否需要新安全需求的過程

風險評鑑審查與變更管理



綜合練習

- 請列出家裡的資產有哪些?
- 對各資產進行資產價值的評估
- 對各資產進行風險評估，取得初始風險值
- 對於不可接受的風險，進行風險改善作為(措施)
- 改善後的資產風險，再進行評估是否有降低
- PDCA循環漸進，持續改善

資訊安全制度建立

- 制定規範文件流程：
  - 流程圖
  - 表格/表單/紀錄
  - 連結各注意細節
  - 宣導/教育訓練
  - 公告
  - PDCA：流程、表單/紀錄、規範

謝謝聆聽

周冠吉

E-MAIL：EDITOR@MAIL.NTPU.EDU.TW