TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

國立臺南大學

111年資訊安全暨個人資料管理規範導入顧問輔導服務案

課程名稱：資產鑑別與風險評鑑執行方法進階操作

授課日期：111年6月15日

授課講師：資安顧問 蔡元豪 Leo

簡報大綱

一 ISMS及PIMS資產盤點方法

二一 ISMS及PIMS
風險評鑑及處理方法

二二 學校各單位保有個人資料檔案
清查盤點系統操作說明

ISMS及PIMS資產盤點方法

資訊是組織營運的資產

- 資訊是組織的重要資產並且也是所有業務流程的一部分。
- 包含營業秘密、專利、人員隱私和業務構想等。

它被視為組織的資產

建立資訊資產所需的成本、技術、時間及資源

資訊資產的資料分類是確保機密性及所有者

它是組織企業形象的一部分

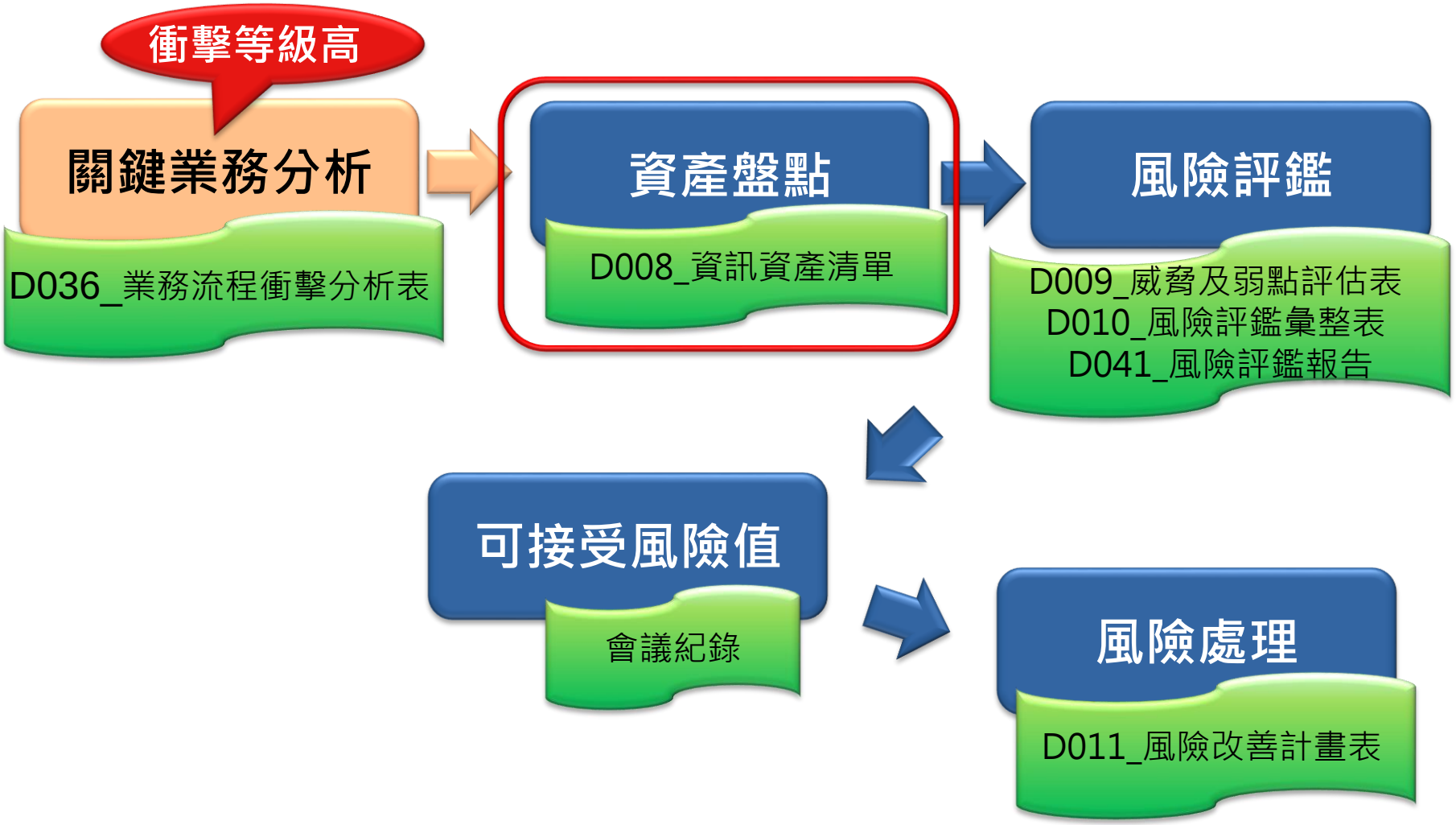
資料損失會**影響**組織在不同業務活動的**投資**

資產管理目的

資訊安全

保護資訊資產，**避免**遭受各種**威脅**及**降低可能**危害

流程簡圖



資產識別與分類

資訊資產權責單位

- 負責所管轄內資訊資產之存取授權，並評估與審核資訊資產分類分級及價值之結果，得另指定資訊資產保管單位。

資訊資產保管單位

- 對於指定資訊資產，具有落實資訊資產權責單位所委託之保護管理責任。

資訊資產使用單位

- 對於資訊資產之使用，必須依據權責單位要求，並具有正確使用操作之責任。

資訊資產分類

文件	• 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	• 作業系統、應用系統程式、套裝軟體等，包含原始程式碼、應用程式執行碼等。
通訊	• 網路設備、網路安全設備及提供資訊傳輸、交換之線路或服務。
硬體	• 主機設備等相關硬體設施。
資料	• 儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊。
環境	• 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。
人員	• 全體同仁及委外廠商。

資訊資產清單

- 資訊資產鑑別

➢ 各資訊資產權責單位應鑑別所管轄之資訊資產，並建立「資訊資產清單」。

➢ 各資訊資產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彙整，資通安全管理規範導入工作小組負責彙整決議，以確保資訊資產編號及清單之完整性。

資訊資產清單之覆核

- 資訊資產清單

➢ 確保資訊資產清單的正確性及完整性

– 定期

- 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 。

– 不定期

- 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。

資訊資產之新增、異動、報廢

- 資訊資產之新增、異動

資訊資產新增或異動時，資訊資產使用單位應填寫「資訊資產異動申請表」，經資通安全管理規範導入工作小組會議決議後，交由文件管理人員保管，並定期更新「資訊資產清單」。

- 資訊資產之報廢

硬體及通訊資訊資產價值為4者，經呈報資通安全官核准後，方可執行報廢；資訊資產價值未達4者，經權責主管核准後，方可執行報廢。

資訊資產價值

- 如何評價資訊資產？
  - 資訊資產價值=依據資訊資產之機密性、完整性及可用性評估之後，取3者之最大值為資訊資產價值。

資訊資產價值鑑別

機密性

評估標準	數值
一般：此資訊資產無特殊機密性要求	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

完整性

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組織造成傷害	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

可用性

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	4

取3者之**最大值**
為資訊資產價值

個人資料資產分類

- 本校個人資料資產分為電子與紙本兩類別，其分類說明如下：

➢ 電子資料（Data；DA）：係指儲存於硬碟、磁帶、光碟等儲存媒介之數位資訊，包含公文、報表、表單、計畫書、合約、外來文件及資料庫資料等電子檔案。

➢ 紙本資料（Document；DC）：係指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、文件等紙本資料。

個資法所稱之個人資料

一般個資

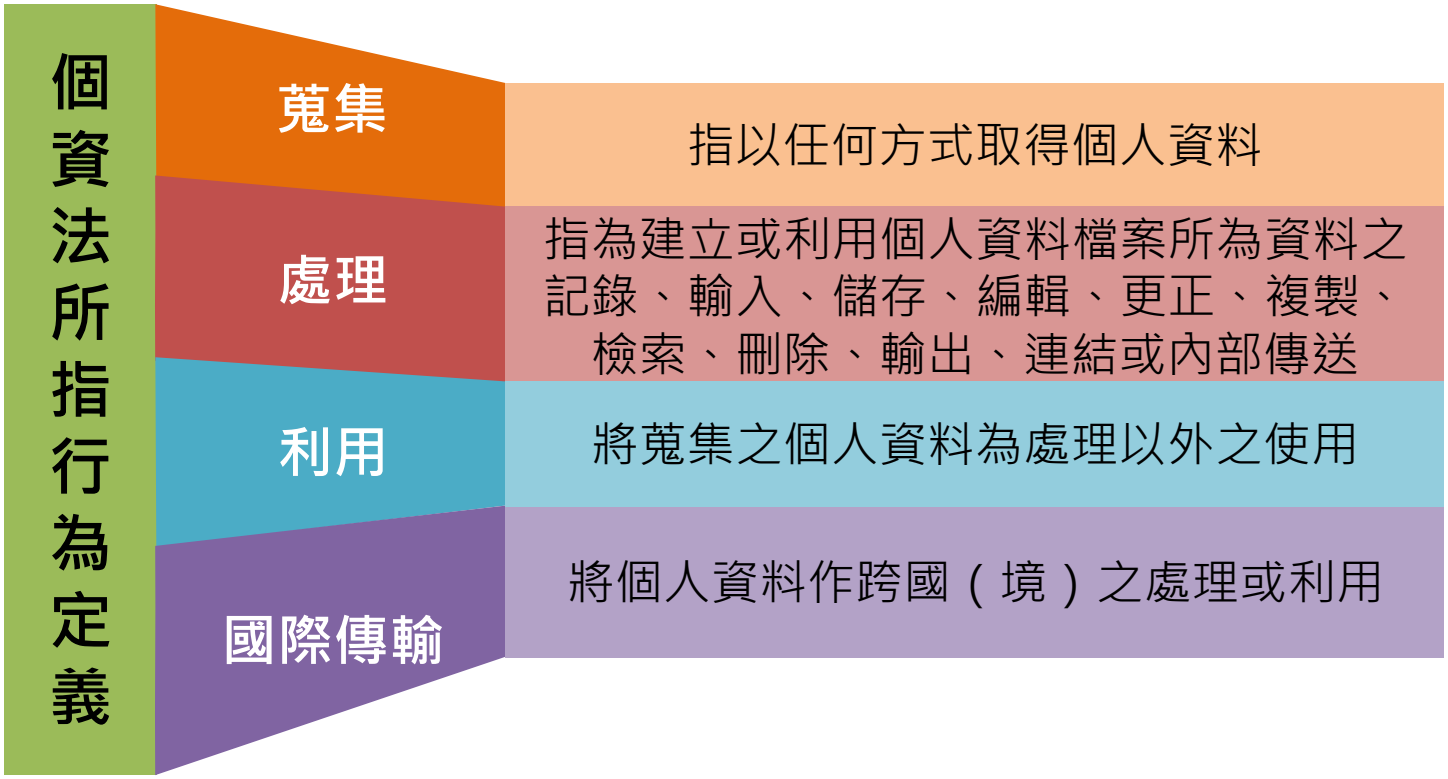
.姓名
.出生年月日
.國民身分
.統一編號
.護照號碼
.特徵
.指紋
.婚姻
.家庭
.教育
.職業
.聯絡方式
.財務情況
.社會活動

特種個資

.病歷
.醫療
.基因
.性生活
.健康檢查
.犯罪前科

得以直接或間接方式識別該個人之資料

個資法所指行為定義 §2



個人資料檔案資產價值

– 個人資料檔案資產價值（衝擊值）評估：

個人資料檔案之資產價值（衝擊值）依據每個個資檔案內容所涵蓋之個人資料範圍，分別給予一般（1）、中度（2）、高度（3）與極高（4）等四個不同之資產價值（衝擊值）。

原版

衝擊 影響程度	資產價值 （衝擊值）	個人資料範圍
極高	4	自然人之姓名或國民身分證統一編號（或護照號碼）及特種個人資料。
高度	3	1. 含自然人之姓名及國民身分證統一編號（或護照號碼），但不含特種個人資料。 2. 含自然人之姓名或國民身分證統一編號（或護照號碼）及財務情況（如：薪資、局帳號），但不含特種個人資料。
中度	2	1. 含自然人之姓名或國民身分證統一編號（或護照號碼），但不包含特種資料。 2. 含自然人之姓名及員工編號（或學號），但不含特種個人資料。
一般	1	不含自然人之姓名及國民身分證統一編號（或護照號碼）。

個人資料檔案資產價值-預計調整

調整為

資產價值	個人資料範圍
4	自然人之姓名或國民身分證統一編號（或護照號碼）及特種個人資料。
3	1. 含自然人之姓名及國民身分證統一編號（或護照號碼），但不含特種個人資料。 2. 含自然人之姓名或國民身分證統一編號（或護照號碼）及財務情況（如：薪資、局帳號），但不含特種個人資料。
2	1. 含自然人之姓名或國民身分證統一編號（或護照號碼），但不包含特種資料。 2. 含自然人之姓名及員工編號（或學號），但不含特種個人資料
1	不含自然人之姓名及國民身分證統一編號（或護照號碼）。

特種個資判斷

- 符合下列條件者，判斷為**資產價值4**：
  - 個資類別為下列其一者
    - **C066 健康與安全紀錄**
    - **C111 健康紀錄**
    - **C112 性生活**
    - **C113 種族或血統來源**
    - **C116 犯罪嫌疑資料**

個人資料特定目的範例

代號	特定目的項目	代號	特定目的項目
○○一	人身保險	○一七	文化資產管理
○○二	人事管理（包含甄選、離職及所屬員工基本資訊、現職、學經歷、考試分發、終身學習訓練進修、考績獎懲、銓審、薪資待遇、差勤、福利措施、褫奪公權、特殊查核或其他人事措施）	○一八	水利、農田水利行政
○○三	入出國及移民	○一九	火災預防與控制、消防行政
○○四	土地行政	○二○	代理與仲介業務
○○五	工程技術服務業之管理	○二一	外交及領事事務
○○六	工業行政	○二二	外匯業務
○○七	不動產服務	○二三	民政
○○八	中小企業及其他產業之輔導	○二四	民意調查
○○九	中央銀行監理業務	○二五	犯罪預防、刑事偵查、執行、矯正、保護處分、犯罪被害人保護或更生保護事務
○一○	公立與私立慈善機構管理	○二六	生態保育
○一一	公共造產業務	○二七	立法或立法諮詢
○一二	公共衛生或傳染病防治	○二八	交通及公共建設行政
○一三	公共關係	○二九	公民營（辦）交通運輸、公共運輸及公共建設
○一四	公職人員財產申報、利益衝突迴避及政治獻金業務	○三○	仲裁
○一五	戶政	○三一	全民健康保險、勞工保險、農民保險、國民年金保險或其他社會保險
○一六	文化行政	○三二	刑案資料管理

個人資料特定目的範例

個人資料類別清單案例

代　號　識別類：

C〇〇一　辨識個人者。

例如：姓名、職稱、住址、工作地址、以前地址、住家電碼、行動電話、即時通帳號、網路平臺申請之帳號、通訊籍地址、相片、指紋、電子郵遞地址、電子簽章、憑證卡、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及任何可辨識資料本人者等。

C〇〇二　辨識財務者。

例如：金融機構帳戶之號碼與姓名、信用卡或簽帳卡之號碼保險單號碼、個人之其他號碼或帳戶等。

C〇〇三　政府資料中之辨識者。

例如：身分證統一編號、統一證號、稅籍編號、保險憑證、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等

代　號　特徵類：

C〇一一　個人描述。

例如：年齡、性別、出生年月日、出生地、國籍、聲音等

C〇一二　身體描述。

例如：身高、體重、血型等。

C〇一三　習慣。

例如：抽煙、喝酒等。

C〇一四　個性。

例如：個性等之評述意見。

代　號　教育、考選、技術或其他專業：

C〇五一　學校紀錄。

例如：大學、專科或其他學校等。

C〇五二　資格或技術。

例如：學歷資格、專業技術、特別執照（如飛機駕駛）、政府職訓機構學習過程、國家考試、考試成績或其他紀錄等。

C〇五三　職業團體會員資格。

例如：會員資格類別、會員資格紀錄、參加之紀錄等

C〇五四　職業專長。

例如：專家、學者、顧問等。

C〇五五　委員會之會員資格。

例如：委員會之詳細情形、工作小組及會員資格因專案產生之情形等。

C〇五六　著作。

例如：書籍、文章、報告、視聽出版品及其他著作等

C〇五七　學生（員）、應考人紀錄。

例如：學習過程、相關資格、考試訓練考核及成績、或其他學習或考試紀錄等。

C〇五八　委員工作紀錄。

例如：委員參加命題、閱卷、審查、口試及其他試務

個人資料檔案清冊-盤點時注意事項

填報單位	
個資資產編號	
業務流程名稱	
個人資料檔案名稱	
資料形式	
法律依據或內部規定	
特定目的	
個人資料類別	
個人資料範圍	
有否特種資料？何種特種資料？	
有無監督管理之非公務機關及其名稱	
蒐集	來源
	方式
	單位
處理	方式
	單位
利用	期間
	地區
	單位
	方式目的
保存	單位
	聯絡人
	期限
銷毀	形式
	頻率
揭露	對象
	目的
	方式
	個資範圍
現有控制措施	
衝擊值	
個資數量	
重要性	
有無訂定個資保護作業規範	

資料形式：電子資料/紙本資料

個人資料範圍：

個資的欄位名稱，如：姓名、電話、身分證字號、學號等

保存-期限：永久保存/法定保存期限制/自訂保存期限
(特定目的持續時間)

銷毀-形式(方式)：無作廢/刪除/碎紙/銷毀/去識別化等
(需留下銷毀紀錄)

銷毀-頻率：無需銷毀/每月/每季/每年，

現有控制措施：加密/上櫃上鎖/專人保管等方式

個資數量：估算目前保有的個資數量(筆數)，
可依保存期限及每年度增加數量推算，
如：每年學生資料增加約1千筆，
此筆個資需保存10年(未銷毀亦需計算)，
故個資數量推估為1萬筆以上。

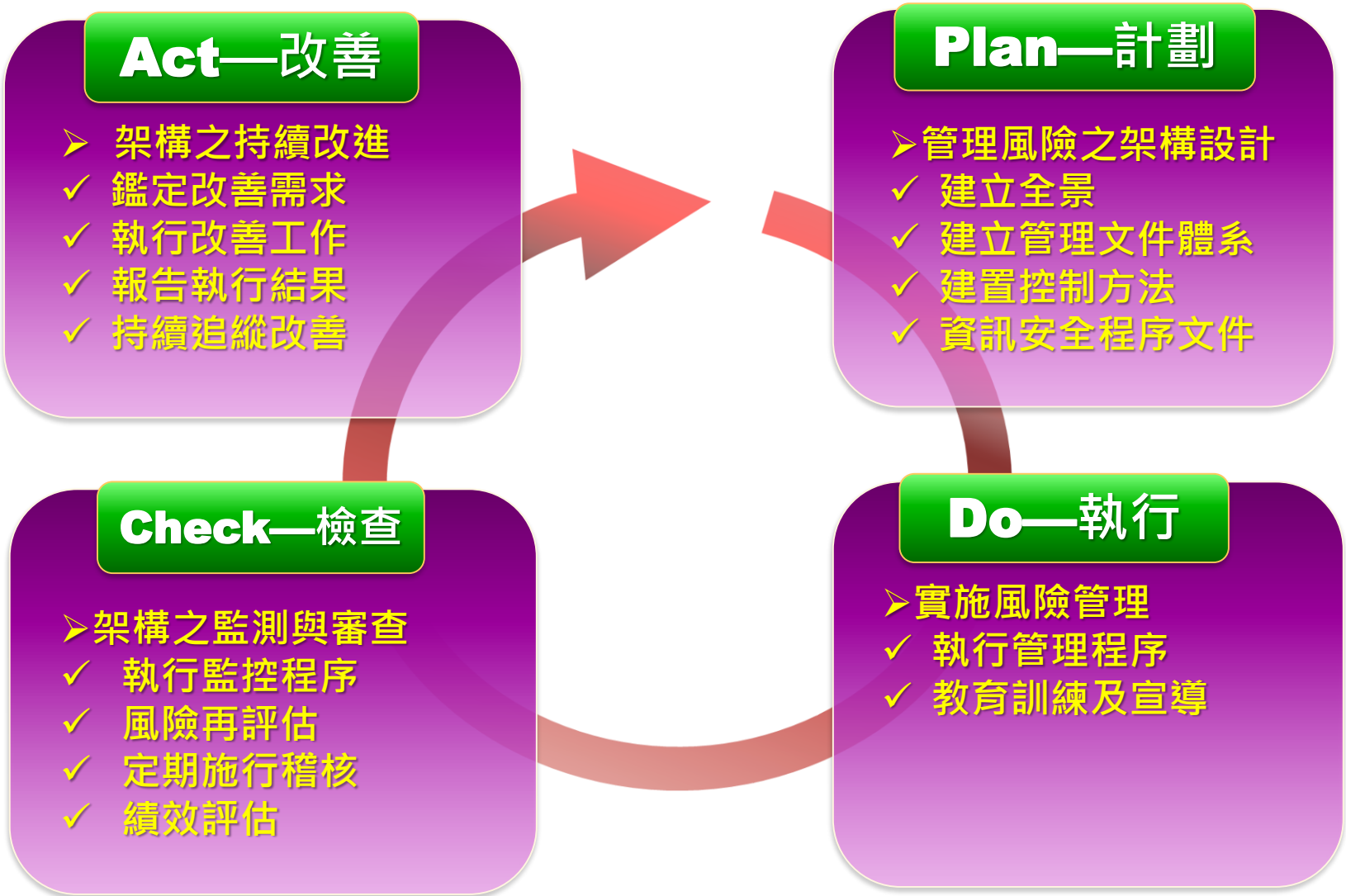
個人資料檔案清冊-蒐集、處理、利用

填報單位	
個資資產編號	
業務流程名稱	
個人資料檔案名稱	
資料形式	
法律依據或內部規定	
特定目的	
個人資料類別	
個人資料範圍	
有否特種資料？何種特種資料？	
有無監督管理之非公務機關及其名稱	
蒐集	來源
	方式
	單位
處理	方式
	單位
利用	期間
	地區
	單位
	方式目的
保存	單位
	聯絡人
	期限
銷毀	形式
	頻率
揭露	對象
	目的
	方式
	個資範圍
現有控制措施	
衝擊值	
個資數量	
重要性	
有無訂定個資保護作業規範	

- **蒐集-來源**：當事人/內部或外部。
- **蒐集-方式**：填寫直接蒐集或間接蒐集。
- **蒐集-單位**： 本身單位或外部單位名稱。
- **處理-方式**：記錄/輸入/儲存/編輯/更正/複製/檢索/刪除/輸出/連結/內部傳送（同個資法第二條定義）。
- **處理-單位**：本身單位或外部單位名稱。
- **利用-期間**：業務期間。
- **利用-地區**：臺灣或其他地區國家名稱。
- **利用-單位**：自己單位或其他組室或外部單位名稱。
- **利用-方式**：電子郵件傳送/電話訪問/紙本傳送等。

ISMS及PIMS
風險評鑑及處理方法

風險管理過程導向 - PDCA



風險管理流程

建立全景

- 界定其組織目標，定義機關風險管理之外部及內部變數，設定範圍及風險條件，包含外部環境與內部環境
- 外部環境包含如政治、法律、法規命令等
- 內部環境如政策、目標、組織架構等

風險辨識

- 組織應辨識其風險來源、衝擊範圍、事件所引起原因及其潛在的後果，以達成其風險管理目標。

風險管理流程

風險分析

- 瞭解風險發展的過程，以提供決策者是否採行最適當的策略與方法，並進一步處理風險。
- 現有之控制措施的效能及效率亦應納入考量

風險評量

- 針對風險分析過程發現事項，進行風險等級區分，並根據風險分析的輸出，包含有哪些風險需要被處理，處理的優先順序等

風險管理流程

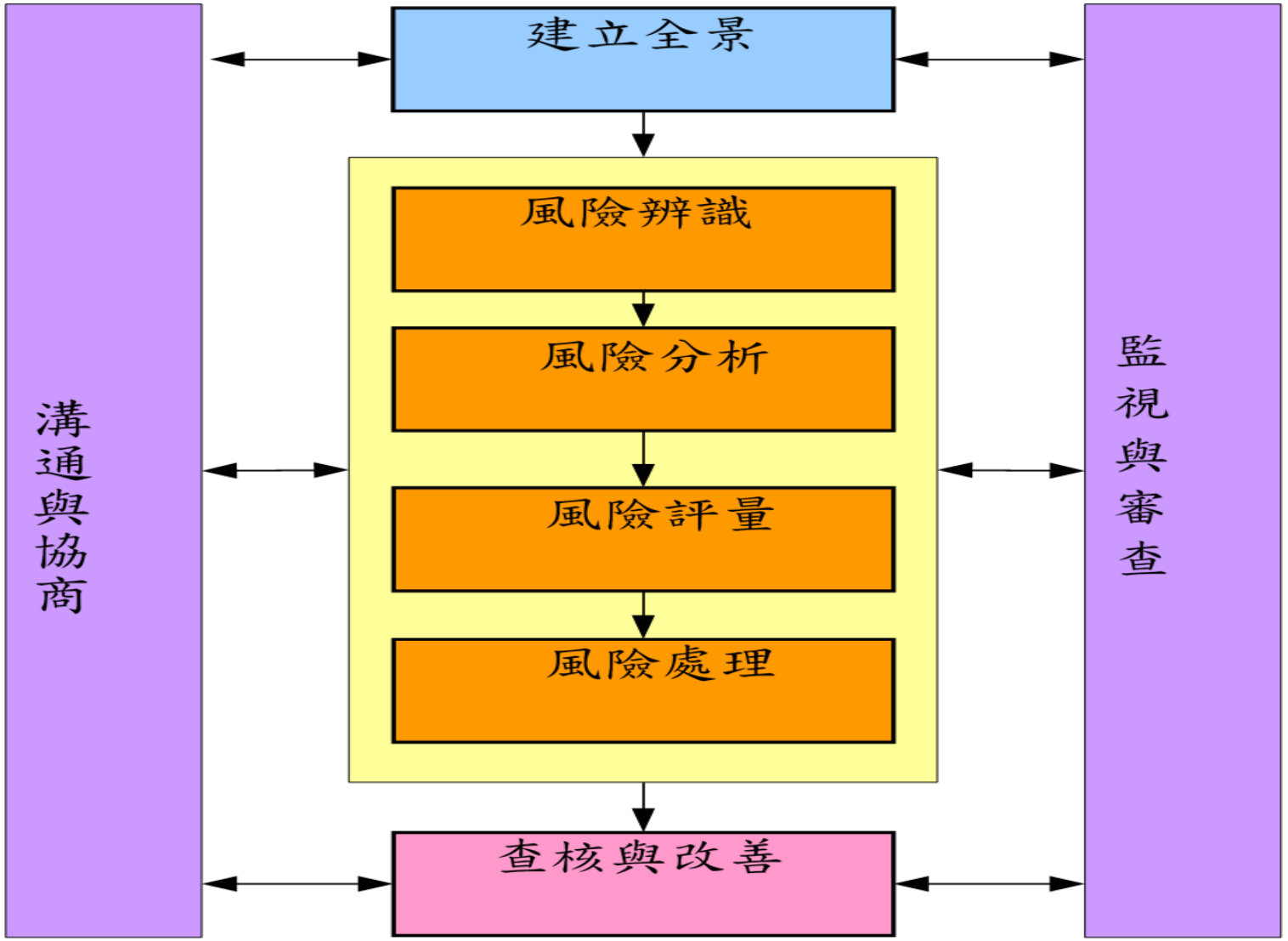
風險處理

- 評鑑風險處理方案的有效性。
- 決定可接受的殘餘的風險值。
- 若無法接受，則產生另一風險處理方案。
- 再評鑑風險處理方案的有效性。

查核與改善

- 確保風險管理的所有過程，所有的控制措施，在設計或操作之效能與效率
- 並獲得進一步的資訊以改善風險評鑑
- 針對事故發生的原因，進行分析與經驗學習
- 偵測機關內、外部的變更
- 識別緊急的風險

風險管理流程圖



風險的定義

- 所謂「風險」乃是當「威脅」利用其相對應「脆弱性」，直接或間接造成組織或政府機關，一個或一群「資訊資產」受到漏失或損害的「可能性」。
- 風險主要運用兩個因素的結合定義其特性，分別為「可能性」與「衝擊」。

威脅脆弱點範例

- 非法人士的攻擊入侵【威脅】是利用個人電腦【資產】（Windows 7）作業系統終止軟體修補作業(EOS)【脆弱點】導致資料外洩【衝擊】。
- 因操作不當【威脅】當負責人員【資產】教育訓練不足【脆弱點】時，業務無法正常運作【衝擊】。
- 機櫃內有重要硬體【資產】但機櫃未上鎖【脆弱點】，因此可能被偷【威脅】造成組織財產損失【衝擊】。

威脅及弱點評估表-修訂前範例

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	威脅等級(發生之可能性)			弱點等級(受到威脅利用容易度)			風險值
						低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	
NUTN-CM-001	CM	中華電信對外光纖線路	4	通訊服務失效	缺乏有效變更控制	1			1			4
				通訊服務失效	連線電纜失效	1			1			4
				通訊服務失效	頻寬不足	1				2		8
				線路受損	未適當保護通訊線路	1			1			4

原ISMS及PIMS評估標準

事件發生可能性/等級對應表

評估標準	等級	評估值
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

弱點的等級對應表

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

ISMS評估標準（預計調整）

風險發生可能性評估表

目前尚未完成改版僅提供參考

評估標準	評估值
每年發生次數小於等於1次	1
每年發生次數為2至3次	2
每年發生次數大於等於4次	3

衝擊值評估表

評估標準	評估值
無傷害 1.對組織無任何影響 2.資料無損毀，組織資料可正常提供 3.組織可容許該風險造成服務失效3工作天以上	1
低度傷害 1.該風險對組織造成的衝擊（含組織聲譽及財務影響）為可接受範圍 2.資料損毀或遭竄改，組織資料可供回復 3.組織可容許該風險造成服務失效8工作小時以上，3工作天以下	2
中度傷害 1.該風險對組織造成一定程度的衝擊（含組織聲譽及財務影響） 2.資料損毀或遭竄改，組織有備份資料可供回復 3.組織可容許該風險造成服務失效4工作小時以上，8工作小時以下	3
重大傷害 1.該風險對組織造成重大的衝擊（含組織聲譽及財務影響） 2.資料損毀或遭竄改且組織無任何備份資料可供復原 3.組織可容許該風險造成服務失效4工作小時34	4

PIMS評估標準（預計調整）

風險發生可能性評估表

評估標準	評估值
每年發生次數小於等於1次	1
每年發生次數為2至3次	2
每年發生次數大於等於4次	3

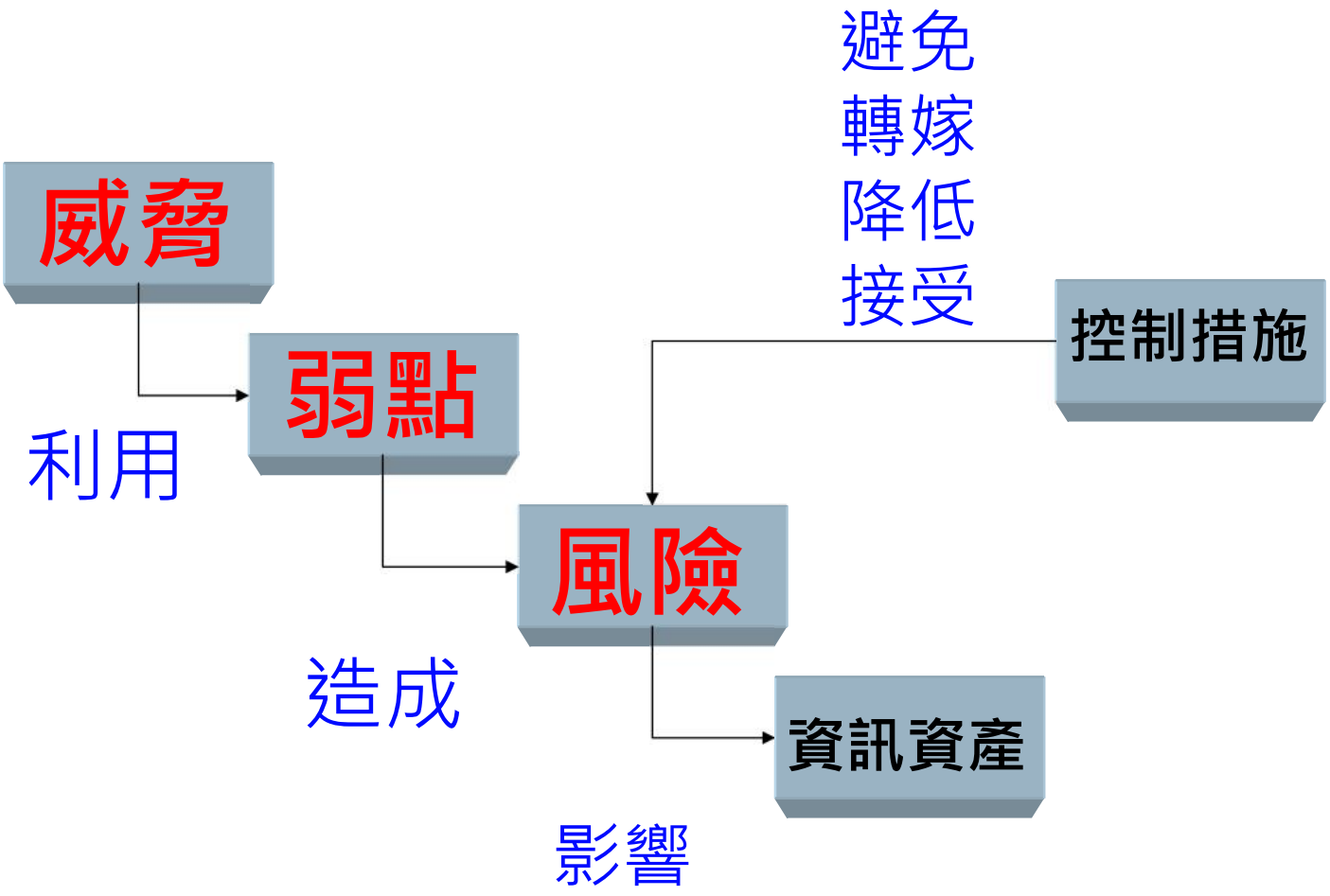
衝擊值評估表

項目 評估值	財務影響	對當事人損害程度
1	保有個資數量500筆(含)以內，全數外洩或處理不當，造成財務影響。	個人資料檔案機敏等級低，資料外洩對不致影響個人權益或僅導致個人權益輕微受損。（如個資資產價值「1」者）
2	保有個資數量逾500筆~5,000筆(含)以內，全數外洩或處理不當，造成財務影響。	資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益部份受損。（如：含身分證號財務資訊，個資資產價值「2」者）
3	保有個資數量逾5,000筆~5萬筆(含)以內，全數外洩或處理不當，造成財務影響。	資料外洩資料外洩可能導致個人隱私遭冒犯，當事人個人權益嚴重受損。（如：含身分證號財務資訊，個資資產價值「3」者）
4	保有個資數量逾5萬筆，全數外洩或處理不當，造成財務影響。	資料外洩將造成個人身心受到危害、社會地位受到損害、或衍生財物損失，當事人個人權益非常嚴重受損。（如：含特種個資、特種身分輔導紀錄等，個資資產價值「4」者）

威脅及弱點評估表-修訂後範例

資產編號	資產類別	資產名稱	資產價值	威脅	弱點	可能性評估值			衝擊值			風險值
						低(1)	中(2)	高(3)	低(1)	中(2)	高(3)	
NUTN-CM-001	CM	中華電信對外光纖線路	4	通訊服務失效	缺乏有效變更控制	1			1			4
				通訊服務失效	連線電纜失效	1			1			4
				通訊服務失效	頻寬不足	1				2		8
				線路受損	未適當保護通訊線路	1			1			4

風險管理關係圖



風險處理的選擇

- 風險處理方式的選擇不一定要在所有情境下並存或單獨存在，可能的選擇有：

① 移除風險來源
② 降低可能性
③ 將風險轉移（分攤）給其他組織
④ 經審慎評估後，決定接受風險。

風險處理評估

- 風險處理包含選擇或使用一種或多種方式控制風險，一旦執行，風險處理將提供或調整控制的方法。
- 風險處理是循環式的程序，包括：

① 評估風險處理方法
② 判斷殘餘風險是否為可接受風險程度
③ 假如無法接受，應設計不同的風險處理方法
④ 評估處理的有效性

風險處理考量

- 風險處理方式的選擇

選擇最適當的風險處理方式需考量法規、其他規定或考量的成本與效益的平衡，其中包括企業社會責任和環境保護。

選擇時應考量罕見且嚴重的風險(發生可能性低但負面影響高)，對這類風險而言，經濟或成本並非處理方式選擇的主要考量。

風險評鑑作業程序

- 鑑別資產
  - 資訊資產之鑑別應依據「資訊資產管理程序書」進行鑑別及分類。
- 鑑別風險
  - 威脅暨弱點評估：

  參考教育體系資通安全管理規範將各類資訊資產可能面臨之威脅與弱點項目，分別建立「威脅及弱點評估表」。

ISMS風險值計算

原版

「風險值」=
風險值=（資訊資產價值 × 威脅等級 × 弱點等級）

調整為

「風險值」=
風險值=（資訊資產價值 × 可能性評估值 × 衝擊值 ）

PIMS風險值計算

原版

「風險值」=
風險值= (資訊資產價值 × 威脅等級 × 弱點等級)

調整為

「風險值」=
風險值= (個資資產價值 × 可能性評估值 × 衝擊值)

訂定可接受風險值

可接受風險值

- 資訊資產之可接受風險值，需經資通安全管理規範導入工作小組開會決議，並記載於會議紀錄中。
- 通安全管理規範導入工作小組每年召開會議檢討可接受風險值。可接受風險必須考量組織環境及作業之安全需求，並進行適當地調整。
- 資通安全管理規範導入工作小組應針對高於可接受風險值項目，產出「風險評鑑彙整表」，並彙整相關綜合風險值，產出「風險評鑑報告」作為風險管理之依據。

風險處理

風險改善計畫

- 資通安全管理規範導入工作小組應檢視「風險評鑑報告」及「風險評鑑彙整表」。
- 若風險值超出可接受風險值之資訊資產，應參考教育體系資通安全暨個人資料管理規範選擇適當之控管措施，隨後產出「風險改善計畫表」，說明風險控管措施之執行辦法。
- 「風險改善計畫表」應陳報資通安全委員會開會審核，並列入追蹤管理程序。

風險再評鑑

- 風險改善狀況的後續追蹤
  - 對風險改善計畫應彙整控管，持續追蹤至完成改善為止。
  - 應於各風險改善措施完成後，進行風險再評鑑，以確保相關改善措施的有效性。

查核與改善

- 監控
  - 實施控制措施必須建立相對應的指標或紀錄，以反應出控制措施實施的狀況及成效，便於管理階層及相關人員做定期或不定期審視。
- 持續改善
  - 為保持本風險評鑑方法之有效性與適用性，資通安全管理規範導入工作小組得定期檢討可接受風險值與威脅及弱點評估表之項目。以期確保資訊資產均處於最佳保護之下，提供持續不中斷的營運。
- 風險重新評鑑
  - 每年應至少執行1次風險評鑑。
  - 當新增系統、系統有重大異動、營運組織或範圍改變時則應執行不定期之風險評鑑。

不定期之風險評鑑

資訊資產之新增、異動

- 資訊資產新增或異動時，
  資訊資產使用單位應填寫「資訊資產異動申請表」，
  經資通安全管理規範導入工作小組會議決議後，
  交由文件管理人員保管，並定期更新「資訊資產清單」。
- 資訊資產價值為4者，
  經呈核至資通安全官並重新檢視威脅弱點評估表及
  執行風險評估作業。

學校各單位保有個人資料檔案清查盤點系統操作說明

各單位保有個人資料檔案清查系統操作業簡介(1/3)

- http://inventory.nutn.edu.tw/(清查系統)
- https://pip.nutn.edu.tw/(個人資料保護宣導網)

各單位保有個人資料檔案清查系統操作業簡介(2/3)

- 各單位保有個人資料清查方向：
  - 法令、法規要求保有之資料。
  - 既有文件判別。
  - 組織業務分析。
  - 作業流程分析。
  - 單位特殊需求保有之資料。

各單位保有個人資料檔案清查系統操作業簡介(3/3)

- 本校各單位保有個人資料檔案清查盤點系統，教職員、計畫助理及工讀生均可以校務系統帳號登入操作使用。
- 國立臺南大學各單位保有個人資料檔案清查盤點系統，依國立臺南大學個人資料檔案清冊需求開發，填報順序依序為P1名稱、P2目的、P3蒐集、P4處理、P5利用、P6保存、P7銷毀、P8揭露、P9重要性。

各單位保有個人資料檔案清查盤點系統填報畫面

單位流水號	業務流程名稱	狀態	填報人員	最後修改日期	編輯	刪除
1	學生校園授權序號申請作業	完成	王元良	2014-10-15 16:05:55	編輯	刪除
2	GM2電子郵件帳號申請	完成	蔡東樺	2014-09-11 15:49:31	編輯	刪除
3	建立學生校務系統帳號	完成	蔡東樺	2014-09-06 17:56:07	編輯	刪除
4	國立臺南大學網路故障報修系統	完成	張育傑	2014-11-28 08:26:31	編輯	刪除
5	國立臺南大學IP申請管理系統	完成	張育傑	2014-11-28 08:26:36	編輯	刪除
6	學生ASP網頁申請作業	完成	吳世逖	2014-10-24 17:16:29	編輯	刪除
7	單位網頁申請作業	完成	吳世逖	2014-10-27 14:19:26	編輯	刪除
8	教師ASP網頁申請作業	完成	吳世逖	2014-11-26 08:42:35	編輯	刪除
9	學生社團網頁帳號申請作業	完成	吳世逖	2014-11-28 10:14:59	編輯	刪除
10	教職員生問題諮詢服務作業	完成	顏志榮	2015-06-02 09:04:42	編輯	刪除

各單位保有個人資料檔案清查盤點系統-新增資料

各單位保有個人資料檔案清查盤點系統-檢視單位清冊

序號	個人資料檔案名稱	保有依據	特定目的	個人資料類別	備註
1	學生校園授權序號申請資料	無	一〇九教育或訓練行政	C〇〇一辨識個人者。	
2	國立臺南大學gm2帳號申請表	google服務規範	一〇九教育或訓練行政	C〇〇一辨識個人者。	
3	學生校務系統帳號	無	〇〇二人事管理	C〇〇一辨識個人者。	
4	國立臺南大學網路故障報修系統	無	〇〇二人事管理	C〇〇一辨識個人者。 C〇一三習慣。 C〇三八職業。	
5	國立臺南大學IP申請管理系統	無	〇〇二人事管理	C〇〇一辨識個人者。	
6	學生ASP網頁申請表	無	一〇九教育或訓練行政	C〇〇一辨識個人者。	無
7	單位網頁申請表	無	一〇九教育或訓練行政	C〇〇一辨識個人者。	無
8	教師網頁帳號申請表	無	一〇九教育或訓練行政	C〇〇一辨識個人者。	無

國立臺南大學
個人資料檔案清冊

國立臺南大學個人資料檔案清冊

文件編號：　　機密等級：□公開使用 □內部使用 □內部限閱 □機密

紀錄編號：　　版次：1.0

填表日期：　　年　　月　　日

個資資產編號		
業務流程名稱		
個人資料檔案名稱		
資料形式		
法律依據或內部規定		
特定目的		
個人資料類別		
個人資料之範圍		
有否特種資料？何種特種資料？		
有無監督管理之非公務機關及其名稱		
蒐集	來源	
	方式	
	單位	
處理	方式	
	單位	
利用	期間	
	地區	
	單位	
	方式目的	
保存	單位	
	聯絡人	
	期限	
銷毀	形式	
	頻率	
揭露	對象	
	方式目的	
	個資範圍	
現有控制措施		
衝擊值		
個資數量		
重要性		
有無訂定個資保護作業規範		

各單位保有個人資料檔案清查盤點系統-說明文件

- 系統右上方「說明文件」連結：http://inventory.nutn.edu.tw/Images/個人資料檔案清查盤點系統操作說明.pdf

學校各單位保有個人資料檔案
威脅及弱點評估表操作說明(表單系統)

國立臺南大學表單填報系統

https://system.nutn.edu.tw/formfill
(表單填報系統)

國立臺南大學表單填報系統

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

Q/A

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

感謝您的參與

歡迎於活動後與講師討論您的任何疑問

本局的臉書粉絲團及部落格可以找到更多資訊

TSC – FB Site

TSC – Blog Site