國立中興大學
National Chung Hsing University

個人資料
隱私衝擊分析與風險評鑑教育訓練

NII 產業發展協進會

109.09.09

109.09.16

109.09.28

財團法人中華民國國家資訊基本建設產業發展協進會
National Information Infrastructure Enterprise Promotion Association

大綱

- 個資盤點-個人資料檔案清冊複習
- 隱私衝擊分析(資產價值-衝擊值)
- 風險管理作業說明
- 實作風險評鑑
- 風險處理與管控

2

個資盤點-個人資料檔案清冊複習

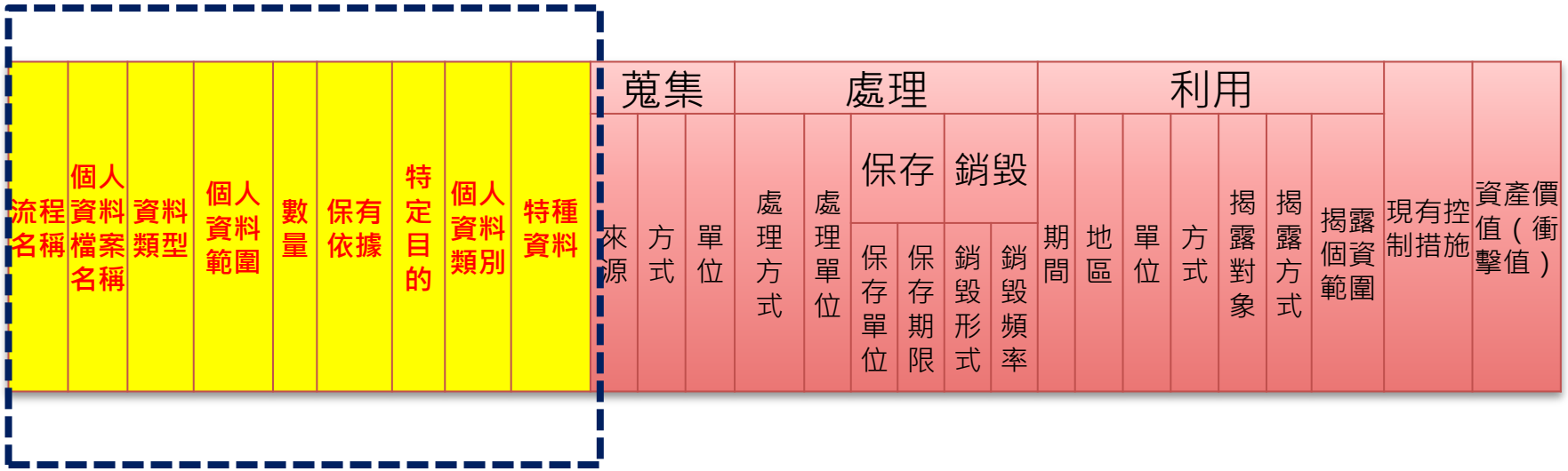
個人資料檔案清冊複習

業務職掌
挖掘個資

分析個資
生命周期

識別現行
保護措施

個人資料
風險管理



個人資料檔案清冊複習(續)

流程名稱	個人資料檔案名稱	資料類型	個人資料範圍	數量	保有依據	特定目的	個人資料類別	特種資料
建議由**業務職掌**來表達個資流程名稱	※	紙本 電子 **(若同時有兩個資產，請分列表示)**	**列出該業務流程中有使用到之個資欄位**	**每年：約XX筆** **總量：約XX筆**	**1、法律明文規定** **2、校內執行業務所需之規定** **3、當事人同意**	以法務部182項特定目的 **(以個人資料之範圍而定)**	依法務部134項個人資料類別項目填寫 常用：C001 辨識個人者、C002 辨識財務者 、C003 政府資料中之辨識者、C038 職業) **(以執行業務，選擇合宜特定目的)**	有 無

個人資料檔案清冊複習(續)

業務職掌 挖掘個資 → 分析個資 生命周期 → 識別現行 保護措施 → 個人資料 風險管理

個人資料檔案清冊複習(續)

蒐集			處理						利用						
來源	方式	單位	處理方式	處理單位	保存單位	保存期限	銷毀形式	銷毀頻率	期間	地區	單位	方式	揭露對象	揭露方式	揭露個資範圍
當事人 其他管道(問卷人力銀行)	直接 間接	最源頭的單位	1.由業務單位提供資料(資料如何來 2.資料處理方式（於自己單位怎麼處理 SOP) 3.資料流向(A、B、C單位) 4.留存副本備查 /資料留存於 「XX系統」備查	自己單位 下一個處理單位(若有)	自己單位 單位不留存	保存N年 不定期更新 單位不留存	碎紙機銷毀、檔案刪除、更新覆蓋集中銷毀 無需銷毀 單位不留存	N年N次/定期或不定期 無需銷毀 單位不留存	無 業務期間	無 臺灣 其他國家	無 自己單位	無 聯絡當事人 揭露	無 揭露單位(若利用方式為「揭露」時)	揭露方式(若利用方式為揭露時) 郵寄 email 傳真 公文 系統介接	1、若無揭露，表達「無」 2、若揭露資料屬全部揭露請表達「同前項個人資料範圍」 3、若非全部揭露請直接表達個資欄位(如姓名、出生年月日)

個人資料檔案清冊說明(續)

業務職掌 挖掘個資 → 分析個資 生命周期 → 識別現行 保護措施 → 個人資料 風險管理

本次課程重點

個人資料檔案清冊說明(續)

紙本文件
(Document)

- 上鎖倉庫、資料櫃、抽屜、防潮箱.....

電子檔案
(Data)

- 個人電腦帳密管理
- 儲放於**XX系統**權限帳密管理
- 共享資料夾權限管理
- 備份硬碟上鎖管理.....

明確說明
系統名稱

9

隱私衝擊分析(資產價值-衝擊值)

隱私衝擊分析(資產價值-衝擊值)cont.

衝擊影響程度	個人資料範圍
極高(4)	符合下列一項: 1. 含自然人之姓名及特種個人資料。 2. 含國民身分證統一編號 (或護照號碼) 及特種個人資料。
高度(3)	符合下列一項： 1.含國民身分證統一編號(或護照號碼)及其他個人資料。 2.含自然人之姓名及財務情況（如：帳號）。
中度(2)	含自然人之姓名及其他個人資料 ，但不包含國民身分證統一編號、財務情況或特種資料。
一般(1)	符合下列一項： 1. 屬於保管單位，且不接觸個人資料。 2. 兩項其他個人資料(含)以上，但不包含姓名、國民身分證統一編號財務情況或特種資料。

隱私衝擊分析(資產價值-衝擊值-範例)

◆針對以下個人資料檔案清冊，進行**資產價值-衝擊值**

個人資料檔案名稱	資料形式	個人資料之範圍	資產價值-衝擊值
教師聘用資料	紙本	姓名、出生年月日、國民身分證統一編號、特徵、教育、職業、家庭、聯絡方式、財務狀況、**醫療(身障手冊影本)**	
職員人事資料	電子	姓名、國民身分證統一編號、性別、出生日期、通訊處及電話、學歷、考試、外國語文、訓練進修、家屬、兵役、教師資格、**身心障礙類別**、經歷及現職、獎懲、考績	
境外交換學生名冊	紙本	姓名、護照號碼、出生年月日、聯絡方式、教育	
學生實習名單	紙本	姓名、聯絡方式、教育	

12

風險管理作業說明

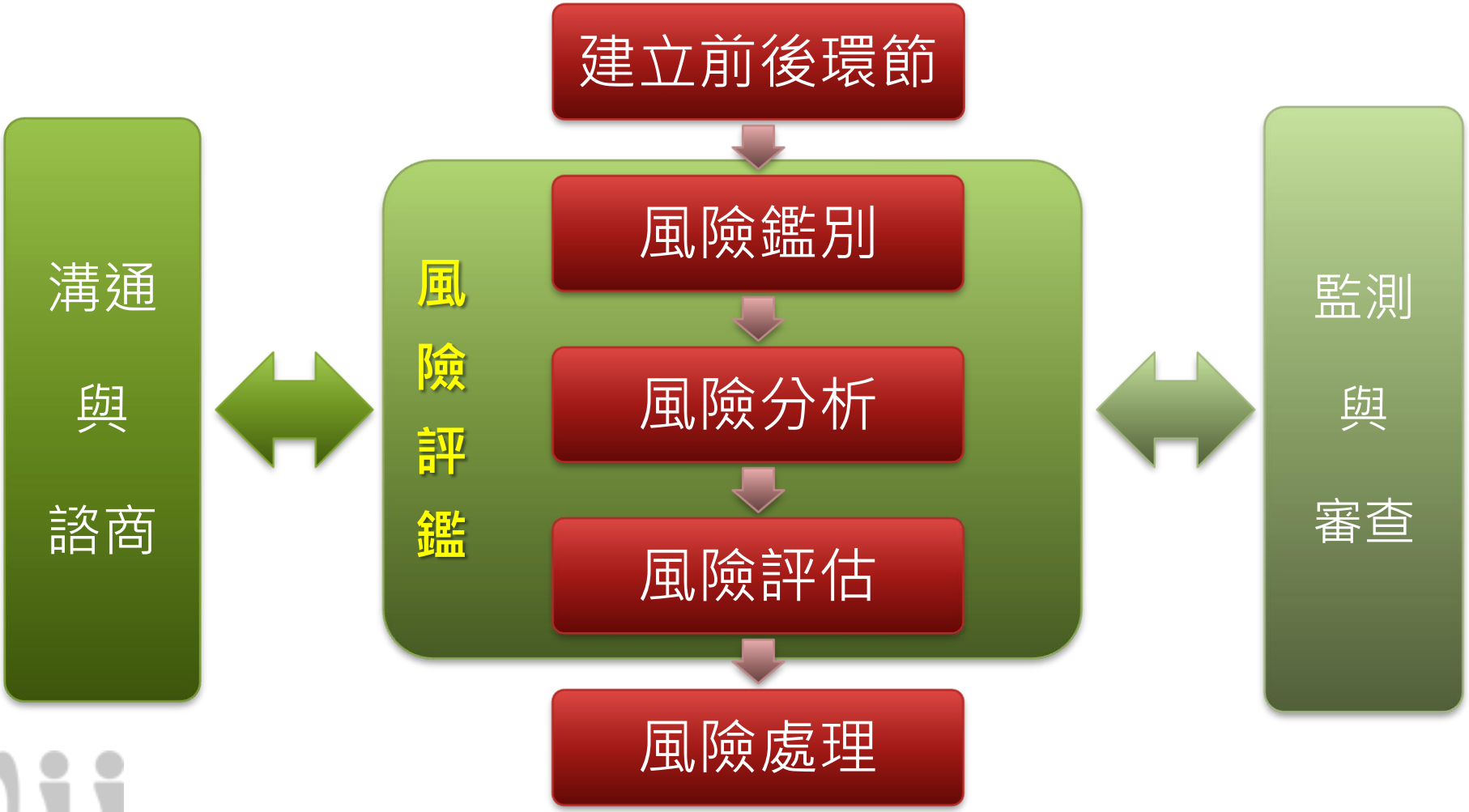
風險管理

- 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**
  - 個人資料遺失
  - 資訊誤用
  - 系統程式不當揭露
  - 資料遭偷竊

風險管理所帶來的效益

- Identify personal data 識別個人資料檔案– **我需要保護什麼?**
- Identify threats 識別風險來源、事件–**我需要採取何種對策?**
- Calculating risks 計算風險–**需要多少時間、人力、或成本來保護重要個人資料檔案?**

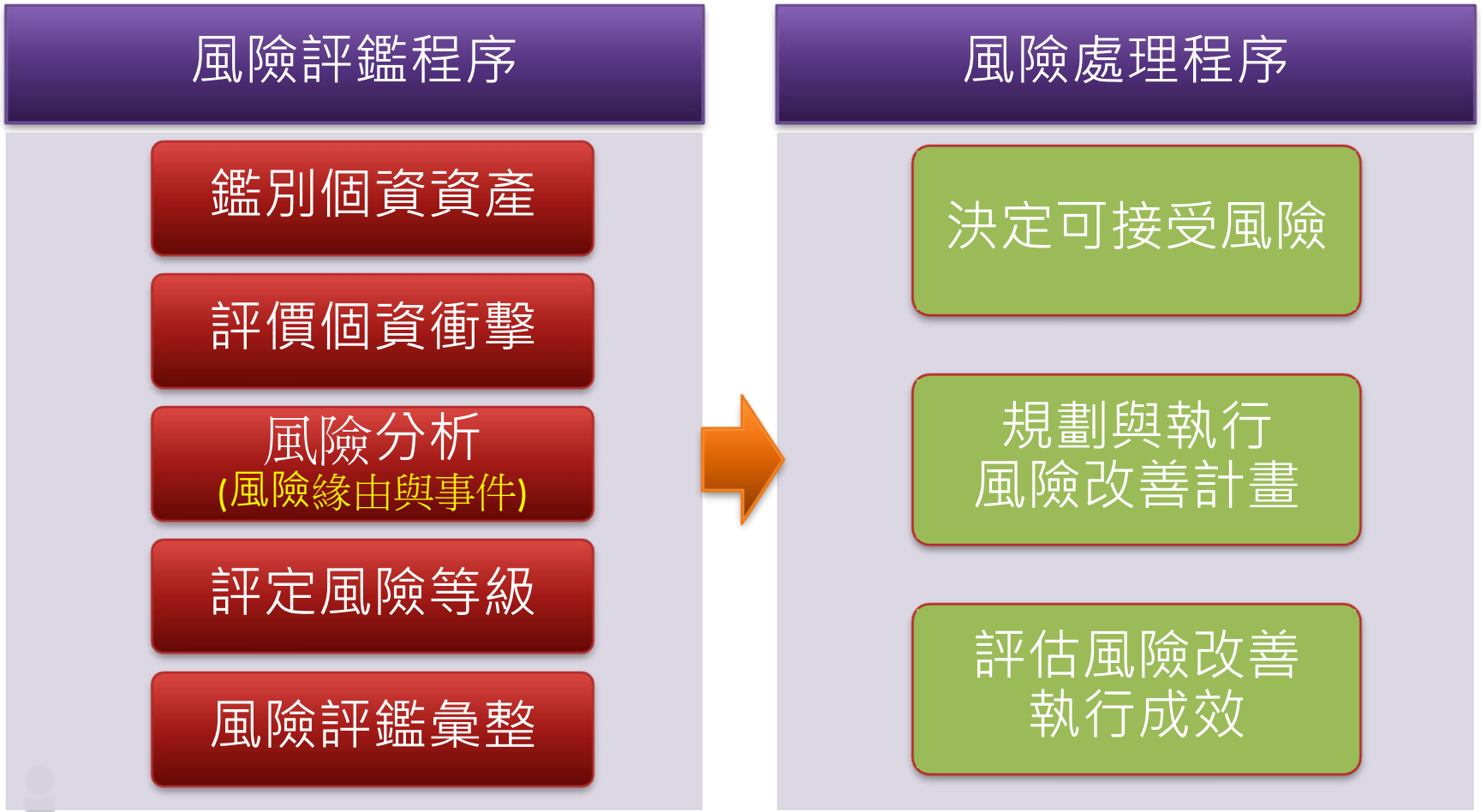
風險管理流程_ISO31000



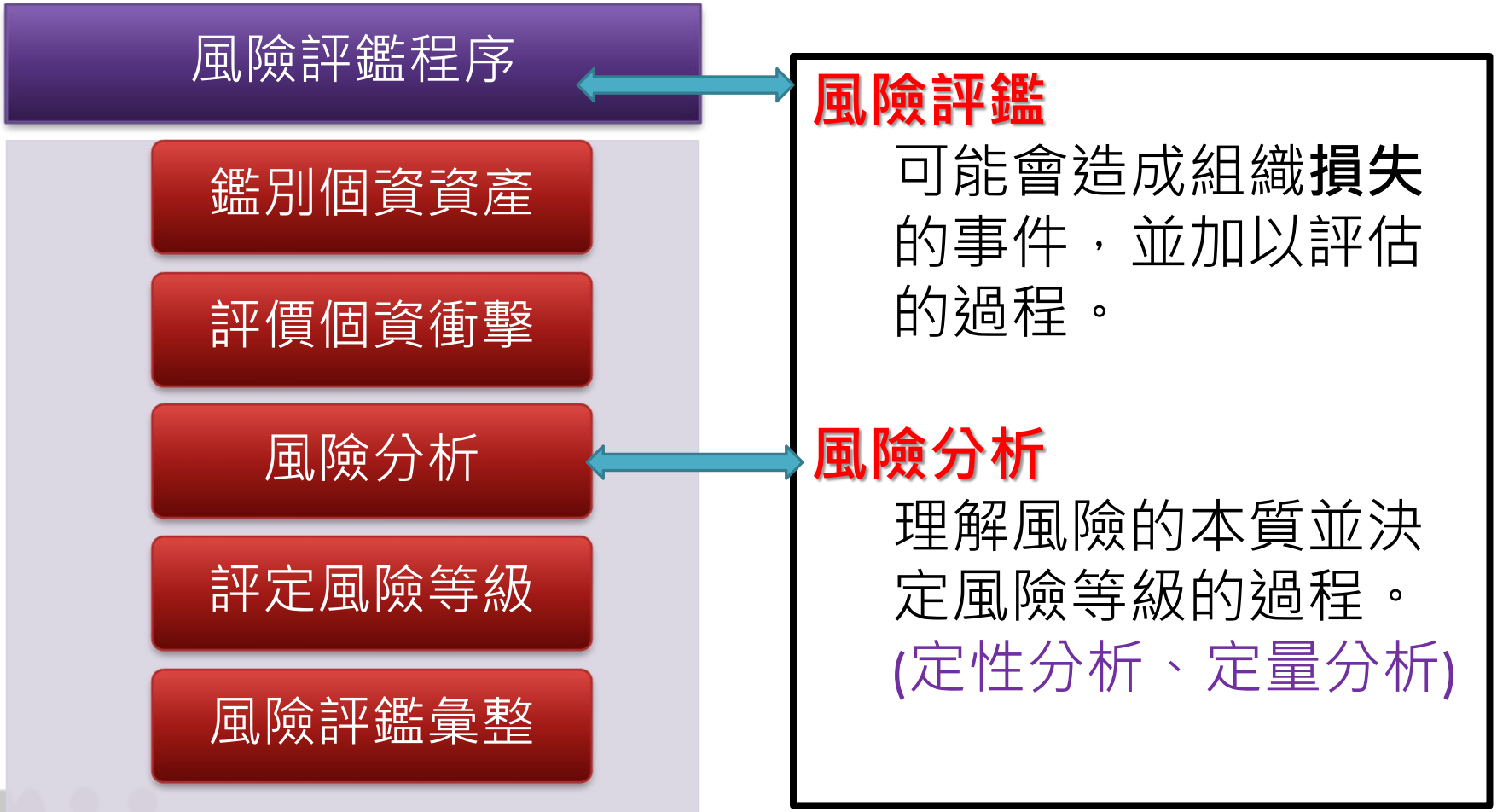
16

實作風險評鑑

風險評鑑與風險處理管理流程



風險評鑑流程



風險分析方式

- **定量分析**
  - 試圖去分配獨立的數量化價值物件作為風險評鑑的要素及潛在損失的評估
  - 如,個資保有數量、財務影響
- **定性分析**
  - 以情節為導向
  - 如,資產價值、弱點及威脅的重要等

風險緣由與事件

風險緣由

- **定義:可能導致風險的要項**
  - 天然災害：颱風、地震、水災及停電等
  - 人為因素：非法存取資料、偷竊及竄改資料等

事件

- **定義:所發生的變動或特定情況**
- 常見事件:
  - 不熟悉法令法規及內部規範。
  - 個人資料被竊取、竄改、毀損、滅失或洩漏。
  - 儲存媒介之不當存取。
  - 誤用資料。

風險評鑑工具-風險評估表

文件名稱：風險評估表(電子)		機密等級：□公開使用 ■內部使用 □內部限閱 □機密	
文件編號：NCHU-PIMS-D-XXX		版次：1.0	
紀錄編號：		填表日期： 年 月 日	
個資資產編號：		蒐集單位：	
流程名稱：		保有單位：	
個人資料檔案名稱：		資產價值(衝擊值)：	
個人資料範圍：			

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值	0
全階段	教育訓練不足	不熟悉法令法規及內部規範				0	
蒐集	未告知個資法要求應告知事項	未遵循法令法規				0	
處理	資料未依使用期限進行銷毀或刪除	誤用資料				0	
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏				0	

風險評估表使用簡介

- **表頭各欄位**
  - 資料由「個人資料檔案清冊」對應而來
- **資料週期**
  - 全階段：蒐集、處理、利用皆有可能會遇到的「風險緣由」/「事件」
  - 呈上，蒐集階段、處理階段、利用階段為該階段才有可能會發生的「風險緣由」/「事件」

風險緣由、事件與風險的關係(範例)

- 工程師在更新網站時，不小心將**活動投保清單**放到網站的**下載檔案區**裡~

■ 個資資產	✓ 活動投保清單
■ 風險緣由	✓ 人員操作失誤
■ 事件	✓ 個人資料被竊取、竄改、毀損、滅失或洩漏
■ 風險	✓ **組織賠償損失、法律責任**

風險評估表-風險緣由/事件(全階段)

資料週期	風險緣由	事件	風險緣由/事件說明
全階段	心生不滿的內部人員	個人資料被竊取、竄改、毀損、滅失或洩漏	有意圖將單位個資竊取、竄改、毀損、滅失或洩漏之人員
全階段	未主動或依當事人之請求更正或補充個人資料	未遵循法令法規	個資法第11條要求
全階段	未提供當事人表示拒絕接受行銷之方式	未遵循法令法規	個資法第20條要求（適用於非公務機關-第20條）
全階段	未履行當事人行使之權利	未遵循法令法規	個資法第3條要求
全階段	委外作業規劃及管理不當	個人資料被竊取、竄改、毀損、滅失或洩漏	若該資產為委外廠商處理時，需依法進行合約、保密切結之簽署及資安管理規定
全階段	個資被竊取、洩漏、竄改未於查明後告知	未遵循法令法規	個資法第12條要求

風險評估表-風險緣由/事件(全階段)

資料週期	風險緣由	事件	風險緣由/事件說明
全階段	個資逾越特定目的之必要範圍	未遵循法令法規	個資法第5、6條要求
全階段	缺乏安全防護機制	個人資料被竊取、竄改、毀損、滅失或洩漏	欠缺蒐集、處理、利用執行過程中之安全管理措施要求
全階段	缺乏實體保護	個人資料被竊取、竄改、毀損、滅失或洩漏	紙本個資之實體環境管理措施
全階段	缺乏稽核監督機制	個人資料被竊取、竄改、毀損、滅失或洩漏	如欠缺內部稽核、委外廠商稽核規劃
全階段	教育訓練不足	不熟悉法令法規及內部規範	接觸個資業務之人員，對於個資管理不熟悉
全階段	意圖不軌的外部人員	個人資料被竊取、竄改、毀損、滅失或洩漏	有意圖將單位個資竊取、竄改、毀損、滅失或洩漏之人員(如委外廠商)
全階段	未清楚提供當事人行使權利(存取、更正、刪除等)的連絡管道或方式	當事人無法即時申張自身權利，導致個人資料被竊取、竄改、毀損、滅失或洩漏	單位未提供當事人於蒐集、處理、利用時，對外的連絡管道(如電話、email)

風險評估表-風險緣由/事件(蒐集)

資料週期	風險緣由	事件	風險緣由/事件說明
蒐集	未告知個資法要求應告知事項	未遵循法令法規	個資法第8條要求
蒐集	未取得當事人同意	未遵循法令法規	個資法第7條要求
蒐集	蒐集特種資料	未遵循法令法規	個資法第6條要求
蒐集	蒐集資訊缺乏正當合理之關聯	未遵循法令法規	個資法第5條要求

風險評估表-風險緣由/事件(處理)

資料週期	風險緣由	事件	風險緣由/事件說明
處理	未於法定期限內准駁	未遵循法令法規	個資法第13條要求
處理	未訂定保存期限	誤用資料	個資法第11條要求，若未設定保存期限，而超過當事人允許的使用期間/範圍，有可能會有資料誤用、導致違反之風險
處理	未經授權下處理資料	個人資料被竊取、竄改、毀損、滅失或洩漏	文件未依敏感等級進行有效的接觸權限管理
處理	存取權限授與不當	儲存媒介之不當存取	
處理	缺乏回收控管機制	個人資料被竊取、竄改、毀損、滅失或洩漏	如內部單位傳送時，無相關管控措施(如無申請單可追蹤、無借閱後回收管理機制)
處理	處理資料時未經確認	誤用資料	執行業務時，無確認所使用的個資是否合理使用(如逾越特定目的)、未經程序由單位主管確認等
處理	資料未依使用期限進行銷毀或刪除	誤用資料	個資法第11條要求，屆滿資產應依法刪除，若未刪隱、銷毀，若管理不當，有可能會有資料誤用、導致違反之風險
處理	資料銷毀處理程序不當或不足	個人資料被竊取、竄改、毀損、滅失或洩漏	銷毀未留存紀錄或未有合理的管理措施(如委外銷毀未約束相關要求)
處理	處理特種個資或分析逾越原特定目的之個資，未進行當事人同意	當事人資料造成高度風險竊取、竄改、毀損、滅失或洩漏可能性	未依個資法第5條及第6條特種個資要求，由當事人同意後方可使用

風險評估表-風險緣由/事件(利用)

資料週期	風險緣由	事件	風險緣由/事件說明
利用	未經授權下利用資料	個人資料被竊取、竄改、毀損、滅失或洩漏	1、文件未依敏感等級進行有效的接觸權限管理， 2、是否有外部來文或合約、協議，使其可對外揭露或連絡
利用	存取權限授與不當	個人資料被竊取、竄改、毀損、滅失或洩漏	
利用	缺乏回收控管機制	個人資料被竊取、竄改、毀損、滅失或洩漏	如外部單位傳送時，無相關管控措施(如無申請單可追蹤、委外協議就專案結束後，未要求委外商返還、刪除等機制)
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏	含敏感性個資(如具身份證字號、特種個資)，傳遞資料應有管控措施
利用	對於法令、法規了解不足(如國際傳輸)	未遵循法令法規	傳送至外部單位，應遵循當地之法令法規

風險評鑑工具-風險評估表

文件名稱：風險評估表(電子)				機密等級：□公開使用 ■內部使用 □內部限閱 □機密			
文件編號：NCHU-PIMS-D-XXX				版次：1.0			
紀錄編號：				填表日期： 年 月 日			
個資資產編號：				蒐集單位：			
流程名稱：				保有單位：			
個人資料檔案名稱：				資產價值(衝擊值)：			
個人資料範圍：							
資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值	0
全階段	教育訓練不足	不熟悉法令法規及內部規範				0	
蒐集	未告知個資法要求應告知事項	未遵循法令法規				0	
處理	資料未依使用期限進行銷毀或刪除	誤用資料				0	
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏				0	

評估構面1

評估構面2

風險評估構面1-衝擊影響

- 衝擊影響以個資數量，設定評估等級標準

評估值	衝擊影響
4	• 個資保管數量50001筆以上，若全數外洩，造成財務影響。
3	符合下列一項： • 個資保管數量5001筆-50000筆以內，若全數外洩，造成財務影響。 • 個資保管數量50001筆以上，但有進行安全管控，且尚無發生過個資事件。
2	符合下列一項： • 個資保管數量501-5000筆以內，若全數外洩，造成財務影響。 • 個資保管數量5001-50000筆(含)以內，但有進行安全管控，且尚無發生過個資事件。
1	符合下列一項： • 個資保管數量500筆以內，若全數外洩，造成財務影響。 • 個資保管數量5000筆(含)以內，但有進行安全管控，且尚無發生過個資事件。

✓ 第1條件：首次導入/非首次導入，但本年有發生個資事件
✓ 第2條件：非首次導入，且未發生個資事件

風險評估構面2-可能性

- 可能性以**安全管控程序、是否落實**，設定評估等級標準

評估值	可能性
4	未建立安全控管程序及相關文件，亦無任何安全控管
3	已建立安全控管程序及相關文件，未實施安全控管
2	未建立安全控管程序及相關文件，已實施安全控管
1	已建立安全控管程序及相關文件，且已落實安全控管

風險評估表-風險值計算方式

- 風險值 = 資產價值(衝擊值) X (衝擊影響 + 可能性)

文件名稱：風險評估表(電子)				機密等級：□公開使用 ■內部使用 □內部限閱 □機密			
文件編號：NCHU-PIMS-D-XXX						版次：1.0	
紀錄編號：						填表日期： 年 月 日	
個資資產編號：				蒐集單位：			
流程名稱：				保有單位：			
個人資料檔案名稱：				資產價值(衝擊值)：			
個人資料範圍：							
資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值	0
全階段	教育訓練不足	不熟悉法令法規及內部規範				0	
蒐集	未告知個資法要求應告知事項	未遵循法令法規					
處理	資料未依使用期限進行銷毀或刪除	誤用資料					
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏					

風險值取各項風險分析結果的「最大值」

風險評估表(範例)

全階段/處理-總量
蒐集-每年量
利用-視需求而定

因舉辦國際交流活動，委託**保險公司**協助**校內/外報名者辦理保險**。
該保險公司已是長期合作廠商，請學校以EXCEL彙整姓名、身分證字號、出生年月日資訊，辦理保險。
助理蒐集報名者資料後，**Email加密**給保險公司。

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
全階段	教育訓練不足	不熟悉法令法規及內部規範				
蒐集	未告知個資法要求應告知事項	未遵循法令法規				
處理	未訂定保存期限	誤用資料				
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏				

風險評估表(範例)

- 有規定須進行個人資料保護宣導，本年度已進行宣導
- 未進行告知事項
- 未訂定保存期限
- 有訂定個資保護規範，且Email寄出時用密碼保護

保險清冊.xls (首次導入)
- 蒐集400筆學生資料
- 已保存20年的歷史資料
- 已建立相關程序

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
全階段	教育訓練不足	不熟悉法令法規及內部規範				
蒐集	未告知個資法要求應告知事項	未遵循法令法規				
處理	未訂定保存期限	誤用資料				
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏				

風險評估表(範例)

因舉辦國際交流活動，委託保險公司協助校內/外報名者辦理保險。該保險公司已是長期合作廠商，請學校以EXCEL彙整**姓名、身分證字號、出生年月日**資訊，辦理保險。

- 「不適用」範例

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
蒐集	未依法蒐集**特種資料**	未遵循法令法規			0	

風險評估(範例)

- **保險清冊**
(姓名、身分證字號、出生年月日)
- 個資範圍評估值 = **3**

風險值-個資範圍評估值 X (衝擊影響 + 可能性)
- 取最大值 = **18**

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
全階段	教育訓練不足	不熟悉法令法規及內部規範	3	1		12
蒐集	未告知個資法要求應告知事項	未遵循法令法規	1	3		12
處理	未訂定保存期限	誤用資料	3	3		18
利用	傳輸過程未有適當之加密或保護	個人資料被竊取、竄改、毀損、滅失或洩漏	1	1		6

風險處理與管控

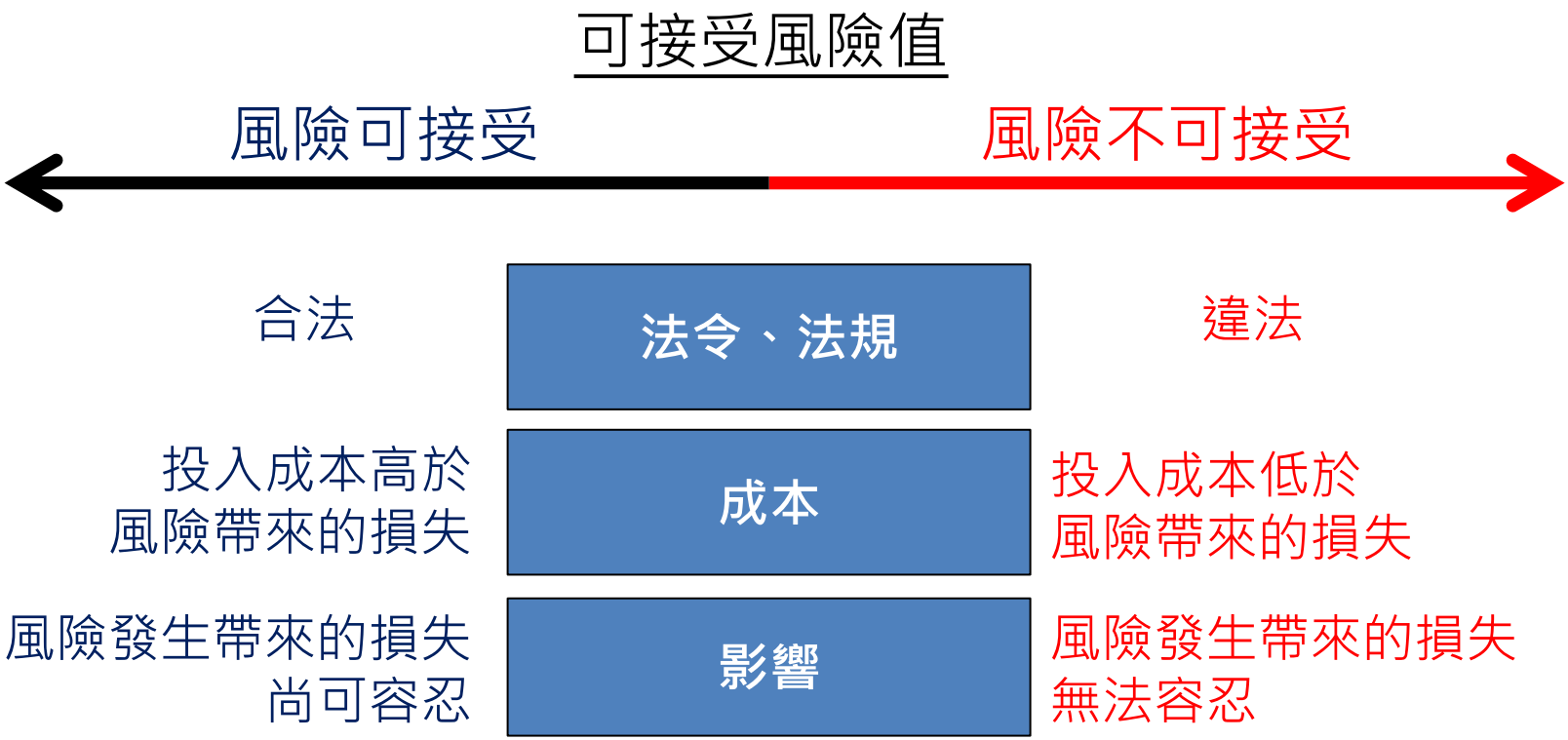
風險處理過程

- **風險處理**是一個循環的過程
  - 評估風險處理結果
  - 決定殘餘風險水準是否是可以容忍
  - 如果無法容忍，產生新的風險處理
  - 評估處理的成效

風險處理流程

決定可接受風險值

- **目的，在於決定何項風險須處理及優先順序。**



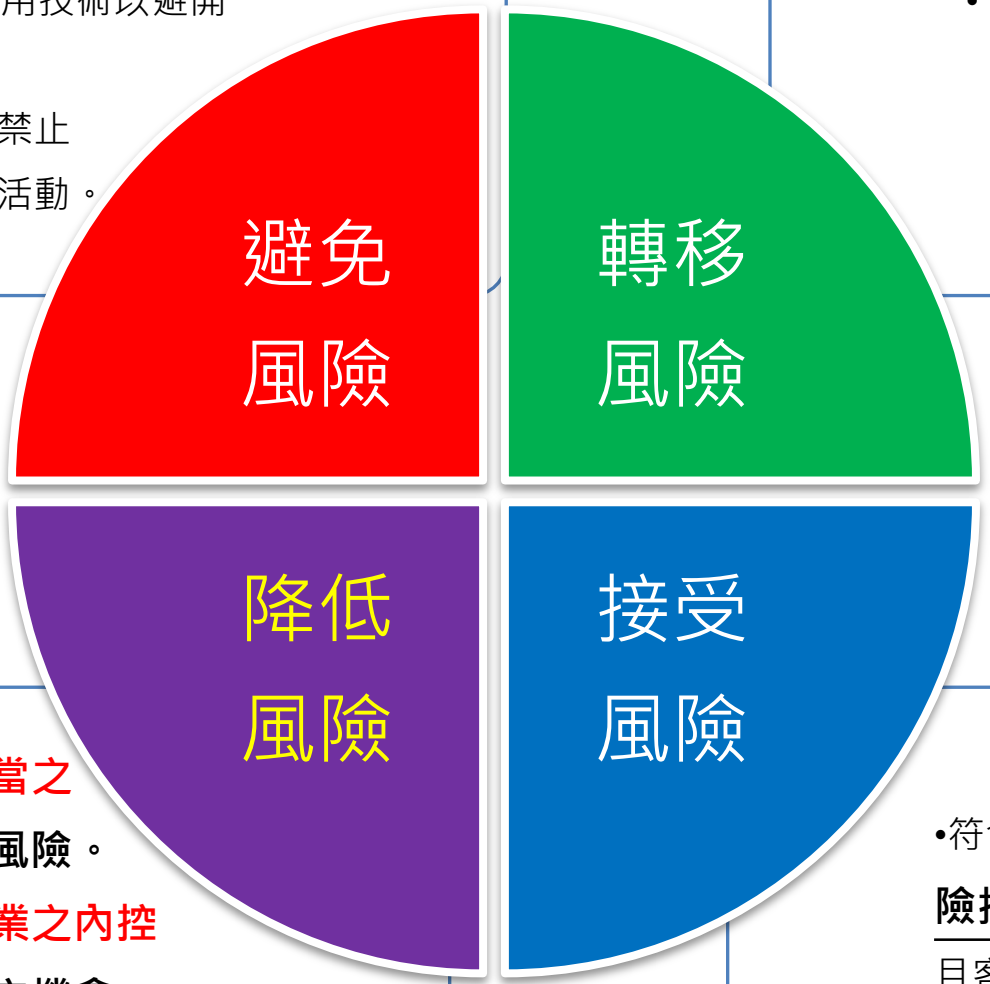
決定可接受風險值(續)

- **資源有限**
- **決定因素**
  - 風險嚴重(衝擊)程度(例如：財務、聲譽...)
  - 風險處理急迫性
  - 可分配的資源(例如：**人力、時間、金錢**)
- **決定方式**
  - 80/20法則(排序百分比法)
  - 基本統計(平均數、中位數)...等統計法
  - **過去經常性發生的個資事件、內外稽發現的問題**...等

風險處理型式

- 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交易或活動。

- 轉移相關之營運風險至他者，例如：承保商、供應商。



- **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。**

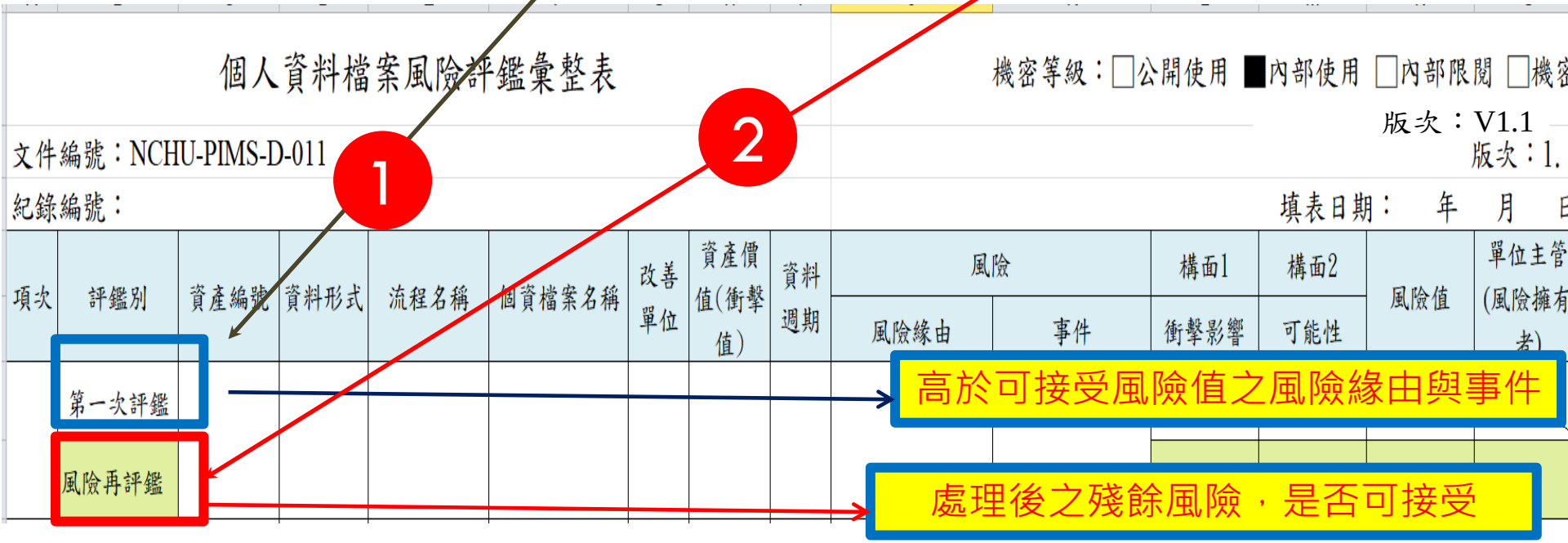
•符合**組織的政策與風險接受準則**，則知悉且客觀地接受風險。

風險控管原則

- 在符合法令要求下，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**
- 確認、控制及降低安全風險至可接受程度所採取的程序

風險處理工具 – 風險評鑑彙整表

用途: 用以(1)彙整**需要處理的風險**，及(2)處理後的**風險再評鑑**。



風險評鑑彙整表(範例)

可接受風險值：15(含)，風險值超過15以上者，必須進行風險處理

個人資料檔案風險評鑑彙整表

機密等級：□公開使用 ■內部使用 □內部限閱 □機密

文件編號：NCHU-PIMS-D-011　　版次：1.1

紀錄編號：　　填表日期：　年　月　日

項次	評鑑別	資產編號	資料形式	流程名稱	個資檔案名稱	改善單位	資產價值(衝擊值)	資料週期	風險		構面1	構面2	風險值	單位主管(風險擁有者)
									風險緣由	事件	衝擊影響	可能性		
1	第一次評鑑	XX組-001	電子	學生保險	保險名冊	XX組	3	處理	未訂保存期限	誤用資料	3	3	18	
	風險再評鑑													

風險處理工具 – 風險處理計畫

用途: 用以**紀錄需要處理高於可接受風險之個資資產**，並提出**風險處理計畫**。

個人資料檔案風險處理計畫

機密等級：□公開使用 ■內部使用 □內部限閱 □機密

文件編號：NCHU-PIMS-D-012　　版　　次：1.1

紀錄編號：　　填表日期：　　年　　月　　日

資產識別暨風險說明										風險處理措施		風險進度追蹤			
項次	單位	個資資產編號	資料類型	流程名稱	個人資料檔案名稱	資料週期	風險緣由	事件	風險值	風險處理型式	改善活動/控制措施	業務承辦人	預定完成日期	實際完成日期	單位主管(風險擁有者)
										□接受風險 □降低風險 □轉移風險 □避免風險					

風險處理計畫(範例)

風險處理計畫，必須由「風險擁有者」-單位主管核准後，方可執行。

個人資料檔案風險處理計畫

機密等級：□公開使用 ■內部使用 □內部限閱 □機密

文件編號：NCHU-PIMS-D-012　　版　　次：1.1

紀錄編號：　　填表日期：　　年　　月　　日

資產識別暨風險說明										風險處理措施		風險進度追蹤			
項次	單位	個資資產編號	資料類型	流程名稱	個人資料檔案名稱	資料週期	風險緣由	事件	風險值	風險處理型式	改善活動/控制措施	業務承辦人	預定完成日期	實際完成日期	單位主管(風險擁有者)
一	XX組	XX組-001	電子	學生保險	保險名冊	處理	未定保存期限	誤用資料	3	□接受風險 ■降低風險 □轉移風險 □避免風險	依本校檔案分類及保存年限區分表，訂定合宜保存期限，並於屆滿時辦理刪除作業	王小花	XXX.XX.XX		李大同

風險處理後

- **追蹤處理現況**
  - **建立評量指標(例如：KPI指標)**，協助控制目標達成
  - **執行內部稽核**，確保控制措施的有效性

- **除每年執行一次外，當有下列情況時，應執行風險評鑑作業**
  - 營運組織變更
  - 作業流程改變
  - 個人資料檔案新增或變更
  - 發生個資安全事件

風險評鑑彙整表(範例)

可接受風險值：15(含)，風險值超過15以上者，必須進行風險處理

個人資料檔案風險評鑑彙整表

機密等級：□公開使用 ■內部使用 □內部限閱 □機密

文件編號：NCHU-PIMS-D-011　　版次：1.1

紀錄編號：　　填表日期：　年　月　日

項次	評鑑別	資產編號	資料形式	流程名稱	個資檔案名稱	改善單位	資產價值(衝擊值)	資料週期	風險		構面1	構面2	風險值	單位主管(風險擁有者)
									風險緣由	事件	衝擊影響	可能性		
1	第一次評鑑	XX組-001	電子	學生保險	保險名冊	XX組	3	處理	未訂保存期限	誤用資料	3	3	18	
	風險再評鑑										3	1	12	李大同

50

個資風險評鑑新舊表單說明

個資風險評鑑新舊表單說明

- **重點目標**
  - 調整方法論**符合國際標準 ISO 31000**風險管理準則與指引精神
  - **減化貴校原風險評估作法，提高作業效率**

原構面

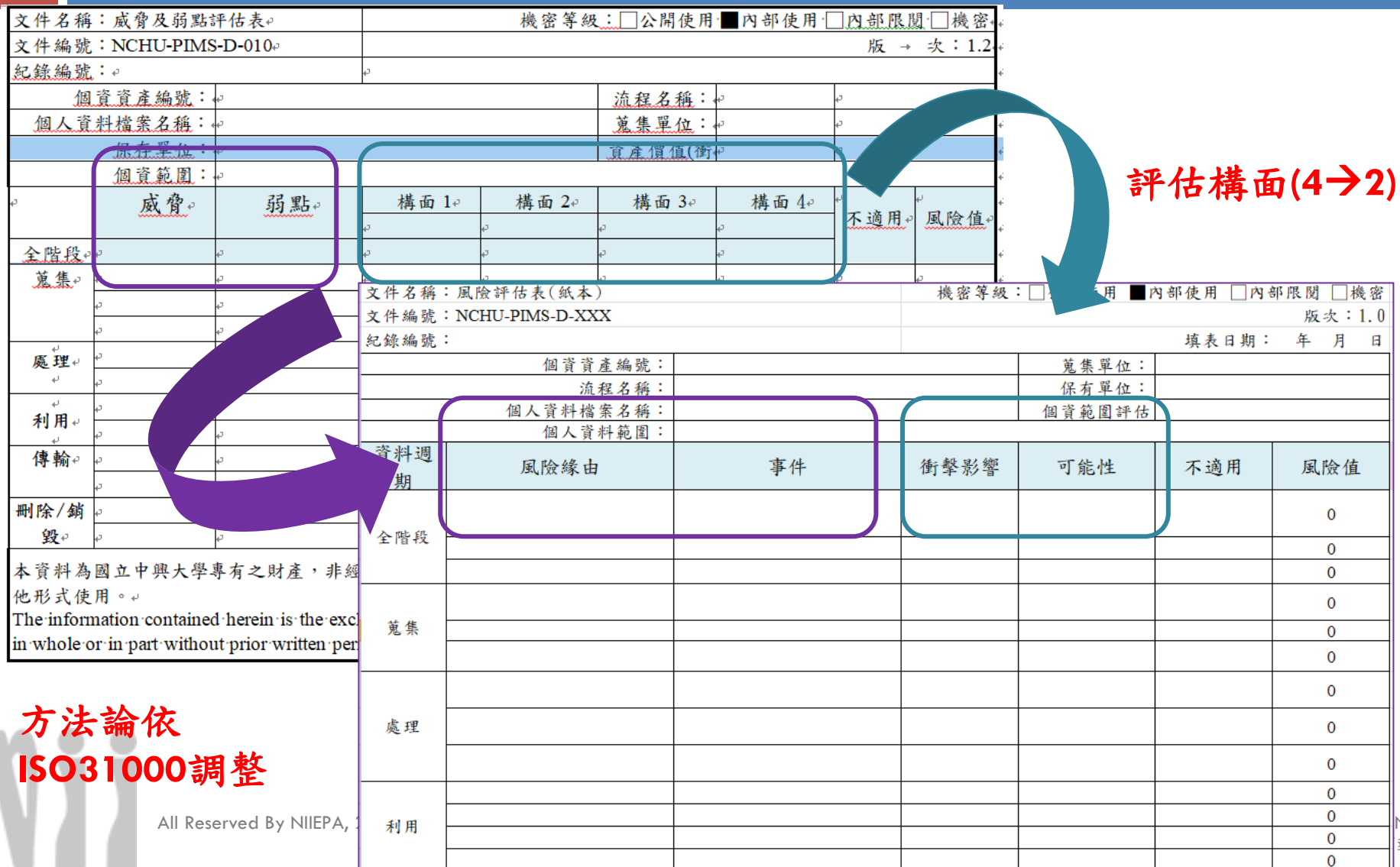
財務影響	違反個資法影響組織營運與聲譽	安全管理制度	內部傳送

「威脅」「弱點」調整為依紙本、電子類型之評估項目

新構面

衝擊影響 (評估個資數量)	可能性 (管理制度執行現況)

個資風險評鑑新舊表單說明(續)



文件名稱：威脅及弱點評估表　機密等級：□公開使用 ■內部使用 □內部限閱 □機密
文件編號：NCHU-PIMS-D-010　版　次：1.2
紀錄編號：

個資資產編號：　流程名稱：
個人資料檔案名稱：　蒐集單位：
保存單位：　資產價值(衝
個資範圍：

	威脅	弱點	構面 1	構面 2	構面 3	構面 4	不適用	風險值
全階段								
蒐集								
處理								
利用								
傳輸								
刪除/銷毀								

本資料為國立中興大學專有之財產，非經
他形式使用。
The information contained herein is the exc
in whole or in part without prior written per

評估構面(4→2)

文件名稱：風險評估表(紙本)　機密等級：□ 用 ■內部使用 □內部限閱 □機密
文件編號：NCHU-PIMS-D-XXX　版次：1.0
紀錄編號：　填表日期：　年　月　日

個資資產編號：　蒐集單位：
流程名稱：　保有單位：
個人資料檔案名稱：　個資範圍評估
個人資料範圍：

資料週期	風險緣由	事件	衝擊影響	可能性	不適用	風險值
全階段						0
						0
						0
蒐集						0
						0
						0
處理						0
						0
						0
利用						0
						0
						0
						0

方法論依
ISO31000調整

簡報完畢，敬請指教

Q & A

109年個人資料管理制度建置細部流程

8-9月	9月	10月	11月	12月
個資盤點	**風險評鑑**	**制度實作**	**內稽作業**	**管審**
• **個資盤點** • 盤點訓練(3場次)	• **風險評估** • **文件修訂發行** • 風險評鑑訓練(3場次) • 文件宣導訓練(I)	• **專案進度會議** • **可接受風險值確認** • **風險處理** • 文件宣導教育訓練(II) • 稽核宣導教育訓練(2場次)	• **內部稽核** • **內稽矯正**	• **管審會議** • **專案結案**

風險評鑑配合事項

- 配合單位：
  - 行政單位（秘書室-校友中心；教務處-招生暨資訊組；主計室）
  - 教學單位（應用數學系）
  - 附屬研究單位（農產品驗證中心、人文與社會科學研究中心）
- 訪談前
  - 請了解參本次教材，確認顧問提供的風險評估表(初評)是否正確
  - 請預借討論會議場地
- 訪談日
  - 風險評估表有疑問之處，進行討論