國立中興大學
建立個人資料保護管理制度
委外顧問服務計畫

個人資料檔案風險評鑑暨
鑑別結果討論說明會

日期：101年09月17、21日

講師：NII產業發展協進會 專業講師群

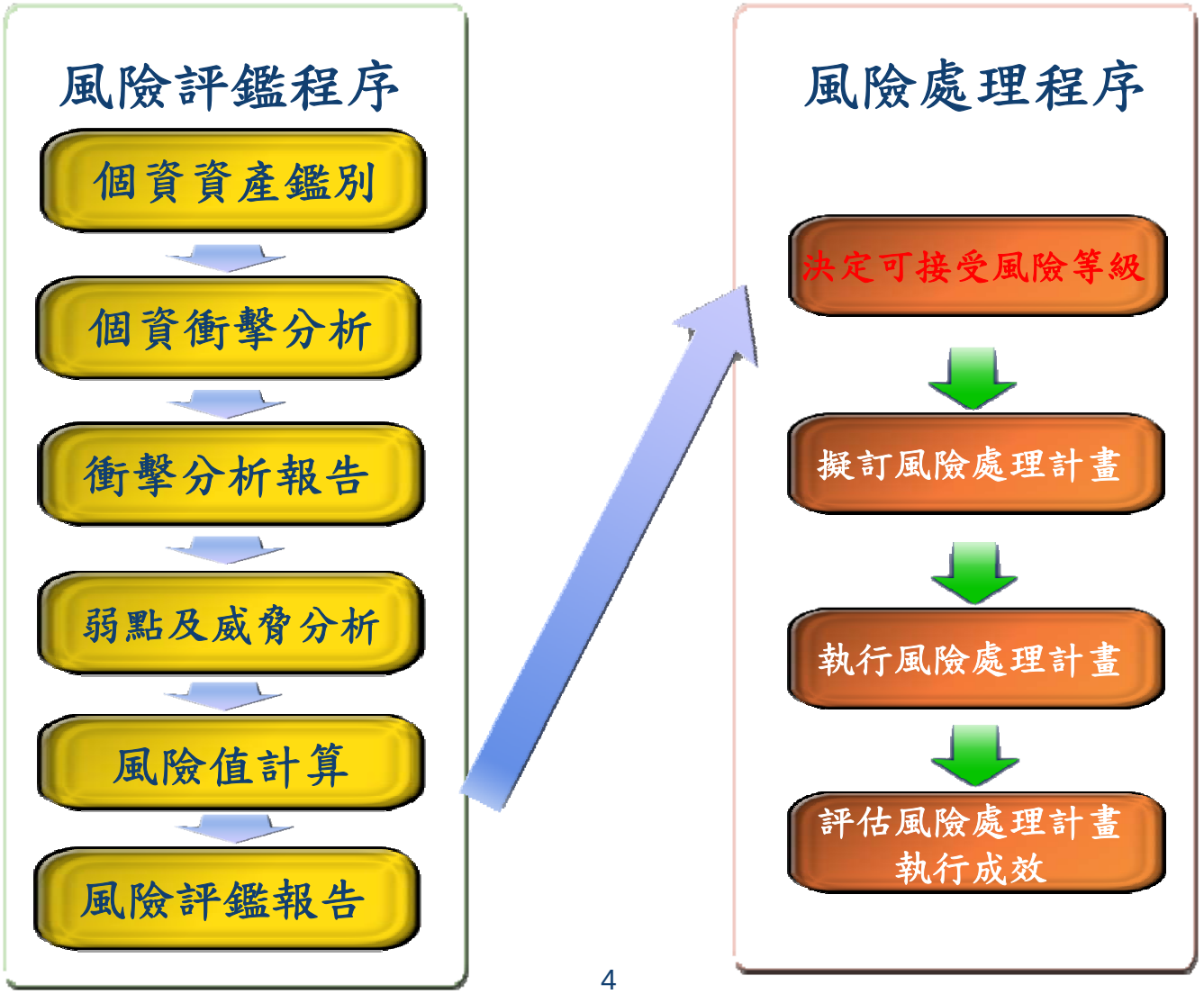
說明會目的

- 識別個人資料之威脅與弱點。
- 分析風險所造成的衝擊與其可能性。
- 識別出正確的安全防護措施。

說明會大綱

- 如何識別個人資料檔案
- 針對個人資料檔案進行風險評鑑
- 個人資料檔案風險管理的必要性
- 案例說明
- 問題與討論

個人資料風險管理程序


風險評鑑程序
個資資產鑑別
個資衝擊分析
衝擊分析報告
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
執行風險處理計畫
評估風險處理計畫
執行成效

說明會大綱

- 如何識別個人資料檔案

個人資料檔案鑑別方式說明

- 步驟一
  - 由　貴單位個人之「工作業務職掌」。
- 步驟二
  - 依據　貴貴單位個人「工作業務職掌」，輔導顧問協助瞭解有使用到個人資料之作業流程。
- 步驟三
  - 訪談、確認與個人資料相關之流程其個人資料資訊流(個人資料生命週期)蒐集、處理、利用、銷毀、傳輸。

個人資料檔案鑑別方式說明(續)

- 您必須瞭解並提供
  - 個人資料之作業過程中若有參考、使用到相關之作業辦法、法令依據、文件、表單、合約、應用系統名稱。
  - 原因
    - 為滿足「個人資料保護法」第八條、第十五條、第十六及第十八條要求。
    - BS 10012
      - ✓4.2辨識及記錄個人資料的使用情況。
      - ✓4.2.1組織應維護一份「個人資料分類清冊」。
      - ✓4.7公正與合法的處理。

個人資料保護法

❖ 第八條

- 公務機關或非公務機關依第十五條或第十九條規定向當事人蒐集個人資料時，應明確告知當事人下列事項：
  - 一、公務機關或非公務機關名稱。
  - 二、蒐集之目的。
  - 三
  - 四
  - 五
  - 六
    權

有下列情形之一者，得免為前項之告知：
一、依法律規定得免告知。
二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
三、告知將妨害公務機關執行法定職務。
四、告知將妨害第三人之重大利益。
五、當事人明知應告知之內容。

個人資料保護法(續)

第十五條

- 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者：
  - 一、執行法定職務必要範圍內。
  - 二、經當事人書面同意。
  - 三、對當事人權益無侵害。

個人資料保護法(續)

第十六條

- 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用：
  - 一、法律明文規定。
  - 二、為維護國家安全或增進公共利益。
  - 三、為免除當事人之生命、身體、自由或財產上之危險。
  - 四、為防止他人權益之重大危害。
  - 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或蒐集者依其揭露方式無從識別特定之當事人。
  - 六、有利於當事人權益。
  - 七、經當事人書面同意。

個人資料保護法(續)

第十八條

- 公務機關保有個人資料檔案者，應指定專人辦理**安全維護事項**，防止個人資料被竊取、竄改、毀損、滅失或洩漏。

個資衝擊分析

- 個資資產(個人資料檔案)權責單位應依據個資資產清冊之評估標準，確認「個資流程衝擊」價值。
- 執行衝擊分析之目的-依據BS10012「資料保護—個人資訊管理系統之要求（Data protection–Specification for a personal information management system）」
  - 確保所有新識別之個人資料風險(不論來自組織內部或外部)皆經評估。

個人資料檔案清冊(範本)

個人資料檔案清冊

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-002　　版　　次：1.0

紀錄編號：　　填表日期：　　年　　月　　日

個資產識號	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	有無監督管理之非公務機關	蒐集			處理		利用				保存		銷毀		揭露			現有控制措施	衝擊值
										來源	方式	單位	方式	單位	期間	地區	單位	方式目的	單位	期限	形式	頻率	對象	方式目的	個資範圍		

各單位鑑別之個人資料檔案情形

單位名稱		約略人數	個資資產統計		
			ALL	DA	DC
人事室	一組	16	45	8	37
	二組		35	8	27
	三組		46	2	44
	四組		53	9	44
			179		
研究發展處	計畫業務組	19	13	4	9
	校務企劃組		16	8	8
	處長室		17	9	8
	頂尖大學計畫辦公室		14	5	9
	貴重儀器中心		9	4	5
	學術發展組		22	6	16
			91		
計資中心	主任室	28	7	2	5
	服務諮詢組		13	4	9
	研究發展組		26	15	11
	校務系統組		22	18	4
	資訊網路組		20	6	14
	資源管理組		5	2	3
			93		
師培中心		2	57	32	25
			57		
校友中心		2	17	11	6
			17		

單位名稱		約略人數	個資資產統計		
			ALL	DA	DC
秘書室	文書組	13	14	7	7
	主任秘書室		5	3	2
	行政議事組		11	6	5
	媒體公關組		6	3	3
			36		
副校長室		1	6	2	4
			6		
國際事務處	國際事務處	9	6	3	3
	大陸事務組		12	6	6
	外籍學生事務組		12	6	6
	學術交流組		13	7	6
			43		
教務處	教務長室	32	8	4	4
	招生暨資訊組		16	10	6
	教學資源暨發展中心		16	9	7
	註冊組		66	8	58
	課務組		10	2	8
			116		
產學智財中心		2	30	6	24
			30		
創新產業推廣學院	企劃行銷組	17	11	6	5
	行政庶務組		6	2	4
	推廣教育組		11	4	7
	進修教育組		7	3	4
			35		

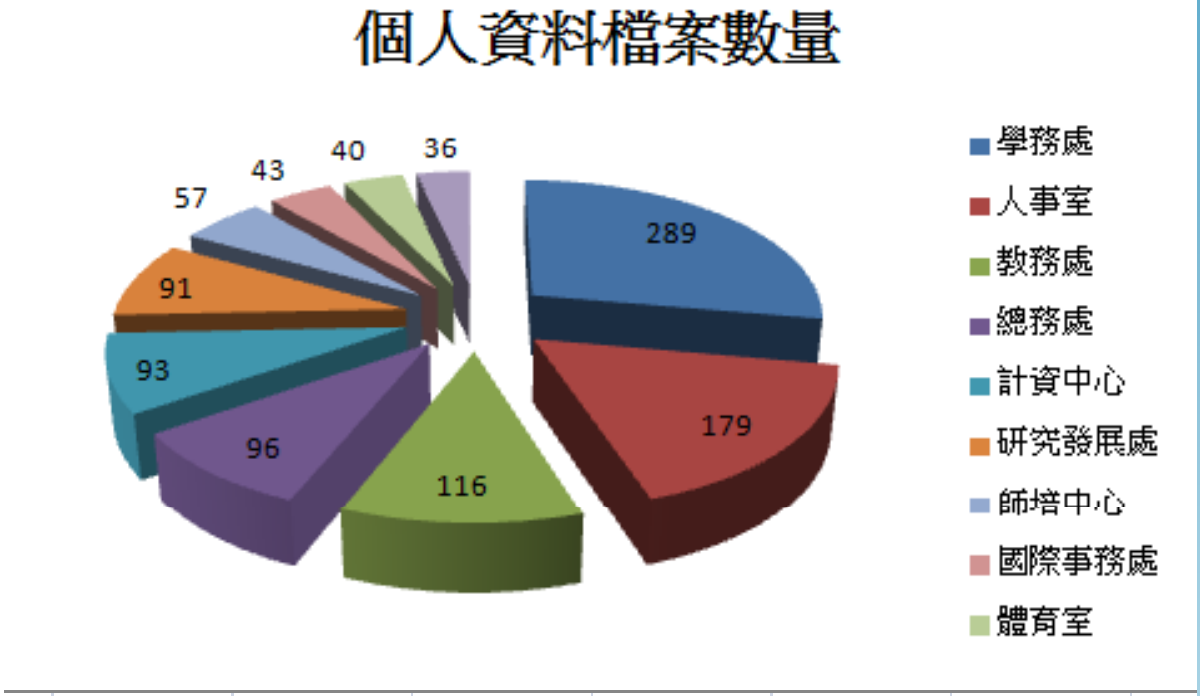
各單位鑑別之個人資料檔案情形(續)

單位名稱		約略人數	個資資產統計		
			ALL	DA	DC
會計室	一組	29	10	5	5
	二組				
	三組				
	四組				
			10		
圖書館	典藏組	31	17	12	5
	校史館組		20	8	12
	參考組		13	5	8
	採編組		6	4	2
	期刊組		9	3	6
	資訊組		16	10	6
	館長室		48	15	33
			129		
學務處	生活輔導組	52	85	34	51
	生涯發展中心		31	16	15
	住宿輔導組		16	6	10
	教官室		44	18	26
	僑生輔導室		16	7	9
	課外活動指導組		22	5	17
	衛生保健組		15	5	10
	學務長室		14	6	8
	諮商中心		46	19	27
			289		
環安中心		4	22	11	11
			22		

單位名稱		約略人數	個資資產統計		
			ALL	DA	DC
總務處	出納組	43	20	7	13
	事務組		10	3	7
	保管組		17	5	12
	經營管理組		13	2	11
	駐警隊		13	5	8
	營繕組		17	6	11
	總務長室		6	3	3
			96		
藝術中心		1	6	4	2
			6		
體育室	教學研究組	5	9	3	6
	場地器材組		9	4	5
	競賽活動組		11	6	5
	體育主任室		11	5	6
			40		
			1295	492	803

個人資料檔案分布情形

- 學務處-289
- 人事室-179
- 教務處-116
- 總務處-96
- 計資中心-93
- 研究發展處-91
- 師培中心-57
- 國際事務處-43
- 體育室-40
- 秘書室-36



個資隱私衝擊分析

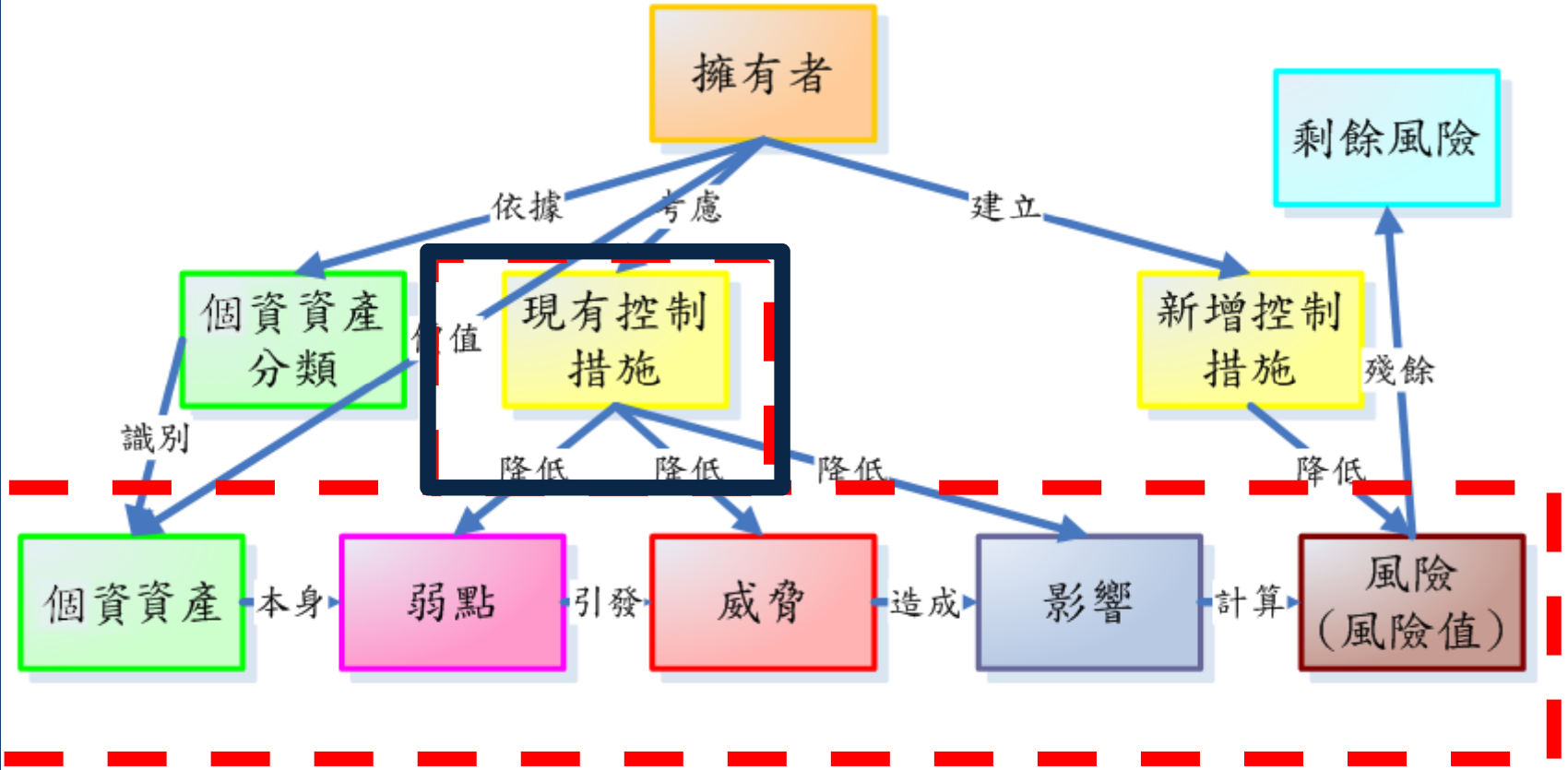
- 以個資法之要求對組織個資作業之衝擊進行評估分析設定評估等級標準，如：

衝擊影響程度	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、員工編號、學號)，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、員工編號、學號)。

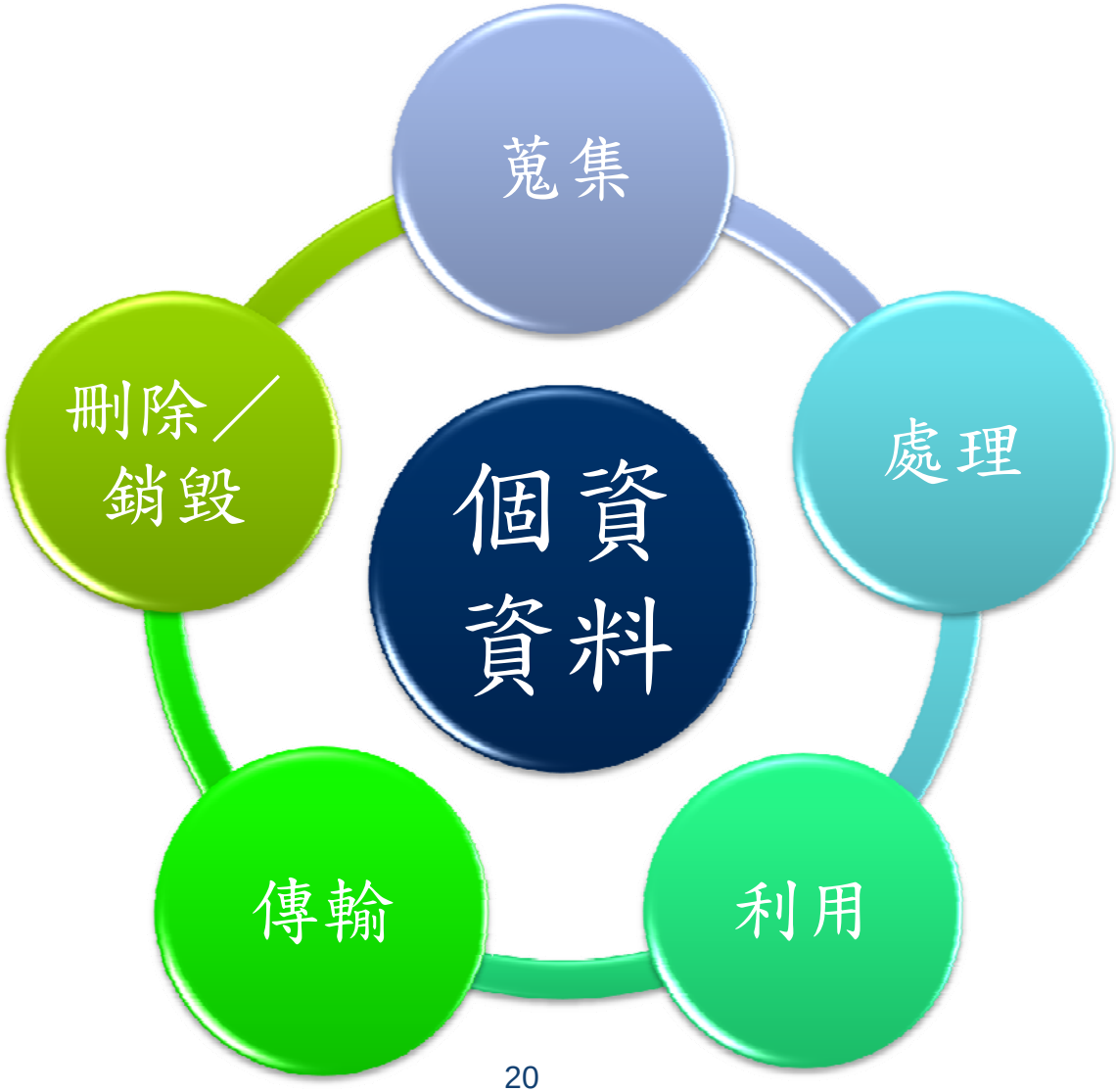
說明會大綱

- 針對個人資料檔案進行風險評鑑

風險評鑑及管理原則


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

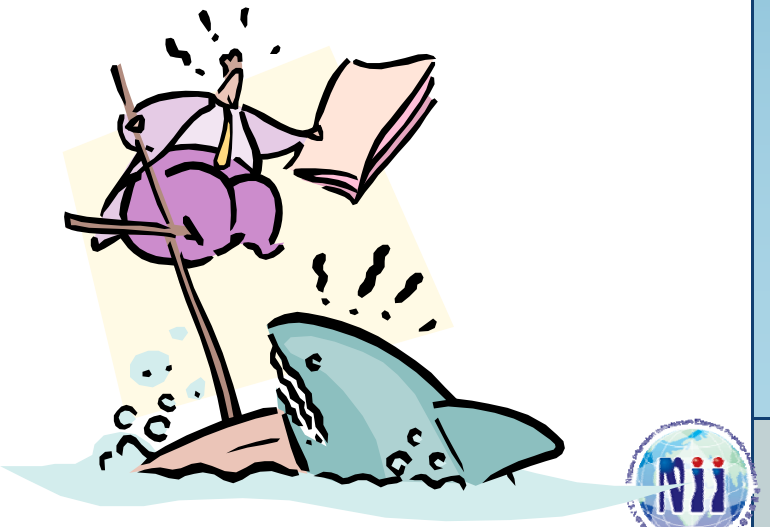
個資生命週期五階段



兩大因子

弱點分析

- 弱點存在於資產本身，若被威脅利用，可能會造成危害
- 可能的安全弱點
  - 識別與認證機制的不足。
  - 存取權限授與不當。
  - 儲存媒介內之資料沒有適當刪除就丟棄或重覆使用。
  - 未保護儲存文件。
  - 人員評選程序不夠嚴謹。
  - 人員教育訓練不足。
  - 缺乏安全警覺。



威脅分析

- 威脅為資產本身外來足以造成資產危害之狀況或事件
- 可分為意外的及蓄意的安全威脅
- 可能的安全威脅
  - 天然災害：颱風、地震、水災及停電等
    - 地震可能威脅到個資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
    - 偷竊可能威脅到個資資產的可用性及機密性

威脅、弱點、風險之間的關係

- 威脅利用弱點而對個資資產在不同的構面所造成傷害
- 風險= f【個資衝擊值 × 威脅利用弱點在不同的構面等級】

風險值的計算

❖ 風險之定義與評估

- 評估個人資料檔案威脅及弱點對構面因子所產生之影響，計算出風險值。
- 風險值計算方式
  - PIA(個人資料檔案價值) x （構面值1*權重+構面值2*權重+構面值3*權重+構面值4*權重+構面值5*權重）=風險值。
- 評估資料之風險值由資安暨個資保護執行小組彙整後產出「個人資料檔案風險評鑑彙整表」。
- 依據個人資料檔案風險評鑑結果撰寫個人資料檔案風險評鑑報告，並由「資安暨個資保護執行小組」提出可接受之風險等級建議。

個人資料檔案弱點暨威脅分析評分構面表

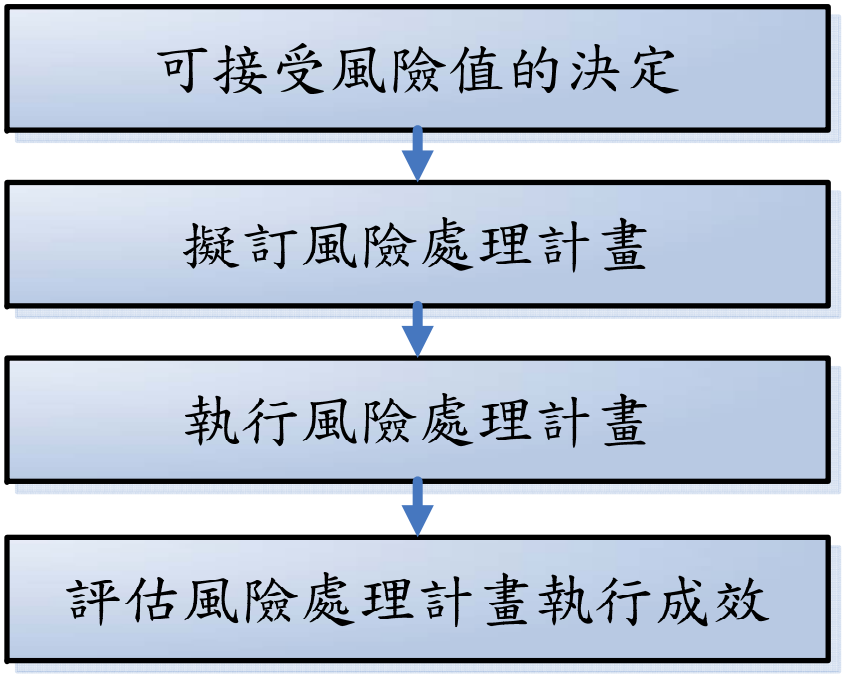
項目 評估值	財務影響	違反個資法影響 組織營運與聲譽	個資蒐集、處理、利用 之範圍與目的	保存、銷毀	安全管理制度
1	個資保管數量 500 筆(含)以內，全數外洩或處理不當，造成財務影響；或可能遭受法院判罰金額 1,000 萬元(含)以下。	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資，影響組織聲譽但不影響該業務流程運作。	已取得當事人同意蒐集、處理、利用個資，且未超過範圍與目的。	已建立保存、銷毀、監督程序，且已落實該等作業。	已建立安全控管程序及相關文件，且已落實。
2	個資保管數量逾 500 筆~5,000 筆(含)以內，全數外洩或處理不當，造成財務影響；或可能遭受法院判罰逾 1,000 萬元，1 億元(含)以下。	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資會影響組織聲譽及該業務流程運作。	1. 已取得當事人同意蒐集、處理、利用個資，雖資料蒐集範圍（過度）與目的不同（目的外之處理、利用），已進行告知，但未取得書面同意。或 2. 已取得當事人同意蒐集、處理、利用個資，未踰越目的，且有進行告知但未取得書面同意。	已建立保存、銷毀、監督程序，但未落實。	已建立安全控管程序及相關文件，但部分未落實。
3	個資保管數量逾 5,000 筆~5 萬筆(含)以內，全數外洩或處理不當，造成財務影響；或可能遭受法院判罰逾 1 億元，2 億元(含)以下。	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資影響組織聲譽及部門業務運作。	已取得當事人同意蒐集、處理、利用個資，但資料蒐集、處理、利用範圍（過度）與目的不同（目的外之處理、利用），且未進行告知或已告知但不同意。	尚未建立保存、銷毀、監督程序，但有部分實施。	尚未建立安全控管程序及相關文件，但有實施部份安全控管。
4	個資保管數量逾 5 萬筆，全數外洩或處理不當，造成財務影響；或可能遭受法院判罰逾 2 億元。	遭禁止蒐集、處理、利用個資或遭命令刪除個資或沒入、銷毀個資影響組織聲譽及組織業務運作。	未取得同意而蒐集、處理或利用個資，也未進行告知。(例如:購買名單或於臉書上搜尋[處理或利用])。	尚未建立保存、銷毀、監督程序，亦無實施任何措施。	未建立安全控管程序及相關文件，亦無任何安全控管。

說明會大綱

- 個人資料檔案風險管理的必要性

個人資料檔案風險處理程序

風險處理(Risk Treatment) - 選擇與實施各項控制措施，以降低風險影響程度



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

說明會大綱

案例說明

案例說明：個人資料檔案威脅及弱點評估表

個資資產編號：	PE1-DC-001	流程名稱：	專兼任教師聘任、升等、敘薪
個人資料檔案名稱：	國立中興大學教師到職通知單	蒐集單位：	人事室
保有單位：	人事室	資產價值(衝擊值)：	2
個資範圍：	姓名、職稱、任職單位		

	威脅	弱點	構面1 財務影響	構面2 違反個資法影響組織營運與	構面3 個資蒐集、處理、利用	構面4 保存、銷毀	構面5 安全管理制度	不適用	風險值
		加權	1	1	1	1	1		
蒐集	資料外洩	委外蒐集資料(125)						0	0
		缺乏監督機制(125)	2	1			3		12
		教育訓練不足(125)	2	1			3		12
	不符合蒐集程序	委外蒐集資料						0	0
		缺乏監督機制	2	1	1		4		16
		教育訓練不足	2	1	1		4		16
	未遵循法令法規	未告知蒐集目的(1235)	2	1	1		4		16
		未取得當事人同意(1235)	2	1	1		4		16
		蒐集特種資料						0	0
		收集過度資訊	2	1	1		4		16
		教育訓練不足	2	1	1		4		16
		未提供拒絕提供個資之權利(25)		1			4		10
		未提供履行當事人權利機制(25)		1			4		10

案例說明：個人資料檔案威脅及弱點評估表

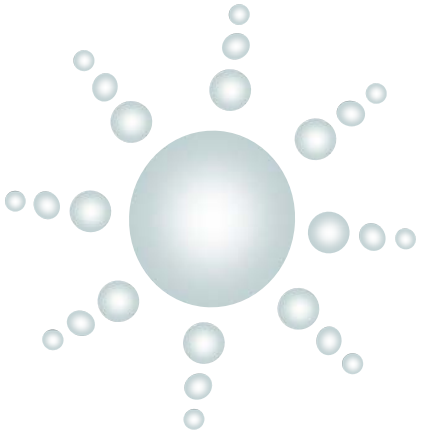
個人資料檔案名稱：	國立中興大學教師到職通知單				蒐集單位：	人事室		
保有單位：	人事室				資產價值(衝擊值)：	2		
個資範圍：	姓名、職稱、任職單位							
	威脅	弱點	構面1 財務影響	構面2 違反個資法影響組織營運與	構面3 個資蒐集、處理、利用	構面4 保存、銷毀	構面5 安全管理制度	不適用	風險值
		加權	1	1	1	1	1		
處理	未遵循法令法規	缺乏資料更新補充機制(25)		1			4		10
		未落實資料更新補充機制(25)		1			4		10
		未提供履行當事人權利機制(25)		1			4		10
		未於法定期限內准駁(25)		1			4		10
		逾越特定目的未告知(235)		1	1		4		12
		個資被竊取、洩漏、竄改未於查明後告知(25)		1			4		10
	資料外洩	委外處理資料(125)						0	0
		缺乏安全防護機制(1245)	2	1		1	3		14
		存取權限設與不當(1245)	2	1		1	3		14
		缺乏監督機制(125)	2	1			3		12
		教育訓練不足(125)	2	1			3		12
		缺乏專人辦理安全維護事項(45)				1	3		8
		資訊未分類(特種資料、一般資料)(5)					3		6

補充說明

- 個資侵害事故之緊急應變教育訓練
  - 個人資料之取得
  - 個資侵害事故回顧與討論
  - 危機處理概念
  - 緊急應變管理思維與責任
  - 個案討論
- 個人資料管理文件宣導教育訓練
  - 個人資料之取得
  - 個人資料之利用
  - 個人資料之管理
  - 個人資料保護政策之變更

補充說明(二)

- 個人資料管理制度稽核教育訓練
  - 稽核基本觀念
  - 如何撰寫稽核計畫
  - 稽核方法及實務技巧
  - 稽核範例
  - 稽核報告與改善建議追蹤
  - 結論



Thank You !