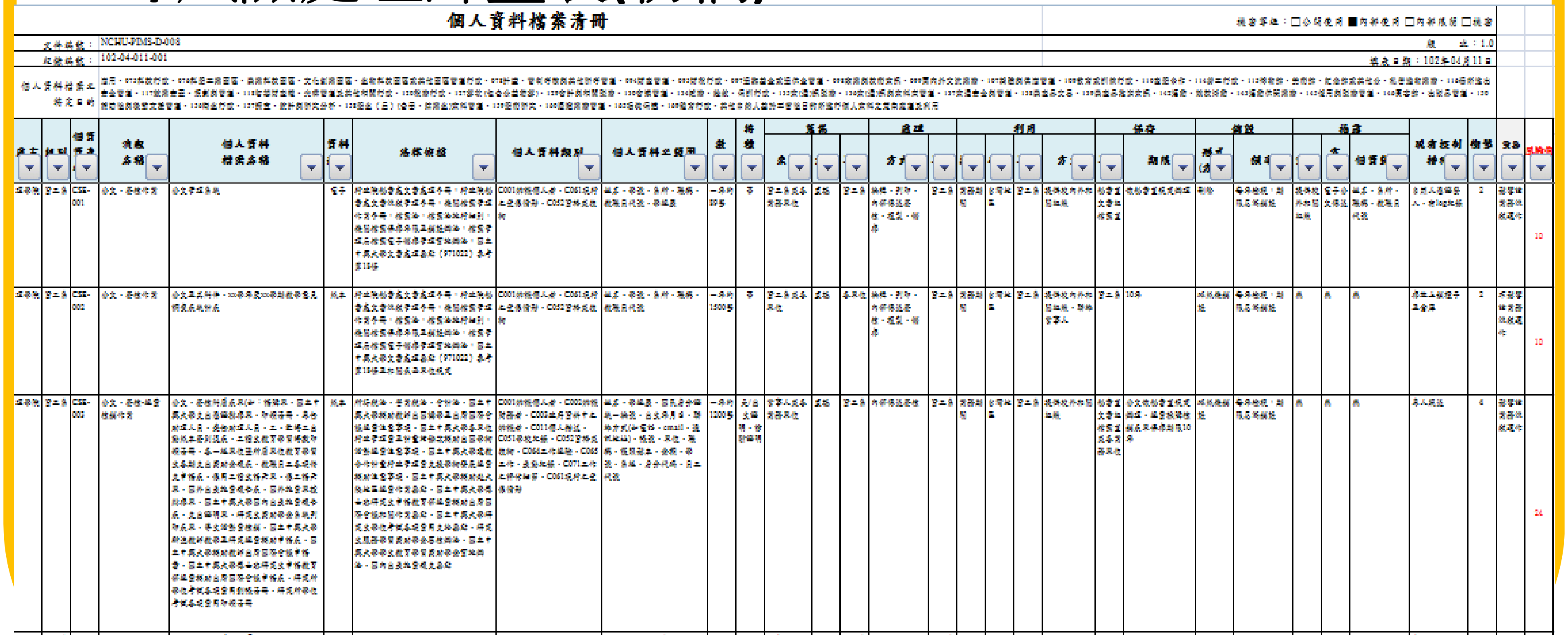
風險處理計畫教育訓練

產製-風險評鑑彙整表階段

- **儘速**提供最終版本之**個人資料檔案清冊**。
- 顧問將**協助產製威脅弱點評估表/風險評鑑彙整表/風險處理計畫表(初稿)**。



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-008　　版　次：1.0

紀錄編號：102-04-011-001　　填表日期：102年04月11日

計算風險值數量(範例1)

	A
1	風險值
2	14
3	10
4	10
5	14
6	10
7	10
8	10
9	14
10	12
11	18
12	8
13	16
14	10
15	15
16	8
17	12
18	15
19	12
20	10
21	10
22	10

- 將「個人資料檔案清冊」風險值複製至空白Excel表中。
- 利用篩選統計各風險值之數量。
- 20-80法則算出需改善之前20%數量。
- 累計值找出落在第8高的風險值。

風險值	數量	累積值		
8	6	38		
10	14	32		
12	4	18		
14	6	14		38*20%=8
15	4	8		
16	1	4		
18	2	3		
20	1	1		
共計	38			

計算風險值數量(範例2)

風險值
15
15
15
10
15
18
18
10
10
10
12
12
12
10
10
15
15
10
18
18
15

- 將「個人資料檔案清冊」風險值複製至空白Excel表中。
- 利用篩選統計各風險值之數量。
- 20-80法則算出需改善之前20%數量。
- 累計值找出落在第15高的風險值。

風險值	數量			
4	1			
5	8			
8	13			
10	29			75*20%=15
12	6			
15	14	18		
18	4	4		
	75			

計算風險值數量(續)

風險評鑑表

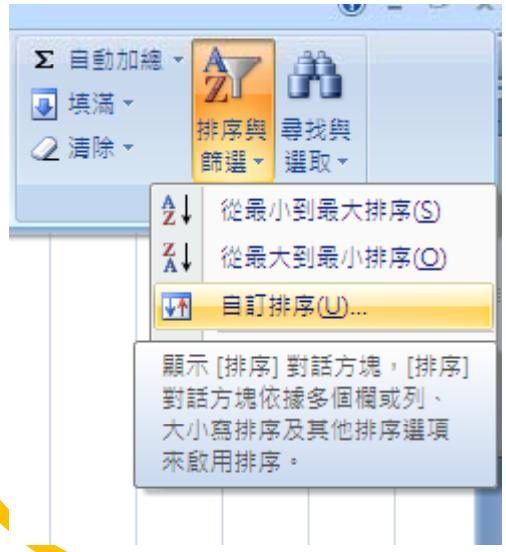
個資資產編號	受訪單位	流程名稱	個人資料檔案名稱	資料類型	個人資料範圍	衝擊值	風險值
6	XX系	會議相關作業	會議資料（施行獎學金申請、各項獎學金申請表單、專業任教師聘任及續聘名冊、教師休假研究申請表、國立中興大學頒授名譽教授提名表、外籍生入學資料、僑生入學資料、交換生業務資料、大陸交換生資料	電子	姓名、現職單位、到校日期、職稱、現職日期、出生年月日、性別、身分證字號、聘期、通訊處、電話（辦公室、行動電話）、E-MAIL、學歷、經歷、學術與貢獻事蹟內容、專利項目、姓名、系所、年級、學業分數、操行分數、名次、照片、性別、年齡、通訊地址、家長姓名、家長職業、電話、年資、國籍、畢業證書影本、成績單、自傳、財力證明書、護照、申請系所志願	3	18
7	XX系	會議相關作業	會議資料（施行獎學金申請、各項獎學金申請表單、專業任教師聘任及續聘名冊、教師休假研究申請表、國立中興大學頒授名譽教授提名表、外籍生入學資料、僑生入學資料、交換生業務資料、大陸交換生資料	紙本	姓名、現職單位、到校日期、職稱、現職日期、出生年月日、性別、身分證字號、聘期、通訊處、電話（辦公室、行動電話）、E-MAIL、學歷、經歷、學術與貢獻事蹟內容、專利項目、姓名、系所、年級、學業分數、操行分數、名次、照片、性別、年齡、通訊地址、家長姓名、家長職業、電話、年資、國籍、畢業證書影本、成績單、自傳、財力證明書、護照、申請系所志願	3	18
19	XX系	系主任選舉作業	國立中興大學農業暨自然資源學院 昆蟲學 系(所)主管被推薦人個人資料表單及其附件（教師證書、學經歷證明	紙本	身分證字號、籍貫、性別、出生年月日、學經歷、現職	3	18
20	XX系	系主任選舉作業	國立中興大學農業暨自然資源學院 昆蟲學 系(所)主管被推薦人個人資料表單	電子	身分證字號、籍貫、性別、出生年月日、學經歷、現職	3	18
1	XX系	公文、簽核作業	公文管理系統	電子	姓名、聯絡電話、電子郵件、內容可能含有身分證字號、職	3	15

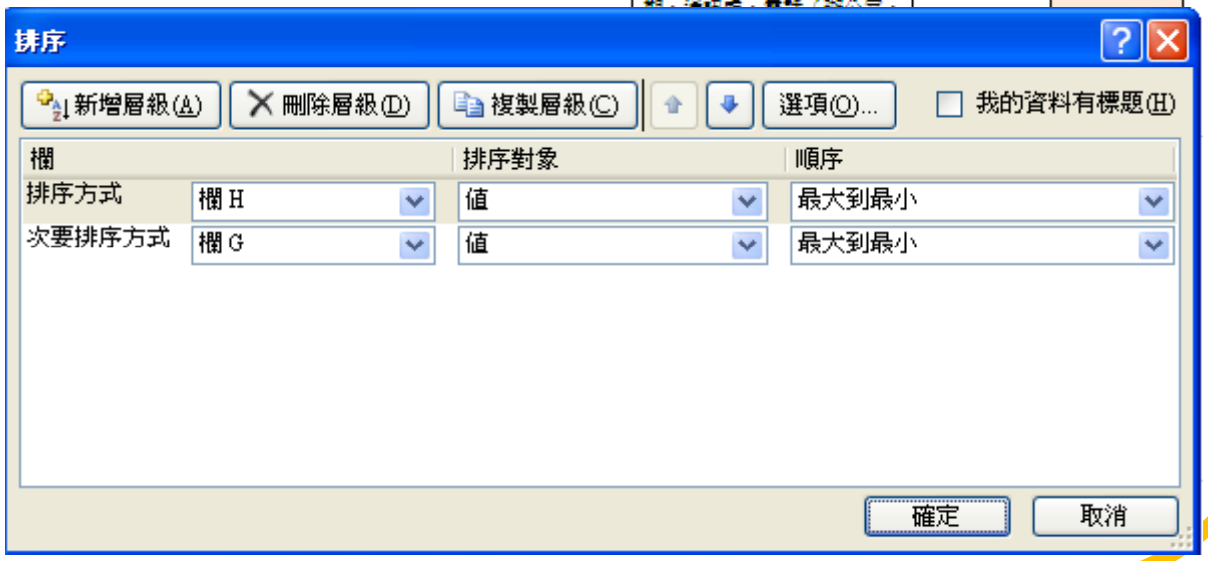
計算風險值數量(續)

- 風險評鑑表排序
  - 排序方式：風險值、衝擊值
  - 由大到小
- 找出落於第15筆資產

風險評鑑表

個人資料範圍	衝擊值	風險值
姓名、現職單位、到校日期、職稱、現職日期、出生年月日、性別、身分證字號、聘期、通訊處、電話（辦公室、行動電話）、E-MAIL、學歷、經歷、學術與貢獻事蹟內容、專利項目、姓名、系所、年級、學業分數、操行分數、名次、照片、性別、年齡、通訊地址、家長姓名、家長職業、電話、年資、國籍、畢業證書影本、成績單、自傳、財力證明書、護照、申請系所志願	3	18
姓名、現職單位、到校日期、職稱、現職日期、出生年月日、性別、身分證字號、聘		





計算風險值數量(續)

- 找出落於第15筆資產，風險值落在15。
- 但風險值15超過11筆。
- 排序風險值15：
  - 風險值15且衝擊值4共計0筆
  - 風險值15且衝擊值3共計14筆
    - 構面值142：0筆
    - 構面值132：0筆
    - 構面值122：14筆
    - 構面值112：0筆
  - 風險值15且衝擊值2共計0筆
- **由於條件相同，故全數採納**，共計18筆資產納入風險改善範圍。

風險值	數量			
4	1			
5	8			
8	13			
10	29			75*20%=15
12	6			
15	14	18		
18	4	4		
	75			

產製-風險處理計畫表階段

- 顧問協助產製「風險處理計畫表」

個人資料檔案風險處理計畫表

機密等級：□公開使用 □內部使用 ■內部限閱 □機密

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		風險追蹤追蹤				
項次	單位	科別	資產編號	流程名稱	個資檔案	型式	個資階段	威脅	弱點	風險說明	風險值	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	風險處理進度
1153	國際事務處		T5	外國學生審查作業	外國學生入學審查及管生與學金線頂審核系統	電子	處理（含內部傳送）	使用錯誤的資料	未主動或依當事人之請求更正或補充個人資料									
1155	國際事務處		T5	外國學生審查作業	外國學生入學審查及管生與學金線頂審核系統	電子	處理（含內部傳送）	使用錯誤的資料	未保護儲存資料									
1157	國際事務處		T5	外國學生審查作業	外國學生入學審查及管生與學金線頂審核系統	電子	處理（含內部傳送）	惡意行為	未保護儲存資料									
1159	國際事務處		T5	外國學生審查作業	外國學生入學審查及管生與學金線頂審核系統	電子	處理（含內部傳送）	惡意行為	存取權限設錯不當									
1161	國際事務處		T5	外國學生審查作業	外國學生入學審查及管生與學金線頂審核系統	電子	處理（含內部傳送）	儲存媒介之不當存取	未保護儲存資料									
1163	國際事務處		T5	外國學生審查作業	外國學生入學審查及管生與學金線頂審核系統	電子	處理（含內部傳送）	儲存媒介之不當存取	未經管儲存媒體									
1165	國際事務處		T5	外國學生審查作業	外國學生入學審查及管生與學金線頂審核系統	電子	處理（含內部傳送）	儲存媒介之不當存取	存取權限設錯不當									
1167	國際事務處		T5	外國學生審查作業	外國學生入學審查及管生與學金線頂審核系統	電子	處理（含內部傳送）	儲存媒介之不當存取	儲存媒介內之資料沒有適當刪除就委託重複使用									

風險處理計畫表(格式)

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：1.0			
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	流程名稱	資產編號	個資檔案	個資型式	個資階段	威脅	弱點	風險說明	風險值	風險處理型式	改善活動/控制措施	負責人	預定完成日期	實際完成日期	覆核人員	風險處理
											□接受風險 □降低風險 □轉移風險 □避免風險						
											□接受風險 □降低風險 □轉移風險 □避免風險						
											□接受風險 □降低風險 □轉移風險 □避免風險						

風險處理計畫表

- 風險說明欄位填寫(範例)
  - 個資外洩
  - 違反個資法
  - 違反BS10012標準規範
  - 違反個資法及BS10012標準規範

風險處理計畫表

- 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交易或活動。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 不熟悉法令法規及內部規範、教育訓練不足：
    - 落實定期辦理個資教育訓練及法令、法規宣導。
  - 未保護儲存資料、未控管儲存媒體、儲存媒介內之資料沒有適當刪除就丟棄或重覆使用、儲存媒介之不當存取、 儲存媒介之不當存取：
    - 落實儲存媒介管理機制
    - 落實個人資料生命週期管理程序
    - 落實個人資料安全控管作業

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 未訂定保存期限、資料未依使用期限進行銷毀或刪除、資料銷毀處理程序不當或不足、缺乏回收控管機制：
    - 落實個人資料檔案保存期限，並辦理銷毀程序
    - 落實個人資料生命週期管理程序
    - 落實個人資料安全控管作業
  - 未提供履行當事人權利機制、未於法定期限內准駁
    - 依據履行當事人權利機制，落實於法定期限內准駁。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 未經授權下處理資料、存取權限授與不當：
    - 落實權責單位進行權限控管並定期審查
    - 落實個人資料安全控管作業
  - 個人資料被竊取、竄改、毀損、滅失或洩漏、.缺乏安全防護機制、惡意行為：
    - 落實個資被竊取、洩漏、竄改於查明後告知之程序
    - 落實安全防護、環境控制、網路存取規劃機制
    - 落實個人資料生命週期管理程序
    - 落實個人資料安全控管作業
    - 落實定期辦理資訊安全教育訓練及宣導

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 缺乏實體保護、缺乏環境控制：
    - 落實安全防護、環境控制、網路存取規劃機制。
  - 設備損壞、操作錯誤
    - 落實因應設備損壞與有效維護之管理機制
    - 落實個人資料安全控管作業
  - 未主動或依當事人之請求更正或補充個人資料
    - 落實資料更新補充機制
  - 未告知個資法要求應告知事項
    - 落實個資法要求應告知事項、逾越特定目的與範圍之告知程序。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 未取得當事人同意：
    - 落實取得當事人同意機制
  - 未於法定期限內准駁、未提供履行當事人權利機制：
    - 履行當事人權利機制，並落實於法定期限內准駁。
  - 未保護儲存資料：
    - 落實個人資料安全防護、環境控制、網路存取規劃機制。
    - 落實電腦與應用系統安全管控機制。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 未訂定保存期限：
    - 依據個人資料檔案保存期限，落實辦理銷毀程序
    - 落實個人資料生命週期管理程序
    - 落實個人資料安全控管作業
  - 未提供當事人表示拒絕接受行銷之方式：
    - 落實拒絕接受行銷之機制
  - 未經授權下處理資料：
    - 權責單位進行權限控管並定期審查
    - 落實個人資料安全控管作業

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 委外利用資料、委外蒐集資料：
    - 落實委外廠商管理及監督機制。
    - 落實委外蒐集作業管理程序。
  - 個人資料被竊取、竄改、毀損、滅失或洩漏：
    - 落實個資被竊取、洩漏、竄改於查明後告知之程序
    - 落實安全防護、環境控制、網路存取規劃機制
    - 落實定期辦理資訊安全教育訓練及宣導
  - 個資被竊取、洩漏、竄改未於查明後告知
    - 落實個資被竊取、洩漏、竄改於查明後告知之程序

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 缺乏安全防護機制：
    - 落實安全防護機制(如：資料傳輸加密、存取權限管控)
  - 缺乏稽核監督機制：
    - 落實稽核監督之管理機制
    - 定期執行稽核查檢作業
  - 惡意或不當行為(外部傳送）：
    - 落實安全防護、環境控制、網路存取規劃機制。
    - 落實個人資料傳輸管理程序。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 缺乏安全防護機制：
    - 落實安全防護機制(如：資料傳輸加密、存取權限管控)
  - 傳輸過程未有適當之加密或保護(資料外洩)：
    - 落實個人資料傳輸管理程序。
    - 落實電腦與應用系統安全管控機制。
  - 傳輸過程未有適當之保護(錯誤資訊)：
    - 落實個人資料傳輸管理程序。
    - 權責單位進行權限控管並定期審查。

風險處理計畫表

- 「改善活動/控制措施」範例：
  - 資料外洩：
    - 落實個資被竊取、洩漏、竄改於查明後告知之程序
    - 落實安全防護、環境控制、網路存取規劃機制
    - 落實定期辦理資訊安全教育訓練及宣導
  - 蒐集特種資料：
    - 落實特種個資蒐集機制(如：告知事項、取得當事人書面同意)
  - 蒐集資訊缺乏正當合理之關聯：
    - 落實定期審查蒐集資訊缺乏正當合理關聯之機制。

&

Thank You !