國立暨南國際大學
National Chi Nan University

105年度各單位個人資料盤點及風險評估作業計畫

本 校 P I M S 驗 證 單 位

中 華 民 國 105 年 xx 月 xx 日

目　錄

壹、計畫目的

為因應「個人資料保護法」、「個人資料保護法施行細則」以及本校個人資料保護管理要點等法規之要求，爰建立本校個人資料檔案盤點與風險評估管理規範，提供本校各單位共同遵行之風險評估標準，採取適當之解決對策或控制措施，以有效降低個人資料檔案遭受損害的風險。

一、個人資料盤點目的

能有效清查及鑑別個人資料之名稱、類別(個人資料欄位)、保有依據、保有單位、特定目的、存在形態(書面/電子)、個人資料使用行為及相關利害關係人等。

二、個人資料風險評估目的

鑑別個人資料所存在之各項衝擊及威脅所導致之風險，並依據風險評估之結果採取技術面及管理面之對策(接受、降低、轉移、迴避風險)或安全控制措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

貳、計畫適用範圍

本計畫適用範圍為本校____個單位(如下表所示)之各項業務相關作業流程產生之個人資料檔案。

表 1　本校 BS 10012 驗證單位一覽表

No	單位名稱	No	單位名稱
1		6	
2		7	
3		8	
4		9	
5		10	

參、時程規劃

以下列出本校各單位個人資料盤點及風險評估作業之時程規劃，各項作業項目之時程與內容如下所述：

No.	工作名稱	開始	完成	2016年 08月	09月	10月	11月	12月	2017年 01月
1	作業文件內容確認	2016/7/18	2016/7/31						
2	辦理教育訓練	2016/8/1	2016/8/15						
3	各單位實地輔導	2016/8/16	2016/10/30						
4	各單位產製盤點表及評估報告	2016/11/1	2016/12/15						
5	執行稽核檢查	2016/12/16	2017/1/16						

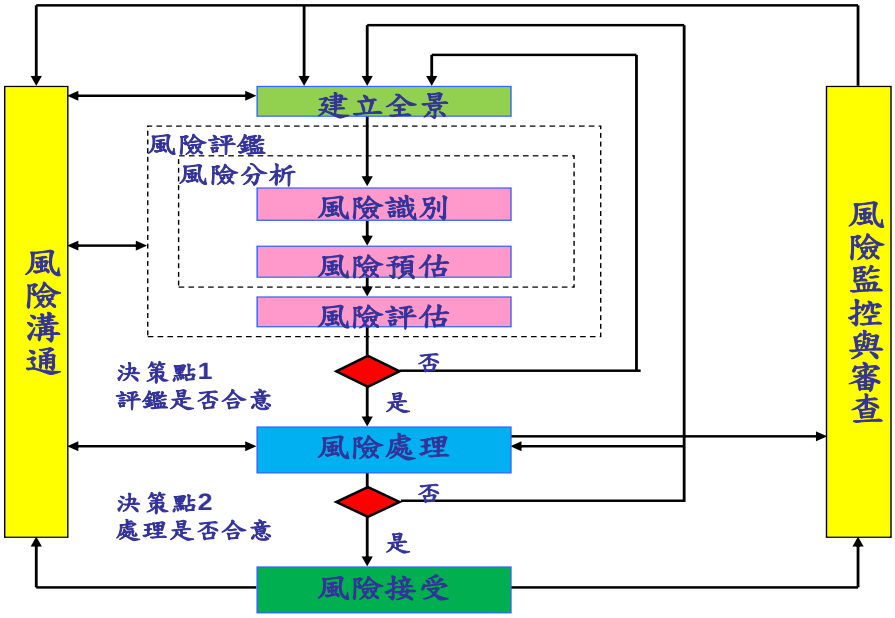
圖 1　個人資料盤點與風險評估作業時程規劃

肆、計畫內容

以下列出本計畫個人資料盤點及風險評估之方法論與執行作業流程，讓各單位於執行本計畫時有一明確之依據，確保計畫執行之進度與品質。

一、個人資料盤點及風險評估方法論

本專案依據ISO/IEC 27005：2011資訊安全風險管理之機制，建立資訊資產風險評估架構。詳見下圖所示。

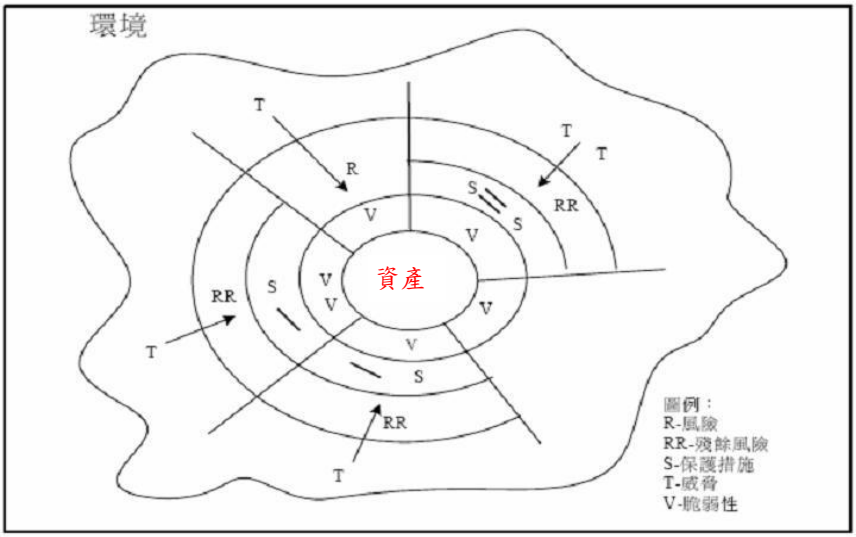


資料來源：ISO/IEC 27005：2011

圖 2　ISO/IEC 27005：2011 資訊安全風險管理架構

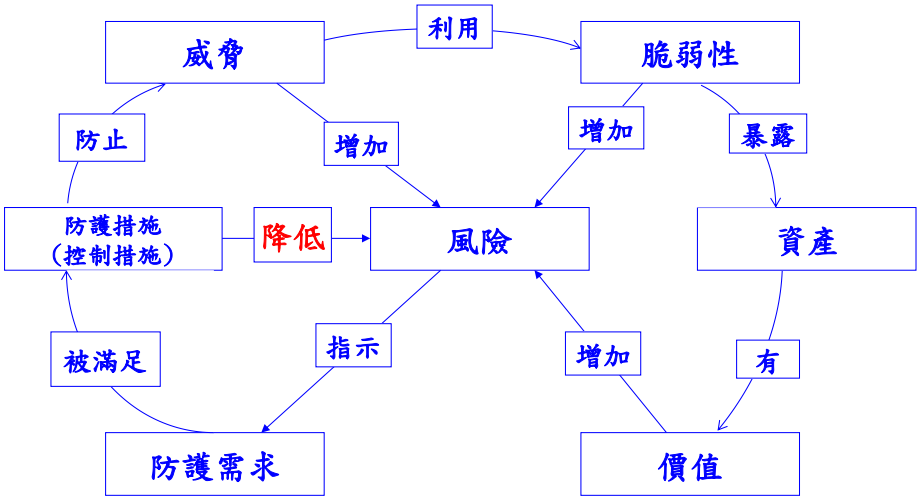
依據ISO/IEC27005之要求，需要識別資產、威脅、現有控制措施、脆弱性，並識別可能造成之後果。風險評估之概念源自於ISO/IEC13335-1，其係以資產為核心，而資產內部存在有若干之脆弱性(V)，外部有許多之威脅(T)。評估已知威脅利用脆弱性之可能性，及對資產造成衝擊之程度，稱之為風險評估。

要降低風險，需要藉助控制措施(S)的施行，才可以拒止威脅或是消除脆弱性。風險可能無法完全去除，剩餘之風險稱之為殘餘風險(RR)，採行控制措施之重點在於要將殘餘風險降低至可接受之水準。



資料來源：CNS 14929-1

圖 3　風險安全元件關係圖



資料來源：CNS 14929-1

圖 4　風險管理要素關聯圖

二、個人資料盤點及風險評估作業流程

建立「個人資料檔案風險評估與管理作業程序」，作業流程、權責單位及相關表件，如下所述：

作業流程	權責單位	相關文件
個人資料盤點(鑑別)	各單位/輔導廠商	個人資料項目盤點表
個資風險評估分析	各單位/輔導廠商	個人資料檔案風險評估彙整表
個資風險等級判定	各單位/輔導廠商	個人資料檔案風險處理計畫
撰寫風險評估報告	各單位/輔導廠商	個人資料風險評估報告
執行稽核檢查	個人資料保護稽核小組	
紀錄保存	各單位	

圖 5　個人資料檔案風險評估與管理流程圖

(一)、個人資料盤點(鑑別)

個人資料之範圍，應考量機關個人資料來源、個人資料類別、內部處理所涉及的角色、流程、期間、地區、利用對象與方式，最終應確認特定目的之範圍，內容詳見下圖所示。

圖 6　界定個人資料之範圍

1、本校各單位個人資料保護專責人員應協調單位同仁進行轄管業務個人資料盤點作業，並視實際狀況進行內容調整。

2、依據業務流程分析結果，執行個人資料檔案鑑別作業，並建立「個人資料項目盤點表」(詳如附件一)。

3、除每年執行一次個人資料檔案鑑別作業外，應於本校組織變更或作業流程改變時，針對變動範圍內的作業程序與個人資料檔案進行個人資料檔案鑑別作業。

4、「個人資料項目盤點表」中之「特定目的」與「個人資料類別」2欄位，應依據法務部「個人資料保護法之特定目的及個人資料之類別」之內容詳實填寫(詳如附件二)。

5、本校各單位所產製之「個人資料項目盤點表」應列出在個人資料保護生命週期中之蒐集、處理、利用、保存、銷毀及揭露等各項須監控與管理之訊息，以符合「個人資料保護法」及「個人資料保護法施行細則」之要求，「個人資料項目盤點表」僅提供本校各單位內部使用。

(二)、個人資料風險評估分析

1、風險評估執行時機

個人資料檔案風險評估作業應於每年內部稽核活動前執行。除每年執行一次外，亦應於發生：營運組織變更、作業流程改變、新增或變更個人資料檔案、發生重大個人資料外洩事件時，針對變動範圍內的作業程序與個人資料檔案進行風險評估。

2、風險評估分析

建立風險評量的標準(如下表所示)，包括：風險發生之機率與影響/衝擊之程度。個人資料檔案之風險評估應依據實際狀況，對照「影響及衝擊等級表」及「風險發生可能性等級表」之內容，並於「個人資料檔案風險評估彙整表」中進行六個評估構面之風險分析。

表 2　影響及衝擊等級表

評估項目(構面)	影響及衝擊等級表(I)		
	輕微(1)	嚴重(2)	非常嚴重(3)
可識別性	個人資詢查詢困難，耗費過鉅或耗時過久始能識別特定當事人者。	僅可以間接識別特定當事人者(**需要**與其他資料進行對照、組合、連結等，始能識別該特定的個人)	可以直接識別特定當事人者(**不需要**與其他資料進行對照、組合、連結等，就能識別該特定的個人)
個資數量	20 筆以下 (團體訴訟不成立)	一般個資 21~20,000 筆 特種個資 21~2,000 筆	一般個資 20,001 筆以上 特種個資 2,001 筆以上
敏感程度	僅有識別資料(未含其他個人活動、財務金融或特種個人資料)	含有個人活動資料或財務金融資料	含有特種個人資料 (**病歷、醫療、基因、性生活、健康檢查、犯罪前科**)
特定目的範圍內利用	僅於特定目的範圍內利用個人資料	有特定目的外利用個人資料，但符合例外條款	有特定目的外利用個人資料，但不符合例外條款
外部利用	無外部利用情形	無償委任關係外部利用	有償委任關係外部利用
國際傳輸	無國際傳輸情形	主管機關未規定之國際傳輸	主管機關訂定規定之國際傳輸
註記：評估項目參考 NIST SP800-122 選定，等級判定依據「個人資料保護法」之相關要求訂定，依據以上項目分項判定，最後依據最高衝擊原則，判定衝擊程度等級。			

表 3　風險發生可能性等級表

等級	可能性	發生機率	描述
3(高)	幾乎確定	61-100%	在大部分的情況下會發生
2(中)	有可能	41-60%	有些情況下會發生
1(低)	幾乎不可能	0-40%	只會在特殊的情況下發生

各單位須針對各項個人資料之使用及控管狀況，依據「影響及衝擊等級表」之各個構面，識別其組織面臨內部弱點及外在威脅所產生之影響與衝擊程度，並將影響及衝擊程度記錄於「個人資料檔案風險評估彙整表」(詳如附件三)。

3、風險值計算

識別風險發生之可能性(P)及影響/衝擊程度(I)，將此 2 項評分進行相乘，即求出該個人資料檔案之風險值。風險值(R) = P × I。

4.風險分布矩陣

將經由風險值計算公式所得之風險值，對應至「風險分布矩陣」以判斷風險值之分布情況。

表 4　風險分布矩陣

風險分布矩陣			
	發生機率		
影響/衝擊程度	幾乎不可能(1)	有可能(2)	幾乎確定(3)
非常嚴重(3)	**3(中度)**	**6(高度)**	**9(極高度)**
嚴重(2)	**2(低度)**	**4(中度)**	**6(高度)**
輕微(1)	**1(低度)**	**2(低度)**	**3(中度)**

(三)、個人資料風險等級判定

1、決定可接受風險值

以下列出可接受及不可接受之風險等級，作為本校各單位後續風險處理之依據。

表 5　風險判別與處理

風險值(R)	風險等級	風險判別與處理	
1 或 2	**1**	**可接受風險**	**接受**
3 或 4	**2**	**可接受風險**	**持續監視**
6 或 9	**3**	**不可接受風險**	**立即控制**

各單位個人資料風險評估可接受之風險等級，每年需檢討並經「個人資料保護管理執行小組」開會決議並記載於會議紀錄中。

2、個人資料風險處理作業

(1).依個人資料風險評估結果及可接受風險值之決議，由各風險項目負責人針對需降低風險值之個人資料擬訂「個人資料檔案風險處理計畫」(詳如附件四)，以期將風險降至可接受等級。

(2).個人資料風險處理計畫之風險處理措施，應根據「個人資料保護法」對各項個人資料保護之安全要求目標，擬訂適當之處理措施及相關執行資源。

(3).個人資料風險處理計畫應提報「個人資料保護管理執行小組」審查後執行，並列入追蹤管理。

3、風險處理計畫執行成效暨殘餘風險處理

風險處理計畫於預訂完成日期結束後，須由各單位執行風險再評估，以確認風險處理計畫之執行是否達到預期目標。

(四)、撰寫風險評估報告

各單位依據個人資料檔案風險評估結果，撰寫「個人資料風險評估報告」(詳如附件五)，並陳單位主管確認。

三、辦理教育訓練

105年07月份開始針對本校同仁，辦理2個梯次之個人資料盤點及風險評估作業之訓練課程。

表 6　教育訓練課程計畫表

課程名稱	時數	梯次	時數小計	上課對象
個人資料盤點教育訓練	3	2	6	各單位個資專責人員 業務承辦人員
個人資料隱私衝擊分析與風險評鑑	3	2	6	

四、實地輔導

自105年07月份開始，由輔導顧問向本校各單位確認輔導時間，進行實地輔導工作，協助各單位進行個人資料檔案盤點及風險評估作業，並產製及確認「個人資料項目盤點表」及「個人資料風險評估報告」。

五、執行稽核檢查

為查驗本校各單位是否依據本計畫落實執行個人資料盤點及風險評估各項作業，以符合本計畫之目的，確保本校保有的個人資料檔案均能落實執行相關個人資料保護措施，依據本校「資訊安全稽核管理作業規範」及「個人資料保護內部稽核作業程序」之作業流程進行稽核工作。

1、擬定稽核計畫

權責人員於執行稽核前，應擬妥「個人資料內部稽核計畫」(詳如

附件六)，並經權責主管核准後實施。計畫內容須包含：受稽核單位、稽核時程、稽核範圍、稽核人員安排...等。

2、稽核標的

稽核重點主要是查驗各單位是否如期如質產出「個人資料項目盤點表」及「個人資料風險評估報告」。

伍、附件

附件一、個人資料項目盤點表

附件二、個人資料保護法之特定目的及個人資料之類別

附件三、個人資料檔案風險評估彙整表

附件四、個人資料檔案風險處理計畫

附件五、各單位個人資料風險評估報告

附件六、個人資料內部稽核計畫(草案)。