國立中興大學

個人資料隱私衝擊分析與風險評鑑教育訓練

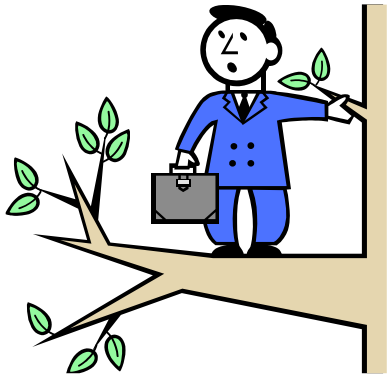
Davies

2013.12

目錄

何謂風險

- 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
  - 物理損壞。
  - 人為錯誤。
  - 設備故障。
  - 內部和外部攻擊。
  - 資訊誤用。
  - 資料遺失。
  - 應用程式出錯。



資訊安全風險

- 風險評鑑
  - 找出可能會造成組織損失的事件，並加以評估的一種方法。
- 風險管理
  - 如何降低該事件至可接受程度，並導入適當方法以維持所有風險皆在可忍受之範圍內。

風險評鑑及風險管理所帶來的效益

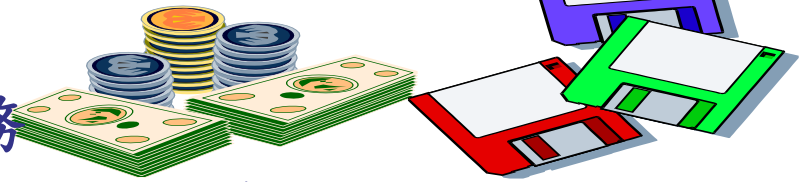
- **Identify assets** 識別資產 – 我需要保護什麼?
- **Identify threats** 識別威脅 – 我需要採取何種對策?
- **Calculating risks**計算風險–需要多少時間、人力、或成本來保護重要資產?

員工

聲譽

實體資源

法務

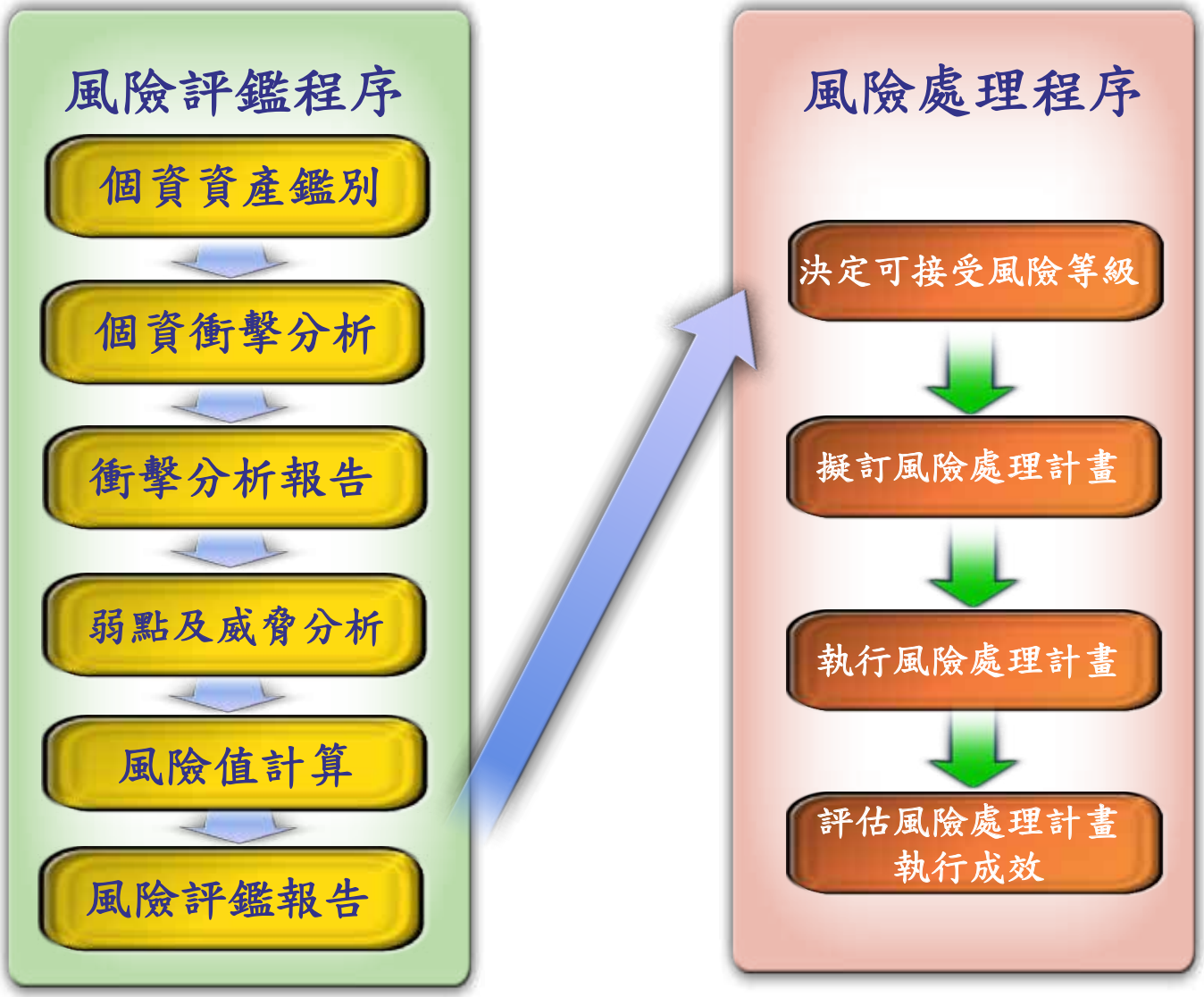


執行業務

財務資源

競爭資料

風險評鑑與處理程序

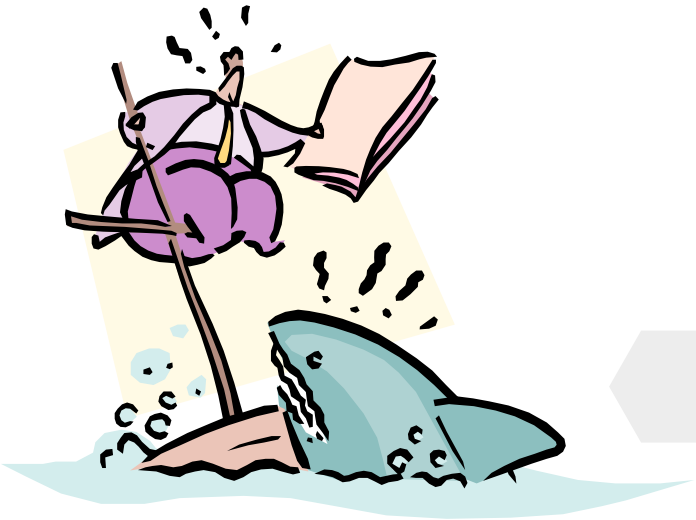

風險評鑑程序
個資資產鑑別
個資衝擊分析
衝擊分析報告
弱點及威脅分析
風險值計算
風險評鑑報告
風險處理程序
決定可接受風險等級
擬訂風險處理計畫
執行風險處理計畫
評估風險處理計畫
執行成效

威脅分析

- 威脅為外部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。

弱點分析

- 弱點存在於資產本身或內在，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、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 × 威脅與弱點在不同的構面等級】

威脅、弱點、風險之間的關係(案例)

- 我家裡現金10萬元，因為出門忘了上鎖，被小偷偷走了，搞得隔天要跑三點半

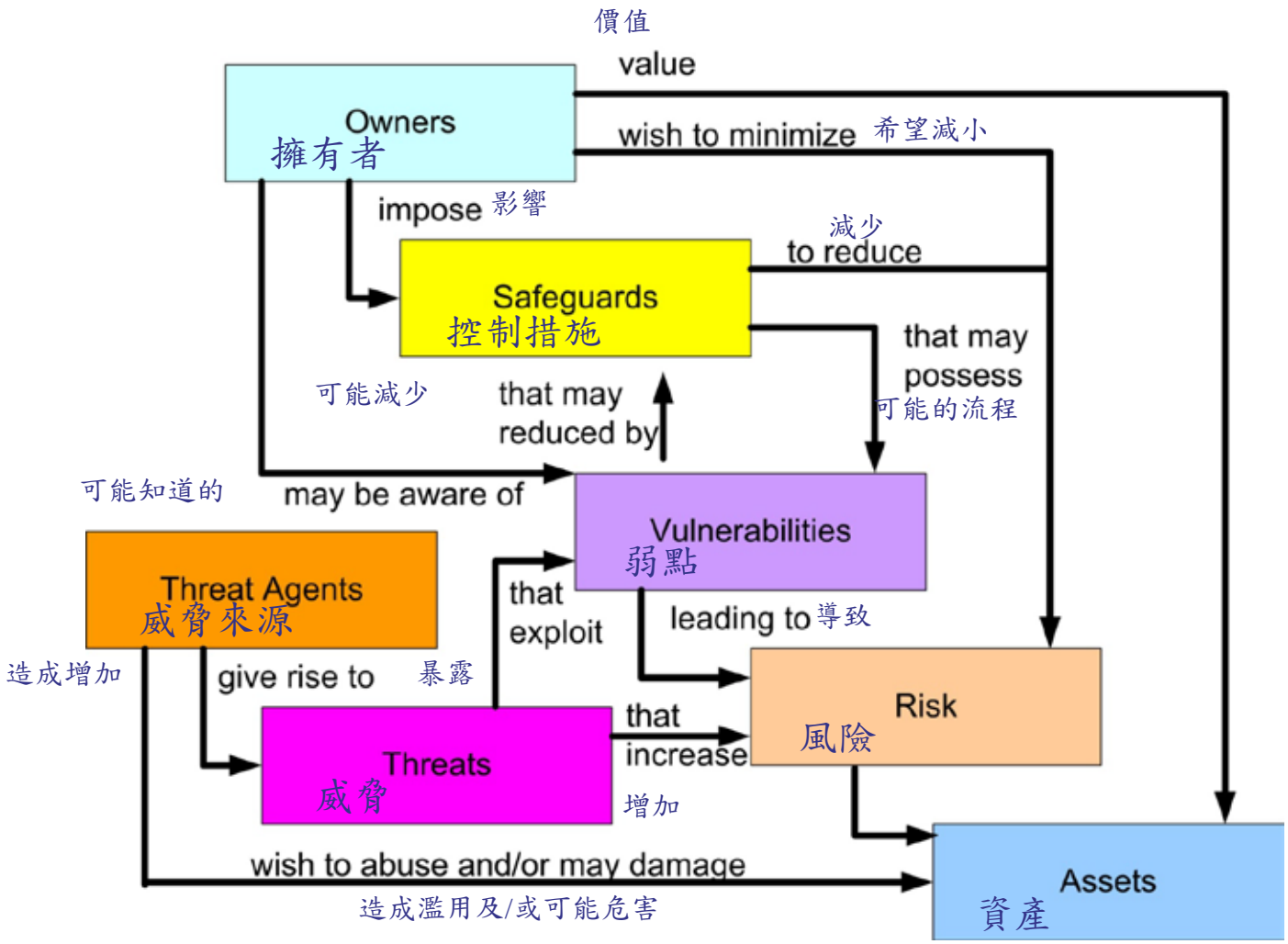
風險= 錢被偷走
資產=10萬元
影響=隔天要跑三點半
威脅=小偷偷竊
弱點=忘了上鎖

目錄

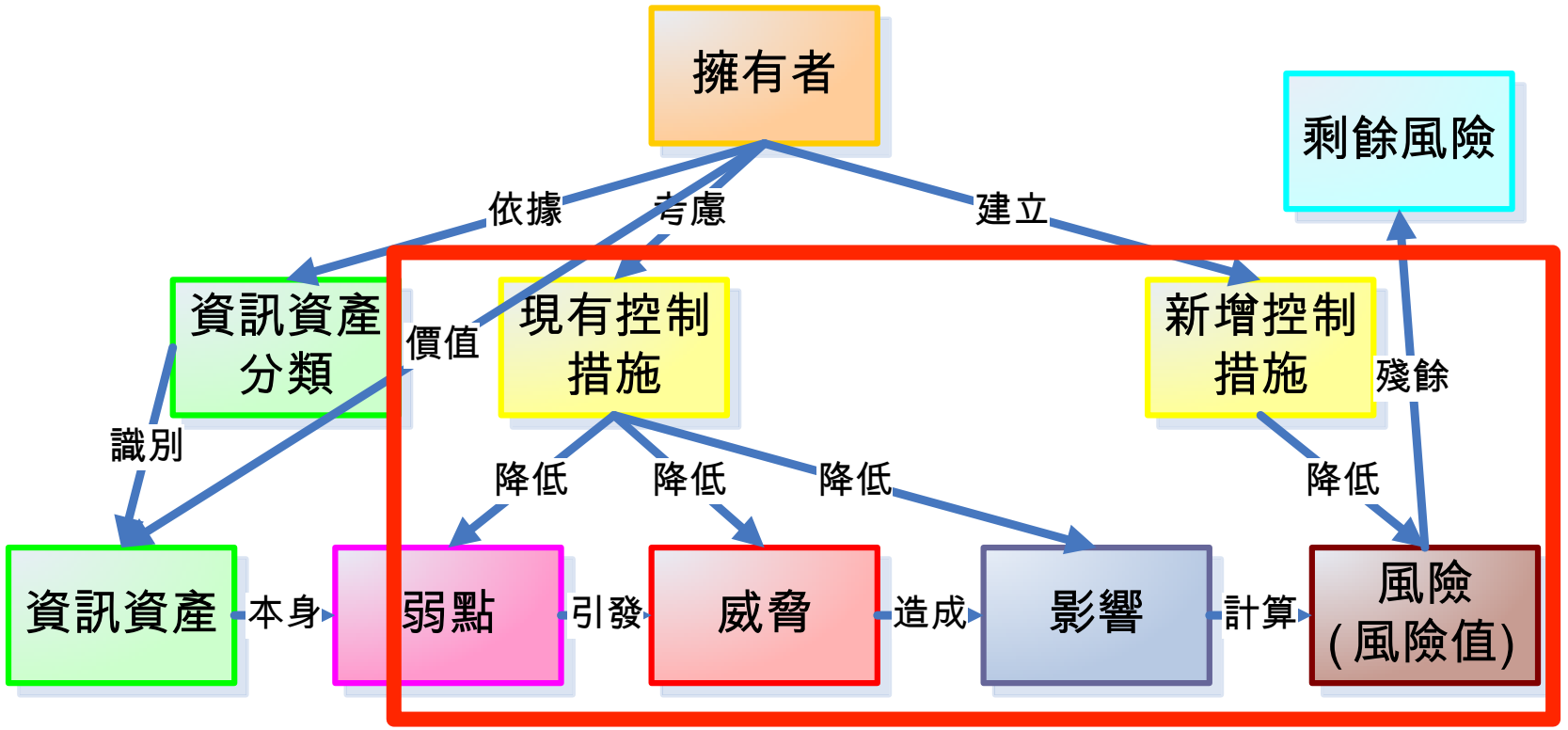
風險管理名稱彙總

- 資產(Asset)-是一種資源(實體或邏輯)，對組織是有價值的。
- 威脅(Threat)-是一種事件，可能會對系統或組織及其資產造成傷害，威脅必須利用資產的弱點才能對資產造成傷害。
- 威脅來源(Threat Agent)-引發潛在威脅的源頭。
- 暴露(Exposure)-弱點誘發威脅的情況。
- 弱點(Vulnerability)-指單一或一系列會讓威脅有機可趁而造成資產損害的狀況。資產的脆弱點本身並不會造成傷害。
- 控制措施(Safeguards) -降低潛在風險的機制。
- 風險(Risk)-有害事件發生的可能性。
- 剩餘風險(Residual Risk)-剩餘的部份風險。

風險管理概念關連圖


價值
value
Owners
擁有者
wish to minimize
希望減小
impose
影響
減少
to reduce
Safeguards
控制措施
that may
possess
可能的流程
可能減少
that may
reduced by
可能知道的
may be aware of
Vulnerabilities
弱點
Threat Agents
威脅來源
that
exploit
leading to
導致
造成增加
give rise to
暴露
Risk
風險
Threats
威脅
that
increase
增加
wish to abuse and/or may damage
造成濫用及/或可能危害
Assets
資產

風險管理原則


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

風險評鑑的分析方式

- 定量分析
  - 試圖去分配獨立的數量化價值物件(例如財務價值)作為風險評鑑的要素及潛在損失的評估。
  - 當全部要素(資產價值、影響、威脅頻率、防護效果、防護成本、不確定性及可能性)是定量化處理，則表示完全定量的考慮。
- 定性分析
  - 以情節為導向。
  - 資產價值、弱點及威脅的重要等級。

風險分析實務

◆組織執行的方式

- 由評鑑人員進行專業判斷(主觀判斷)。
- 以會議的方式進行討論(較為客觀)。

◆顧問常用的方式：

- 觀察-觀察實體環境、作業流程。
- 訪談-詢問資訊資產負責人或管理人。
- 檢視-相關文件(事件的報告、系統稽核及安全檢查的結果)。
- 測試及驗證-針對控制或作業的程序及結果進行正確性確認。
- 問卷-透過問卷瞭解眾人的意向。
- 其他-外部安全事故的經驗、資訊安全事件通報、資訊安全相關論壇。

(以ISO 27005、ISO 31000為基礎)

評估三構面

財務影響

影響組織營運與聲譽

安全管理制度

評估構面 – 財務影響

個資法第29條：

非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。**但能證明其無故意或過失者，不在此限。**
依前項規定請求賠償者，適用前條第二項至第六項規定。

個資法第28條：

公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，負損害賠償責任。但損害因天災、事變或其他不可抗力所致者，不在此限。

被害人雖非財產上之損害，亦得請求賠償相當之金額；其名譽被侵害者，並得請求為回復名譽之適當處分。
依前二項情形，如被害人不易或不能證明其實際損害額時，得請求法院依侵害情節，**以每人每一事件新台幣五百元以上二萬元以下計算。**
對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計最高總額以新台幣二億元為限。但因該原因事實所涉利益超過新台幣二億元者，以該所涉利益為限。
同一原因事實造成之損害總額逾前項金額時，被害人所受賠償金額，不受第三項所定每人每一事件最低賠償金額新台幣五百元之限制。
第二項請求權，不得讓與或繼承。但以金額賠償之請求權已依契約承諾或已起訴者，不在此限。

財務影響

財務影響：

評估值	1	2	3	4
內容	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。	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。	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。	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。

- 損害賠償請參酌個資法第25(非公務）、28條(公務機關）。
- 營利之個資外洩事件，組織或業務承辦人可能依判決有刑責。

數量係依據單位可容忍資料外洩筆數調整

財務影響之評估(範例)

	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聲譽	構面3 安全管理制度	不適用	風險值
全階段	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6
蒐集	資料外洩	委外蒐集資料				0	0
		缺乏安全防護機制	1	1	1		6
	未遵循法令法規	委外蒐集資料				0	0
		未告知個資法要求應告知事項	1	1	2		8
		未取得當事人同意	1	1	2		8
		蒐集特種資料				0	0
		蒐集資訊缺乏正當合理之關聯	1	1	1		6
		未提供當事人表示拒絕接受行銷之方式	1	1	2		8

違反個資法影響組織營運與聲譽

違反個資法影響組織營運與聲譽：

評估值	1	2	3	4
內容	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。	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。	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。	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。

影響組織營運與聲譽之評估(範例)

	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聲譽	構面3 安全管理制度	不適用	風險值
全階段	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6
蒐集	資料外洩	委外蒐集資料				0	0
		缺乏安全防護機制	1	1	1		6
	未遵循法令法規	委外蒐集資料				0	0
		未告知個資法要求應告知事項	1	1	2		8
		未取得當事人同意	1	1	2		8
		蒐集特種資料				0	0
		蒐集資訊缺乏正當合理之關聯	1	1	1		6
		未提供當事人表示拒絕接受行銷之方式	1	1	2		8

安全管理制度

安全管理制度：

評估值	1	2	3	4
內容	已建立安全控管程序，且已落實。	已建立安全控管程序，但部份未落實。	尚未建立安全控管程序，但有實施部份安全控管。	未建立安全控管程序，亦無任何安全控管。

安全管理制度之評估(範例)

	威脅	弱點	構面1	構面2	構面3	不適用	風險值
			財務影響	違反個資法影響組織營運與聲譽	安全管理制度		
全階段	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
全階段	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6
蒐集	資料外洩	委外蒐集資料				0	0
蒐集	資料外洩	缺乏安全防護機制	1	1	1		6
蒐集	未遵循法令法規	委外蒐集資料				0	0
蒐集	未遵循法令法規	未告知個資法要求應告知事項	1	1	2		8
蒐集	未遵循法令法規	未取得當事人同意	1	1	2		8
蒐集	未遵循法令法規	蒐集特種資料				0	0
蒐集	未遵循法令法規	蒐集資訊缺乏正當合理之關聯	1	1	1		6
蒐集	未遵循法令法規	未提供當事人表示拒絕接受行銷之方式	1	1	2		8

風險值的計算

◆ 風險之定義與評估

- 計算方式 PIA ×（構面值1+構面值2+構面值3）=風險值

威脅	弱點	構面1	構面2	構面3	不適用	風險值
		財務影響	違反個資法影響組織營運與聲譽	安全管理制度		

目錄

風險評鑑工具-1

資產編號	流程名稱	個人資料檔案名稱	資料形式	法律依據	特定目的	個人資料類別	個人資料之範圍	特種個資	蒐集			處理		利用				保存		銷毀		揭露			現有控制	衝擊值
									來源	方式	單位	方式	單位	期間	地區	對象	方式	保有單位及聯絡方式	期限	形式	頻率	對象	方式	個資範圍		
SEC-DA-0001	賀卡通訊錄維護作業	賀卡通訊錄	DA電子	OO許可辦法	150輔助性與後勤支援管理	C001識別個人者	位公姓、名稱絡話、訊址單或司、職聯電通地	否	名片信件網路	直接	秘書室	記錄	秘書室	聖誕至節間節春期	台灣地區	當事人	寄送賀年卡	秘書室	永久	更新	每年一次	無	無	無	PC帳密保護	2

風險評鑑工具-2

	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聲譽	構面3 安全管理制度	不適用	風險值
全階段	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6
蒐集	資料外洩	委外蒐集資料				0	0
		缺乏安全防護機制	1	1	1		6
	未遵循法令法規	委外蒐集資料				0	0
		未告知個資法要求應告知事項	1	1	2		8
		未取得當事人同意	1	1	2		8
		蒐集特種資料				0	0
		蒐集資訊缺乏正當合理之關聯	1	1	1		6
		未提供當事人表示拒絕接受行銷之方式	1	1	2		8
		未提供履行當事人權利機制	1	1	2		8
		委外處理資料				0	0

風險評鑑工具-3

	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聲譽	構面3 安全管理制度	不適用	風險值
全階段	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6
蒐集	資料外洩	委外蒐集資料				0	0
		缺乏安全防護機制	1	1	1		6
	未遵循法令法規	委外蒐集資料				0	0
		未告知個資法要求應告知事項	1	1	2		8
		未取得當事人同意	1	1	2		8
		蒐集特種資料				0	0
		蒐集資訊缺乏正當合理之關聯	1	1	1		6
		未提供當事人表示拒絕接受行銷之方式	1	1	2		8
		未提供履行當事人權利機制	1	1	2		8
		委外處理資料				0	0

風險評鑑工具-4

	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聲譽	構面3 安全管理制度	不適用	風險值
	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
全階段	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6
						0	0

評估值	1	2	3	4
內容	已建立安全控管程序，且已落實。	已建立安全控管程序，但部份未落實	尚未建立安全控管程序，但有實施部份安全控管。	未建立安全控管程序，亦無任何安全控管。

- 本年度已進行個資教育訓練或宣導則評估值為 1
- 本年度尚未進行個資教育訓練或宣導則評估值為 2

風險評鑑工具-5

	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聲譽	構面3 安全管理制度	不適用	風險值
	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
全階段	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6

評估值	1	2	3	4
內容	已建立安全控管程序，且已落實。	已建立安全控管程序，但部份未落實。	尚未建立安全控管程序，但有實施部份安全控管。	未建立安全控管程序，亦無任何安全控管。

- 本年度個人資料被竊取、竄改、毀損、滅失或洩漏已落實稽核、監督則評估值為 **1**
- 本年度個人資料被竊取、竄改、毀損、滅失或洩漏尚未落實稽核、監督則評估值為 **2**

風險評鑑工具-6

資產編號	流程名稱	個人資料檔案名稱	資料形式	法律依據	特定目的	個人資料類別	個人資料之範圍	否有種特種資料？何種特種資料？	蒐集			處理		利用				保存		銷毀		揭露			現有控制	衝擊值
									來源	方式	單位	方式	單位	期間	地區	對象	方式目的	保單及聯絡方式	期限	形式	頻率	對象	方式目的	個資範圍		
SEC-DA-0001	賀卡通訊錄維護作業	賀卡通訊錄	DA電子	OO許可辦法	150輔助性與後勤支援管理	C001識別個人者	單位或公司、姓名、職稱、聯絡電話、通訊地址	否	名片、信件、網路	直接	秘書室	記錄	秘書室	聖誕節至春節期間	台灣地區	當事人	寄送賀年卡	秘書室	永久	更新	每年一次	無	無	無	PC帳密保護	2

無揭露則無對外傳輸，故威脅弱點評估表傳送階段為不適用 0

風險評鑑工具-7

	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聲譽	構面3 安全管理制度	不適用	風險值
全階段	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6
蒐集	資料外洩	委外蒐集資料				0	0
		缺乏安全防護機制	1	1	1		6
	未遵循法令法規	委外蒐集資料				0	0
		未告知個資法要求應告知事項	1	1	2		8
		未取得當事人同意	1	1	2		8
		蒐集特種資料				0	0
		蒐集資訊缺乏正當合理之關聯	1	1	1		6
		未提供當事人表示拒絕接受行銷之方式	1	1	2		8
		未提供履行當事人權利機制	1	1	2		8
		委外處理資料				0	0

•本年度個人資料蒐集並無委外，故評估值為不適用**0**

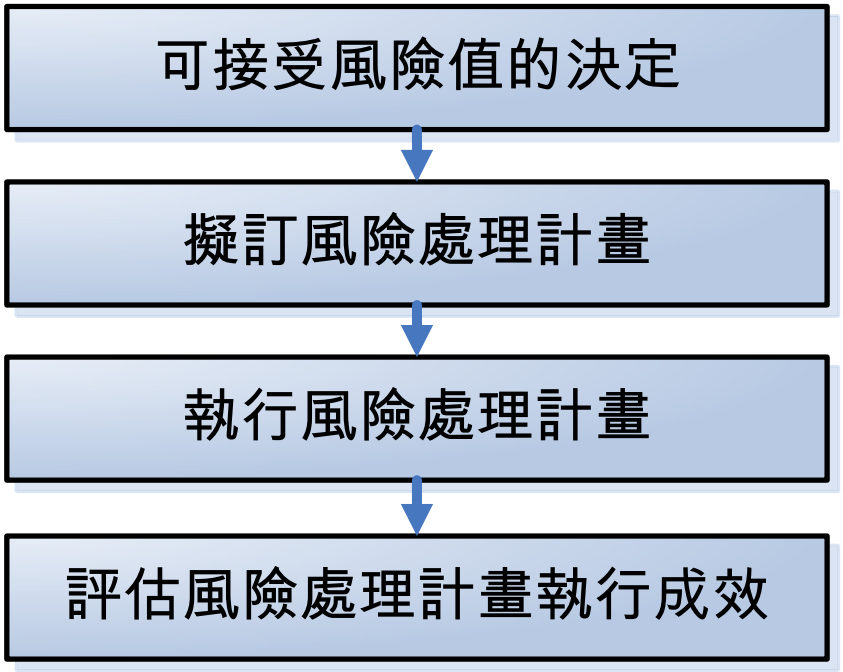
風險評鑑工具-8

	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聲譽	構面3 安全管理制度	不適用	風險值
全階段	不熟悉法令法規及內部規範	教育訓練不足	1	1	1		6
	個人資料被竊取、竄改、毀損、滅失或洩漏	缺乏稽核監督機制	1	1	1		6
蒐集	資料外洩	委外蒐集資料				0	0
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丟棄或重覆使用	1	1	1		6
利用	未遵循法令法規	逾越特定目的與範圍未告知	1	1	1		6
		個資法施行前非當事人提供之個資處理或使用前未告知(實施一年內須告知之資訊)	1	1	2		8
		未主動或依當事人之請求更正或補充個人資料	1	1	1		6
		未提供履行當事人權利機制	1	1	2		8
		個資被竊取、洩漏、竄改未於查明後告知	1	1	1		6
傳送(外部)	資料外洩	傳輸過程未有適當之加密或保護				0	0
	惡意或不當行為	資訊設施未做適當之安全管控				0	0
		未保護敏感性資料的傳輸				0	0
	未遵循法令法規	對於法令、法規了解不足(如國際傳輸)				0	0

目錄

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

實務－風險接受度

- 風險接受度應該用組織可接受或不可接受來分類。
- 不可接受的風險乃經再三考量可能不被容許存在的。
- 管理者要決定是否因為不願花費額外且昂貴的保護措施來降低不可接受的風險，進而選擇接受這些風險。

可接受風險值的決定-1

- **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)
  - 高階統計分析(變異與標準差、常態分配)
  - 檢視法。

可接受風險值的決定-2

- 高於可接受風險值的資產，應依據識別的弱點、威脅進行風險處理計畫的擬訂。
- 新增控制措施，降低弱點、威脅的發生機率。
- 將資產的風險值降低至可接受風險值以下。

例外原則:擬訂風險處理計畫時，仍檢視可接受風險值下的資產，是否仍有較高的潛在風險。

實務－可接受風險值

- **依據：ISO 27001本文4.2.1(c)(2)，發展風險接受準則，並識別風險可接受等級。**
- **實務作法：**
  - 可接受風險值，需經**管理審查會議決議**，並記載於會議紀錄中。
  - 決定可接受風險值時，須首先考慮必須在適法性的要求下。
- **管理審查會議須定期召開會議，並檢視／討論可接受風險值。**
- **可接受風險值得考量組織環境及作業之安全需求作適當調整。**

風險管理作業

- **確認、控制及降低安全風險至可接受程度所採取的程序**
- **管理作業**
  - 訂定風險可接受等級。
  - 檢視安全威脅及弱點。
  - 檢視目前使用之控制措施。
  - 加強其他控制措施。
  - 訂定相關個人隱私保護政策及作業程序。

選擇控制措施

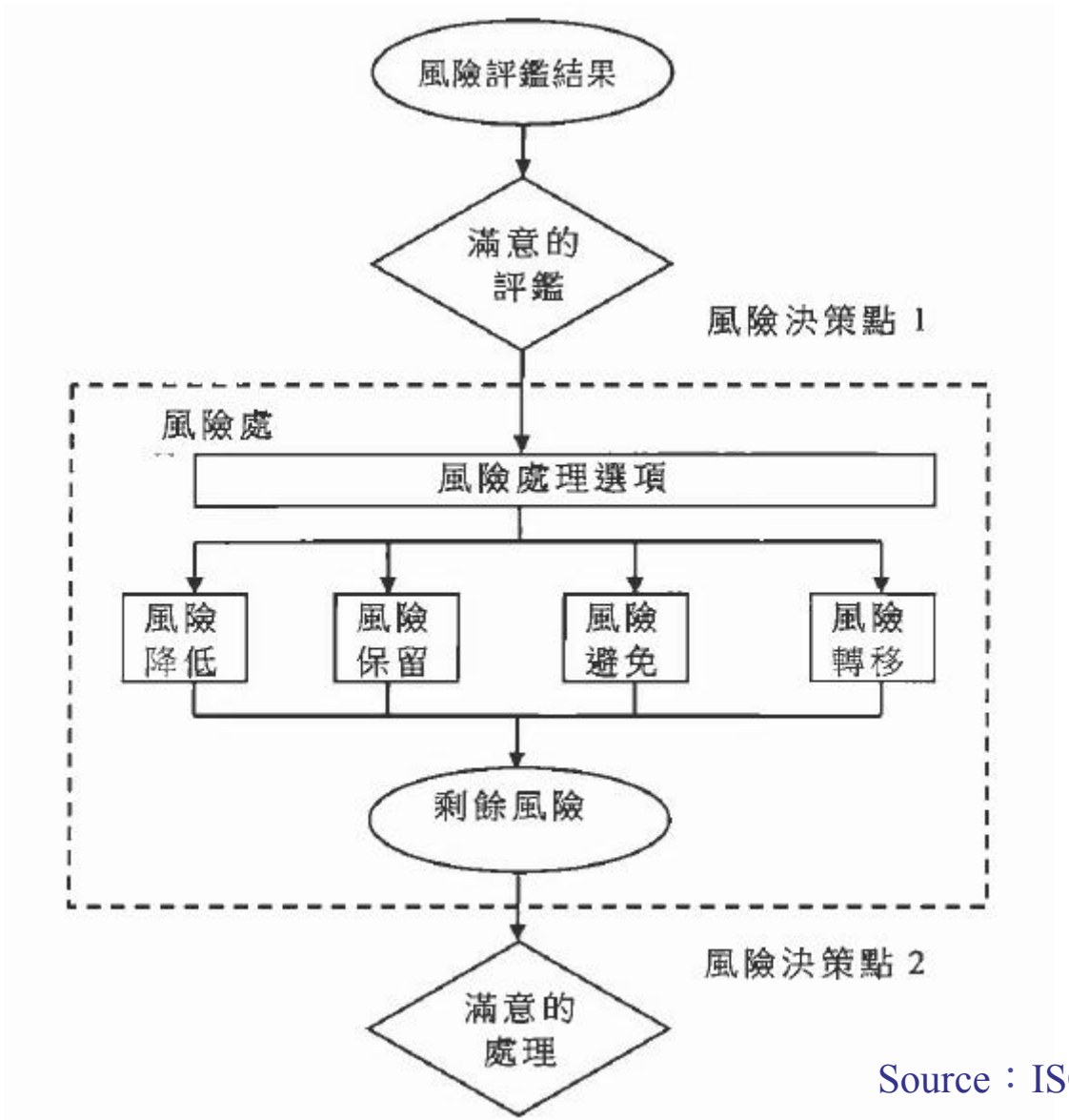
考慮因素

- 需要的風險接受等級。
- 所需費用是否合理。
- 安全風險所造成之影響。
- 是否容易執行。
- 需花費多少時間。
- 與現有環境及技術之整合是否可行。
- 符合法令規定。
- 相關契約規定。

控制風險策略說明

- **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。
- **轉移風險**
  - 轉移相關之營運風險至他者，例如：承保商、供應商。
- **保留風險**
  - 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。

風險處理活動



Source：ISO 27005

控制措施的選擇考量

- 時效性
  - 控制執行時間及有效期限為何。
- 人力
  - 每年需要多少工時來監控和維護。
  - 負責執行、監控及維護控制的人員需要接受多少訓練。
  - 必須容易執行，了解對使用者造成多少程度不便。
- 成本
  - 是否有預算執行這項控制措施。
  - 控制的費用相對於資產價值而言合理嗎？ (成本)
  - 控制成本<資產價值<威脅損失。
- 法規或合約要求

風險處理

- 依據資產風險評鑑的結果，對於超出組織風險值可接受程度之風險，進行處理。
- 目的：降低風險發生機率及風險發生時產生之損害。
- 工具：風險處理計畫。

風險處理建議及規劃

- **系統使用之資料或傳輸加解密技術存在弱點，遭利用造成資訊不當揭露**
  - 預防性措施：
    - 制定委外服務安全管理程序，規範委外服務的安全管理方式。
    - 禁止服務提供者及其人員接觸任何與加解密有關的系統及傳輸之檔案。
    - 提出提升加解密安全性之需求。
    - 對委外廠商實施資訊安全宣導。
    - 制定委外服務廠商安全須知，並要求簽署。
    - 修定安全事件處理程序增加委外服務人員之安全事件處理準則，考量以下事項：
      - 證據保全
      - 合約及法律責任
      - 法務的參與

風險處理計畫範例

機密等級：□一般 ■限閱 □密 □機密

文件編號：　　版　　次：1.0

紀錄編號：　　填表日期：XXX年XX月XX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	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
	人力資源處		人事作業	人事資料	DA	利用	販賣個資圖利	缺乏安全之管控與保護	個資外洩	48	□接受風險 ■降低風險 □轉移風險 □避免風險	權責單位進行權限控管					
	人力資源處		人事作業	人事資料	DC	利用	販賣個資圖利	缺乏安全之管控與保護	個資外洩	48	□接受風險 ■降低風險 □轉移風險 □避免風險	權責單位進行權限控管					
	人力資源處		人事作業	人事資料	DA	利用	販賣個資圖利	缺乏安全之管控與保護	個資外洩	48	□接受風險 ■降低風險 □轉移風險 □避免風險	權責單位進行權限控管					
	人力資源處		人事作業	人事資料	DC	利用	販賣個資圖利	缺乏安全之管控與保護	個資外洩	48	□接受風險 ■降低風險 □轉移風險 □避免風險	權責單位進行權限控管					
	人力資源處		人事作業	人事資料	DA	刪除/銷毀	販賣個資圖利	資料未依使用期限進行銷毀或刪除	個資外洩	48	□接受風險 □降低風險 □轉移風險 ■避免風險	宣導避免觸法（如有違反送考績委員會議處）					
	人力資源處		公務人員健保作業	健保名冊	DA	刪除/銷毀	販賣個資圖利	資料未依使用期限進行銷毀或刪除	個資外洩	48	□接受風險 □降低風險 □轉移風險 ■避免風險	依使用期限進行銷毀或刪除					

風險處理後

- 建立一套量測系統(例如：KPI指標)，協助控制目標的達成。
- 執行內部稽核，確保控制措施的有效性。
- 當有下列情況時，執行風險評鑑作業。
  - 每年定期執行。
  - 營運組織變更。
  - 作業流程改變。
  - 資產新增或變更。
  - 發生重大個資安全事件。

Q&A 問題與討論

聯絡資訊

王吉祥 講師暨資深經理

+886 970 350 128

dvings@gmail.com