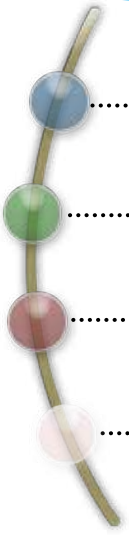
中興大學

個人資料管理
第三方稽核暨委外管理教育訓練

王吉祥(Davies)
2014.5

課程大綱



- 個人資料安全稽核機制
- 第三方稽核作業查核重點
- 委外管理暨查核要項
- 個案分析與討論

個人資料安全稽核機制

作業要項

- 實地審查重點
  - ✓ 文件化的管理系統是否符合相關標準。
  - ✓ 管理程序是否確實執行。
  - ✓ 管理系統方面是否能達到持續改善及法規遵循。

若此階段沒有不符合事項，第三方驗證單位會說明：建議「證書持續有效」。

不符合事項定義-1

- 主要不符合
  - ✓ 個人資訊管理系統過程中，程序或運作全面失效。
  - ✓ 對應標準之某項要求完全缺乏。
  - ✓ 未執行個人資料保護管理之要求，或多個次要缺失集中於同一控制措施者。
  - ✓ 對所提供之服務造成立即危害。

不符合事項定義-2

- 主要不符合
  - ✓ 在被推薦登錄前必須矯正且核可結案。
  - ✓ 若追蹤稽核發出，可能導致證書登錄停權。

不符合事項定義-3

- 次要不符合
  - ✓ 未能完全遵循個人資料保護管理之要求，但為單一、偶發、非連續之事件者。
  - ✓ 上次稽核觀察事項於後續的稽核中，經重新抽樣發現新的具體不符合要求之事證。

不符合事項定義-4

- 次要不符合
  - ✓ 允許有較多的時間來矯正。
  - ✓ 通常於下次追蹤稽核拜訪時確認。
  - ✓ 如未被適切結案，則可能導致主要缺失。

不符合事項範例-1

❖ 次要不符合

條款5.1.2要求組織應選擇適當稽核員，且稽核員應盡責進行稽核，以確保稽核方案的客觀性及公正性；目前內部稽核規劃中，缺乏足夠證據證明組織已適當考量獨立性來選擇內部稽核小組成員。

- ✓ 根因分析：內部稽核人員規劃未考量客觀性、公正性及獨立性。

條款5.1.1要求應考量政策要求，規劃、建立和維持稽核方案，以監督和檢討組織處理個人資訊管理系統的有效性及效率；目前內部稽核紀錄中，缺乏證據證明已適當確認稽核報告與工作底稿紀錄發現事項的一致性

- ✓ 根因分析：內稽之報告與工作底稿紀錄內容不一致。

不符合事項範例-2

❖ 次要不符合

條款6.1.3要求對已於內部稽核中確認的不符合事項，組織應確認不符合事項之根因，並建立相關之矯正行動。

- ✓ 根因分析：內部稽核之不符合事項，未根因分析。

標準要求所有人員均必須遵守政策，實踐組織相關流程與程序，組織亦應備妥獎懲制度、適當的人員發展訓練，以及對任何不符要求狀況的處理程序；本此發現組織有一個不符合事項在於缺乏足夠證明組織已訂定獎處措施的程序。

- ✓ 根因分析：目前未訂定個資相關懲處措施。

不符合事項範例-3

- 次要缺失

於BS 10012 : 2009 標準條款 4.7.3，如組織是直接從個人蒐集資訊，個人資訊管理系統應包含適當程序，確保組織在蒐集任何個人資訊之前，將必須提供給個人的任何隱私權公告或線上隱私權聲明提供給個人，或讓個人能取得此等公告或聲明。抽樣顯示本項要求未被完全滿足，如：合作提案網頁。

- ✓ 根因分析：導入PIMS過程中，主管已針對網路會員合作提案之功能未達到當初預期，且蒐集客戶個人資訊之隱私權聲明部份要項不足，組織已決議移除本功能，但尚未實施。

不符合事項範例-4

- 次要缺失

於BS 10012 : 2009標準條款 4.7.2，個人資訊管理系統應包含適當程序，以維持隱私權公告及線上隱私權聲明的紀錄。此等紀錄的保留時間至少應與其相關的個人資訊保留時間一樣長，經抽樣顯示本項要求未被完全滿足，如：會員註冊。

- ✓ 根因分析：系統未考量網站會員註冊之隱私權聲明是否確認已被當事人閱讀，且未保留相關同意紀錄。

觀察事項定義

- **觀察事項**
  - ✓ 值得關切的部份。
  - ✓ 因見解不同，讓客戶從質疑中獲得啟發。
  - ✓ 發現可能對個人資料保護管理造成影響的事實及事件，但未有足夠證據顯示會影響「個人資料管理政策」及個人資料之保護暨管理目的(目標)的達成，卻因未來可能成為缺失而需要再覆核。
  - ✓ 改進的建議。

觀察事項定義範例

- **觀察事項**

請組織再行檢視以確保所蒐集的個資為相關且不過度，例如：匯款簽收表格（電話、傳真機號碼、電子郵件）。

- ✓ 根因分析：考量匯款會有失敗之虞，故請當事人提供多重連絡管道，（電話、傳真號碼、電子郵件等資訊），未評估是否蒐集過度。

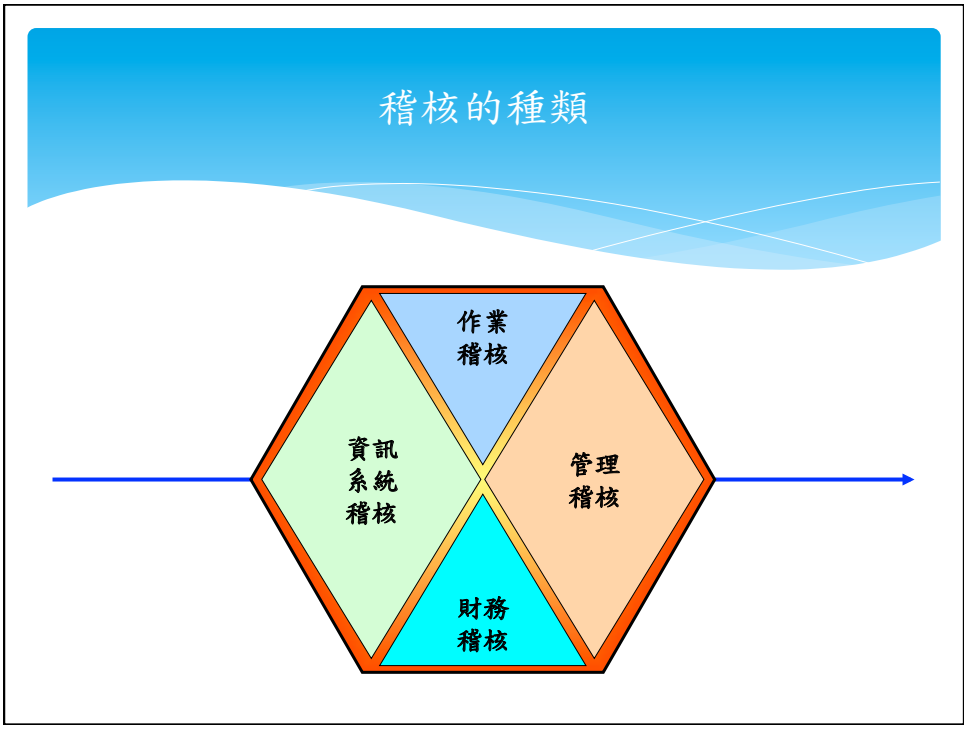
組織請再次審查檔案伺服器存取權限之適切性，如：同仁簡歷。

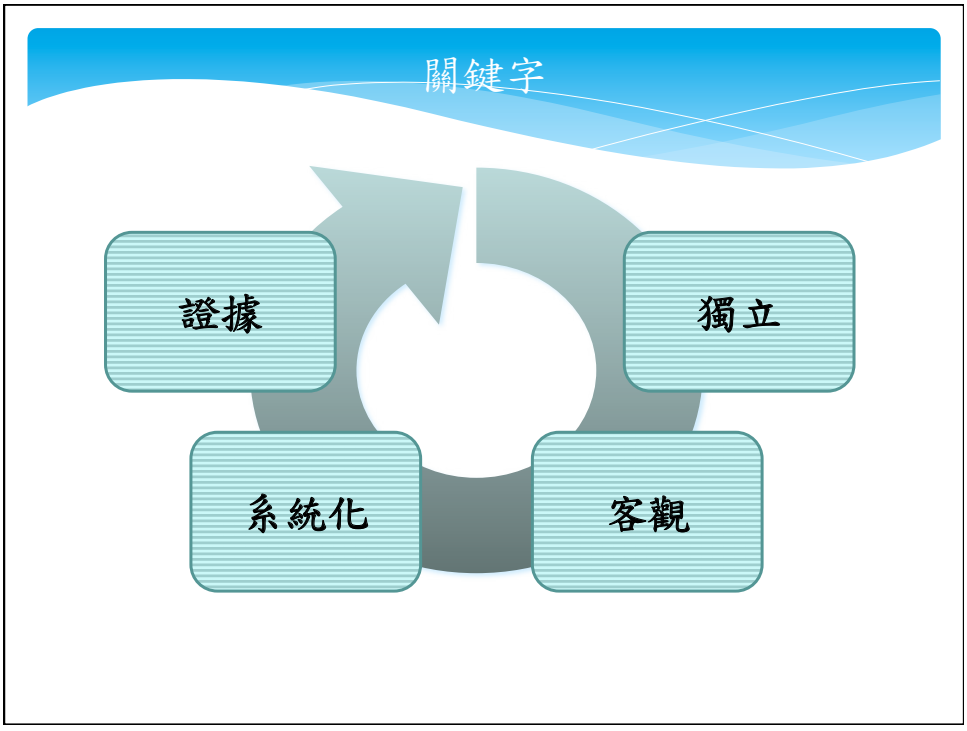
- ✓ 根因分析：單位同仁簡歷之存取權限控管不足，導致全組織皆可讀取同仁簡歷。

事項定義

- 建議事項
  - ✓ 發現可能對個人資料保護管理造成影響的潛在問題，可提出建議之改善措施，以預防未來發生之可能性。

第三方稽核作業查核重點


稽核的種類
作業
稽核
資訊
系統
稽核
管理
稽核
財務
稽核


關鍵字
證據
獨立
系統化
客觀

稽核目標

目標

* 確保單位遵循政策及標準程序、衡量管理制度之有效性
  * 控管程序是否落實。
  * 檢查與評估控制措施之缺失。
  * 評估管理成效。
  * …… 。

稽核測試的方式

遵循測試

* 測試是否遵循其要求執行
  * 法令、法規、契約要求。
  * 驗證標準。
  * 制度、規範、程序。

證實測試

* 測試其執行結果與要求或預期相符合
  * 系統功能。
  * 公式、計算結果。

問題思考

遵循測試 or 證實測試？

* 稽核人員發現個資資產清冊所列清單有所遺漏?
* 稽核人員發現系統未能依組織政策要求在帳號輸入密碼強度時，未依程序落實?

驗證過程注意事項-1

- 先聽完問題再回答
- 問題不了解可以請稽核員再說明
- 如果明確了解請直接回答
- 如果不記得，請先翻「個人資料管理相關文件」或您的筆記、問對人後再回答
- 視情況請其他同事支援，不要硬答

驗證過程注意事項-2

- 驗證過程中你(妳)要做或可以做的事
  - 相信個人資料管理制度的有效性
  - 個人資料管理制度有助於現行業務個資的控管
  - 管理文件、程序及說明書等公告文件為主
  - 提供執行證據
  - 客氣回答與請教語氣
  - 適時導向其他負責人員說明
  - 多請教與聊天

驗證過程注意事項-3

- 驗證過程中你(妳)不要做的事……
  - 激辯、強烈反駁
  - 說謊、圓謊
  - 否定稽核員的發現
  - 抱怨
  - 私下的作法
  - 反駁其他同事的回答
  - 回答「不知道」
  - 搶話
  - 麻煩
  - 冷漠
  - 拿驗證範圍外的東西解釋
  - 遲遲不提供證據

查核重點實務暨範例討論

委外管理暨查核要項

委外稽核依據-1(細則§7)

* 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。

委外稽核依據-2(細則§8)

委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。
監督至少應包含下列事項：

一. 預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間

二. 受託者就第十二條第二項採取之措施。

三. 有複委託者，其約定之受託者。

四. 受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。

五. 委託機關如對受託者有保留指示者，其保留指示之事項。

六. 委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。

委外稽核依據-3(細則§8)

委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。

* 第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。
* 受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

個資法施行細則所列之安全維護事項

	保護標的： 防止個人資料被竊取、竄改、毀損、滅失或洩漏
1	配置管理之人員及相當資源
2	界定個人資料之範圍
3	個人資料之風險評估及管理機制
4	事故之預防、通報及應變機制
5	個人資料蒐集、處理及利用之內部管理程序
6	資料安全管理及人員管理
7	認知宣導及教育訓練
8	設備安全管理
9	資料安全稽核機制
10	使用紀錄、軌跡資料及證據保存
11	個人資料安全維護之整體持續改善

個資外洩管道

- 問卷
- 電話客服中心
- 網購
- 掛馬網站、設計不良的網站
- 駭客入侵
- 社群網站
- P2P軟體使用
- 銀行申請單
- 會員手冊

- 信用卡
- 內部人員
- 補習班
- 電子謄本系統
- 直銷公司
- 盜版光碟
- 即時通訊軟體(IM)
- 無個資保護認知
- 釣魚網站
- 委外廠商

台灣Nokia行銷網站被駭，150萬個資可能外洩

* Nokia委外經營的5個台灣行銷網站遭駭客入侵，目前駭客已公佈17萬筆資料，由於缺乏證據證實駭客取得的資料數量，Nokia估計約150萬筆資料可能被竊。
* Nokia發生重大資安事件，台灣委外經營的5個行銷活動網站被駭客入侵，約150萬筆消費者個資可能被竊，Nokia已關閉這些網站，同時通知用戶防範。
* 台灣Nokia對外發出聲明，表示該公司委託網路行銷公司Agenda經營的5個台灣行銷活動網站遭駭客入侵，駭客已公佈17萬筆資料，經過調查後，Nokia可能有150萬筆先前在台灣舉辦行銷活動的消費者個人資料外洩，Nokia已採取因應措施，關閉網站、修復伺服器漏洞，移除資料庫，同時以電子郵件、簡訊通知客戶。

資料來源：isecurity

案例：美國Honda外洩490萬車主資料

* 美國接連傳出因為委外廠商安全漏洞導致客戶資料外洩的事件，先是美國麥當勞發表聲明證實客戶資料外洩一事，事件主角換成日本本田汽車的美國分公司(以下簡稱美國Honda)，駭客總共竊取了490萬筆車主資料，兩起事件的原因，同樣都是委外廠商系統漏洞所引起。
* 根據外電報導，駭客入侵美國Honda合作的第三方行銷團隊，成功竊取220萬名車主的登入資訊、電子郵件及車牌號碼，以及270萬名Acura車主的電子郵件，至於車主的社會安全碼、生日、銀行帳戶及其他資訊則未洩露。Honda未公佈合作夥伴的名稱，僅告知其業務是發送「歡迎訊息」的電子郵件，給Honda Owner Link或My Acura的帳戶使用者。
* 由於駭客很可能以「特殊服務」為主旨、大量發送釣魚郵件，藉此誘騙受害者揭露更多敏感性個人資料，因此，美國Honda主動通知資料遭外洩的車主，並成立FAQ網站，告知客戶後續該如何處理。

資安事故原因分析

未有資料保護及相關法律責任之警覺，導致違法情事

預防措施

1. **提高個資保護認知**
2. **委外相關安全控管**

新聞來源：資安人

案例：職訓局委外電訪 被轟洩個資

* 勞委會職訓局進行一項仲介公司服務品質調查，針對外勞及僱主作抽樣訪問，但因職訓局是委託《聯合報》民意調查中心進行，因此遭民眾質疑「《聯合報》是民營單位，勞委會憑什麼把我的資料洩露給非公務機關？」對此，職訓局說，調查目的是為促進仲介品質，而且和承辦機構簽有保密條約。但法務部則認為，應先經由當事人書面同意再訪問才妥當。

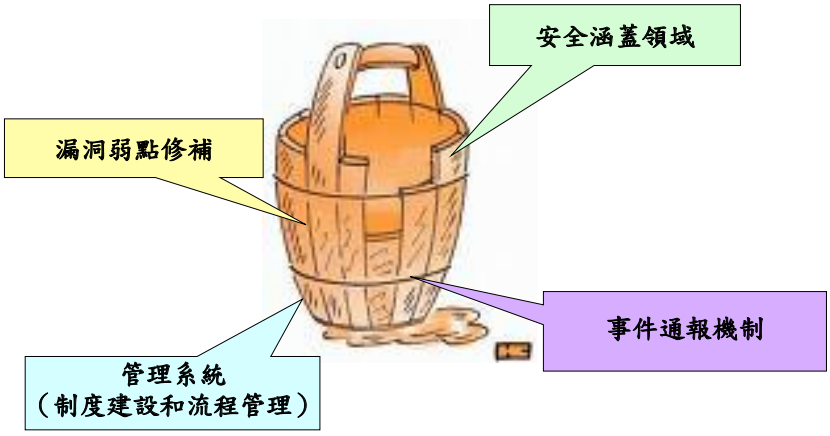
桃園黃先生突然接到一通《聯合報》民調中心的電話，說是受勞委會委託，要針對仲介公司的問題進行電話訪問，他覺得不妥。「對方一打電話來，就知道我是誰，還知道我家有外傭，連什麼名字都知道，這樣一來，不是我的資料全都外洩了嗎？」
他反問對方，怎麼會有他的資料？對方告知，是勞委會給的，他再詢問勞委會，確認有此事。
黃先生覺得不安，「《聯合報》是民營公司，勞委會怎麼可以把這麼重要的資料交給民間機構？如果資料被詐騙集團取得，不是很糟？」「即使職訓局自己電訪，都很不妥，更何況是交給第三者來做？」他因此拒訪法務部法律事務司認為，勞委會應先徵得當事人書面同意，再訪問，才較合適。法務部說，《個人資料保護法》的主要精神就是「沒有經過我的同意，怎麼可以把我的資料交給其他人？」以此來看，勞委會的作法並不妥當，若民眾覺得自己的資料外洩，權益受損，可依《個資法》提出告訴，要求勞委會賠償。

個資觀點:
1.個資法律熟悉度與符合性
2.委外廠商保密協議與溝通

洩露資料行為

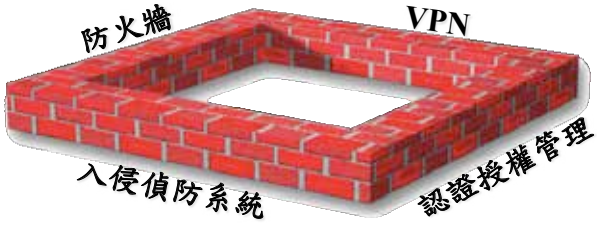
- 電梯、茶水間公共場所交談
- 未開啟螢幕保護
- 未收存辦公桌面機密性文件
- 使用網路瀏覽器儲存密碼等個人資料
- 機密資料沒有控管機制，隨意存放於電腦中

木桶理論



個案：委外作業時，一般都會注意...

建立安全的周邊環境...



結果是...

據統計有80%的資料遺失,是因為人員有意或無意之下所造成的結果

規劃策略

以組織而言：

* 確實掌握委外業務之風險。
* 落實管理之有效性。

以委外廠商而言：

* 了解作業之風險。
* 掌握未來管理改善之方向。

從主管機關的觀點

* 承接委外案件之廠商、外包人員，視同機關的延伸，亦應加強安全管理

行政院及所屬各機關資訊安全管理要點

五、各機關應就下列事項，訂定資訊安全計畫實施，並定期評估實施成效：

（一）資訊安全政策訂定。

（二）資訊安全權責分工。

（三）人員管理及資訊安全教育訓練。

（四）電腦系統安全管理。

（五）網路安全管理。

（六）系統存取控制管理。

（七）系統發展及維護安全管理。

（八）資訊資產安全管理。

（九）實體及環境安全管理。

（十）業務永續運作計畫管理。

（十一）其他資訊安全管理事項。

從自身的觀點

加強安全管理與落實稽核工作，將有助於：

- ✓提升內部管理效率並降低管理負擔
- ✓使人員有標準得以遵循
- ✓降低作業風險
- ✓提升業主之滿意度
- ✓增加公眾信心
- ✓加強單位、組織之形象
- ✓確認各項管理機制能落實執行
- ✓確保符合各項法規規範

常見委外廠商稽核整體發現-1

稽 核 發 現
• 多數單位未能明確鑑別個資價值與風險
• 未明確規範私人資訊設備攜至辦公處所使用相關規定 • 資訊資產缺乏分級及標示
• 委外合約缺乏安全條款或對著作權無明確規範 • 缺乏相關教育訓練

常見委外廠商稽核整體發現-2

稽 核 發 現
•系統更新機制無法有效執行 •缺乏資料備份或備份機制不完善 •缺乏系統時間校正與系統操作日誌 •涉及機敏性資料未加密處理
•系統帳號未定期清查，存在離職人員或預設帳號 •使用預設之管理員帳號 •未設螢幕保護程式 •共用帳號或密碼強度不足 •未建立資料存取紀錄

洩露資料如何防止

防範機密資料洩露方法

* 減少在公共場所討論
* 離開座位，使用螢幕保護程式
* 不使用或下班將機密文件收妥
* 機密文件不遺留傳真機或影印機
* 傳真前通知對方領取
* 碎紙機銷毀機密文件
* 機密檔案櫃子或房間上鎖
* 會議室文件帶走及白板擦拭乾淨
* 儲存媒體清除內容

委外稽核計畫

* 稽核依據與稽核目的(確認相關業務)
* 稽核範圍及受稽對象(合約相關內容確認)
* 稽核日期
* 稽核作業方式
* 稽核（抽樣）期間
* 稽核團隊
* 稽核項目
* 稽核報告說明

委外業務安全稽核規劃建議方向

將委外業務依據性質、單位屬性...等
進行群組化分類與客製化查核項目

設計之評分標準以及分析方法，
符合對於委外查核之要求，並達成　雙贏之目標。

委外業務安全稽核，建議可與現行
資訊安全管理系統之風險評鑑及風險處理計畫進行連結

受稽單位文件之準備

共同類文件：

一、單位內之個資、資安政策。
二、保密切結書。
三、個資清冊。
四、人員工作職掌。
五、協力廠商之合約書。

非共同類文件(依專案型態)：

一、人員進出實體環境登記。
二、系統操作日誌檔。
三、機敏性資料存取與備份紀錄。

稽核當天雙方配合事項

受稽單位

* 提供相關文件與紀錄。
* 配合稽核人員執行稽核工作。
* 請協助提供稽核會議場地、印表機...等
* 針對稽核總結提出改善承諾並訂定改善期限。

稽核單位

* 指派稽核人員。
* 執行稽核訪視工作。
* 於稽核活動結束後提出稽核發現總結並提出相關建議。

稽核執行方式(範例參考)

稽核工作將分為2階段2梯次執行

稽核(第一階段)

* 重要委外業務稽核將分2梯次進行。每梯次稽核作業將視受查委外業務地理區域、委外業務範圍及內容、人員時程安排等，排定執行稽核作業。

複查(第二階段)

* 委外業務中，如遇下列情形，應複查之委外業務建議。
  * **重大缺失**
  * **不符合事項過多**
  * **該委外業務安全管理現況遠低於群組表現**
  * **不立即改善將會有重大之風險**

查核範例說明與討論

Q&A 問題與討論

聯絡資訊

王吉祥(Davies) 講師暨資深經理

+886 970 350 128

dvings@gmail.com