個資管理制度稽核教育訓練

NII產業發展協進會

講師群

課程大綱

1. 稽核基本觀念
2. 如何撰寫稽核計畫
3. 稽核方法及實務技巧
4. 稽核範例
5. 稽核報告與改善建議追蹤
6. 結論

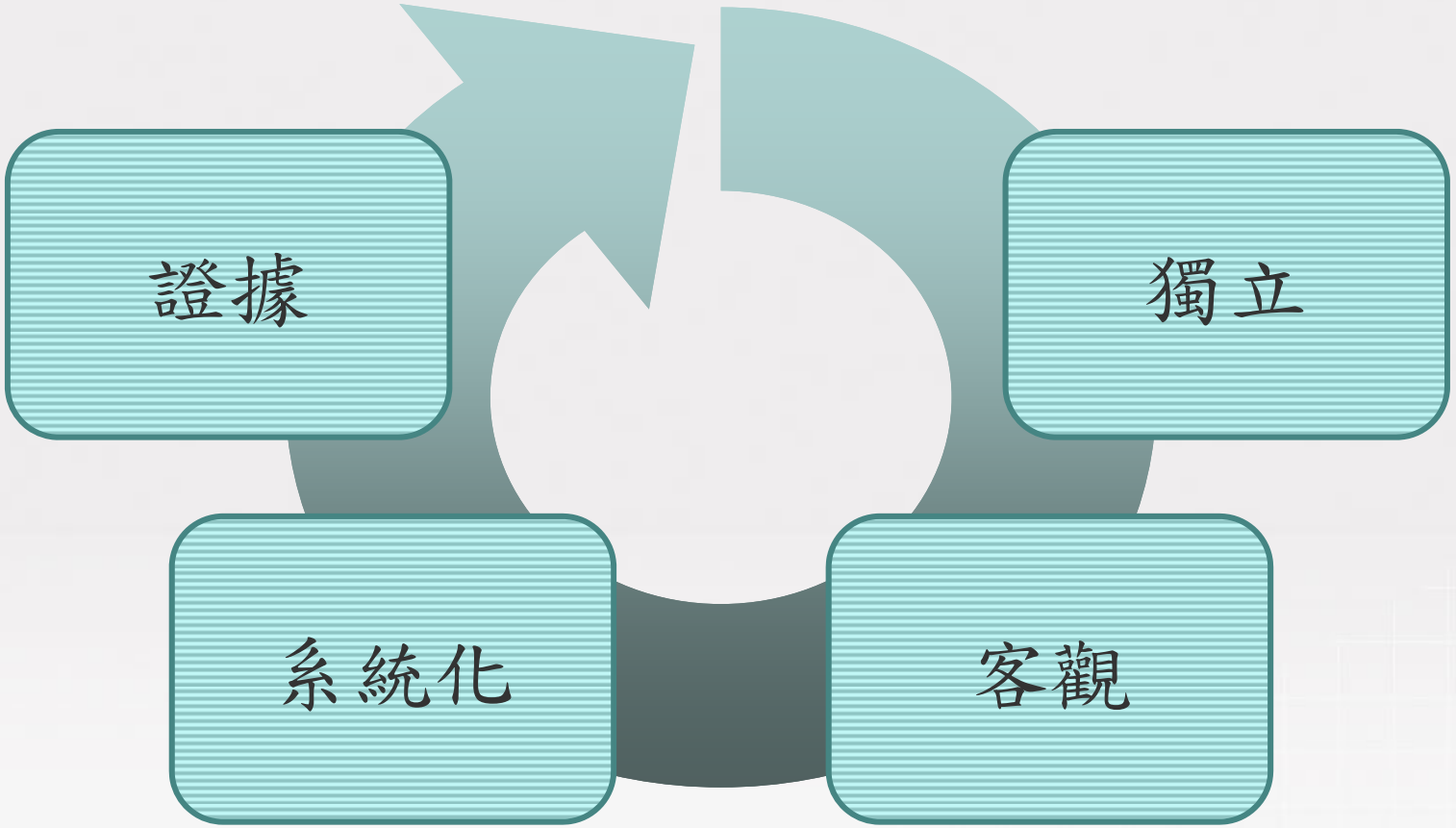
課程大綱

1. 稽核基本觀念
2. 如何撰寫稽核計畫
3. 稽核方法及實務技巧
4. 稽核範例
5. 稽核報告與改善建議追蹤
6. 結論

稽核簡介

- 稽核
  - 對某項特定活動所進行之獨立調查。
- ISO 19011定義的稽核
  - 透過系統化、獨立性及文件化的流程取得稽核證據，並透過客觀地評估，以鑑別其稽核準則所涵蓋的範圍是否達成。
- BS 10012定義的稽核
  - 以系統化的檢查來確定活動和相關的結果是否符合計劃的安排，這些安排是否得到有效實施並適用於實現組織的政策和目標。

關鍵字



稽核簡介（續）

- 內部稽核
  - 為獨立、客觀之確認性服務及諮詢服務，用以增加價值及改善機構營運。內部稽核協助機構透過有系統及有紀律之方法，評估及改善風險管理、控制及治理過程之效果，以達成機構目標。（中華民國內部稽核協會）

內部稽核與外部稽核

- 內部稽核
  - 組織內部預先進行的稽核作業，自行找出組織作業流程的缺失，提出建議改進。
- 外部稽核
  - 上級機關對組織進行的稽核。
  - 申請驗證所接受的稽核。

稽核性質

- 第一方稽核 → 內部稽核。
- 第二方稽核 → 外部稽核。
- 第三方稽核 → 外部稽核。

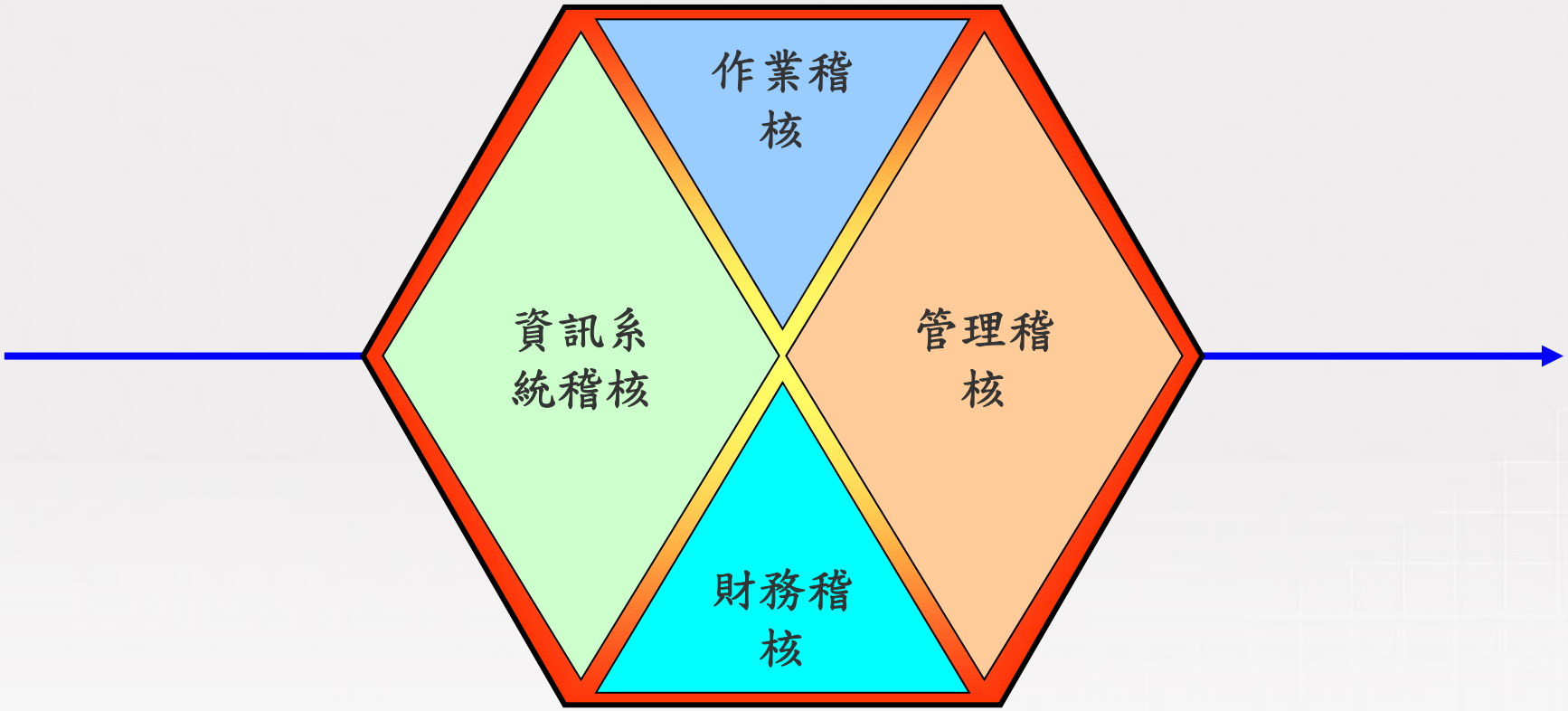
第一方稽核

- 第一方稽核
  - 由組織內部所發起的稽核活動。
  - 確保管理制度的維護、發展與改善符合目標。

第二方與第三方稽核

- 第二方稽核
  - 組織對其供應商或外包商所進行之稽核。
  - 評估供應商與外包商或下游單位是否符合合約要求或規定。
  - 例如：Apple對富士康的查核。
- 第三方稽核
  - 由具有公信力且獨立的機構對組織進行稽核。
  - 決定組織是否符合標準，建立、施行並維護文件化之管理制度。
  - 例如：Apple請求美國公平勞動協會（Fair Labor Association, FLA）調查富士康工作環境。

稽核的種類

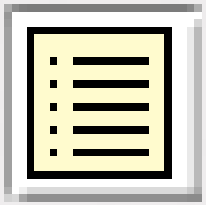


稽核目標

- 稽核的目標
  - 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？
  - 稽核人員發現作業人員確實依規定於每週一上班前檢查並維護機器。
  - 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在帳號輸入密碼錯誤達5次以上時，自動鎖定帳號。

控制措施的類別

類別	功能	運用範例
預防性	■企圖於問題發生前預測可能發生問題及調整 ■預防錯誤、遺漏或惡意破壞行為之發生	■職能分工 ■實體設備存取控制 ■建立適當之授權程序 ■完整之程式編輯檢核
偵測性	■運用偵測以發現及控制錯誤、遺漏或惡意破壞之情況	■生產過程之檢核點 ■傳輸時之回應控制 ■磁帶標籤之錯誤訊息 ■內部稽核功能
更正性	■辨識問題之影響，將威脅影響最小化 ■修正偵測性控制所發現之問題 ■更正問題產生之錯誤 ■讓問題發生機率減低	■業務持續性計畫 ■備份程序 ■保險（分攤風險） ■調整作業程序

BS 10012的稽核要求

- BS10012- 5.1內部稽核
- 內部稽核計畫
  - 組織應制訂內部稽核程序，以監控及審查處理個人資料過程之有效性，且該程序應被規劃、建立及維護，亦可將個人資料管理政策之考量納入。
  - 內部稽核程序之範圍應涵蓋所有具高風險之個人資料處理流程(參見4.2.2)及所有由其它組織所執行之個人資料處理流程(參見4.16)。

BS 10012的稽核要求(續)

- BS10012- 5.1內部稽核
- 稽核員的挑選
  - 為確保內部稽核之客觀及公平性，組織應選擇適當之稽核員並審慎的執行稽核作業。

BS 10012的稽核要求(續)

- BS10012- 5.1內部稽核
- 內部稽核需求
  - 內部稽核應依所規劃之時間執行，以確認PIMS 是否：
  - a) 依個人資料管理政策及既有之程序執行；及
  - b) 依技術需求執行及維護之。
- 稽核報告應詳實說明任何違背政策及程序之事項，並應將之提供予管理階層。
- 稽核報告亦應識別所有可能會影響政策遵循之技術或程序的議題。

資訊系統稽核與控制參考準則

- 來源：國際電腦稽核協會(ISACA)
  - 範圍。
  - 獨立性。
  - 職業道德及準則。
  - 專業能力。
  - 規劃。
  - 稽核工作之執行。
  - 報告。
  - 追蹤作業。

➢國際電腦稽核協會（ISACA®，網址：www.isaca.org）是全球公認提供資訊系統確認性與安全、企業資訊治理及資訊相關風險與遵循之知識、認證、社群、倡導與教育訓練的非營利、獨立性組織，會員遍佈逾160個國家，總數超過 95,000 人。
ISACA® 成立於 1969 年

資訊系統稽核與控制參考準則(1/4)

- 範圍
  - 記載責任、權限及可靠性。
- 獨立性
  - 職業獨立性。
  - 關聯獨立性。
    - 稽核之職能獨立於受稽單位。

資訊系統稽核與控制參考準則 (2/4)

- 職業道德及準則
  - 職業道德規範。
  - 專業稽核素養。
- 專業能力
  - 專業技術能力。
  - 執行稽核工作的技巧與知識。

資訊系統稽核與控制參考準則 (3/4)

- 規劃
  - 依稽核目標及稽核準則規劃稽核工作。
- 稽核工作之執行
  - 彙整可靠、相關的證據。
  - 證據經適當的分析及詮釋，以支持查核所發現的事項。

資訊系統稽核與控制參考準則 (4/4)

- 報告
  - 稽核報告說明稽核範圍、目標、涵蓋期間及工作，陳述稽核發現、建議及任何保留的意見。
- 追蹤作業
  - 依稽核發現結果進行適當評估，以瞭解受檢單位是否已妥善處理。

課程大綱

1. 稽核基本觀念
2. 如何撰寫稽核計畫
3. 稽核方法及實務技巧
4. 稽核範例
5. 稽核報告與改善建議追蹤
6. 結論

稽核計畫

- 稽核依據與稽核目的
- 稽核範圍及受稽對象
- 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

稽核依據與稽核目的

- 稽核依據與稽核目的
  - 確認符合
    - 法令、法規、合約要求。
    - BS 10012標準。
    - 組織政策目標。
    - …….。

稽核範圍

- 稽核範圍
  - 例如全公司、XX部門、資訊中心....
- 稽核範圍之界定（補充）
  - 實體區域
  - 組織、單位
  - 預計受稽核之活動與流程
  - 產品/業務
  - 系統

稽核日期與作業方式

- 稽核日期
- 稽核作業方式
  - 訪談、書面審查、實地審查...
  - 稽核依據
    - 例如BS 10012個人資訊管理標準、個人資料保護法、...

稽核（抽樣）期間

- 稽核（抽樣）期間
  - 文件發行日期～迄止日期
  - 上次稽核日期～本次稽核日期

稽核團隊

- 稽核團隊
  - 組長：主導稽核員
  - 組員：配合組長指示執行稽核作業
- 團隊成員資格
  - 具有基本與正確的稽核認知
    - 取得BS 10012LA證照
    - 上過稽核相關教育訓練課程
    - 具有實際稽核之經驗

稽核項目

- 稽核項目
  - 例如BS 10012的各章節等

稽核報告說明

- 稽核報告說明
  - 說明稽核報告的交付與後續事項

相關人員參與的稽核工作/責任

- 資訊安全暨個人資料保護推動委員會/召集人/執行秘書
  - 督導作業
- 資安暨個資保護稽核小組（稽核團隊）
  - 稽核作業事宜
  - 追蹤改善情形
- 受稽核單位
  - 相關業務人員接受稽核
  - 提供文件與紀錄
  - 針對稽核發現提出矯正及預防措施

稽核進行流程

稽核前準備(一)	擬訂「個人資料管理制度內部稽核計畫」，陳資訊安全暨個人資料保護推動委員會核定後，執行內部稽核
稽核前準備(二)	受稽核單位配合準備文件及紀錄
執行稽核	啟始會議（範圍、流程、配合事項） 進行稽核 稽核結束會議（稽核發現）
撰寫稽核報告	提出稽核報告並經受稽核單位代表簽名確認 追蹤事項（矯正與預防處理）

稽核計畫其他注意事項

- 與受稽核單位確認稽核時程
- 相關資料可請受稽核單位預先準備
- 特殊地點、資料調閱是否須事先提出申請
- 不同稽核地點的交通時間

練習

- 試訂自單位的稽核計畫
  - 稽核依據為BS 10012標準
  - 稽核範圍界定為個人資料蒐集、流通、處理、儲存及銷毀流程
  - 人員、時間等自訂

課程大綱

1. 稽核基本觀念
2. 如何撰寫稽核計畫
3. 稽核方法及實務技巧
4. 稽核範例
5. 稽核報告與改善建議追蹤
6. 結論

稽核專業素養

- 勿頤指氣使、氣勢凌人
- 不預設立場、不預設答案

稽核方法

- 訪談
- 書面審查
  - 文件（政策綱要/規範/要點/計畫、作業說明書、紀錄...等)
- 實地審查
- 工具輔助查核
  - 較適於電腦稽核

訪談提問技巧

- 開放式提問
  - 請問您如何處理？(5W1H)
- 封閉式提問
  - 請問您的某作業情況是否依某規定處理？

訪談提問技巧（續）

- 循序漸進
- 旁敲側擊
- 不要害怕問自己不懂的問題
  - 保持謙和態度
  - 請對方解釋相關流程

觀察受訪者

- 突然遲疑、語塞？
- 言詞閃爍、矛盾？
- 微露不安又故作鎮定？

訪談溝通技巧

- 詢問正確對象
- 不要給予對方過大的壓力
- 聆聽，避免打斷
- 不預設否定的立場

書面審查

- 文件
  - 依稽核依據檢視規範文件是否已具相關控制項，例:
    - 個人資料管理系統之目標並未建立。
    - 間接取得個資之蒐集、處理與利用之程序並未建立。
    - 個人資料管理系統政策中，宜加入並說明利害關係人之參與及期許。
    - 個人資料管理系統管理代表為資訊安全官，目前採年度任務編組派任，請進一步考量現行年度調換之規則，是否可呼應個資法中專人管理之要求。
    - 請釐清個人資料檔案清冊維護與更新之時機、頻率與作法。

書面審查(續)

- 文件
  - 依稽核依據檢視規範文件是否已具相關控制項，例:
    - 個資事故、個資訴訟判決等資訊，如何輸入至風險評鑑進行必要評估，其關聯性可再釐清。
    - 現行個資文件中，僅針對個資外洩之狀況時通知當事人；應可考量修正為個資事故發生時，通知當事人。
    - 隱私權聲明文件中，有關對第三方揭露個資之要求，請再釐清。
    - 既有已蒐集之個資，如何進行適切、相關且不過度之必要調整，請再釐清。

文件稽核範例

- 4.7.2隱私公告與聲明之紀錄
- PIMS 中應制訂一維護(線上)隱私權聲明紀錄之程序。該紀錄之保存時限應至少等同於其個人資料。
  - 本組織所提供之服務若含個人資料，應制定及維護隱私權聲明，經權責主管核准並留存相關紀錄，且該紀錄之保存期限不得低於個人資料之保存期限。
  - 本組織相關活動（網站）之隱私權聲明，可參酌本組織「隱私權政策聲明範本」修訂，陳核後方可實施。此聲明應讓當事人易於取得與閱讀。
  - 本組織所辦理之活動（網站）或業務需直接從當事人取得個人資料前，本組織應以e-mail或書面方式提供當事人該隱私權聲明，或公告於網站上。

實地審查

- 檢視相關之人、事、物是否依文件中所訂之規範落實執行
- 現場觀察
  - 環境、電腦之系統設定等
- 人員訪談
  - 訪談人員的操作流程。
- 紀錄確認
  - 是否依文件中所訂之規範落實紀錄

實地審查(續)

- 本次稽核驗證時，許多流程有效性紀錄尚未產生，如當事人請求紀錄、正確性審查、個資檔案銷毀紀錄、間接蒐集個資告知紀錄、個資事故通告紀錄及客戶抱怨紀錄等，稽核員將於下次定期審查確認有效性。
- 個資風險評鑑及衝擊評估中，財務結構面之分級判斷因子，可再釐清。
- 個人電腦內含個人資料之加密落實性，可再加強；名片管理之安全，可再加強。
- 請再注意執行PIMS內部稽核的公正與客觀性。例如：稽核員避免稽核自身事務。
- 針對內部教育訓練後，有效性衡量的記錄，宜再提供的更具體。
- DMZ區域Web主機病毒定義檔更新的即時性，可更加強。
- XX主機及XX資料庫主機的作業系統仍為Windows 2000，宜慎重考量其無後續支援所造成的資安風險。
- 宜慎重考量現行log備份方式及範圍的適切性。
- 資料庫主機管理及操作軌跡的記錄，可更加強。另外，每週進行備份的方式，亦應考量其軌跡不連續性的風險。
- 螢幕保護密碼啟動機制的確認，可更加強。
- 弱點掃描所發現高風險項目處理的即時性，可更加強。

現場查核範例

- 系統管理者密碼設置，至少6碼

  →檢查管理者密碼長度是否為6碼？

紀錄稽核範例

- 個資當事人透過電話、E-mail、傳真等方式申訴時，由相關受理人員填寫「個人資料抱怨及申訴事件紀錄單」並陳核單位主管後，轉請本校之個人資料管理窗口判定申請內容，再轉交業務權責單位進行後續處理。
- 受理單位接獲個資當事人之抱怨與申訴後，應於10個工作日內回應當事人本行已受理申訴之訊息。

  →個人資料抱怨及申訴事件紀錄單

紀錄稽核技巧

- 檢查不同紀錄間的一致性，以確認完整性與有效性

  →個人資料抱怨及申訴事件紀錄單

  →個資抱怨申訴E-mail、傳真

稽核技巧重點綜合說明

- 說（訪談）、寫（文件）、做（實地）是否一致
- 聆聽受稽單位的執行說明，思考可能遺漏的環節
- 善用執行程序的連貫性來稽查是否確實落實
- 使用客觀、顯著、可驗證性的證據來判別與撰寫稽核發現結果

其他稽核規劃事項

- 稽核動線的安排
- 不同稽核項目間的連貫性
- 避免抽查單一部門、系統或人員
- 稽核時間避免安排於稽核範圍內有重大關鍵活動

練習

- 試述您想像 / 規劃 / 預計採用的稽核技巧
  - 例如試舉例針對某一控制項，您準備怎麼查核？
  - 例如您準備抽查哪些對象，為什麼？
  - 例如您準備如何驗證受稽對象的說辭是否屬實？

課程大綱

1. 稽核基本觀念
2. 如何撰寫稽核計畫
3. 稽核方法及實務技巧
4. 稽核範例
5. 稽核報告與改善建議追蹤
6. 結論

稽核項目

- 個資資產與風險評鑑
- 個人資料管理系統
  - 規劃個人資料管理系統(PIMS)
    - 建立與管理**PIMS**
    - 界定**PIMS** 適用範圍及設定目標組織
    - 個人資料管理政策
    - 政策內容
    - 職責與歸責性
    - 資源提供
    - 將**PIMS** 嵌入組織文化

稽核項目(續)

- 實作與運作個人資料管理系統(PIMS)
  - 責任的配置
  - 辨識及記錄個人資料的使用情況
  - 認知與教育訓練
  - 風險評鑑
  - **PIMS** 的持續更新
  - 通告
  - 公正與合法的處理
  - 個人資料處理的目的
  - 適當、相關及不過度
  - 正確性
  - 保留及處置
  - 個人權利
  - 安全議題
  - 將個人資料傳輸於**EEA** 外
  - 揭露予第三方
  - 轉包處理
  - 維護

稽核項目(續)

- 監視與審查個人資料管理系統(PIMS)
  - 內部稽核
  - 管理審查
- 改進個人資料管理系統(PIMS)
  - 矯正與預防措施
  - 持續改善

規劃個人資料管理系統PIMS

- 3.1 建立和管理 PIMS
- 3.2 PIMS 的範圍和目標
- 3.3 個人資料管理政策
- 3.4 政策內容
- 3.5 職責和歸責性
- 3.6 資源提供
- 3.7 將PIMS嵌入組織文化

規劃個人資料管理系統PIMS

- 3.1 建立和管理 PIMS
  - 組織應建立、實作、維護及持續改進PIMS以符合3.2～3.7的要求
- 3.2 PIMS 的範圍和目標
  - a) 個人資料管理需求
  - b) 組織的目標與義務
  - c) 組織可接受的風險等級
  - d) 適用之法令、規章、契約(合約)與專業職責
  - e) 個人和其他利害關係人之利益

規劃個人資料管理系統PIMS

- 3.3 個人資料管理政策
  - 組織應確保高階管理階層被附與發行及維護個人資料管理政策之責，而其政策中應明訂政策框架，並展現對於遵循個人資料保護法與好的實務的支持與承諾。

規劃個人資料管理系統PIMS

- 3.4 政策內容
  - a) 僅於合法組織需求下，始得進行個人資料之處理
  - b) 僅針對特定目的蒐集必要的個人資料，且不過度的處理個人資料
  - c) 明確告知當事人其個人資料將如何被使用及被誰使用
  - d) 僅處理相關且適當的個人資訊
  - e) 公平與合法的處理個人資訊(參考 4.7);
  - f) 組織應維護一份個人資料清冊(參考 4.2);
  - g) 確保個人資料的正確性，並於必要時進行更新
  - h) 僅依法或合法的組織目的下保存個人資料

規劃個人資料管理系統PIMS

- i) 尊重當事人對其個人資料所能行使之權利，包含其申請閱覽權
- j) 確保所有個人資料安全
- k) 當組織將個人資料傳輸之非歐盟成員之國家時，應確保其具善良保護之機制
- l) 個人資料保護法令所允許之例外情形的應用
- m) 發展與建立PIMS，使個人資料保護政策能實行
- n) 鑑別內、外部利害關係者及其參與PIMS治理與運作的程度
- o) 於PIMS明確界定員工之責任和歸責性(參考3.5)

規劃個人資料管理系統PIMS

3.5 職責和歸責性

高階管理團隊應負起組織管理個人資料之責。(可參考4.1.1).

- 職責應包含：
  - a) 核准個人資料管理政策
  - b) 依政策發展和施行PIMS
  - c) 應遵循政策執行安全及風險管理 (可參考4.13.1)
- 應指派一位或多位合適或具經驗的同仁負責日常個人資料管理政策的遵循(可參考4.1.2)
- 藉由流程與程序的實行、適當的員工發展或對於不符合事項制訂管控程序，以確保所有同仁皆能遵循個人資料管理政策之要求

規劃個人資料管理系統PIMS

- 3.6 資源提供
- 組織應決定並提供建立、實行、操作和維護PIMS 的資源。

規劃個人資料管理系統PIMS

3.7 將PIMS嵌入組織文化

a) 透過持續的教育訓練與認知課程，以提高、 強化與維持所有員工對PIMS的認知

b) 建立對PIMS認知訓練有效性評量程序

c) 對所有員工傳達以下的重要性：

- 1) 達成PIMS目標
- 2) 遵循政策
- 3) 對政策的持續改善

d) 確保每個員工都瞭解他們如何影響組織PIMS

PIMS的建置與運作

- 4.1 責任的配置(Key appointments)
  - 4.1.1 高階管理階層
  - 4.1.2 遵循政策的日常職責
  - 4.1.3 資料保護代表
- 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
  - 4.2.2 具高風險的個人資料
- 4.3 認知及教育訓練
- 4.4 風險評鑑

PIMS的建置與運作

- 4.5 PIMS 持續更新
- 4.6 通告
- 4.7 公正與合法的處理
  - 4.7.1 個人資料的蒐集與處理
  - 4.7.2 隱私公告與聲明之記錄
  - 4.7.3 隱私公告與聲明之取得
  - 4.7.4 隱私公告與聲明之可用性
  - 4.7.5 第三方

PIMS的建置與運作

- 4.8 個人資料處理的目的
  - 4.8.1 處理準則
  - 4.8.2 新目的的同意
  - 4.8.3 資料分享
  - 4.8.4 資料配對
- 4.9 適當、相關且不過度
  - 4.9.1 適當性
  - 4.9.2 相關且不過度
- 4.10 正確性

PIMS的建置與運作

- 4.11 保留及處置
- 4.12 個人的權利
  - 4.12.1 個人的權利(符合法定時間限制)
  - 4.12.2 抱怨與申訴
- 4.13 安全議題
  - 4.13.1 安全控制
  - 4.13.2 儲存及管理
  - 4.13.3 傳輸
  - 4.13.4 存取控制
  - 4.13.5 安全評估
  - 4.13.6 安全事故管理

PIMS的建置與運作

- 4.14 將個人資料傳輸於EEA(歐盟)之外
  (EEA=European Economic Area)
- 4.15 揭露予第三方
- 4.16 轉包處理
- 4.17 維護

PIMS的監控與審查

- 5.1 內部稽核
  - 5.1.1 稽核計畫
  - 5.1.2 稽核員的挑選
  - 5.1.3 稽核需求
- 5.2 管理審查

5.2管理審查

- 5.2 管理審查
  - a)來自PIMS 使用者之回饋
  - b)由組織人員所辨識及提升之風險
  - c)稽核結果
  - d)程序審查之紀錄
  - e)資訊技術提升及替換之結果
  - f)來自主管機關評估後之正式要求
  - g)抱怨事件的處理
  - h)已發生之資安事故及資料外洩事件
- 管理審查應提供所有可能造成PIMS變更之詳細資訊，其資料來源可為政策的調整、可能影響作業遵循之程序與技術。
- 當PIMS發生重大變更後，應立即執行稽核作業。

內部稽核應注意事項

- 針對受稽單位之個資收集的作業流程，應按時間(例如：每周或每月)累進的增加數量，按照合適之比例進行抽樣確認。抽樣數量與抽樣方式需能代表樣本母體，且應考慮下列事項：
  - 稽核時間；
  - 作業流程之複雜度；
  - 個資之防護措施的現況情況；
  - 過去一年是否有重大抱怨、申訴案件；
  - 過去一年是否有關之法律爭議；
  - 是否有委外處理或派遣人員經手個資(例如：蒐集、存放、列印或銷毀)。

內部稽核應注意事項(續1)

- 稽核中所抽樣之個資資訊，任何能直接或間接識別特定人之資訊，稽核員不得註記於任何工作底稿中，以避免洩密之風險並降低受稽單位之顧慮。
- 稽核中，註記抽樣之個資樣本應以代碼、案號、進案日期、身份證字號第一碼(英文字母)與最後六碼(數字)，或是以僅能由受稽方進行單向確認的資料存錄方式進行註記。
- 此一作法應於啟始會議(Opening meeting)與閉幕會議(Closing meeting)中，由領隊明確說明並澄清任何有關之疑慮。

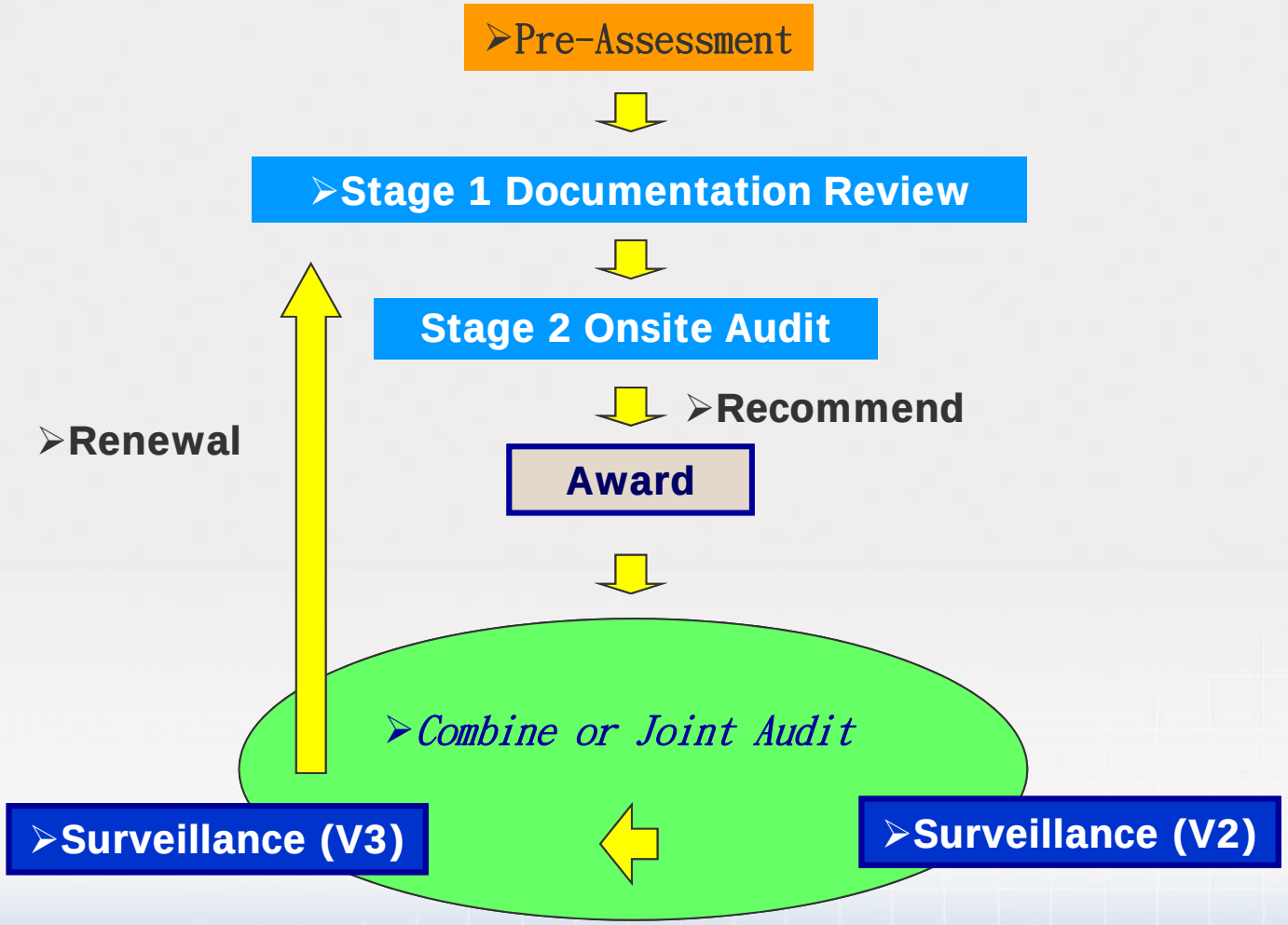
內部稽核應注意事項(續2)

- 為因應個資法的要求，稽核員應抽樣確認個資資訊收集的範圍是否超出其宣告，並確認其運用是否與個資擁有者之授權相符合。如為書面授權，則應一併確認其保存方式與保存狀況。
- 實地稽核均應確認受稽單位之風險評鑑(risk assessment)的內容與結果，定期追查則應確認前後兩次的風險評鑑的異動與理由的適當性與合理性。
- 應確認後續之風險處置(risk treatment)以善盡專業之責(due diligent)。

PIMS的改善

- 6.1 矯正與預防措施
  - 6.1.1 概述
  - 6.1.2 預防措施
  - 6.1.3 矯正措施
- 6.2 持續改進

第三方驗證流程



應確認下列管理活動已於稽核前執行

- 個資管理政策(政策綱要)

  業已擬定並經決策高層核可後公告

- 風險評鑑

  應涵蓋客戶、員工或因業務關係所得知之個人隱私資訊

- 風險處置
- 內部稽核
- 管理審查

練習

- 試對下列領域舉例簡述您的查核項目，並說明依據何項控制要點？
  - 儲存與處理
  - 存取控制

課程大綱

1. 稽核基本觀念
2. 如何撰寫稽核計畫
3. 稽核方法及實務技巧
4. 稽核範例
5. 稽核報告與改善建議追蹤
6. 結論

稽核報告

- 稽核依據與稽核目的
- 稽核範圍
- 稽核日期
- 稽核期間
- 稽核人員
- 稽核發現

改善建議事項追蹤

- 改正行動追蹤
- 追蹤時機
  - 重要性
  - 稽核人員的判斷
- 追蹤方式
  - 建立稽核專案
  - 查詢現況或列為下次稽核觀察事項

課程大綱

1. 稽核基本觀念
2. 如何撰寫稽核計畫
3. 稽核方法及實務技巧
4. 稽核範例
5. 稽核報告與改善建議追蹤
6. 結論

結論與提醒

- 稽核準備階段
  - 稽核員的角色及責任
  - 稽核作業規劃與執行必需依組織事先定義好的流程辦理，包含：稽核目標、範圍等
- 稽核執行階段
  - 稽核人員必需以公正的立場、委婉卻堅定的態度、敏銳的觀察力，查明事實與隱藏在事實背後的真相

結論與提醒（續）

- 稽核完成階段
  - 撰寫稽核報告前宜與受稽核單位溝通以取得一致的稽核結果意見
  - 勿在證據不足的情況下，妄下稽核結論
  - 應持續追蹤，以確認受稽單位是否對於建議的事項採取承諾的改正行動

簡報完畢，敬請指教

附錄：稽核判定原則

- 符合
  - 無缺失
  - 文件完整具體
  - 執行確實
- 不符合
  - 有一項以上缺失
  - 文件不甚完整，仍有改善空間
  - 執行不甚確實
- 不適用

  若稽核單位無該項稽核需求者，則判定為不適用