課程大綱

1. 個人資訊管理系統(PIMS)稽核
2. 稽核實務
3. 執行個資管理稽核
4. 矯正與預防程序
5. 稽核報告範例說明

2

課程大綱

1. 個人資訊管理系統(PIMS)稽核
2.
3.
4.
5.

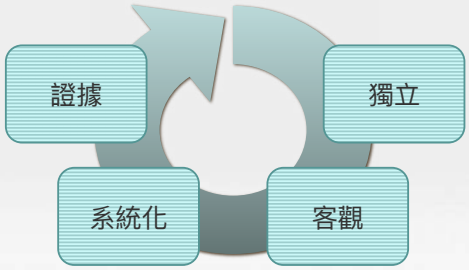
3

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。

4

關鍵字



5

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）

6

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。

7

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

8

稽核性質(續)

- 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。
- 第二方稽核
  - 組織對其供應商或外包商所進行之稽核。
- 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。

9

BS 10012的稽核要求

- 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及所有由其它組織所執行之個人資料處理流程。

10

BS 10012的稽核要求(續)

- 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。
- 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。

11

課程大綱

1.
2. 稽核實務
3.
4.
5.

12

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

13

系統稽核與控制參考準則(續)

- 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。
- 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。

14

系統稽核與控制參考準則(續)

- 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。
- 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。

15

系統稽核與控制參考準則(續)

- 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。

16

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

17

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？
- 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

18

訪談溝通技巧

- 突然遲疑、語塞？
- 言詞閃爍、矛盾？
- 微露不安又故作鎮定？
- 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

19

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

20

課程大綱

1
2
3 執行個資管理稽核
4
5

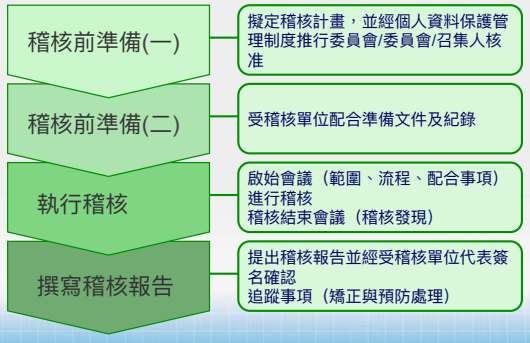
21

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

22

稽核進行流程(範例參考)



23

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等時間

24

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。
    - …… 。

25

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

26

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

27

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

28

實例參考與討論

個人資料保護工作事項檢核表

29

課程大綱

1
2
3
4 矯正與預防程序
5

30

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

31

課程大綱

1
2
3
4
5 稽核報告範例說明

32

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

33

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

34

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

35