資訊安全稽核介紹與實務

課程大綱

稽核簡介

資安稽核方法與技巧

稽核人員與受稽人員之注意事項

實作案例

稽核的定義

- 廣義而言，所有對某項特定活動所進行之獨立調查均可稱為稽核。而根據其性質不同，又可細分為財務報表稽核、作業稽核、遵行稽核等。
- ISO 19011中稽核之定義：
  - Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.
  - 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。

稽核的定義（續）

- **中華民國內部稽核協會**
  - 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。
- **稽核的關鍵字（Key words）**
  - 系統
  - 獨立
  - 客觀
  - 證據

稽核的性質

- **內部稽核(Internal audit)**
  - First Party（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
- **外部稽核(External audit)**
  - Second party（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是否符合合約要求或規定
  - Third party（第三方稽核）
    - 由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

資訊安全稽核種類

- **管理遵行性**
  - 依據標準、規範，進行書面文件、執行軌跡與落實程度之評估稽核
- **技術遵行性**
  - 弱點偵測掃描(Vulnerability scanning)
  - 攻擊與滲透測試(Attack & penetration testing)
  - 技術稽核(Technique audit)
    - 信任關係、帳戶密碼原則、存取控制
    - 網路拓撲、網路設備、防火牆、入侵偵測系統、作業系統、應用系統、資料庫系統等重要設定參數稽核

內部資安稽核目的

- **確保單位遵循資訊安全政策及標準程序，達成資訊安全稽核目標：**
  - 覆核控管程序是否落實
  - 評估管理成效
  - 協助發現缺失
  - 提供改善方案
  - 達到控制風險的最終目的（機密性、完整性、可用性）

資安稽核的方法

- **常用稽核方法**
  - 書面檢閱
  - 人員訪談
  - 實地觀察
  - 紀錄與表單抽樣
  - 工具輔助查核與取樣

稽核技巧

- **提出問題**
  - 開放語句：請問 貴單位資訊安全訊息公告的方式為何？
  - 封閉語句：請問 貴單位是否有公告資訊安全訊息？
- **觀察受訪者**
  - 言詞閃爍
  - 坐立難安
  - 雙手顫抖
  - 前後矛盾

稽核技巧（續）

- **不要害怕問自己不懂的問題**
  - 稽核也是學習（見賢思齊、見不賢而內自省）
  - 請受稽代表說明作業流程
  - 洋蔥式問法（以系統帳號管理為例）
- **不要催促受稽代表**
  - 態度決定資訊來源品質
  - 循序漸進式
  - 輕鬆訪談式（緩和稽核時的緊張或對立）
  - 旁敲側擊

稽核技巧（續）

- **建立共識**
- **專業知識與證據**
  - 證據可包含稽核人員的觀察、訪談的筆記、自內部文件或信件

    中取得之資料、及稽核測試程序所產生的結果
  - 稽核人員應評估查核證據的質與量
- **持續追蹤改善進度**

內部稽核常見問題

- 內部稽核標準為何？
- 做不到=不適用？
- 訂定中長期改善計畫，可以視為合理的矯正措施嗎？
- 同仁當場修改缺失，稽核員仍要紀錄嗎？
- 如何稽核自己不熟悉的業務，例如網路防禦技術、資訊機房等？
- 稽核的深度與廣度為何？
- 如何進行勾稽與深入查證？
- …其他

受稽單位應答時要...

- 明確且有自信
- 根據稽核員所提問內容回答
- 依據文件規範內容回答
- 若非自己負責之業務應請適當的人回答
- 若對文件內容不熟悉，應回答：我們有相關的規範，我馬上找出來
- 視情況請其他同事支援不要硬答
- 若不確定稽核員的問題，請直接要求稽核員說明
- 問題不了解可以請稽核員再說明

受稽單位應答時不要...

- 思索過久
- 自我衍生其他的問題
- 以自己的想法解讀問題
- 代替別人回答問題
- 忌答：不知道
- 若有顧問陪同稽核，但不能說這是顧問做的，或說是顧問要我們做的，或看著顧問不知道怎麼回答
- 激辯、強烈反駁、反駁其他同事的回答
- 說謊、圓謊
- 抱怨
- 說明私下的作法

實作案例

練習1

* 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？

稽核計畫

練習2

* 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？
  * 人員安全管理
  * 實體與環境安全
  * 通訊與作業管理
  * 存取控制
  * 資訊系統獲取、開發及維護

資訊安全政策

* 管理階層是否瞭解資訊安全目的並給予支持？
* 資訊安全政策文件是否由管理階層核准，並正式發布予員工？
* 資訊安全政策是否定期評估，並作必要調整？

安全組織

* 是否具管理階層或成立跨部門單位負責推動、協調及監督資訊安全管理事項？
* 是否指派專人或專責單位負責規劃、執行資訊安全控管工作？
* 是否規範員工的資訊安全作業程序與權責？
* 是否訂定資訊設備的安全作業程序？

資產管理

* 是否建立資產清冊並適時更新？
* 重要資產是否均指定專人負責管理？
* 資訊是否分級？是否建立資訊安全等級之分類標準？
* 對於機密等級的資訊是否標示清楚？

人員安全管理

* 對於具有存取較機密性資訊權限之員工，是否進行分工以分散權責？
* 人員之調動、離職，是否立即取消其各項識別碼與通行碼？
* 是否依員工職務層級進行適當的資訊安全講習？
* 員工是否瞭解組織的資訊安全政策？

實體與環境安全

* 資訊設備設置地點是否已作安全考量？
* 是否檢查及評估水、火、灰塵、電力供應等對於資訊設備之危害？
* 電源供應及備援電源是否作安全考量？
* 設備報廢前是否將機密性資料及版權軟體移除？

通訊與作業管理

* 是否建立系統變更程序？
* 是否全面使用防毒軟體並更新病毒碼？
* 對重要資料及軟體是否定期作備份？
* 儲存媒體是否依保存要求存放在安全的環境？

存取控制

* 多人使用之資訊系統，是否建立使用者註冊管理程序？
* 是否定期檢查並刪除重覆或閒置的使用者帳號？
* 應用系統是否具作業結束或一定期間未操作即自動登出之保護機制？
* 是否管制使用者的連線功能？

資訊系統獲取、開發及維護

* 應用系統在規劃分析時是否將安全需求維入考量？
* 機密性資料在傳輸或儲存過程是否使用加密技術？
* 如須用真實資料進行測試，是否於事前將足以辨識個人身份之資料隱蔽？

資訊安全事故管理

* 是否建立資訊安全事件通報與處理程序？
* 是否建立資訊安全事故管理責任與應變程序？
* 資訊安全事件中相關證據資料是否有適當保存措施？

業務持續管理

* 是否擬訂關鍵性業務及其風險評估、衝擊影響？
* 是否訂有緊急應變計畫？
* 緊急應變計畫是否定期演練與修正？

遵循性

* 是否使用合法軟體？
* 是否依「個人資料保護法」規定辦理？
* 是否定期稽核資訊安全事項辦理情形？

Q&A 問題與討論