資安事件、追蹤、內部稽核教育訓練

100年1月6日

邱瑩青 副理

NII產業發展協進會

大綱

- 資訊安全事件通報
- 矯正與預防
- 資訊安全內部稽核
- 資訊安全內部稽核注意事項
- 結論

- 資訊安全事件通報
- 矯正與預防
- 資訊安全內部稽核
- 資訊安全內部稽核注意事項
- 結論

資訊安全事件通報相關項目

- 異常事件
- 資訊安全事件
  - 顯示可能為安全政策違返或保護措施失效
- 資訊安全事件影響等級
- 資訊安全事件相關外部單位

資訊安全事件影響等級範例(1/4)

- 4級事件
  - 影響本中心業務運作甚鉅，可能造成所有業務停擺
  - 機敏性之核心業務資料遭洩漏
  - 核心業務系統或資料遭竄改，影響嚴重
  - 事件須3天（含）以上才能處理完成
  - 造成媒體、教職員生與民眾對本中心聲譽嚴重批評與不信任

資訊安全事件影響等級範例(2/4)

- 3級事件
  - 影響本中心部份核心業務停擺
  - 非屬機敏性之核心業務資料遭洩漏
  - 核心業務系統或資料遭竄改，影響輕微
  - 事件須8個工作小時（含）以上，3天以內才能處理完成
  - 造成媒體、教職員生與民眾對本中心聲譽批評與不信任

資訊安全事件影響等級範例(3/4)

- 2級事件
  - 影響本中心部分業務停擺，核心業務運作受影響或效率降低
  - 非核心業務資料遭洩漏
  - 非核心業務系統或資料遭竄改，影響嚴重
  - 事件須4個工作小時（含）以上， 8個工作小時以內才能處理完成
  - 造成媒體、教職員生與民眾對本中心聲譽批評與不信任

資訊安全事件影響等級範例(4/4)

- 1級事件
  - 影響本中心部分業務運作延遲，但不影響核心業務正常運作
  - 非核心業務資料遭部分洩漏
  - 非核心業務系統或資料遭竄改，影響輕微
  - 事件可於4個工作小時以內處理完成
  - 造成教職員生對本中心聲譽批評與不信任

資訊安全事件相關外部單位

- 委外（第三方）廠商
- 司法警政及消防機關
- 政府網路危機處理中心（GSN-CERT/CC）
- 國家資通安全會報技術服務中心
- 教育機構資通安全通報小組
- 台灣電腦網路危機處理暨協調中心（TWCERT/CC）等

作業說明

- 日常監控
- 事件通報
- 事件辨識
- 事故抑制
- 事故排除
- 事故檢討與學習

日常監控

- 應建立資訊安全監控機制，以偵測違反資訊安全之行為，安全監控機制應包含下列事項：
- 實體環境安全監控
- 網路存取監控
- 重要應用系統存取監控
- 作業系統存取監控
- 資料庫存取監控
- 機房操作人員作業監控

事件通報

- 為建全通報體系，應建立「組織成員表」與「外部單位聯絡清單」，內部資訊安全事件通報處理流程步驟說明如下：
- 本中心員工或委外服務廠商如發現疑似資訊安全事件時，應向資安業務承辦人反應
- 資安業務承辦人接獲通知後，應與相關人員共同判斷是否為資訊安全事件
- 若為資訊安全事件，資安業務承辦人應依狀況評估事件影響等級，並填寫「資訊安全事件通報單」，依狀況確認事件影響等級呈報

事件辨識

- 資安業務承辦人於通報後，經識別影響等級為3、4級者，應依資訊安全事件類別及破壞程度協調相關人員處理
- 處理過程中如發現事件造成之影響大於原先判定，資安業務承辦人應立即向上級報告，重新進行事件分析辨識
- 辨識工作完成前，應避免系統重新開機，以保全完整證據，若系統必須重新開機，則應儘量於重新開機前保留系統稽核紀錄檔案

事故抑制

- 抑制措施應以隔離或暫停發生事故之設備、系統、連線、環境及存取權限為原則

事故排除

- 依資訊安全事故發生之原因，協調相關人員，進行事故排除作業
- 為避免事故排除作業造成重要資料或鑑識證據之遺失，應於事故排除作業前完成重要設定檔、資料與鑑識紀錄檔之備份
- 重大資訊安全事件應保留發生之證據，如有需要得向教育機構資通安全通報小組申請協助
- 事故排除作業除需移除資訊安全事件外，應就事故發生原因加強防範，以避免相同事故再次發生

事故檢討與學習

- 資訊安全事故排除後，召集相關單位或人員進行事故處理檢討會議
- 資訊安全事故處理結果，彙整填寫「資訊安全事故報告單」，經資安業務承辦人跟催處理結果，於結案後陳核
- 「資訊安全事故報告單」在無牽涉個人隱私與本中心業務機密之情況，權責單位應將事件發生原因、過程、處理方式、注意事項及改善建議等內容製成案例，以網站、電子郵件或教育訓練等方式宣導，以作為中心內部資訊安全事故學習之參考

表單範例

- 組織成員表
- 外部單位聯絡清單
- 資訊安全事件通報單
- 資訊安全事故報告單

資訊安全事件通報常見疏失

- 資訊安全事件報告單之權責單位欄位宜請相關權責人員簽核確認
- 宜進一步釐清異常、資安事件之鑑別方式以利後續矯正預防管理作業之運作
- 資訊安全事件通報流程宜與主管機關之通報程序一致，並注意主管機關相關規定之版次更新

- 資訊安全事件通報
- 矯正與預防
- 資訊安全內部稽核
- 資訊安全內部稽核注意事項
- 結論

矯正預防執行時機

- 自行發現或內、外部稽核缺失及發生資訊安全事件（含重大異常事件），缺失權責單位應提出矯正措施或預防措施，並填寫於「資訊安全矯正與預防處理表」

矯正與預防措施評估

- 缺失權責單位提出矯正與預防措施時，得區分為暫時性對策及永久性對策，防止類似事件發生
- 評估措施時須考慮成本效益及可行性

矯正預防執行狀況追蹤

- 矯正與預防措施之執行狀況，應由缺失人員依據「資訊安全矯正與預防處理表」確實執行
- 有關執行狀況之追蹤，由資訊安全稽核小組組長、組員或相關權責人員負責
- 追蹤人員應於「資訊安全矯正與預防處理表」上留存追蹤軌跡

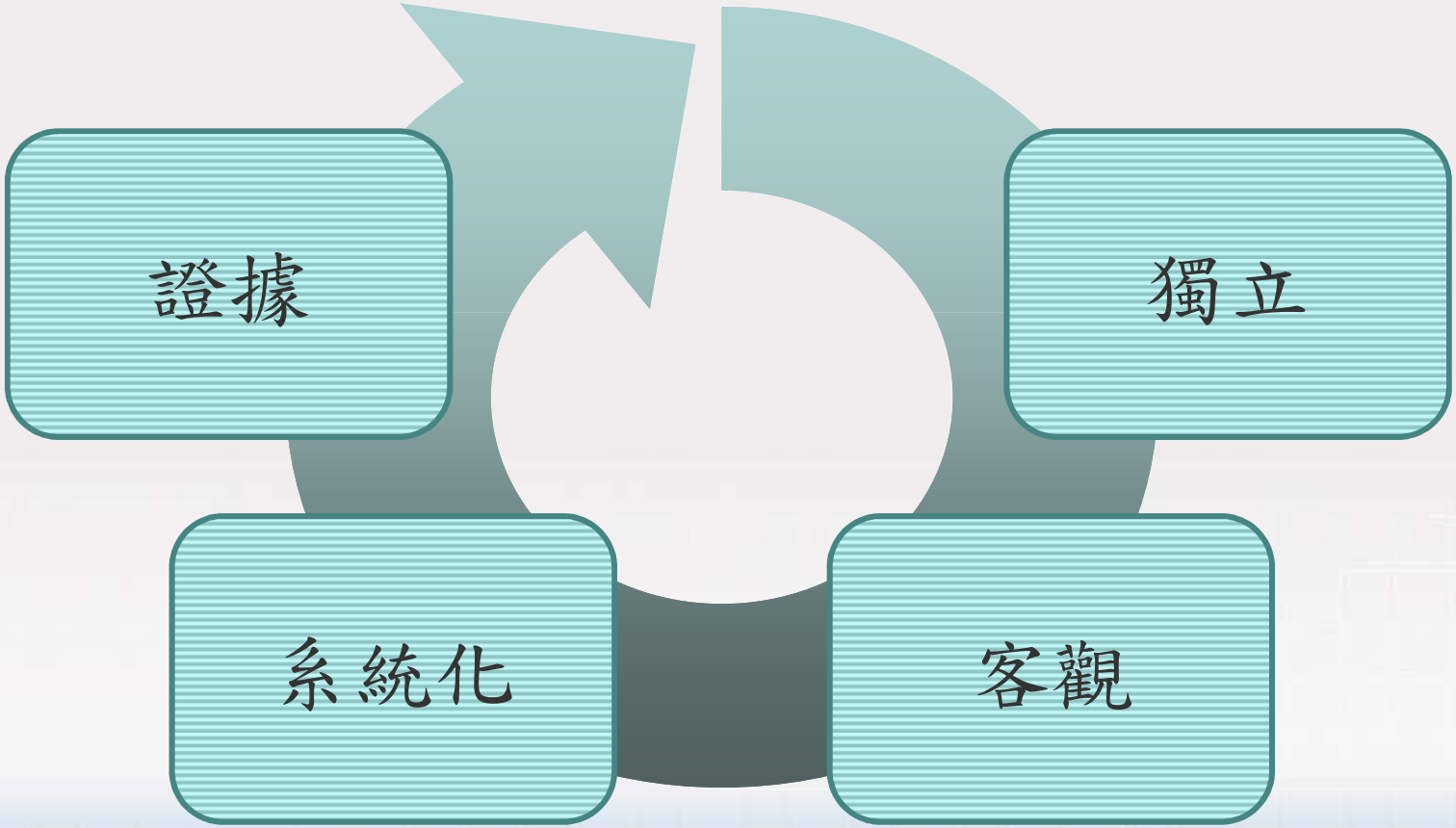
表單範例

- 資訊安全矯正與預防處理表

- 資訊安全事件通報
- 矯正與預防
- 資訊安全內部稽核
- 資訊安全內部稽核注意事項
- 結論

稽核簡介

- 稽核
  - 所有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



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

資訊安全稽核簡介

- 驗證是否符合資安標準與法令的要求
- 可評估資訊安全管理制度的有效性

資訊安全稽核簡介

- 對資訊及其處理設施或系統，在各方面、各部分的查核評估

資訊安全稽核

- 資訊安全稽核的目標
  - 確保單位遵循資訊安全政策及標準程序、衡量資訊安全管理制度之有效性
  - 例如：
    - 控管程序是否落實
    - 檢查與評估資安控制措施之缺失
    - 評估管理成效
    - …

資訊安全稽核 (續)

- 資訊安全稽核的意義
  - 安全稽核機制並不能直接保護系統的安全，它是整體資訊系統的第二線防禦機制，組織籍由稽核檢視資訊安全作業的實際執行情況

資訊安全稽核機制

- 管理遵行性
  - 依據標準，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
  - 弱點掃描、滲透測試
  - 技術稽核
    - 帳戶密碼原則、存取控制、監控與稽核、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

ISO 27001的資訊安全稽核要求

- ISO/CNS 27001 - 本文6. ISMS 內部稽核

  依已規劃的期間施行ISMS 內部稽核，以判定其ISMS 之控制目標、控制措施、過程及程序是否

  - 符合ISO27001標準及相關法律或法規的要求
  - 符合所識別的資訊安全要求
  - 被有效的實作與維持
  - 如預期的履行

資訊安全稽核的目標

- 檢查、評估資安控制措施的缺失
- 衡量資安管理制度的有效性
- 適時提供改進建議

- 資訊安全事件通報
- 矯正與預防
- 資訊安全內部稽核
- **資訊安全內部稽核注意事項**
- 結論

訪談提問技巧

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

受稽人員回答須知

- 聽完問題再回答；
  若不瞭解問題，可請稽核員再說明
- 如果不記得規範內容，
  可翻閱文件再回答
- 不確定的答案，
  可請瞭解的同事幫忙回答

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

文件稽核範例

- 10.5.1資訊備份
  宜依據所議定的備份政策，定期進行資訊與軟體的備份與測試
  - 各項系統設定檔、網頁資料、伺服器檔案及資料庫資料均應由各系統負責人員訂定備份週期，並依據週期執行系統排程或手動備份，備份狀況應記錄於「備份狀況紀錄表」
  - 應定期於測試主機上測試備份復原是否正確

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
  - 環境、電腦之系統設定等
- 紀錄
  - 是否依文件中所訂之規範落實紀錄

現場查核範例

- 禁止使用或下載未經授權或與業務無關之軟體

→檢查使用者電腦是否安裝非授權軟體

- 系統管理者密碼設置，至少7碼

→檢查管理者密碼長度是否為7碼

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
  - 防火牆規則申請單→防火牆管理記錄→防火牆規則設定

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

機房環境準備 (1/2)

- 紀錄
  - 門禁進出登記
  - 監視器紀錄
  - 消防安檢紀錄、電源設備維護紀錄
  - 日常檢查紀錄
  - 設備異動紀錄
- 文件櫃、儲存媒體櫃
- 設備標示
- 溫濕度

機房環境準備 (2/2)

- 其他相關紀錄
  - 資訊資產清單
  - 外部單位連絡清單

辦公室環境準備

- 螢幕保護
- 桌面上的文件與資訊設備
- 軟體版權
- 防毒軟體
- 文件櫃的實體安全控管

- 資訊安全事件通報
- 矯正與預防
- 資訊安全內部稽核
- 資訊安全內部稽核注意事項
- 結論

- 建置資訊安全事件處置程序，資訊安全事件發生時不致手忙腳亂
- 只發現問題不追蹤改善，仍是沒有解決問題
- 稽核可以驗證符合性與有效性，並提供改善機會

簡報完畢，敬請指教