國立中央大學電算中心
100年度教育部提升校園資訊安全服務計畫
區縣網ISMS顧問到點服務-資安內部稽核課程
講師：吳昭儀 資深經理
100/09/07(三) 14:00~16:00

財團法人中華民國國家資訊基本建設產業發展協進會

課程大綱

第一章：資安稽核基本觀念介紹
第二章：資安稽核計畫擬定
第三章：資安稽核計畫執行
第四章：資安稽核報告與改善追蹤
第五章：課程結論

第一章
資安稽核基本觀念介紹

- 資安稽核規定
- 資安稽核定義
- 資安稽核規章
- 資安稽核準則
- 資安管理目標
- 資安控制標準
- 資安稽核種類
- 資安稽核人員應具備的素養
- 資安稽核規劃
- 資安風險組成
- 資安稽核步驟
- 資安稽核測試方式

資安稽核規定

國家/國際標準CNS/ISO 27001
資訊安全管理系統要求事項
第六章

- 組織應規劃稽核計畫，界定稽核範圍、頻率及方法
- 依規劃的期間施行資訊安全管理系統內部稽核
- 稽核人員應遵守稽核準則，不應稽核本身的工作

.....等規範

何謂稽核

- 稽核是由**有能力且獨立**之人員客觀取得與評估證據，以支持其聲明是否符合之報告的系統化過程

資安稽核定義

- 資安稽核之定義爲：對資訊及其處理設施或系統(含相關聯之非自動化處理部分，及其間之介面)各方面或各部分之查核評估。

資安稽核規章

- 稽核角色與職責之建立
- 稽核功能之授權
- 稽核準則
- 高層主管核准

資安稽核資源管理

- 資安稽核資源之安排及使用
- 資安稽核技術之訓練

資安稽核準則

國際電腦稽核協會(ISACA)資訊系統稽核準則，如下：

- 010稽核規章
  - 010010責任、權限及可靠性
- 020獨立性
  - 020010職業上之獨立性
  - 020020組織系統上之關聯性
- 030職業道德及準則
  - 030010職業道德規範
  - 030020盡職業上應有之注意
- 040專業能力
  - 040010專業技術及知識
  - 040020持續性的專業教育訓練
- 050規劃
  - 050010稽核規劃
- 060稽核工作之執行
  - 060010監督
  - 060020證據
- 070報告撰寫
  - 070010報告內容及格式
- 080後續追蹤作業
  - 080010追蹤

資安管理目標

資安管理目標包括：

- 資產之保護
- 確保一般作業系統環境之安全性，包括網路及管理作業
- 確保敏感性資料及重要應用系統之安全性
- 確保作業之執行效率及有效性
- 符合使用者需求及組織政策與程序、法令規範及要求。
- 研擬備援/復原計畫。
- 規劃意外事件回報及處理程序，例如：企業持續性計畫及災復原計畫

資安稽核

- 資安稽核之目標在於檢查、評估資安控制措施之缺失及衡量資訊安全管理制度之有效性，適時提供改進建議，以合理確保該制度得以持續有效的實施
- 資安稽核人員必須將資安管理目標轉化爲資安稽核程序

資安稽核的效益

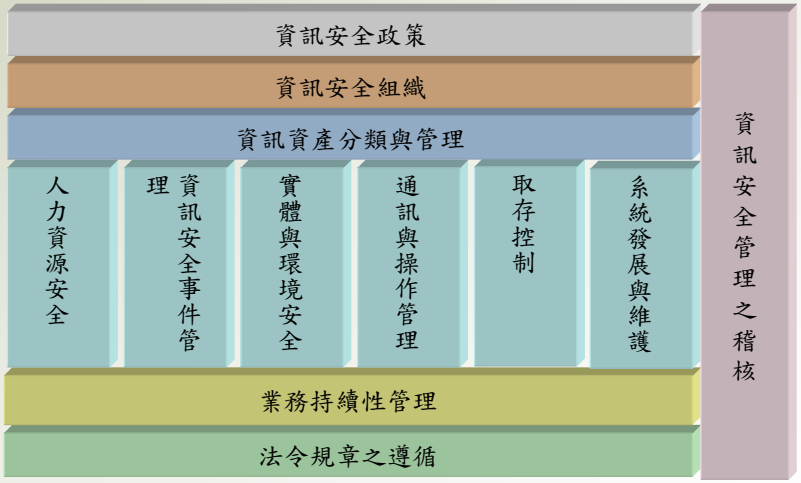
- 可驗證是否符合資安標準與法令要求
- 可評估資訊安全管理制度的有效性
- 減少資訊安全管理系統失效的風險
- 爲管理階層審查提供訊息
- 提升資安意識
- 提供改善的機會
- 落實資訊安全的最後一道防線

資安控制標準介紹

標準	說明
COBIT	共34個高階控制目標，分爲四個階段：規劃與組織、取得與建置、交付與支援，以及監督。其更細分爲300多個細部控制目標
CNS/ISO 27001	CNS/ISO 27001：共11個領域、39個控制目標、133項控管要點
COSO	□ 三大目標：(1)營運之效果及效率(2)財務報導可靠(3)遵循法令 □ 五大要素： (1)監督(2) 資訊及溝通(3)控制作業(4)風險評估(5)控制環境
ITBPM	德國聯邦IT基準安全防護手冊，爲德國國家標準，是組織建置IT安全管理制度的依據
Basel Ⅱ	由國際清算銀行制定之新巴塞爾資本管理協定
NIST	由美國國家標準與技術協會發展之資訊安全參考文件

CNS/ISO 27001

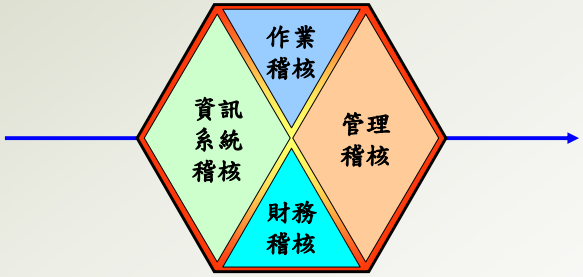
11 個領域、 39 個控制目標、 133 個控制措施



資安控制措施的類別

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、遺漏或惡意破壞行爲之發生	□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

資安稽核的種類



執行稽核的單位

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

CNS 27006-9.1.5稽核方法論

驗證機構應具有程序，要求客戶組織能展示內部 ISMS 稽核已排定，以及計畫與程序係可運作，且能顯示為可運作。

驗證機構之程序不宜預先假設實作 ISMS 之特定方式，或文件與紀錄之特定求，且符合客戶組織之政策與目標。

稽核計畫宜識別，於適當時，稽核期間將利用之網路輔助稽核技術。

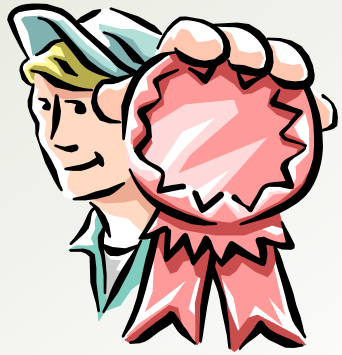
備考：網路輔助稽核技術可包括，例如：遠距會議、網路會議、互動式網頁式通訊，以及遠距電子存取 ISMS 文件及/或 ISMS 過程。該等技術之重點宜在於增進稽核有效性與效率，並宜支援稽核過程之完整性。

Exercise I

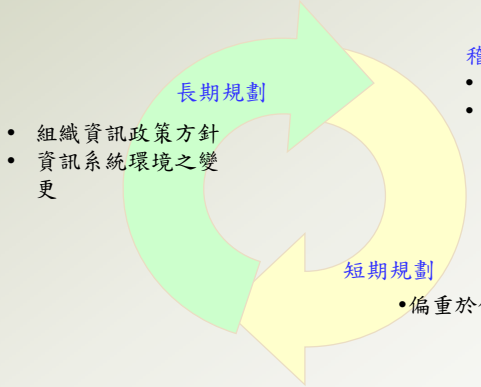
- 請依目前的教育訓練簡單寫一份教育訓練通知。

資安稽核人員應具備的素養

- 熟悉欲驗證之標準或規範
- 具備正確的資安認知
- 瞭解職業道德規範
- 稽核技巧熟練
- 正確的心態
- 開放的心胸



資安稽核規劃



相關法令要求
- 國家機密保護法
- 電腦處理個人資料保護法
- CNS/ISO 27001

資安稽核規劃範例

查核週期	查核次數	查核主題
年	1	□ 風險評鑑及管理 □ 資訊安全政策 □ 資訊安全組織 □ 人力資源安全 □ 遵循性 例如：至少一次員工資訊安全教育訓練
半年	2	□ 資產管理 □ 存取權限審查 □ 實體與環境安全 □ 營運持續管理 例如：災害復原計畫演練測試查核
季	4	□ 資訊系統獲得、開發與維護 □ 資訊安全事故管理
月	12	□ 通訊與作業管理 □ 存取控制

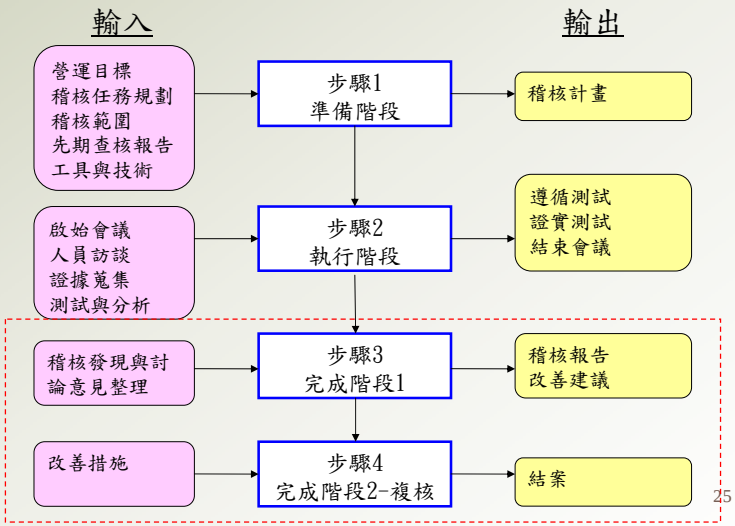
風險分析與資安稽核

- 風險分析是資安稽核規劃之一部份，其協助辨識風險及威脅，讓稽核人員可決定需運用何種控制轉移風險。
- 風險處理對策：
  - **避免風險**(例如：禁止員工使用非法軟體)
  - **轉移風險**(例如：火災保險)
  - **減少威脅**(例如：安裝防火牆抵禦駭客攻擊)
  - **減少弱點**(例如：更新安全修補程式)
  - **減少可能的衝擊**(例如：建置備援機制)

資安風險的組成

- ☐ 資訊基礎架構風險 (Infrastructure Risk)
- ☐ 資訊可取得風險 (Availability Risk)
- ☐ 完整性風險 (Integrity Risk)
- ☐ 存取/機密性風險 (Access / Confidentiality Risk)
- ☐ 攸關風險 (Relevance Risk)

資安稽核步驟



資安稽核測試的方式

- 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

稽核階段	
稽核主題	決定稽核的範圍
稽核目標	決定稽核目的、例如：確認原始程式碼必須在良好且有控管的環境下，才允許變更
稽核範圍	決定組織中要查核之系統或單位、例如：上述程式變更的例子，稽核範圍的說明，必須限制查核某一系統或某一段期間。
查核前規劃	□決定需要的技術能力及資源 □決定查核所需資訊的來源，如政策、標準、程序等 □決定查核地點或設施 □更新現有的查核程式 □取得及評估以前相關稽核發現之適當資訊
查核程序及步驟	□搜集資料、列出需要訪談的名單 □決定查核或測試控制的方式 □發展稽核工具或方法，來測試及查核所有控制
評估測試或檢視查核結果之程序	□依組織之特性
與管理者溝通之程序	□依組織之特性
稽核報告之撰寫	□後續之複核程序 □評估或測試作業效率和效能的程序 □測試控制的程序 □查核及評估文件、政策及程序完備性

第二章
資安稽核計畫之擬定

- 擬定資安稽核計畫考量重點
- 資安稽核計畫內容
- 稽核時間規劃技巧
- 稽核人員安排與工作項目分配

稽核計畫擬定前準備事項

擬定稽核計畫前，稽核人員應

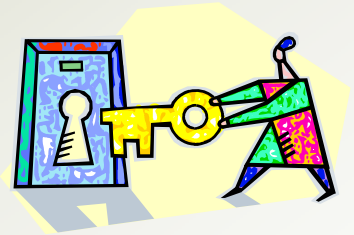
- 取得了解營運目的、目標、作業及技術
- 執行風險分析
- 資安制度覆核
- 設定稽核範圍及目標
- 研擬稽核方法或稽核策略

稽核員了解組織之步驟：

- 參觀組織主要設施
- 閱讀背景文件
- 覆核長期策略計畫
- 訪談主要管理人員以了解組織問題
- 覆核上年度報告

擬定稽核計畫考量的重點

- 可行性
- 周延性
- 風險之掌握
- 保密



資安稽核計畫之內容

◆請幫稽核員陳先生，想想稽核計畫中需要擬定的項目有那些？

資安稽核計畫

- ☑ 稽核主題
- ☐ 稽核目標
- ☐ 稽核範圍
- ☐ 稽核抽樣方式及取樣期間
- ☐ 稽核方式或使用之工具
- ☐ 稽核時程安排
- ☐ 查核表（Check List）

稽安稽核計畫之擬定

資安稽核計畫撰寫範例

資訊安全內部稽核計畫

一、稽核主題：

○○○組織推動相關資訊安全作業，針對是否確實建立、執行並有效維持ISMS ，符合CNS/ISO27001標準並達成組織資訊安全管理目標，須實施資訊及決策參考。

二、稽核目標：（明確的指出稽核的具體目標）

透過實地檢查，瞭解○○○組織營運服務相關之資訊安全管理作業是否確實執行且符合CNS/ISO27001之標準。

三、稽核作業方式：

採書面審查、訪談及實地審查等方式。抽樣方式採相關記錄各抽三筆之方式進行。

四、受稽對象：

以○○○營運服務之相關人員為受稽對象。

五、稽核範圍：

以○○○營運服務相關之資訊安全作業為稽核範圍。

資安稽核計畫之擬定

資安稽核計畫撰寫範例

稽核日期： 98年06月01日。
資訊安全稽核小組成員 ：
報告編撰及處理：
1.資訊安全稽核小組組員應於資訊安全稽核小組內部會議討論、彙整稽核發現，並由資訊安全稽核小組組長提出稽核報告 。
2.資訊安全稽核小組組長應於稽核完成後召開稽核結束會議，由資訊安全稽核小組組長報告稽核發現，並對疑義進行澄清，「RT4-S21-01-資7訊安全內部稽核報告」應請受稽核單位代表簽名
九、啓始會議及結束會議時程

時　程	會議目的	與會人員
98/06/01 09:00~ 09:30	稽核之啓始會議	稽核人員：○○○ 受稽人員：○○○
98/06/01 09:00~ 09:30	稽核之結束會議	稽核人員：○○○ 受稽人員：○○○

資安稽核計畫之擬定

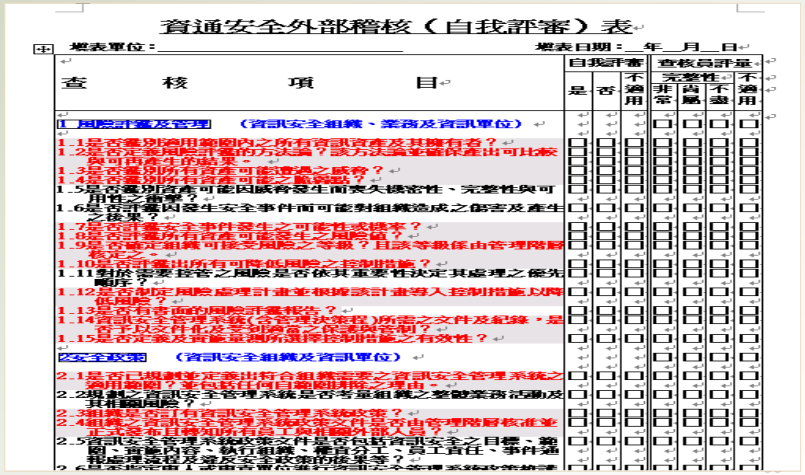
資安稽核計畫撰寫範例

十、稽核之查核時程：

時　程	書審/實審項目	受稽對象	稽核人員
98/06/01 10:00~11:00	1. 風險評鑑及管理 2. 資訊安全政策 3. 資訊安全組織	資訊安全組織、業務、人事及資訊單位	○○○
98/06/01 11:00~12:00	1. 文件審查		○○○
98/06/01 14:00~17:30	1. 資產管理 2. 實體與環境安全 3. 通訊與作業管理	資訊及業務單位 （實地審查，地點機房）	○○○
98/06/01 09:00~10:00	1. 人力資源安全 2. 存取控制	人事、資訊及業務單位	○○○
98/06/01 10:00~12:00 13:30~14:30	1. 資訊系統獲取、開發及維護 2. 資訊安全事故管理 3. 營運持續管理 4. 遵循性	資訊安全組織、資訊及業務單位	○○○

資安稽核計畫之擬定

資安稽核計畫撰寫範例



資通安全外部稽核（自我評審）表

受稽單位：＿＿＿＿＿＿＿＿＿＿　　填表日期：＿年＿月＿日

查核項目	自我評審 是	否	不適用	查核員評量 完整性 非常	尚屬	不盡	不適用
1 風險評鑑及管理 （資訊安全組織、業務及資訊單位）							
1.1是否界定適用範圍內之所有資訊資產及其擁有者？							
1.2是否決定適用於評鑑的方法論？該方法論並確保產出可比較與可再產生的結果。							
1.3是否識別所有資產可能遭遇之威脅？							
1.4是否識別所有資產可能之脆弱點？							
1.5是否識別資產可能因威脅發生而喪失機密性、完整性與可用性之衝擊？							
1.6是否評鑑因發生安全事件而可能對組織造成之傷害及產生之後果？							
1.7是否評鑑安全事件發生之可能性或機率？							
1.8是否計算所有資產可能發生之風險值？							
1.9是否確立組織可接受風險之等級？且該等級係由管理階層核准？							
1.10是否評鑑出所有可降低風險之控制措施？							
1.11對於鑑別出之風險是否依其重要性決定其處理之優先順序？							
1.12是否制定風險處理計畫並根據該計畫導入控制措施以降低風險？							
1.13是否有書面的風險評鑑報告？							
1.14資訊安全管理系統(含管理決策程)所需之文件及紀錄，是否予以文件化之控制與管理？							
1.15是否定義及實施量測所選擇控制措施之有效性？							
2 安全政策 （資訊安全組織及資訊單位）							
2.1是否已規劃並正確出符合組織需求之資訊安全管理系統之適用範圍？並已敘述四周圍邊界之理由？							
2.2規劃之資訊安全管理系統是否考量組織之整體業務活動及其相關風險？							
2.3組織是否訂定資訊安全管理系統政策？							
2.4組織之資訊安全管理系統政策文件是否由管理階層核准並正式發布且對相關外部人員可存取？							
2.5資訊安全管理系統政策文件是否與其資訊安全之目標、範圍、背景內容、執行組織、權責分工、員工責任、事件通報處理過程及對安全政策的支援等？							
2.6是否指定由上述相關單位進行資訊安全管理系統政策檢討							

稽安稽核計畫之擬定

- 擬定稽核計畫
- 經過長官的核准、通知受稽單位主管
- 請相關人員準備與配合

稽核人員
陳先生

稽核時間規劃技巧

- 考量不同稽核地點的交通時間
- 考量啓動會議、稽核發現報告整理時間
- 考量稽核動線的安排
- 考量不同稽核項目間的連貫性
- 避免重複稽核同部門、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時
- 文件審查通常優先於遵循審查
- 使用自動化工具稽核多半需要較長執行時間，應提早啓動工具，利用工具執行期間進行其他稽核工作

稽核人員安排與工作項目分配

- 視需要籌組稽核小組
- 依據稽核員之經驗背景安排適當之工作項目
- 考量稽核員工作負荷，避免閒置或工作量過重
- 稽核範圍內有特殊資訊系統或專門技術時，應考量安排技術專家協助稽核
- 避免選擇與稽核範圍有利害關係之稽核員，或安排稽核員稽核有利害關係之範圍

Exercise II

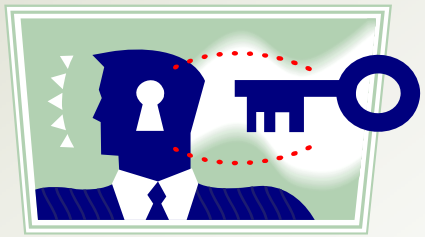
- 請依去年稽核計畫，試擬今年之稽核計畫及相關分工。

第三章
資安稽核計畫之執行

- 執行資安稽核計畫要點
- 資安稽核證據蒐集
- 常見資安稽核手法
- 資產管理稽核
- 風險評鑑及管理稽核
- 安全政策稽核
- 資訊安全組織稽核
- 人力資源安全稽核

執行資安稽核計畫要點

公正/獨立性



時程與人員之掌握

客觀性

一致性

資安稽核證據蒐集

- 可靠性
- 客觀性
  - 質：適切
  - 量：充分
- 可驗證性
- 查核證據應妥善保存
  - 防止未經授權存取或更改
  - 保存期限：法令、規範或政策

常見資安稽核手法

- 訪談
- 檢查表
- 抽樣
- 勾稽
- 自動化工具
- 滲透測試
- 情境模擬與實際操作
- 自評與覆核

訪談

- 對組織內人員以詢答或談論方式取得稽核證據
- 多爲開放式問答，不限制回答方向與內容
- 需要較佳的溝通技術與較豐富的經驗

稽核溝通技巧

- 讓被稽核者放輕鬆
- 詢問簡短的問題
- 表現正面的態度
- 微笑和眼神接觸
- 避免中斷
- 避免即席和高傲的言辭
- 給予適當的讚美
- 詢問和聆聽
- 表示興趣
- 機智有禮貌
- 顯示耐心和理解力
- 除掉個人問題
- 記得說"謝謝"和"請"
- 詢問正確的人
- 當你不理解時不要說你理解

稽核詢問技巧

- 開放式提問
  - 這些問題需要更多資訊，而非僅是"是"或"不是"
- 封閉式提問
  - 這些問題應該誘出"是"或"不是"的答案，用來總結一連串的問題
- 引導式提問
  - 用來迅速的獲得"答案"。"引導"受稽核方以得到答案

檢查表

- 設計好固定的檢查項目來檢驗實施現況
- 常用於例行性、高頻率或項目固定的檢查工作
- 難度低，易執行、亦較容易維持稽核水準

檢查表製作要領

- 確保稽核深度和持續性的重要輔助工具
- 將規範、要求轉換成問題或檢查項目
- 將計畫查看和尋找的證據轉換成檢查項目

資訊安全政策
6.1凡同仁工作職責需使用或處理資訊者，應簽署「保密切結書」課予機密維護責任。

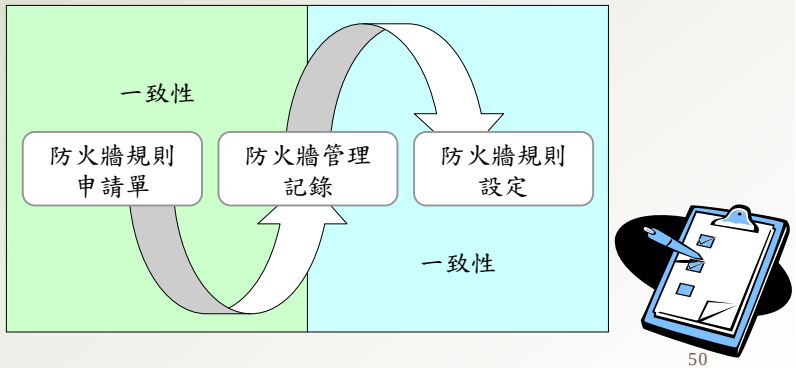
同仁工作職責需使用或處理資訊者，是否簽署「保密切結書」以課予機密維護責任？

抽樣

- 抽樣應用於時間及成本無法於母體作100%的查核
- 抽樣是經由檢查母體中樣本的特性，以推斷母體的特性
- 抽樣方式
  - 統計抽樣：採用客觀的方法來決定樣本大小及選擇之基準
    - 亂數抽樣
    - 有系統的抽樣
  - 非統計抽樣：利用稽核人員的判斷，來決定抽樣的方法及母體中被查核項目的數量
    - 隨意抽樣
    - 判定抽樣

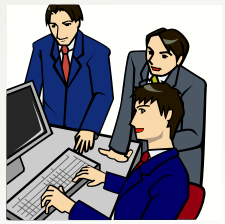
勾稽

- 檢查不同紀錄間的一致性，以確認實施的完整性與有效性



自動化工具

- 在電腦系統上以自動化工具執行重複、固定項目或繁複的稽核工作
- 簡化稽核工作，減輕稽核人員工作負荷
- 避免人為疏失，提高稽核證據準確性
- 多用於電腦系統安全性之稽核



自動化工具輔助稽核技巧

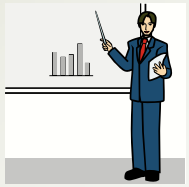
- 利用弱點掃瞄工具或滲透測工具協助發掘資安弱點，或是證實安控之有效性
- 須考量使用工具對正常營運之影響
- 使用前應告知並取得受稽核單位之同意
- 使用工具須遵守受稽單位資安相關規定

滲透測試

- 站在攻擊者的角度，以攻擊行動驗證攻擊目標之安全性
- 滲透測試具有風險，應於良好管制與嚴謹監督的環境下執行

情境模擬

- 稽核員下達模擬情境後，觀察受稽單位實施情況以驗證其有效性
- 常用於稽核特定程序或特定規範



實際操作

- 稽核員從旁觀察受稽單位日常實施情況以驗證其有效性
- 通常需要較長的稽核時程

自評與覆核

- 由受稽人員自行檢核實施狀況，稽核員再以勾稽或抽樣覆核自評作業執行之有效性
- 適用於大範圍全面性的稽核
  - 主計處資通安全外部稽核自我評審表
  - 內控說明書

Exercise III稽核情境模擬演練

99月7月13日 稽核當日
稽核人員○○○
來到受稽單位

第四章
資安稽核報告與改善追蹤

- 資安稽核結果與討論
- 資安稽核報告及內容
- 建議事項之改善追蹤

資安稽核結果與討論

- 稽核結束會議：與受稽單位主管取得對於稽核結果一致的意見，並討論改正行動的方向
- 稽核人員切勿在證據不足的情況下，便妄下稽核結論。

稽核結果與討論

稽核報告架構及內容

完成稽核工作，經過和受稽核單位的詳細討論後，接下來要完成稽核報告的撰寫

稽核報告--
- 資安稽核工作最終的產品
- 稽核人員向主管報告稽核發現及提供建議的工具
- 不同的組織可能會需要不同格式的稽核報告

撰寫稽核報告前宜：
- 確認報告上所陳述的事實之正確性
- 確定所提建議能否實用且符合成本效益
- 對於已同意的建議事項研訂出執行之日期

資安稽核報告架構及內容

請幫稽核員陳先生，想想稽核報告中需要擬定的項目有那些？

資安稽核報告
- ✓ ☑稽核報告簡介
- ✓ ☐稽核結論
- ✓ ☐稽核證據
- ✓ ☐稽核發現
- ✓ ☐稽核結論

建議事項之改善追蹤

- 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
  - 查詢現況或列爲下次稽核觀察事項

建議事項之改善追蹤

上次稽核列的追蹤事項，已經過了執行的日期。打個電話給受稽單位的林小姐，確認一下是不是有如期執行？

陳先生，您好：有的，我們在隔天就補公告了安全政策；另外也在上週規劃好今年度不同層級的資安教育訓練...

建議事項之改善追蹤

矯正與預防處理單

紀錄編號：

提出單位		提出人員		提出日期	
處理單位		處理人員		填寫日期	
缺失分類： □主要缺失□次要缺失□觀察□建議			事件來源： □內部稽核 □外部稽核 □資訊安全事件 □自行提出 □其他		
問題或缺失說明					
原因分析					
矯正與預防措施評估	暫時性對策：（控制缺失的擴大或消除單一事件的影響） 預訂完成日期： 年 月 日				
	追蹤紀錄：		確認結果：		
	永久性對策：（消除缺失或潛在風險的根本原因，防止類似事件發生）				

追蹤是否如期完成

CNS 27006-9.1.6驗證稽核報告

9.1.6.1 驗證機構可採用適合其需要之報告程序，但此等程序至少應確保

(a) 離開客戶組織場域之前，稽核小組與客戶組織管理階層召開會議，會中稽核小組提供：

(1) 關於客戶組織 ISMS 與特定驗證要求相比較之符合性的書面或口頭指示。

(2) 客戶組織對各項發現與其依據，有詢問問題之機會。

(b) 稽核小組提供一份其對客戶組織 ISMS 與所有驗證要求相比較之符合性的發現之稽核報告給驗證機構。

9.1.6.2 稽核報告宜提供下列資訊

(a) 包括文件審查之彙總的稽核紀錄。

(b) 客戶組織資訊安全風險分析之驗證稽核紀錄。

(c) 所使用之稽核總時間，以及用於文件審查、風險分析評鑑、現場稽核及稽核報告之詳細時間。

(d) 已跟催之稽核項目查詢、其被選擇之理由闡述及所採用之方法論。

CNS 27006-9.1.6驗證稽核報告(續)

9.1.6.3 提供給驗證機構之稽核發現報告應足夠詳盡，以協助及支持驗證決定，且其應包含：

(a) 稽核所涵蓋之區域（例如：驗證要求及受稽核之場域），包括跟催之重要稽核存底(audit trail)，以及所利用之稽核方法論（參照 IS 9.1.5）。

(b) 正面（例如：值得注意之特點）與負面（例如：可能之不符合事項）之觀察事項。

(c) 所識別之所有不符合事項之細節，並以客觀證據支持之，且記錄判定此等不符合事項所引用之 ISMS 標準 CNS 27001 要求或驗證所需其他文件之要求。

(d) 對客戶組織 ISMS 與驗證要求相比較之符合性的說明，具不符合事項之清楚陳述與所引用之適用性聲明版本。若適用，亦含客戶組織先前的驗證稽核結果之所有有用對照。

填妥之問卷表、查檢表(checklist)、觀察事項、日誌、或稽核員筆記可構成稽核報告之一部分。若使用此等方法，此等文件應提交給驗證機構，作為支持驗證決定之證據。關於稽核期間所評估樣本之資訊宜納

CNS 27006-9.1.6驗證稽核報告(續)

填妥之問卷表、查檢表(checklist)、觀察事項、日誌、或稽核員筆記可構成稽核報告之一部分。若使用此等方法，此等文件應提交給驗證機構，作為支持驗證決定之證據。關於稽核期間所評估樣本之資訊宜納入稽核報告或其他驗證文件中。

報告應考量由客戶組織提供對 ISMS 之信賴度所採用之內部組織與程序之適當性。

除 CNS 17021 第 9.1.10 節之報告要求外，報告宜涵蓋：

(1) 對內部 ISMS 稽核與管理階層審查之可靠程度。

(2) 關於 ISMS 實作與有效性之最重要的正面與負面觀察事項之彙總。

(3) 稽核小組對客戶組織之 ISMS 是否可授與驗證之建議，以及支持此建議之資訊。

Exercise IV稽核結束之口頭報告

99月7月13日 稽核結束
稽核人員○○○
口頭報告相關發現

第五章
課程結論

結論

☐稽核準備階段

- 組織內資安稽核員的角色及責任必需被建立
- 資安稽核依組織制度進行長、短期規劃
- 資安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、流程、證據蒐集、稽核發現、結論與建議等
- 稽核計畫應經過正式授權與核准程序

結論

☐稽核執行階段

- 稽核人員必需以公正的立場，態度需堅定有禮貌，敏銳的觀察力，查明：
  - 隱藏在事情表面的事實
  - 隱藏在事實背後的真相

☐稽核完成階段

- 撰寫稽核報告前宜與受稽單位溝通以取得一致的稽核結果意見，並討論改正行動的方向
- 切勿在證據不足的情況下，便妄下稽核結論
- 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

參考資料

- 電腦稽核實務導覽
- 資訊安全稽核介紹與實務 陶靖霖
- 行政院資通安全外部稽核(自我評審)表
- IS Standards ,Guidelines and Procedures for Auditing and Control Professionals
- CNS27006:2010

Q & A