TSC CAPITAL GROUP
The Bridge to the Asia Pacific Region

國立臺南大學

111年資訊安全暨個人資料管理規範導入顧問輔導服務案

課程名稱：資通安全與個資保護稽核實務

授課日期：111年 7月 20日
授課講師：德欣寰宇 資安/個資顧問 邱立德

課程活動

時間	課程大綱
14:00~17:00	➢ ISMS及PIMS內部稽核 ➢ 稽核計畫安排與準備 ➢ 稽核實務與說明 ➢ 稽核技巧與爭議處理

ISMS及PIMS內部稽核

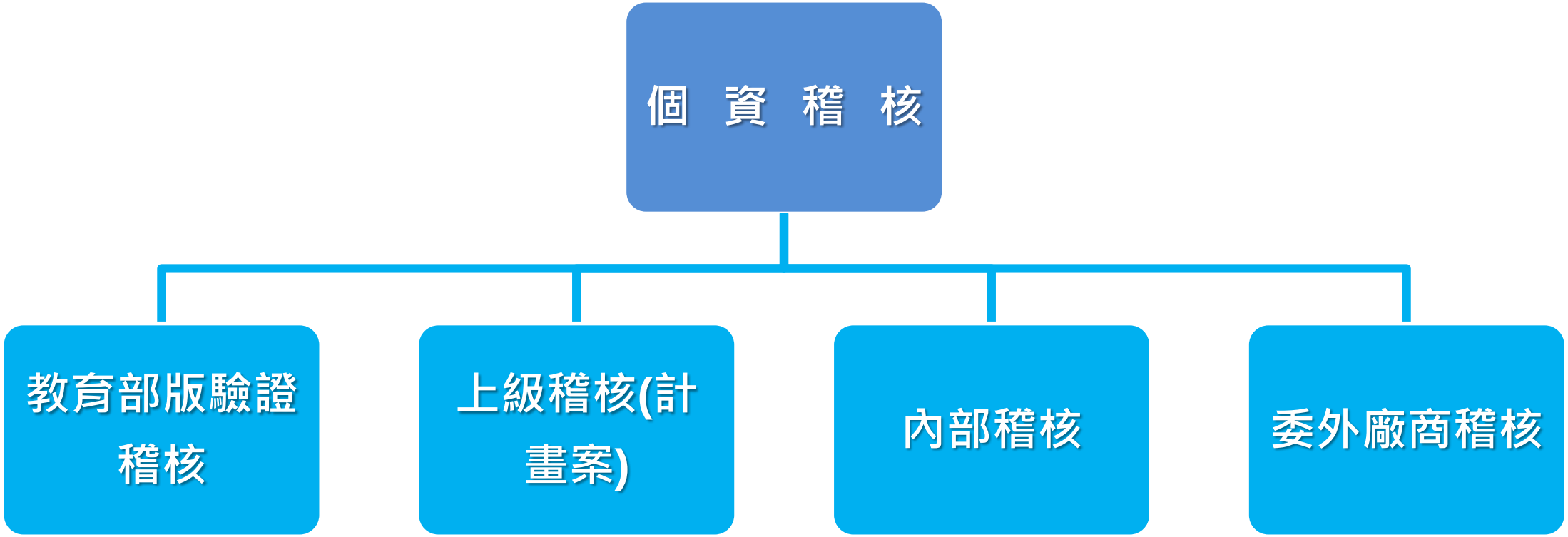
推動資訊安全及個資稽核的意義

- 可展現管理階層對資訊安全及個資保護的支持
- 是檢視資訊安全及個資保護控制措施是否有效及落實的方法
  - 可提昇同仁的**安全意識**、**參與感**及**行動的動機**
- 提供合理、客觀的持續改善方向及目標
  - 引導組織思考可能面對的威脅/風險/事件
  - **採取適當的方法來預防/應變/回復**
  - 提供管理階層**確認**ISMS&PIMS推動的**有效性**之參考，以進行後續政策調整或更正
- 應至少包含涉及核心業務之個人資料蒐集、處理與利用流程之行政單位，以及資訊管理單位。

資安管理制度稽核種類

- 資安稽核
  - 非技術性
    - 外部驗證稽核
    - 主管或上級機關稽核
    - 內部稽核(含所屬單位)
    - 資通服務委外廠商稽核
  - 技術性
    - 資安健診
    - 弱點掃描
    - 滲透測試
    - 主管或上級機關網路攻防

個資管理制度稽核種類



資安及個資管理標準結構

- 標準本文ISO Directive, Annex SL 結構：
  - PD**C**A循環

規劃 → 執行 → **確認** → 改善行動

- 4.組織全景
- 5.領導作為
- 6.規劃
- 7.支援
- 8.運作
- **9.績效評估**
- 10.改善

ISO 27001:2013 本文：9.2內部稽核

組織應依規畫之期間施行內部稽核，以提供資訊安全管理系統之下列資訊

- 是否遵循下列事項
  - 組織本身對其資訊安全管理系統之要求事項
  - 本標準之要求事項(包含資通安全管理法、上級機關要求及規範)
- 是否有效實作及維持

教育體系資通安全暨個人資料管理規範
六、績效評估 (2 內部稽核)

組織應於計畫期間對 PIMS 執行內部稽核，以提供以下資訊

1. 應定期（**至少每年一次**）或於**重大變更後**執行一次內部稽核

2. 稽核程序應包括頻率、方法、職責、規劃要求事項及報告。稽核計畫應包含**適用範圍內核心業務**與**高風險個人資料流程或系統**，並將前次稽核之結果納入考量

3. 稽核員應受適當培訓並具備稽核能力，且**不得稽核自身經辦業務**，以確保稽核過程之客觀性及公平性

4. 稽核結果應對相關管理階層報告，**留存相關紀錄以作為稽核計畫及稽核結果之證據**

ISO 27001:2013 &教育體系資通安全暨個人資料管理規範內部稽核

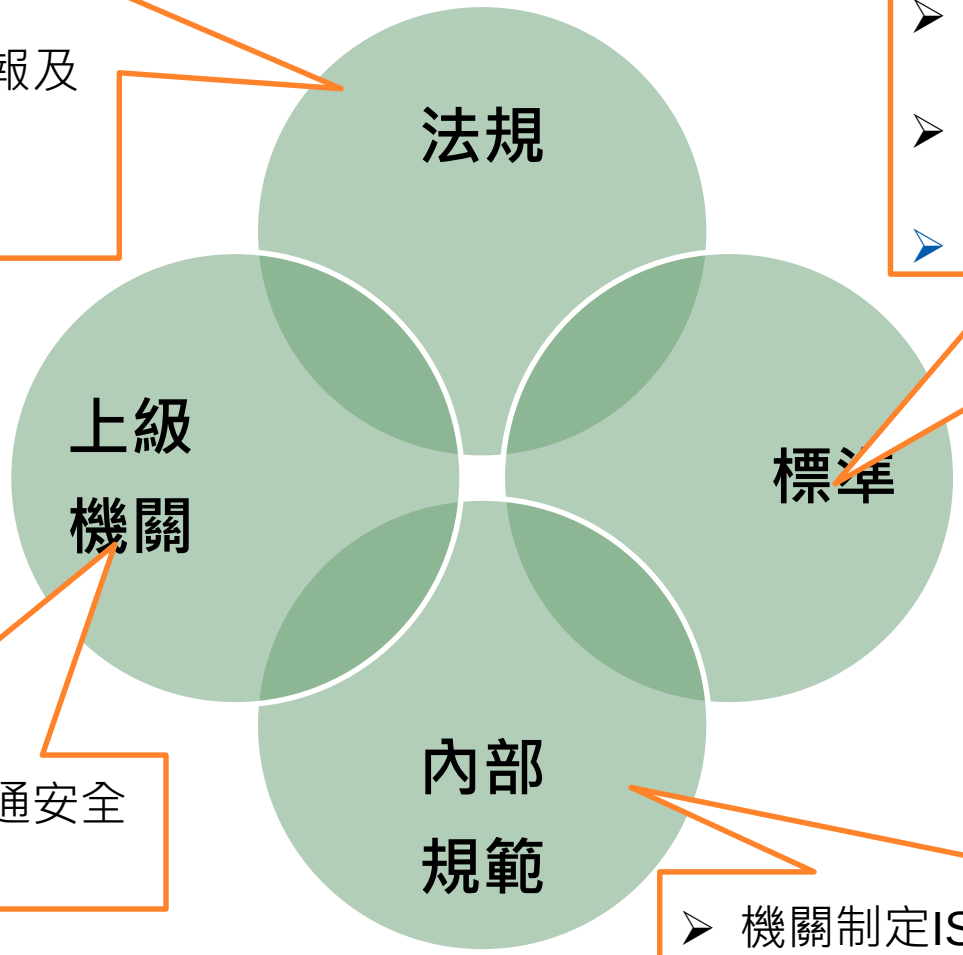
組織實施內部稽核時應

- 規劃、建立、實作及維持稽核計畫，包括頻率、方法、責任、規劃要求事項及報告。該稽核計畫應將所關注之重要過程及前次稽核之結果納入考量。
- 定義各稽核之準則及稽核之範圍。
- 選擇稽核員施行稽核，以確保稽核過程之客觀性及公平性。
- 確保稽核之結果對相關管理階層報告。
- 保存文件化資訊作為稽核計畫及稽核結果之證據。

稽核準則來源

- 資通安全管理法及子法
- 各機關資通安全事件通報及應變處理作業程序
- 個人資料保護法……

- ISO 27001:2013本文+附錄A資通安全管理規範
- 教育體系資通安全暨個人資料管理規範文+
- 附錄B個人資料管理規範



- 教育部對所屬機關之資通安全維護計畫實施情形

- 機關制定ISMS、PIMS文件、章程……

稽核範圍

- 行政院資安法FAQ：

4.9. 機關內部資安稽核的範圍，是否僅限資訊單位？或需涵蓋全機關各單位？針對無資通系統之單位，應如何稽核？	機關內部資安稽核應涵蓋全機關，非僅限資訊單位，另建議先擬定整體稽核計畫，確認各單位之稽核頻率、稽核委員組成及稽核發現之後續追蹤管考機制等。 針對無建置資通系統之單位，稽核重點可針對同仁對資通系統之使用行為、社交工程演練落實情形及資安意識訓練等。

稽核計畫安排與準備

各類稽核活動之流程

ISO 19011 6.

本校稽核小組權責說明

一.ISMS-資通安全稽核小組(NUTN-ISMS-B002資通安全組織程序書)

二.PIMS-個人資料管理規範導入工作小組(NUTN-PIMS-B001個人資料保護組織程序書)

三. 內稽活動包括：

1.擬定稽核計劃。
2.執行稽核項目。
3.撰寫內部稽核報告。
4.針對稽核結果提出建議。
5.追蹤改善方案之執行成果。

內部稽核規劃

1. 定期稽核：
   - 定期實施內部資訊安全及個資保護管理制度稽核作業。
   - 主辦稽核於計畫執行前規劃當年度「稽核計畫」。
   - 「稽核計畫」之執行，須於稽核前以電子郵件通知受稽核單位，以利稽核作業執行。

2. 有下列之情形**可考量**不定期執行稽核：
   - 內部有**三、四級資安及個資事故發生**，致使**營運中斷**或**當事人受損害**時。
   - 組織變革、業務調整及管理環境改變。
   - 高階主管對現行作業有所疑慮時。

不定期稽核應於稽核前，應召開臨時稽核會議，說明稽核目的與步驟，並於會議結束後通知受稽核單位，以利稽核作業執行。

規劃內部稽核計畫

- 何謂稽核計畫
  - ✓稽核計畫用以規劃稽核之時程頻率、範圍、項目、人力、資源等，使受稽核單位可據以安排與準備。
  - ✓稽核計畫常分為**整體稽核計畫**與**細部稽核計畫**。

- 整體稽核計畫
  - ✓規劃**一段時間內之稽核頻率**、**時程**、**範圍**、**項目**、與其他資安活動之關係等。
  - ✓常以年度、半年或季為一階段規劃稽核活動。

- 細部稽核計畫
  - ✓規劃**當次稽核之詳細時程**、**範圍**、**項目**與**工作分派**、**人力與資源使用(人天)**等稽核活動細節。
  - ✓需於每次稽核前先行提供給受稽核單位。

製作稽核查檢表

「ISO27001：2013」、「教育體系資通安全暨個人資料管理規範」、「資通安全維護計畫」製作「稽核查檢表」，以稽核相關**管理目標、控制措施**是否有達到已下項目：

- 符合「資通安全管理法」、「個人資料保護法」或其他相關法令、法規之各項要求。
- 符合資訊安全管理制度及個人資料安全相關程序之規定，並如預期執行。
- 與日常操作之作業規範相符合，且有效實施與維持。
- 前一次的稽核不符合事項之矯正、持續改善。

製作稽核查檢表

ISMS

D038_資通安全管理制度內部稽核表
「ISO27001：2013」+附錄A資通安全管理規範
資通安全管理法及相關子法
資通安全責任等級分級辦法C級公務機關應辦事項
資通安全維護計畫

PIMS

D023_個人資料管理制度內部稽核表
教育體系資通安全暨個人資料管理規範+附錄B個人資料管理規範
個人資料保護法及施行細則

受稽核方的準備

- 程序文件與紀錄(含前次內外稽缺失之改善完畢證明)的準備是否完整
- 提供稽核場址資訊及安排受稽核人員
- 安排週邊設施 ： 會議室、投影設備、影印機、茶水 ……
- 預約主管啟始會議、結束會議及管理階層訪談的時間

稽核執行

- 稽核人員於稽核時，受稽核之單位主管、同仁或其代理人須在場配合稽核作業。
- 稽核人員應依據「稽核查檢表」之內容，以調閱紀錄或詢問之方式，進行作業狀況之查證。
- 稽核人員於稽核時，若發現不符合事項時，應確實填寫「稽核查檢表」，描述不符合事項之狀況。

稽核執行後

- 稽核作業完成後，必須邀集受稽核單位主管及同仁，說明稽核結果與所有稽核時發現之不符合事項，並確定受稽核單位同仁，對稽核發現之缺失，是否皆已確切瞭解。
- 稽核小組成員依據已確認之「稽核查檢表」彙整為「稽核報告」。
- 受稽核單位依據「稽核報告」內容開立「矯正措施單」，並交由業務權責單位負責擬定及填寫矯正預防措施，後續改善追蹤及確認由矯正相關權責單位負責。

不符合事項定義

主要缺失 (Major nonconformity)

- 業務上某程序完全沒有執行，或同一程序有多個次要缺失使得該程序無法有效執行
- 違反業務/程序要求事件，且會**引起顯著**資安或個資保護風險
- 重大資訊安全或個資保護風險並未被鑑別及檢討改善
- 不符合法規 (個人資料保護、資訊安全)
- 前一次次要缺失未作改善

次要缺失 (Minor nonconformity)

- 單獨違反業務/程序要求事件，且**不會**引起顯著資訊安全損失的風險

部分符合事項定義

改善機會 (Opportunity For Improvement)

- 組織中其他的流程能因此受益的優良實務
- 改善資訊安全管理系統有效性之建議措施

觀察事項 (Observation)

- 發現系統/程序有潛在不恰當的情形
- 具有潛在資訊安全損失的風險
- 提供客戶及評審員在後續評審中的參考

追蹤及確認

追蹤

- 不符合事項由發生單位主管及稽核小組雙邊確認改善有效性
- 或由管理單位進行追蹤有效性
- 觀察事項應定期追蹤改善之情形
- 將不符合事項改善有效性於管理審查會議中進行討論

確認

- 為保證矯正預防措施均能有效符合當初稽核出具缺失之改善，故應由管理單位人員或是原稽核人員進行確認。

稽核實務與說明

稽核查檢項目解析

- 管理階層支持與政策
- 資安組織與職責
- 人員認知與能力
- 稽核、矯正與管理審查
- 文件與記錄管制
- 人力資源安全管理
- 資產、風險管理及安全目標
- 作業安全管理
- 實體與環境安全
- 備份管理
- 存取控制與網路安全管理
- 系統獲取、開發與維護
- 供應商管理
- 資訊安全事件管理
- 營運持續管理
- 法律法規遵循

- 存取權限檢視
- 人員作業安全檢視
- 委外作業安全檢視
- 法律法規遵循
- 個資流程與資產稽核

管理階層支持與政策 - 本文4 組織全景：檢視項目

了解組織
及其全景

了解關注方
之需要及期望

決定資訊安全
管理系統之範圍

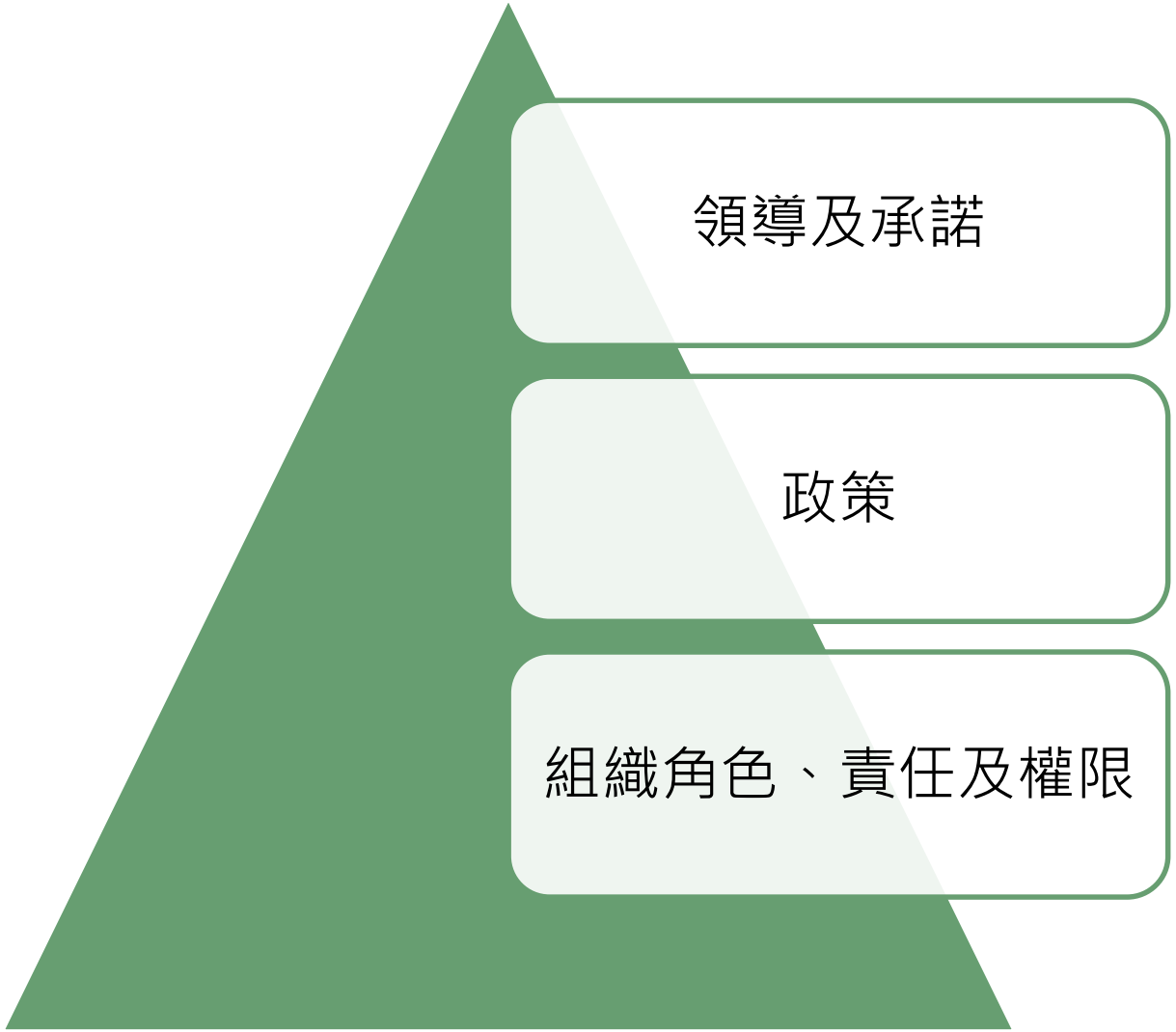
資訊安全
管理系統

1. **檢視項目**：
   資通安全管理政策
   個人資料保護管理政策

2. **檢視重點**：
   資安政策及管理系統範圍可反映內外部關注議題，並有對應量測目標。

3. **相關資料**：
   1) ISMS範圍包含全校
   2) PIMS範圍包含核心流程

管理階層支持與政策 - 本文5 領導作為：檢視項目



1. **檢視項目**：
   1) 資通安全管理政策
   2) 資通安全組織程序書
   3) 個人資料保護管理政策
   4) 個人資料保護組織程序書
   5) 各行政與教學單位業務管理制度

2. **檢視重點**：
   1) 資安長及行政與教學單位支持資訊安全管理制度運作。
   2) 資安長及行政與教學單位指派相關活動權責人員。

政策

- A.5.1 資訊安全政策
- B.1個人資料管理政策

控制措施	稽核重點
資通安全管理政策 個人資料保護管理政策	1. 資通安全與個資保護最高管理單位審核紀錄 2. 對內外部傳達及公布。 3. 定期審查政策。
政策之審查	

組織與職責

- A.6.1內部組織
- B.2個人資料管理組織、B.10.1.2個人資料安全控管措施

控制措施	稽核重點
資訊安全與個資保護之角色及責任	1. 定義及分配資訊安全權責。(資安長、**個資長、個資保護長)** 2. 相衝突之職務及責任（業務單位及稽核單位）予以區隔。 **3. 配合現有資訊安全管理組織，建立個人資料相關人員之角色與責任(個)**
職務區隔	
與權責機關之聯繫	1. 與上級機關(教育部、區網中心、技服中心....)溝通方式。 2. 與專業機關（資安廠商、技術協會、警消單位.....）聯繫方式。
與特殊關注方之聯繫	
專案管理之資訊安全	1. 專案（不論形式）專案管理中因應資通安全 2. 例如：軟體開發商資通安全作為自評情形
日常作業管理責任(B2.1.3)	1. 具有經驗的人，確保符合個資管理政策
個資管理窗口(B2.1.4)	1. 日常作業的執行

資產、風險管理及安全目標 - 本文6 規劃：檢視項目

因應風險及機會之行動

資訊安全目標及其達成之規畫

1. 檢視項目：
1) 風險評鑑與管理程序書
2) 風險評鑑方法論

2. 檢視重點：
1) 資訊資產威脅與弱點項目之審查
2) 可接受風險值。

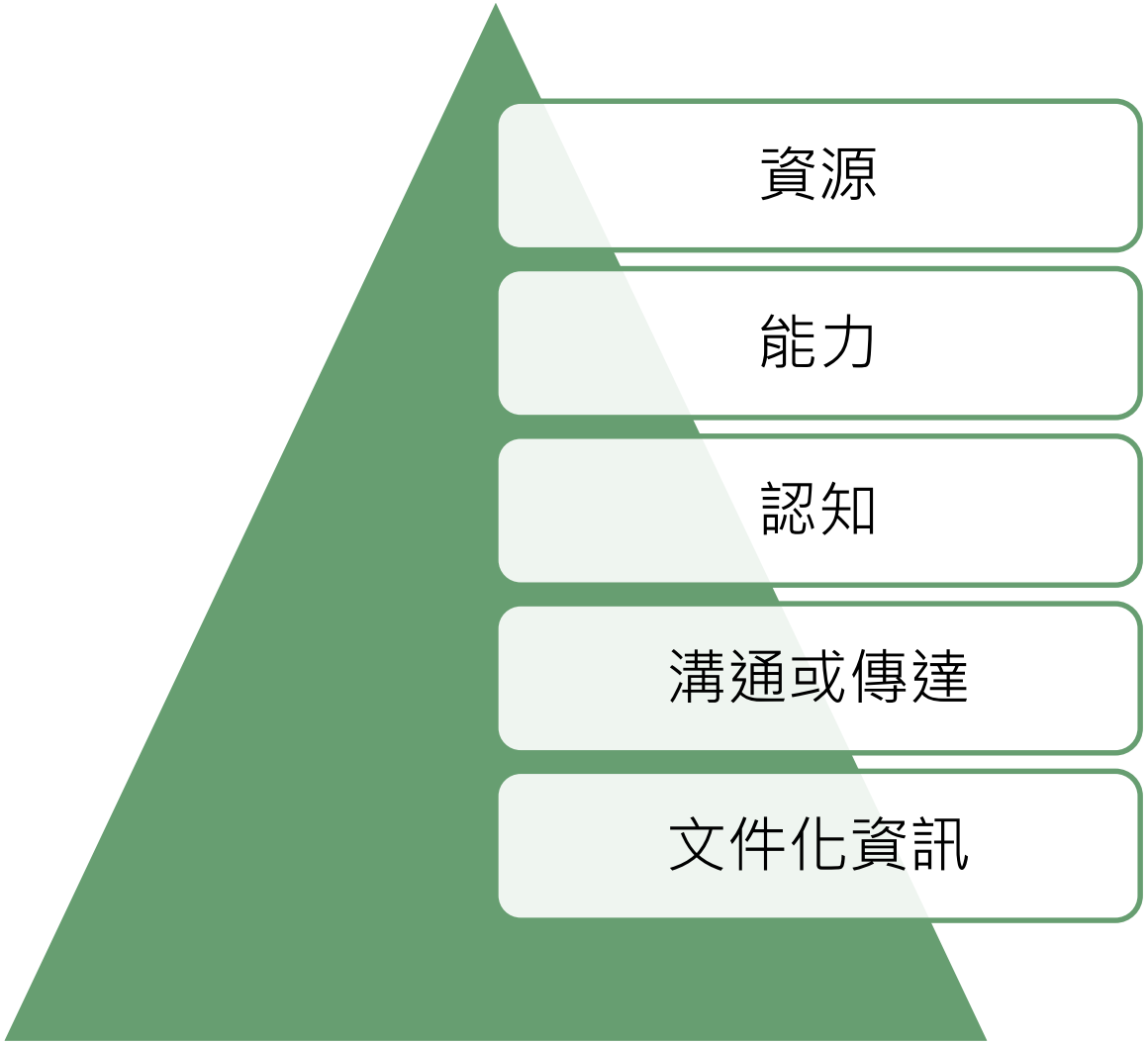
3. 相關資料：
1) 適用性聲明書
2) 風險評鑑彙整表
3) 風險評鑑報告
4) 風險改善計畫表
5) 目標達成計畫與量測表
6) ISMS有效性量測表

個資風險管理

- B.4.2個人資料之風險管理

控制措施	稽核重點
風險管理	**1. 風險接受準則** **2. 履行隱私風險評鑑之準則(含外部要求的資訊)** **3. 應用資料保護原則於資料流中，藉以識別隱私風險**
風險評鑑流程中識別	1. 相關隱私法規、標準與框架。 2. 對自然人權利與自由的衝擊。 3. 任何自然人實體、物質或非物質損害 4. 對組織的衝擊(包含但不限於聲譽、法律監管、財物損失等)

人員認知與能力 - 本文7 支援：檢視項目

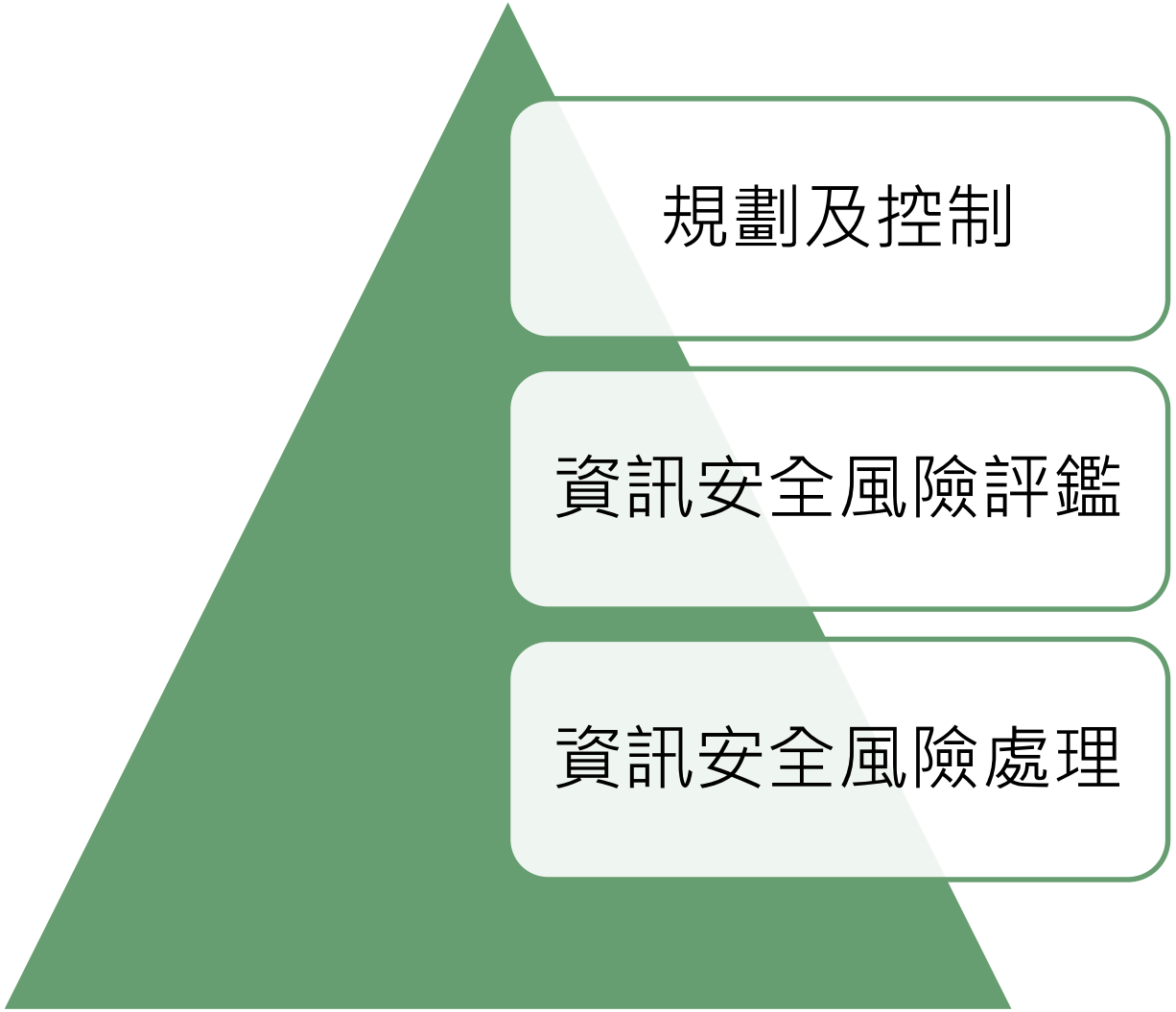


1. **檢視項目**：
   1) 資通安全組織程序書
   2) 文件管理程序書
   3) 人員安全與教育訓練程序書書

2. **檢視重點**：
   資訊安全管理系統所需行政支援是否被滿足，標準要求之文件化項目是否皆符合。

3. **相關資料**：
   1) 資訊安全與個資保護聯絡人員表
   2) 外來文件管制表
   3) 資通安全管理文件列表
   4) 保密切結書(學校人員)
   5) 人員職掌清冊
   6) 教育訓練簽到表
   7) 專業證照
   8) 職能證書

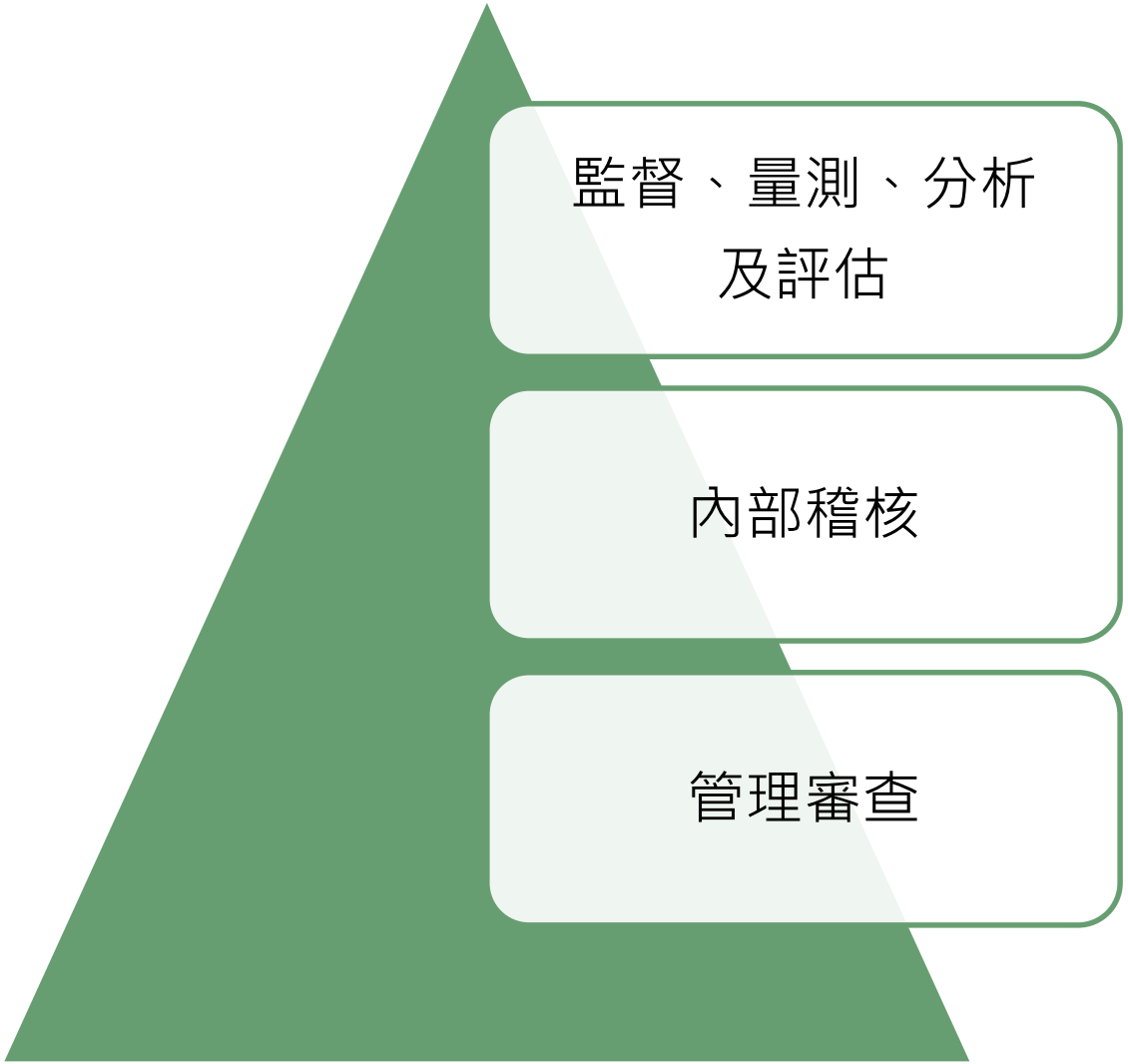
文件與記錄管制 - 本文8 運作：檢視項目



1. **檢視項目**：
   1) 資通安全管理審查會議紀錄
   2) ISMS有效性量測表
   3) 目標達成計畫與量測表
   4) 風險評鑑報告
   5) 風險評鑑彙整表
   6) 風險改善計畫表
   7) 適用性聲明書
   8) B.4.2個人資料風險評鑑及管理

2. **檢視重點**：
   1) 控制規劃之變更，並審查非預期變更之後果
   2) 實作風險評鑑及風險處理

稽核、矯正與管理審查 - 本文9.績效評估：檢視項目



1. **檢視項目**：
   1) 資通安全管理政策
   2) 實體安全管理程序書
   3) 資通安全事件管理程序書
   4) 資通安全稽核作業程序書

2. **檢視重點**：
   1) ISMS有效性量測表
   2) 目標達成計畫與量測表
   3) 日常維運監督量測情形
   4) 內部稽核
   5) 管理審查

3. **相關資料**：
   1) 日常資訊或個資環境監督量測之紀錄(機房、庫房設備、溫溼度記錄表)
   2) 資訊安全管理系統目標與評量機制查核記錄
   3) 內部稽核計畫及報告
   4) 管理審查會議議題及決議

本文10.改善：檢視項目

不符合項目
及矯正措施

持續改善

1. **檢視項目**：
   矯正管理程序書

2. **檢視重點**：
   1) 原因分析
   2) 矯正與預防措施評估
   3) 暫時性對策
   4) 長期性對策
   5) 完成日期

3. **相關資料**：
   1) 矯正處理單
   2) 佐證資料
   3) 審核過程

行動裝置及遠距工作

- A.6.2行動裝置及遠距工作

控制措施	稽核重點
行動裝置政策	1. 訂定行動裝置（筆記型電腦、平板電腦、手機……）管理方式 2. 管理方式：禁用、限制安裝軟體、禁止連接公務網路、使用前掃毒……
遠距工作	1. 訂定遠端連線工作管理方式。

人力資源安全

- A.7.1聘用前

控制措施	稽核重點
篩選	1. 聘用或委外人員之審查（相應法規、其將存取資訊或機關營運持續需求）。 2. 資安法施行細則第四條：選任及監督受託者。
聘用條款及條件	合約書敘明雙方資訊安全責任。

人力資源安全

- A.7.2聘用期間
- B.3人員認知與訓練、B.10.1.2個人資料安全控管措施

控制措施	稽核重點
管理階層責任	1. 主管要求員工及委外廠商配合**資訊安全與個資政策及程序**。 2. 管理表單紀錄簽核至管理階層。
資訊安全認知、教育及訓練	1. 員工教育訓練紀錄（資安責任等級應辦事項：資安專責人員、資訊人員、一般及主管人員）。 2. 委外廠商教育訓練或宣導紀錄。 **3. 使所有員工了解處理個資的責任。(個)** **4. 確保個人資料處理人員的責任、認知訓練。(個)**
懲處過程	1. 人員懲處規定 2. 公務機關所屬人員資通安全事項獎懲辦法

人力資源安全

- A.7.3聘用之終止及變更
- B.10.1.2個人資料安全控管措施

控制措施	稽核重點
聘用責任之終止或變更	1. 對員工及委外廠商傳達：聘用中止或變更後，資安責任及義務仍然有效。 2. 保密切結書。 **3. 個人資料流程相關人員之管理，以及責任終止後的義務(個)**

資產管理

- A.8.1資產責任
- B.4.1個人資料之識別與維護、B.10.1.2個人資料安全控管措施
- B.10.1.3存取權限管理程序

控制措施	稽核重點
資產清冊	1. 資產清冊（包含資訊及資訊處理設施相關資產）。 2. 資產皆有擁有者（管理責任者）。 3. 清查並維護個人資料清冊
個資清冊(個)	
資產之可被接受使用	1. 令員工及委外廠商認知資訊資產使用或存取之安全要求事項。 2. 資訊資產：個人電腦、資料、資通訊系統……。
安全設備或防護措施(個)	**個人資料處理、儲存與傳輸與其載體(如紙本、儲存媒體)之安全管理、存取權限管理(個)**
資產之歸還	1. 離職人員或合約結束廠商資產繳回/移交程序。 2. 對應繳回紀錄。

資產管理

- A.8.2資訊分級
- B.4.1.2高風險個人資料

控制措施	稽核重點
資訊之分級	1. 資訊分級（依法律要求、價值、重要性、機密性、完整性……）。 2. 依分級適當標示資訊。 3. 依分級實作管理程序（處理、儲存及傳遞……） **4. 應鑑別高風險個人資料(身分證字號、銀行帳號、特種個資)(個)**
資訊之標示	
資產之處置	

資產管理

- A.8.3媒體處置
- B.8.1保存與銷毀

控制措施	稽核重點
可移除式媒體	1. 訂定可移除式媒體（外接式硬碟、隨身碟……）管理方式。 2. 管理方式：禁用、限制存取設備、使用前掃毒……
媒體之汰除	1. 媒體汰除之安全處理程序 2. 避免資料外洩方法：資料抹除、消磁、實體破壞……
實體媒體傳送	1. 儲存資料之媒體傳送時保護方式 2. 保護方式：專人遞送及簽收、加密上鎖、防磁……
資料保存與銷毀程序	**1. 業務終止後個人資料處理方法**

存取控制

- A.9.1存取控制之營運要求事項

控制措施	稽核重點
存取控制措施	文件化及審查存取控制措施： 帳號申請、權限異動、特權帳號管理、存取權限與資訊分級一致……
對網路及網路服務之存取	僅提供使用者存取已被授權使用之網路及網路服務

存取控制

- A.9.2使用者存取控制管理

控制措施	稽核重點
使用者註冊及註銷	1. 帳號權限管理程序及程序 2. 新增及移除之帳號 3. 所有帳號之權限設定
使用者存取權限之配置	
具特殊存取權限之管理	1. 是否僅有必要人員配置特權帳號（admin、root……） 2. 共用帳號管理：禁止、經常或使用後立即變更密碼……
使用者之秘密鑑別資訊的管理	管理配置之密碼（預設或暫時密碼）：安全傳送方式、配置前確認使用者身分、強制使用後立即變更……
使用者存取權限之審查	定期清查帳號權限
存取權限之移除或調整	人員離職或異動時權限調整

存取控制

- A.9.3使用者責任

控制措施	稽核重點
秘密鑑別資訊之使用	1. 避免密碼留存（禁止手寫、儲存或需有安全控制） 2. 密碼長度及複雜度 3. 不建議多系統共用同一組密碼(社交工程/撞庫攻擊)

存取控制

- A.9.4系統及應用存取控制
- B.10.1.3存取權限管理程序

控制措施	稽核重點
資訊存取限制	1. 限制特定使用者可存取之資料或系統 2. 控制使用者存取權限（讀取、寫入、刪除、異動） **3. 個人資料處理系統與設備之存取權限管理(個)**
保全登入程序 (同防護基準識別與鑑別)	1. 連續登入失敗5次即鎖定15分鐘 2. 保留登入成功及失敗之紀錄 3. 登入過程不明文顯示輸入密碼 4. 限制連線時間或經過特定時間無動作即終止連線 5. 其他非通行碼驗證方式（生物辨識或實體金鑰）
通行碼管理系統 (同防護基準識別與鑑別)	1. 強制要求使用者使用合格之密碼 2. 強制要求首次登入立即變更暫用密碼 3. 密碼記憶，不與前3代重複

存取控制

- A.9.4系統及應用存取控制(續)

控制措施	稽核重點
具特殊權限公用程式之使用	1. 限制可能影響系統之公用程式（防毒軟體、磁碟清理、剪貼簿、檔案壓縮加密……）的使用。 2. 移除非必要之公用程式。
對程式源碼之存取控制	1. 程式源碼不保存於運作系統上。 2. 控制可存取程式源碼之人員權限。 3. 保留存取程式源碼之稽核軌跡紀錄。

密碼學

- A.10.1密碼式控制措施
- B.10.1.1安全機制/對策、B.10.1.3存取權限管理程序

控制措施	稽核重點
使用密碼式控制措施之政策	1. 依風險評鑑及資訊分級結果使用加密保護。 2. 保護行動裝置、可移除式媒體或網路傳送之資訊。
金鑰管理	1. 金鑰生命週期管理（產生、儲存、更新、汰除及銷毀） 2. 為不同系統產生金鑰 3. 管理活動之存錄及稽核
安全機制/對策(個)	**1. 採去識別化或資料加密等原則的安全控制(個)**
加密控制	**個人資料處理、儲存與傳輸的加密措施(個)**

實體與環境安全

- A.11.1保全區域
- B.10.1.2個人資料安全控管措施

控制措施	稽核重點
實體安全周界	1. 機關定義之保全周界範圍 2. 人員、資產或裝置進出保全周界之管控措施 **3. 個人資料處理、儲存與傳輸設備置放環境與維護管理(個)** 4. 參考：B006_實體安全管理程序書
實體進入控制措施	
保全之辦公室、房間及設施	辦公環境資訊安全： 1. 關鍵設施避免置於公眾進出場地 2. 機密資訊不宜讓未經授權者輕易取得
防範外部及環境威脅	1. 防範天災人禍：地震、火災、淹水、人為攻擊…… 2. 參考：B006_實體安全管理程序書
於保全區域內工作	訂定進入保全區域工作之規範及實作
交付及裝卸區	1. 物品交付或裝卸之工作規範 2. 參考：B006_實體安全管理程序書

實體與環境安全

- A.11.2設備
- B.8.1保存與銷毀

控制措施	稽核重點
設備安置及保護	防範實體設備遭受外部環境損害： 溫溼度管控、漏水偵測、消防（使用氣體式）……
支援之公用服務事業	1. 電力備援設置：UPS、發電機 2. 其他：供水、空調、電信……
佈纜安全	1. 電力及網路線隔離 2. 纜線保護（套管、高架、理線……）
設備維護	設備定期檢測或保養維護紀錄 機櫃設備配置圖
資產之攜出	設備攜出管制，參考：C009_機房進出管理作業說明書

實體與環境安全

- A.11.2設備(續)
- B.8.1保存與銷毀

控制措施	稽核重點
場所外設備及資產之安全	1. 攜出機關或於機關外使用裝置之管制
設備汰除或再使用之保全	1. 設備汰除或再利用前：機敏資訊銷毀、授權軟體移除
資料保存與銷毀程序(個)	**1. 業務終止後個人資料處理方法**
無人看管之使用者設備	螢幕保護裝置設定
桌面淨空及螢幕淨空政策	1. 電腦桌面及辦公桌面淨空(有無機敏資料或未加密) 2. 是否設置螢幕保護程式，並設有密碼鎖定

運作安全

- A.12.1運作程序及責任

控制措施	稽核重點
文件化運作程序	1. 建立資訊處理及設備操作之作業手冊，並提供給必要之使用者 2. 例如：校務行政系統操作手冊、UPS設備操作手冊
變更管理	1. 控制影響資安之變更：組織、營運流程、設施、系統…… 2. 宜有正式審核、測試、 傳達及變更失敗時復原之程序
容量管理	1. 監控資源使用並預做規劃 2. 參考：機房/資訊工作日誌/Log server/CCTV硬碟容量
開發、測試及運作環境之區隔	確認開發、測試及運作環境隔離情形

運作安全

- A.12.2防範惡意軟體

控制措施	稽核重點
防範惡意軟體之控制措施	惡意軟體偵測、預防及復原控制： 1. 禁止未經授權安裝軟體 2. 阻擋惡意網站 3. 安裝並持續更新防毒軟體 4. 定期掃描 5. 遭攻擊後復原方案……

運作安全

- A.12.3備份

控制措施	稽核重點
資訊備份	1. 建立並實作備份政策 2. 定期測試備份回復 3. 異地備份的規劃與實作 4. 一般人員對機敏資料的備份方式(媒體保護) 防護基準普級以上：營運持續計畫 - 系統備份

運作安全

- A.12.4存錄及監視
- B.10.1.2個人資料安全控管措施、B.10.2.1安全事故管理程

控制措施	稽核重點
事件存錄	1. 依防護基準及「各機關資通安全事件通報及應變處理作業程序」產出並留存稽核軌跡紀錄。 2. 保護稽核軌跡紀錄：另行備份（Log Server、NAS、燒錄光碟……）、設定存取權限 **3. 個人資料處理設備日常管理、惡意軟體防治、備份、軌跡紀錄等管理(個)** 4. 各單位系統帳號權限清查紀錄 5. 各單位監視器影像紀錄 6. 參考：存取控制程序書、使用者帳號及權限管理作業說明書 **7. 訂定管理程序，以妥善處理安全事故並留存可供後續追查的紀錄(個)**
日誌資訊之保護	
管理者及操作者日誌	
鐘訊同步	統一校時機制（系統、設備及紀錄）

運作安全

- A.12.5運作中軟體之控制

控制措施	稽核重點
對運作中系統之軟體安裝	系統安裝新軟體或升級新版本前評估測試程序及造成不良影響之對策： 1. 技術性檢測 2. 保留舊版本 3. 還原策略……

運作安全

- A.12.6技術脆弱性管理

控制措施	稽核重點
技術脆弱性管理	**1. 系統、軟體更新狀態(包含公用電腦)** **2. 弱點掃描、滲透測試結果及修補報告**
對軟體安裝之限制	**無未經允許安裝之軟體(包含公用電腦、可攜式電腦)**

運作安全

- A.12.7資訊系統稽核考量

控制措施	稽核重點
資訊系統稽核控制措施	1. 技術檢測之範圍，獲同意並受控制 2. 稽核測試限於讀取軟體及資訊，讀取外之行為宜施行於隔離之副本 3. 於營運時間外執行可能影響系統可用性之測試 4. 監視並存錄所有存取行為

通訊安全

- A.13.1網路安全管理

控制措施	稽核重點
網路控制措施	1. 建立網路設備之管理責任及程序 2. 鑑別連接網路之系統
網路服務之安全	1. 防火牆設置（政策申請、異動及清查） 2. 其他網路安全設備管理維運
網路之區隔	1. 內外網段區隔及DMZ設置 2. 參考：資安健診報告、網路架構圖

通訊安全

- A.13.2資訊傳送
- B.6.2資料分享與揭露、B.10.1.2個人資料安全控管措施
- B.11.1國際傳輸管理

控制措施	稽核重點
資訊傳送政策及程序	通信與作業管理程序書 **個人資料蒐集、處理、利用與安全管理程序書(個)** **個人資料傳送政策與書面協議，以及傳送安全管理(個)** **B.11.1.1境外管理協議與保護(個)** **B.11.1.2傳輸法令遵循(個)**
資訊傳送協議	
電子傳訊	
機密性或保密協議	保密切結書

系統獲取、開發與維護

- A.14.1資訊系統之安全要求事項
- B.10.1.2個人資料安全控管措施

控制措施	稽核重點
資訊安全要求事項分析及規格	依系統防護基準「系統之發展生命週期需求階段」規範 **涉及個人資料處理之資訊系統安全規格建立，測試要求。(個)**
保全公共網路之應用服務	保護外網可存取之應用系統服務： 1. 使用者身分鑑別 2. 傳輸資料加密 3. 簽章金鑰……
保護應用服務交易	保護交易涉及之資訊： 1. 存取權限設定 2. 限定透過第三方支付或銀行支援……

系統獲取、開發與維護

- A.14.2於開發及支援過程中之安全

控制措施	稽核重點
保全開發政策	1. 建立系統開發安全政策 2. 系統變更授權紀錄 3. 系統變更紀錄
系統變更控制程序	
運作平台變更後，應用之技術審查	作業系統、資料庫平台變更申請紀錄
軟體套件變更之限制	參考： B010_系統開發與維護程序書

系統獲取、開發與維護

- A.14.2於開發及支援過程中之安全(續)
- B.10.1.2個人資料安全控管措施

控制措施	稽核重點
保全系統工程原則	B010_系統開發與維護程序書
保全開發環境	1. 區隔不同開發環境 2. 存取控制措施 3. 監控及管理變更
委外開發	1. 委外監督管理 2. 參考：委外合約、委外稽核紀錄、專案會議紀錄……
系統安全測試	開發階段安全性檢測報告 **涉及個人資料處理之資訊系統測試(個)**
系統驗收測試	系統驗收、測試流程

系統獲取、開發與維護

- A.14.3 測試資料
- B.10.1.2個人資料安全控管措施

控制措施	稽核重點
測試資料之保護	測試資料含機敏資訊時保護措施： 1. 去識別化 2. 取得授權 3. 測試完成後刪除 **4. 涉及個人資料處理之資訊系統測試資料處理管理(個)**

公正與合法的處理

- B.5.1蒐集與處理
- B.5.2告知與同意

控制措施	稽核重點
蒐集與處理	1. 定期審查作業流程 2. 公正且合法 3. 蒐集與處理的安全性
告知與同意	1. 告知事項應符合個人資料保護法令要求 2. 確保告知作業之執行及執行證據保存 3. 使用的語言、文字 4. 獲得當事人、**(未成年人)**法定監護人同意

個人資料特定目的處理

- B.6.1蒐集與處理特定目的
- B.6.2資料分享與揭露、 B.6.3資料比對

控制措施	稽核重點
蒐集與處理特定目的	1. 個人資料僅於特定目的下處理與使用 2. 個人資料用於新增特定目的應取得當事人書面同意 3. 當處理未成年人相關個人資料時，應包含取得法定監護人同意的機制
資料分享規劃與協議 資料揭露程序 開放資料	1. 資料分享應符合法令規範， 2. 簽訂資料分享協議取得合法使用承諾 3. 並留存可供稽核紀錄。 4. 確保僅於合法且必要情況下揭露個人資料 5. 「開放資料」的動機公開時，個人資料應去識別化
資料比對	將不同來源或特定目的取得的個人資料，進行比對而產出的個人資料，如透過多筆間接識別個人資料比對以產生的直接識別個人資料，其使用應符合特定目的或遵循相關法律要求

適當相關與正確性

- B.7.1適當性相關且不過度

控制措施	稽核重點
適當性管理	1. 檢視所蒐集的個人資料，對特定目的而言是適當的 2. 個人資料的處理技術與流程，確保其持續適當性。
相關且不過度管理	1. 符合法令要求及特定目的要求下，處理最少量的個人資料 2. 不處理超出告知事項的額外個人資料，除非已取得當事人同意 3. 個人資料處理之新系統、流程或作業表單，應審查處理之個人資料是相關且不過度。 4. 組織重大變更時，針對調整後的個人資料相關作業流程及表單進行審查，以確保其相關且不過度

適當相關與正確性

- B.7.2個人資料正確性

控制措施	稽核重點
正確性管理	1. 所處理之個人資料的完整性與正確性保護方式，並藉以檢視管理個人資料於蒐集、處理或利用過程的正確性 2. 與當事人確認其個人資料正確性，並告知其當事人權利行使方式 3. 發現個人資料不正確時，應適時更正或補充，通知曾提供利用之對 4. 當事人對其個人資料之正確性提出質疑，並在檢驗當事人身分及更正資訊之真實性後加以修正。
錯誤資料的更正	1. 單位主動或被動得知個人資料錯誤或非最新時通知資料分享的第三方，不可使用於影響當事人權益的決策 2. 依個人資料保護法律要求或情況允許時，傳遞正確之個人資料予第三方
新流程的審查	1. 已盡可能避免記錄任何錯誤或過時的個人資料 2. 修正錯誤或過時的個人資料

當事人權利

- B.9.1當事人權利行使

控制措施	稽核重點
當事人權利行使程序	1. 聯絡窗口、聯絡方式，以及處理流程 2. 以個人資料管理小組為管理單位，並由各單位個資管理窗口擔任單位連絡窗口 3. 明定個人資料當事人可行使的權利，及回覆時效(個資法第13條)。
資料處理或利用情形	1. 處理目的、個人資料的類別 2. 個人資料儲存的設定期限；如無法知道，則其用於決定保存期限的準則 3. 依個人資料保護法律要求或情況允許時，傳遞正確之個人資料予第三方 4. 個人資料傳輸至第三國或國際組織時(揭露)，所採用適當的安全措施
更正	1. 確保自然人可及時更正其不正確的個人資料。 2. 該程序應同時確保自然人可以補充不完整資訊

當事人權利

- B.9.1當事人權利行使

控制措施	稽核重點
刪除	1. 依原始蒐集或處理目的，個人資料已無保留必要 2. 處理作業是基於同意書，而自然人已撤銷其同意書 3. 個人資料須予以刪除以符合法律義務
處理限制（停止蒐集處理利用）	1. 組織不再需要處理目的所需個人資料，但為了自然人法律案件成立、執行或辯護所要求保留。 2. 自然人反對處理作業，且該限制要求因驗證組織是否有法律依據可超越自然人權利，而為暫停狀態
資料查詢閱覽複製	1. 針對自然人提出查詢閱覽複製個人資料處理作業請求時，進行考量與回應的程。 2. 確保自然人對其資料可請求製給複製本之權利，或可攜性的權利。

當事人權利

- B.9.1當事人權利行使

控制措施	稽核重點
拒絕	1. 自然人拒絕直接行銷目的相關的個人資料處理作業時，施行單位應確保對該自然人的處理作業已經停止
自動決策與資料剖析	1. 應識別由自動決策，包含可能明顯影響自然人的資料剖析，所產生的個人資料處理作業
抱怨與申訴流程	1. 定義接受當事人抱怨，與對抱怨處理方式提出申訴之窗口與流程。 2. 當事人抱怨與申訴之處理進度與結果，應每年至少清查一次，清查結果宜納入持續改善的考量。

委外作業安全

- A.15.1供應者關係

控制措施	稽核重點
供應者關係之資訊安全政策	1. 委外資安管理程序 2. 參考：資通安全管理法施行細則、委外安全管理作業說明書
於供應者協議中闡明安全性	1. 委外合約訂定資安要求事項 2. 參考：委外安全管理作業說明書
資訊及通訊技術供應鏈	1. 委外廠商複委託管理 2. 限制使用或採購危害國家資通安全產品 **3. 執行受委託機構評選，僅選擇可達成科技面、實體面及組織面安全要求的機構進行合作(個)**

委外作業安全

- A.15.2供應者服務交付管理
- B.12.1.2委託協議要項

控制措施	稽核重點
供應者服務之監視及審查	1. 委外合約、委外稽核紀錄、專案會議紀錄…… **2. 應依個人資料保護法施行細則第八條規定對受託者為適當之監督，並明確約定相關監督事項及方式(個)**
管理供應者服務之變更	1. 系統、服務、人員或管理程序變更之審查

資訊安全事件管理

- A.16.1資訊安全事故及改善之管理
- B.10.2.1安全事故管理程序與紀錄

控制措施	稽核重點
責任及程序	1. 訂定管理程序 2. 內部及外部通報紀錄 3. 情資分享紀錄 4. 設置個資保護聯絡人員及重大個資事件單一通報與聯繫管道，將個資保護聯絡方式（如：電話、email）置於單位網站 **5. 建立個人資料安全事故管理與應變機制(個)** **6. 查明事故發生原因及損害狀況後，以適當方式通知當事人(個)**
通報資訊安全事件	
通報資訊安全弱點	
對資訊安全事件之評鑑及決策	
對資訊安全事故之回應	
由資訊安全事故中學習	事件應變處理後教育訓練或宣導紀錄
證據之收集	**依據「政府機關（構）資安事件數位證據保全標準作業程序」或相關證據保全作業規範，進行數位證據之蒐集與保存。(個)**

營運持續管理

- A.17.1資訊安全持續

控制措施	稽核重點
規劃資訊安全持續	1. 訂定管理程序 2. 營運持續規劃及實作 3. 參考：營運衝擊分析、營運持續計畫、營運持續演練紀錄/報告 4. 資通安全維護計畫、資通系統盤點表(MTPD一致性)
實作資訊安全持續	
查證、審查並評估資訊安全持續	

營運持續管理

- A. 17.2多重備援

控制措施	稽核重點
資訊處理設施之可用性	依可用性要求實作多重備援（備品、HA、備援設備……） 防護基準中級以上：營運持續計畫 - 系統備援

法律法規遵循性

- A.18.1對法律及契約要求事項之遵循

控制措施	稽核重點
適用之法規及契約的要求事項之識別	1. 現行規範及實作符合法規 2. 參考：相關文件控管程序書、外來文件管制表等
智慧財產權	1. 軟體、影像、文件……皆有合法授權 2. 參考：學校智財權宣導(網站、教育訓練…) 3. 參考：學校授權軟體、自由軟體
紀錄之保護	紀錄保護符合法規： 1. 檔案法 2. 個人資料保護法 3. 各機關資通安全事件通報及應變處理作業程序…… 4. 參考：相關文件控管程序書，個資檔案保存期限….

法律法規遵循性

- A.18.1對法律及契約要求事項之遵循(續)

控制措施	稽核重點
個人可識別資訊之隱私及保護	**涉及個人資料之保護措施符合個人資料保護法：** **1. 合法蒐集處理利用** **2. 告知並取得當事人同意** **3. 資料保護……**
密碼式控制措施之監管	資通安全責任等級分級辦法附表十 - 防護基準控制措施： 1. 等級中高之系統，以密碼鑑別時，密碼應加密或經雜湊處理後儲存 2. 等級高之系統應採用加密機制 3. 等級高之系統靜置資訊及相關機密資訊應加密儲存

法律法規遵循性

- A.18.2資訊安全審查
- B.10.1.4安全控制措施審查

控制措施	稽核重點
資訊安全之獨立審查	審查人員獨立於審查範圍(外部稽核或內稽委外或跨部門稽核) **配合資訊安全管理系統稽核機制，每年或於重大變更後檢查個人資料安全控管措施是否落實執行(個)**
安全政策及標準之遵循性	定期審查安全處理及程序遵循政策及標準要求(管審會) **資通系統防護基準各項控制措施之遵循**
技術遵循性審查	資通安全責任等級分級辦法應辦事項(C級機關)： 弱點掃描 滲透測試 資安健診 資通安全弱點通報機制(VANS)（112年） 防毒軟體、防火牆、郵件過濾機制

稽核技巧與爭議處理

稽核原理 - 3E原則

尋找客觀的證據符合

3E

- Exist
  - ISMS、PIMS存在於組織內
- Execute
  - ISMS、PIMS有在組織內運作
- Effectiveness
  - ISMS、PIMS於組織內被有效執行

稽核方式

- 面談 (Interview)
- 觀察 (Observe)
- 抽樣 (Sampling)
- 審查文件 (Review documents)
- 審查記錄 (Review records)
- 總結，分析和評估 (Summarise,analyse and evaluate)

稽核前應該準備...

可以觀看時間的物件

- 手機、手錶、現場的時鐘等，隨時注意稽核時間

記錄稽核各階段用的物件

- 白紙、筆記本、筆、平板電腦等各式可用於記錄的物品

稽核啟動和結束時的文件

- 於稽核啟動會議及結束會議時用的簡報、文件或附件等

稽核技巧 - 面談

對受稽方人員以詢答或談論方式取得稽核證據

- 詢問正確的人，不要害怕問自己不懂的問題

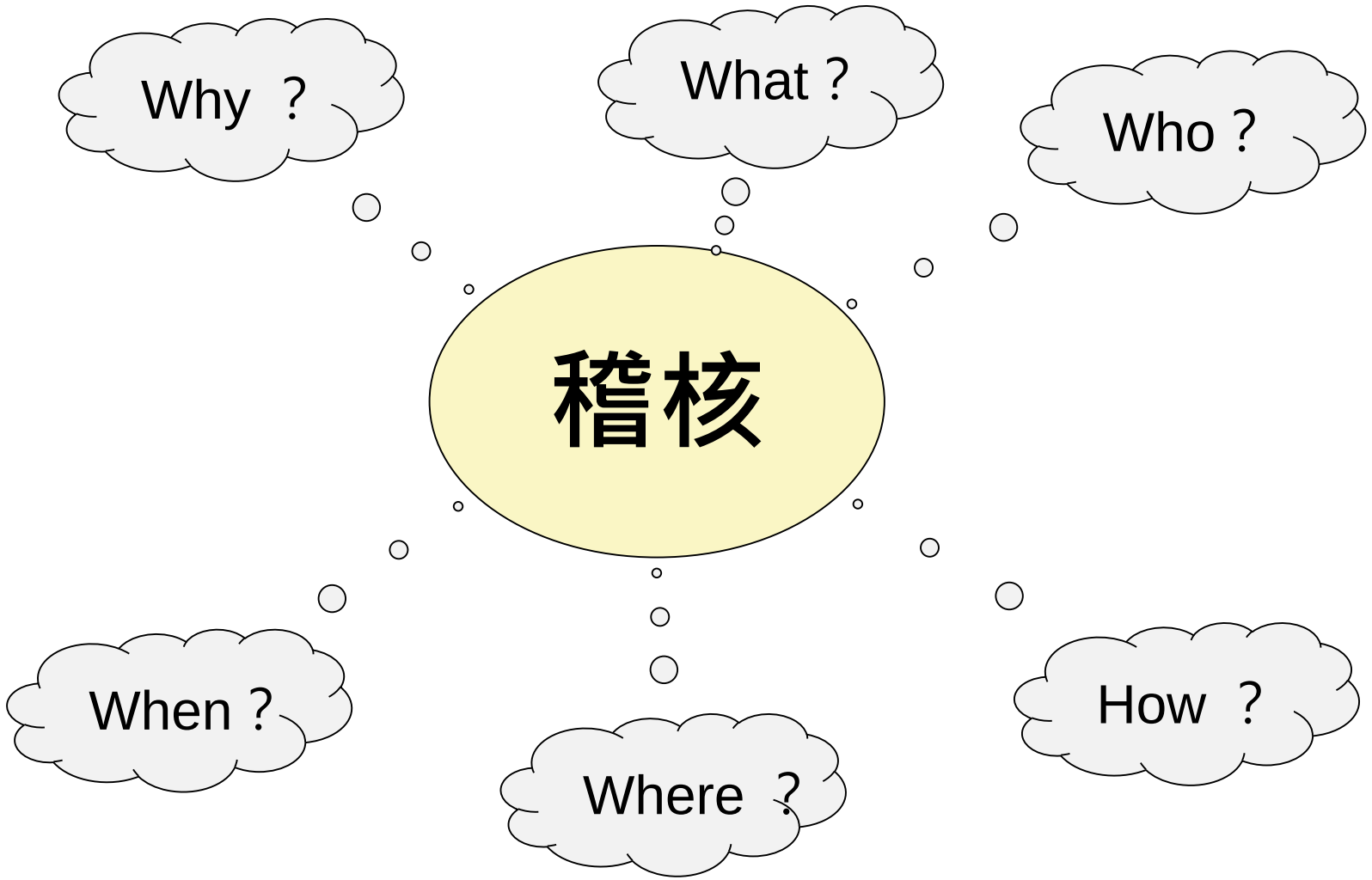
開放式問答，不限制回答方向與內容，讓受稽方多說

- 澄清所聽到的回答，必要時進一步確認

可搭配使用預先設計之問卷或查檢表

- 將規範和準則轉換成問題或檢查項目

開放式面談技巧 - 5W1H



What(執行什麼)

- 知道過期文件銷毀的相關規範是什麼嗎?
- 有多少份類似的文件還沒銷毀?
- 了解受稽人員是否知道並清楚該做什麼

When(什麼時候執行)

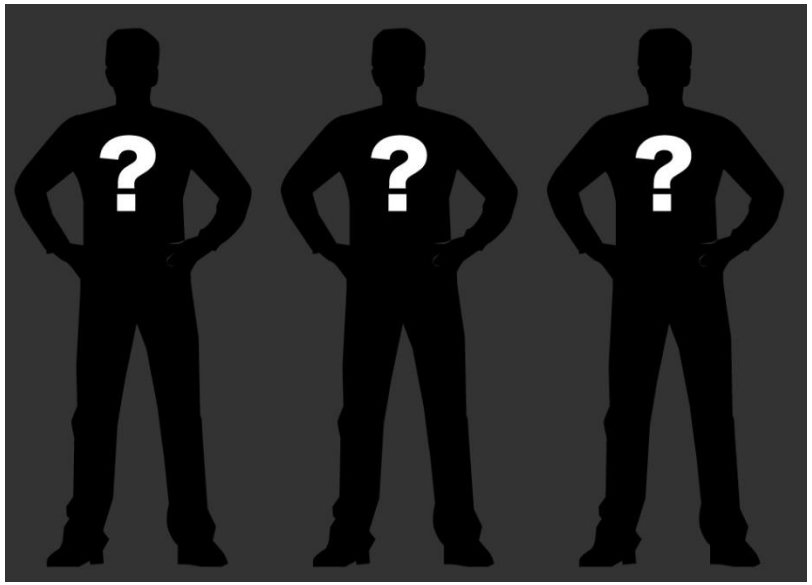
- 文件保存期限是多久?
- 什麼時候該銷毀或歸檔?
- 電腦上的文件又是保存多久?
- 了解受稽人員是否了解業務上的時限規定

Where(什麼地方執行)

- 未過期文件平常該放在哪裡?
- 過期文件又該先暫存於哪裡?
- 了解受稽人員是否熟悉該於何處執行業務

Who(誰來執行)

- 知道這份文件該由誰保管嗎?
- 誰有權限過目這些文件?
- 了解受稽人員是否清楚業務流程各階段的管理人是誰

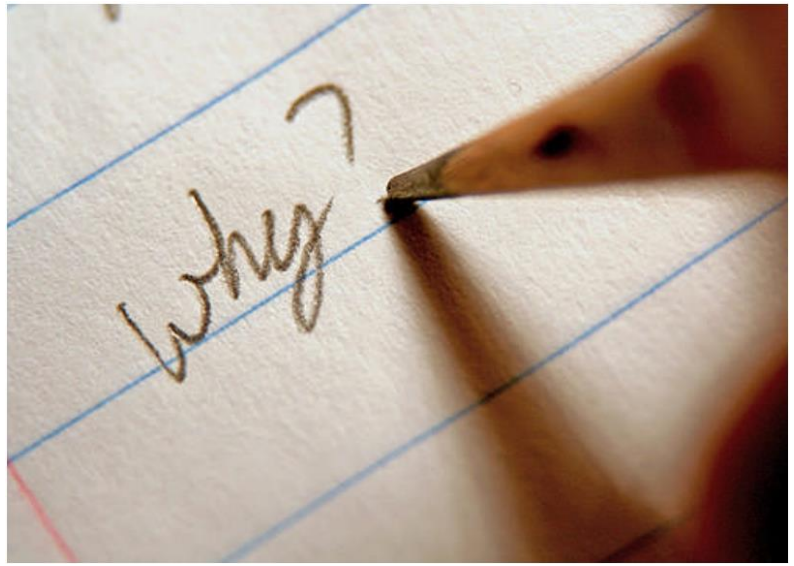


How(如何執行)

- 過期文件該如何銷毀?
- 文件涉及機敏資訊該如何收存?
- 如何確保機敏文件的安全?
- 了解受稽單位於業務流程是否與自身程序相符

Why(為什麼執行)

- 請問為什麼不把過期文件銷毀，而要繼續留存?
- 了解來龍去脈後，讓受稽人員了解是否清楚問題在哪



其他稽核面談技巧

- 一次只問單一的問題，不一連串的問
- 聚焦於受稽核人員的業務
- 試著運用其共同語言或可理解的領域
- 受到質疑時，請受稽核人員或單位提出依循什麼標準
- 盡量避免催促受稽核人員

稽核技巧 - 觀察

觀察受稽方環境及氛圍

- 隨時注意環境氛圍是否有異狀及人員是否感受到壓力，調整稽核方式

保持態度，放低姿態

- 控制情緒，保持微笑，多傾聽，適度的稱讚，降低衝突機率

眼觀整體，注意細節

- 注意受稽方環境是否符合面談所說或文件記錄所載

稽核技巧 - 抽樣

於稽核範圍中，抽取部分樣本以檢驗其有效性

- 採取隨機抽樣，或抽取特定樣本(EX：高風險、高重要性)
- 樣本盡量具有代表性(EX：核心業務相關、高風險高機敏資料或文件)
- 風險越高，抽樣越多；機敏越高，抽樣越少

抽樣結果不一定代表整體實施情況

- 須視實際稽核要求，有時必須對稽核範圍全面稽核

勾稽

- 檢查相關紀錄間的一致性

稽核技巧 - 查文件及紀錄

辦公環境

- 網路架構圖
- 防火牆相關紀錄
- 機房或庫房進出紀錄
- 消防或環控設備保養紀錄
- 監視器影像調閱紀錄
- 事件通報紀錄
- 教育訓練紀錄

資訊系統

- 帳號權限清查紀錄
- 日誌備份、清查紀錄
- 系統維護或變更紀錄
- 系統備份及備份測試紀錄
- 系統營運持續演練紀錄
- 系統委外合約及保密切結
- 防護基準控制措施

業務流程

- 業務流程盤點紀錄
- 資訊資產或個資盤點紀錄
- 風險評鑑及處理計畫
- 資料或文件銷毀紀錄
- 業務營運持續演練紀錄
- 業務委外合約及保密切結(個資銷毀)
- 適用性聲明

稽核技巧 - 作筆記

記錄面談所得到的資訊

- 將面談時受稽人員的敘述的資訊記錄

記錄確實看過的證據

- 於每個抽樣查核點記錄所看到的文件名稱、編號、電腦名稱、IP等資訊

筆記的完整度

- 筆記應能協助自身回憶稽核過程，切勿字跡潦草或不明所以

稽核結果討論及報告撰寫

尋求有效之證據，建立對不符合事項的共識

- 正式文件及記錄
- 雙方同意之觀察跡象

撰寫符合及不符合事項簡潔扼要

- 簡單描述並明確指出符合或不符合哪個控制措施或是程序

建議解決方案

- 給予受稽核單位從稽核中發現還有不足的方面能朝什麼方向改善

報告撰寫技巧

DEF三元素

- D=Document(文件)
  所知道的法令、合約、組織政策、單位及管理系統標準的規定或要求之內容
- E=Evidence(證據)
  所發現的證據
- F=Fact(事實)
  所收集的事實

舉例：
稽核發現OO單位OO業務需學生提供個資，於個人資料檔案清冊中之個資類別與填寫表單(證據)欄位不一致(事實)，不符合 B.4.1.1個人資料清冊(文件)之要求。

稽核爭議處理

稽核的不符合項目一定會有不被受稽核單位認同的情形，例如：

1. 所開缺失沒有經費或人力改善
2. 所開缺失與受稽核單位認知不同(沒那麼嚴重、只是小缺點等)
3. 所開缺失產生受稽核單位內的矛盾

當遇到不被認同或有爭議的情形時，可以：

- ✓ 多傾聽多溝通，勿有太多情緒語言或太大的肢體動作
- ✓ 反問不認同的理由，符合哪個標準或規範
- ✓ 給出**明確的證據**和**事實**，說明缺失不符合的嚴重性
- ✓ 針對不符合事項，若嚴重程度較低或經討論可長期規劃改善，降低其缺失等級(次要缺失->觀察事項)
- ✓ 必要時引用標準或規範解釋，釐清單位內矛盾的癥結點

改善和追蹤

稽核人員收到矯正措施單後，評斷矯正或改善措施有效性應考量：

1. 是否針對缺失進行根因分析
2. 是否規劃後續如何避免再次發生此缺失(EX：短中長期、暫時/永久性)
3. 是否補足所開缺失的事證

再下次稽核時，應針對前次稽核缺失及矯正改善措施進行追蹤稽核，確定是否已依照規劃逐步改善或完全改善。

追蹤改善本身不是結果，是達到結果的方法

稽核應有之內涵

專業素養	資訊安全管理系統或個資管理系統主導稽核員考試通過並**持續保持證書有效性**
	維持獨立、公平、客觀：不稽核自身工作、標準一致、驗證客觀證據
心態正確	驗證有效性與**尋求改善機會**，不是挑毛病
	過程嚴謹，態度輕鬆
	不預設立場，不拘泥於固定實施方法

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

Q/A

課後評量

TSC CAPITAL GROUP

The Bridge to the Asia Pacific Region

感謝您的參與

歡迎於活動後與講師討論您的任何疑問

本機關的臉書粉絲團及部落格可以找到更多資訊

TSC – FB Site

TSC – Blog Site