國立台灣大學計資中心

ISO27001：2013內稽實務及稽核重點

29 七月 2015

目錄

單元 1
稽核程序與框架介紹

PDCA循環

- 執行適當修正
- 實施成果報告
- 確認目標達成
- 持續改善

- 定義ISMS範圍
- 風險評估
- 確認控制目標
- 選擇控制點

- 執行管理程序
- 風險再評估
- 紀錄及追蹤檢討
- 定期稽核
- 績效評估

- 建立管理計劃
- 專案管理
- 建置控制點
- 文件及程序管理

稽核應有之內涵

- 系統化的過程
- 符合管理階層之經營策略
- 查核證據
- 客觀性
- 與公認標準相符合
- 傳達查核結果

稽核目的

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

針對特殊目的之驗證性稽核

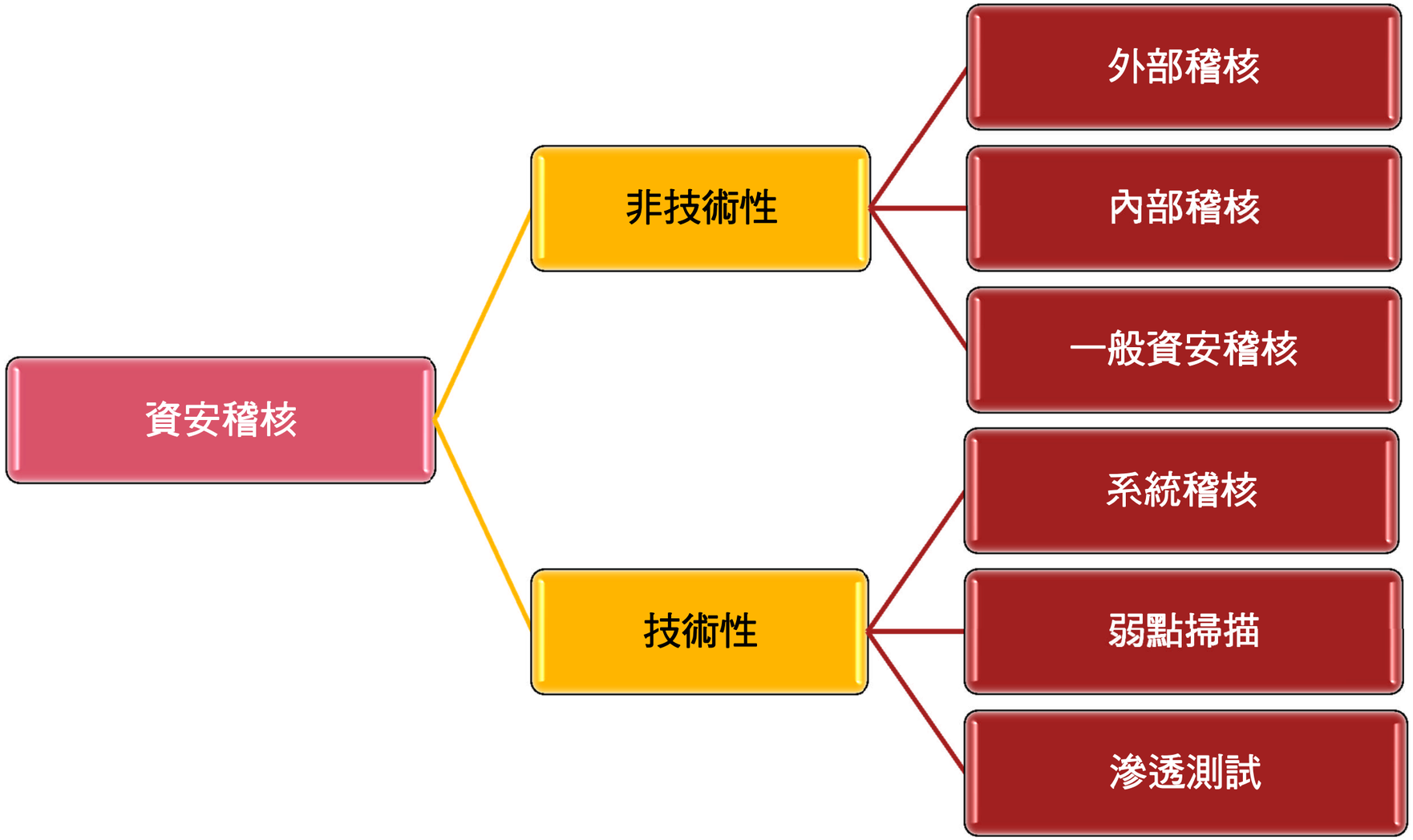
控制風險

達成組織目標

資安稽核目的

- 審查該組織係透過資訊安全管理系統之協助，以落實組織之計劃，並設計適當之制度有效執行之。
- 審查該組織資訊安全管理系統衡量、處理及保存之資訊，係為完整且正確之資訊；提供該等資訊給適當人員使用係依據適當設計之制度執行。
- 審查該組織設立維持資訊安全管理系統保持運作之辦法，係適當設計之制度有效執行之。

資安稽核的種類



稽核工作程序介紹

資安管理制度稽核程序（續）

內部稽核

- 自行執行資訊安全管理制度稽核作業。

外部稽核

- 透過驗證公司、顧問公司或外部專家，協助進行資訊安全管理制度稽核作業。

稽核計畫

- 稽核人員依據稽核目的，並參考前次內部稽核與外部稽核追蹤事項所製作之工作計畫。

稽核底稿

- 稽核人員於執行稽核作業前，先行準備稽核項目，並依循稽核項目執行稽核作業。

稽核報告

- 稽核人員完成各項稽核作業後，先行整理、彙總及歸納相關稽核文件資料，再行編撰稽核報告。

稽核規劃

稽核時機

1. 定期稽核：
   - 每年至少實施一次內部資訊安全管理制度稽核作業。
   - 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. 有下列之情形得執行不定期稽核：
   - 內部有三、四級個資事件發生，致使當事人損害時。
   - 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。

稽核規劃（續）

3. 稽核小組成員：
   - 稽核小組成員由主辦稽核指派適當人員擔任。
   - 為求公正與客觀，稽核人員禁止對自己本身職務進行稽核，以保持內部稽核之獨立性。
   - 稽核小組經驗不足時，可將稽核事務委交外部顧問公司輔導稽核，或由公正之稽核公司進行稽核，從中學習稽核方式，提昇稽核品質。
4. 稽核小組成員資格：

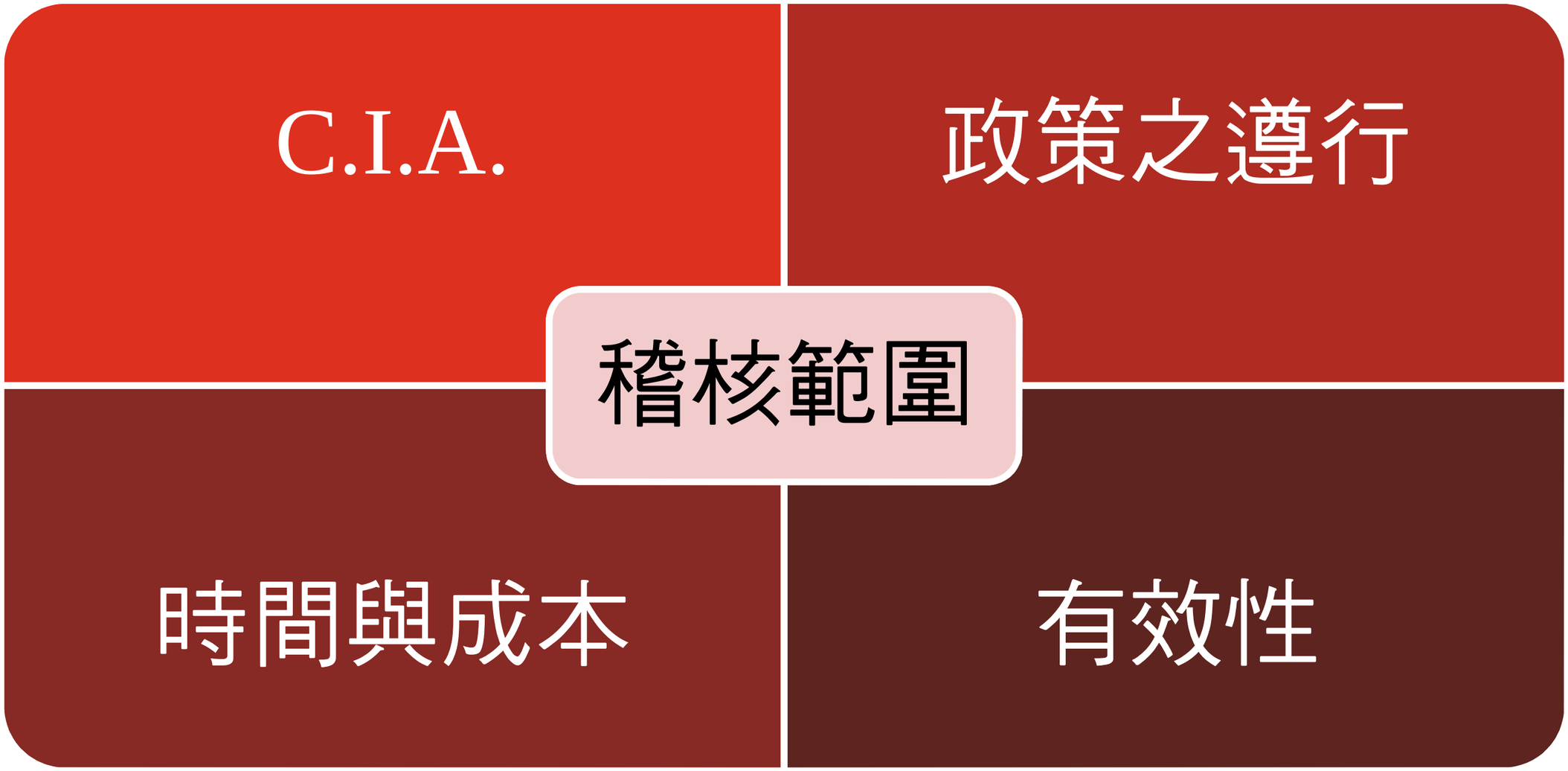
可於貴中心程序書裡面要求。

稽核規劃（續）

5. 規劃稽核計畫

- 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、人力與資源使用等稽核活動細節。
  - ✓ 需於每次稽核前先行提供給受稽核單位。

確認稽核範圍的決定



稽核作業說明

製作稽核查檢表：

稽核人員依據「稽核計畫」之稽核範圍，同時參考 「ISO27001 : 2013」製作「稽核查檢表」，稽核相關管制目標、控制措施、各過程及程序是否有達到：

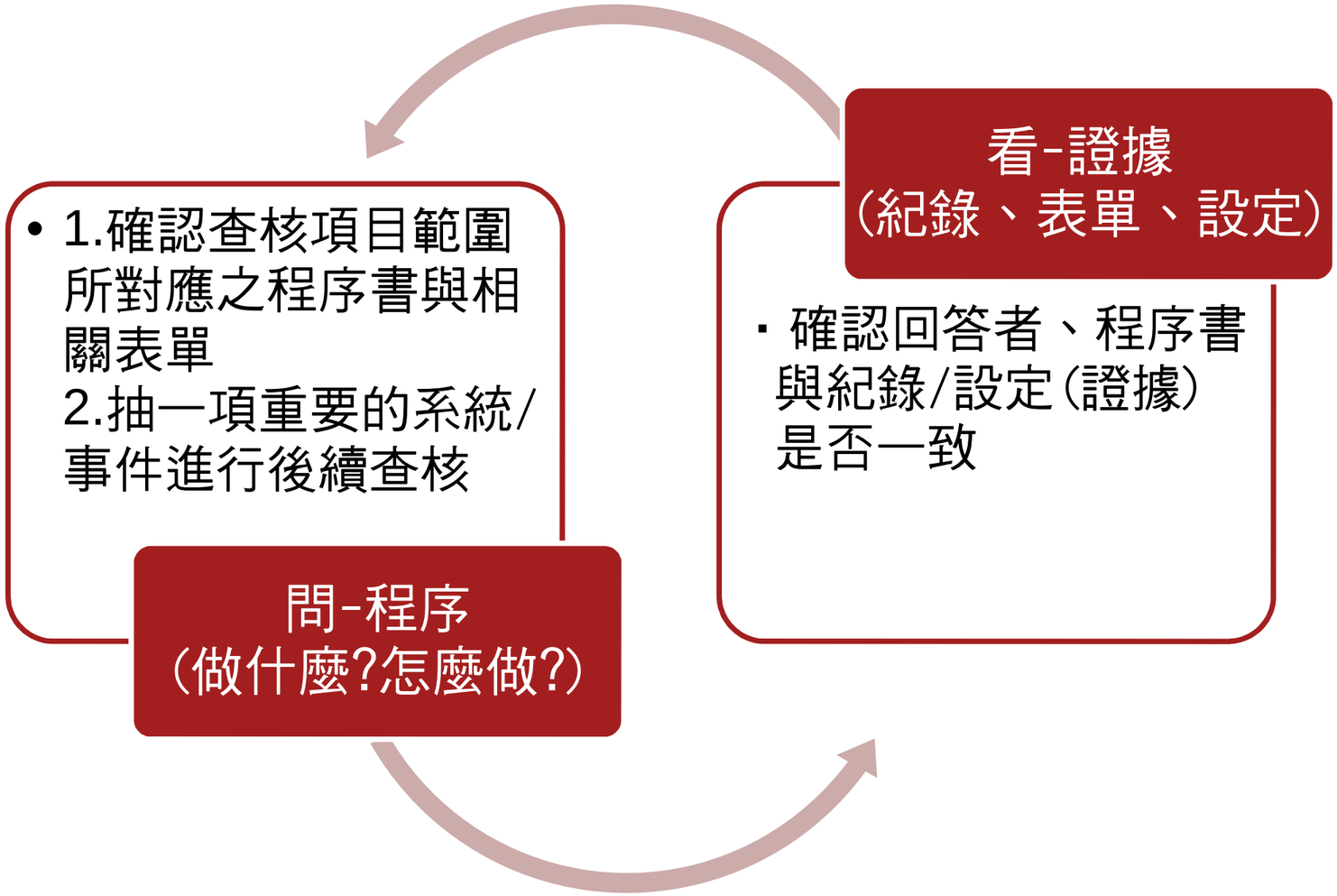
- 符合「個人資料保護法」或其他相關法令、法規之各項要求。
- 符合所鑑別之資訊安全管理制度要求。
- 符合資訊安全管理制度相關程序之規定，並如預期執行。
- 與日常操作之作業規範相符合且有效的實施與維持。
- 前一次的稽核不符合事項。

稽核作業說明（續）

稽核執行

- 稽核人員於稽核時，接受稽核之單位主管或同仁必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

稽核作業說明（續）


看-證據
(紀錄、表單、設定)
• 確認回答者、程序書與紀錄/設定(證據)是否一致
問-程序
(做什麼?怎麼做?)
• 1.確認查核項目範圍所對應之程序書與相關表單
2.抽一項重要的系統/事件進行後續查核

稽核作業說明（續）

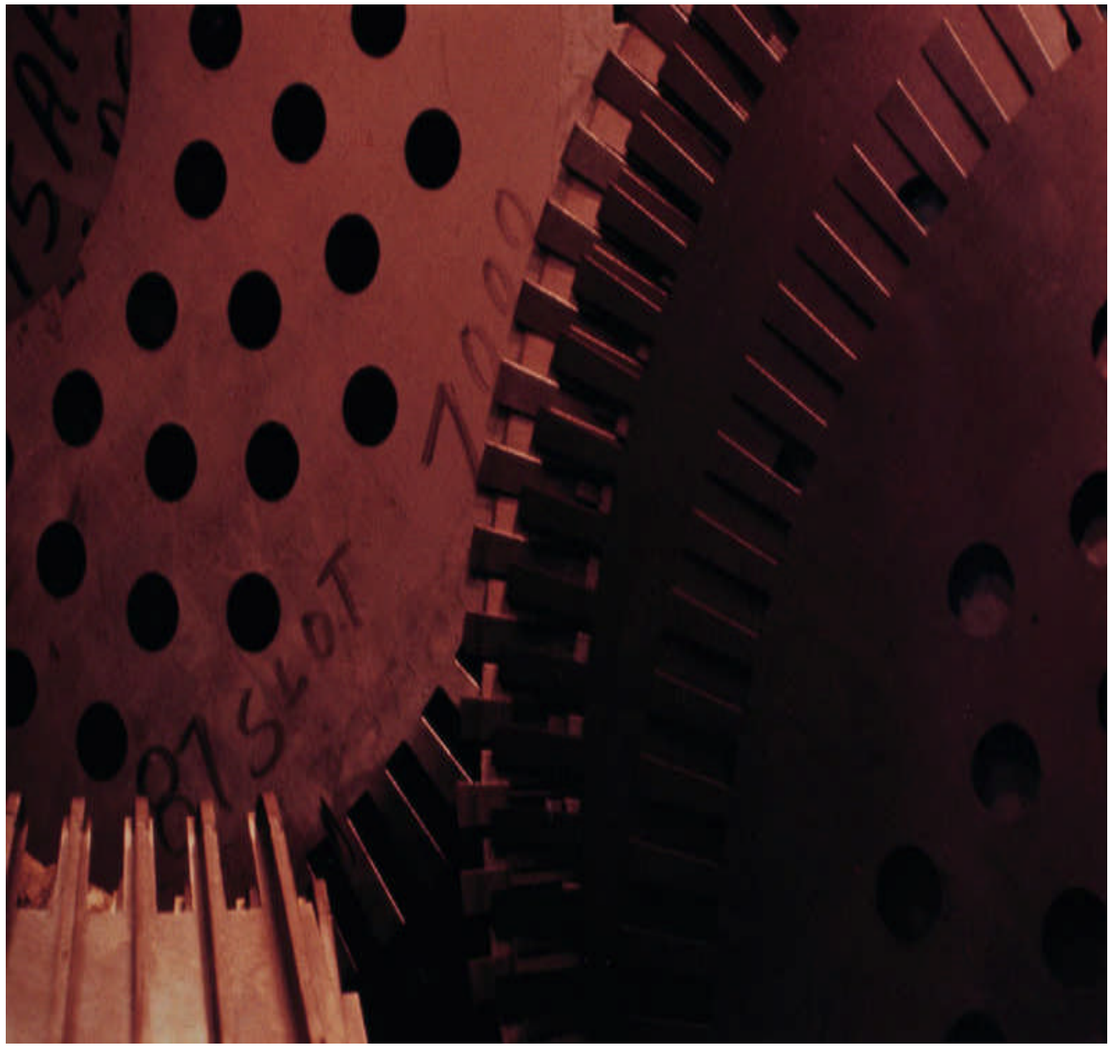
稽核結果

- 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，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資訊安全小組負責。

單元 2
資安查核技巧分享

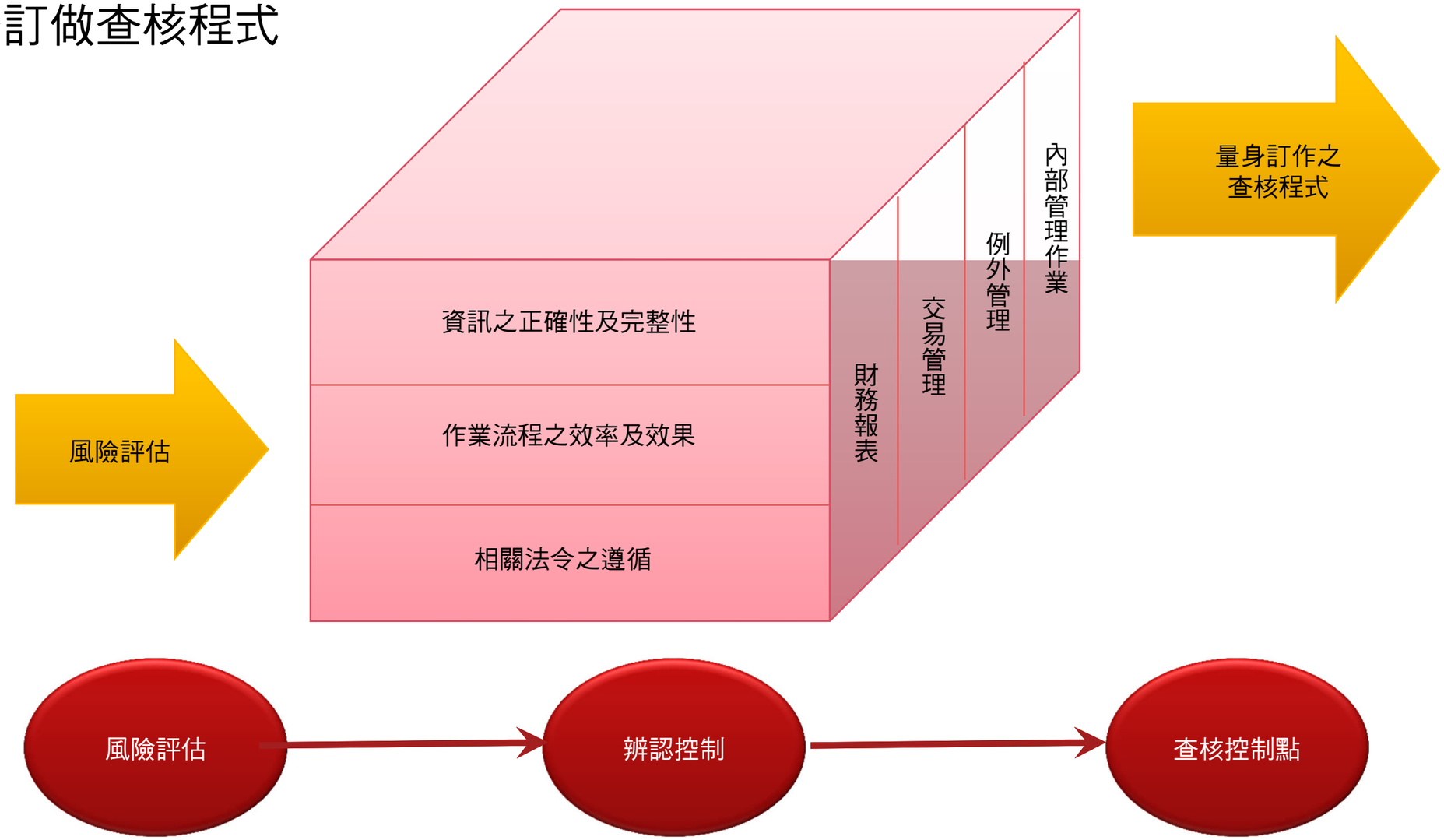
稽核計畫應考量…

- 公正性、獨立性
- 客觀性
- 一致性
- 時程與人員之掌握



查核程式之擬定方法

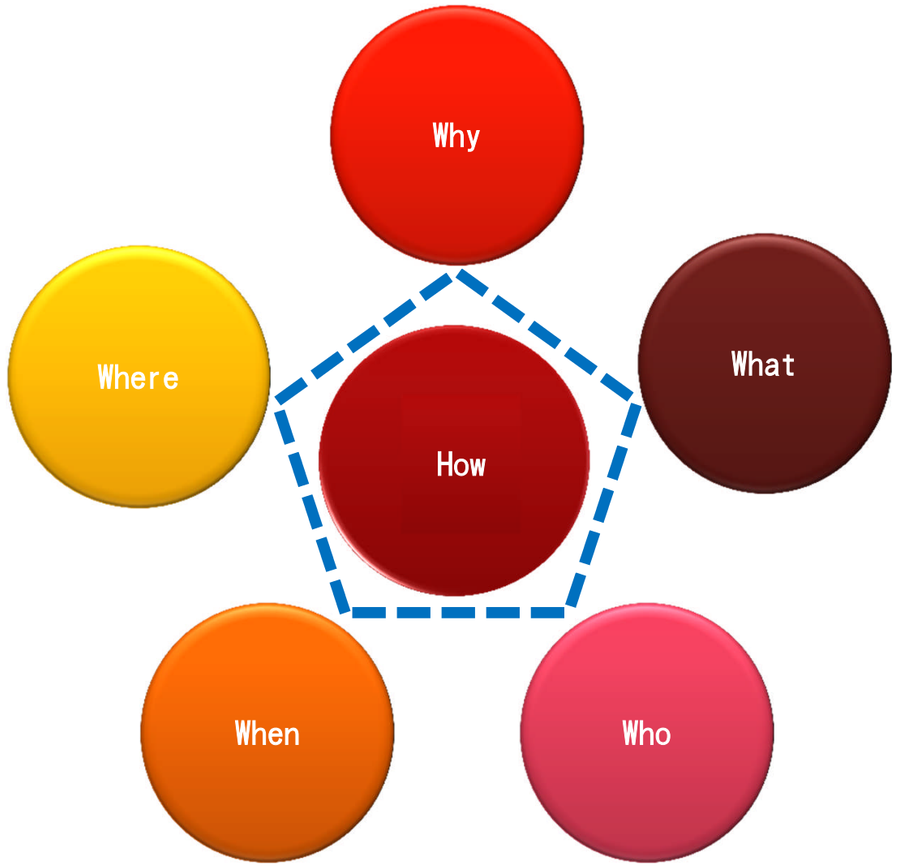
量身訂做查核程式



稽核方法與執行技巧

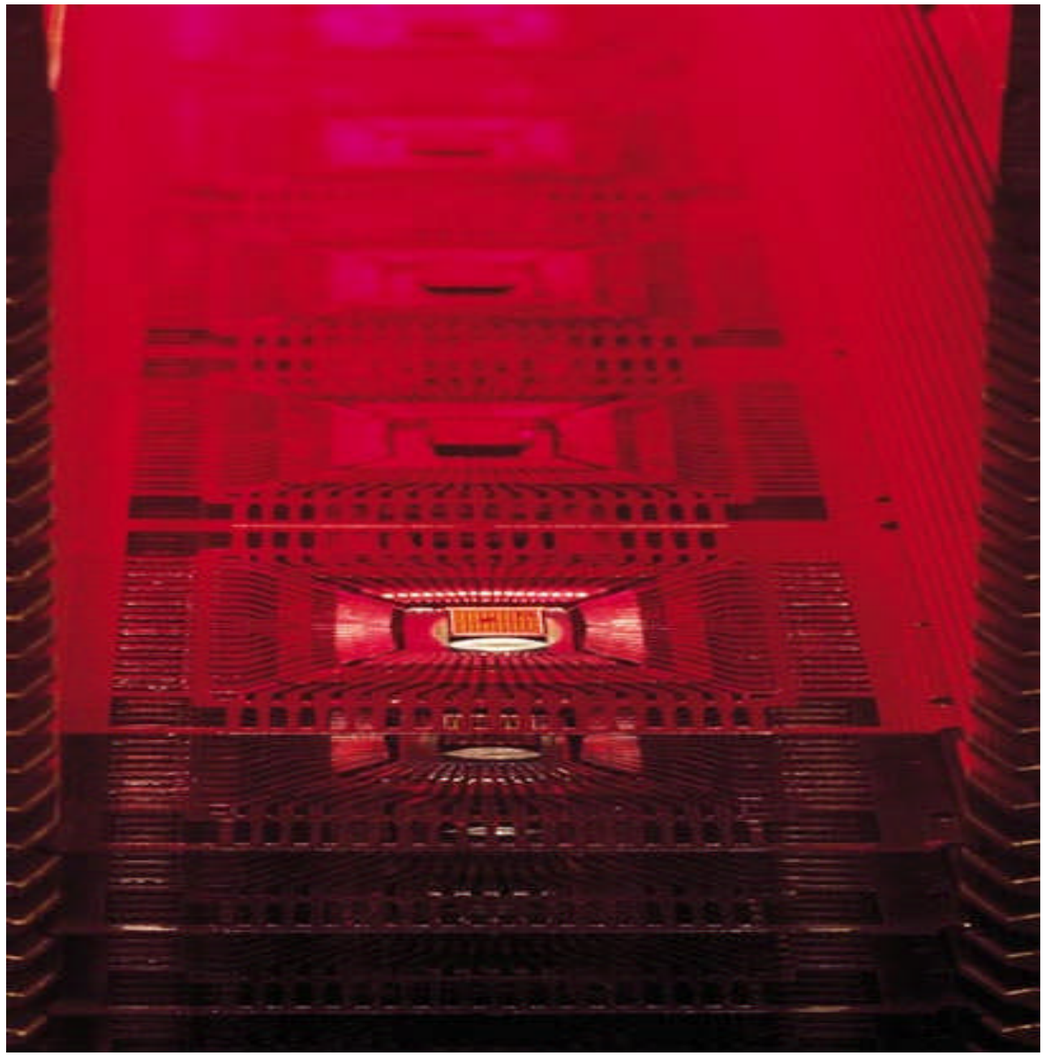
- 文件檢視
- 訪談
- 抽樣
- 觀察
- 使用電腦輔助查核
- 選擇和測試控制點

執行稽核的5W1H



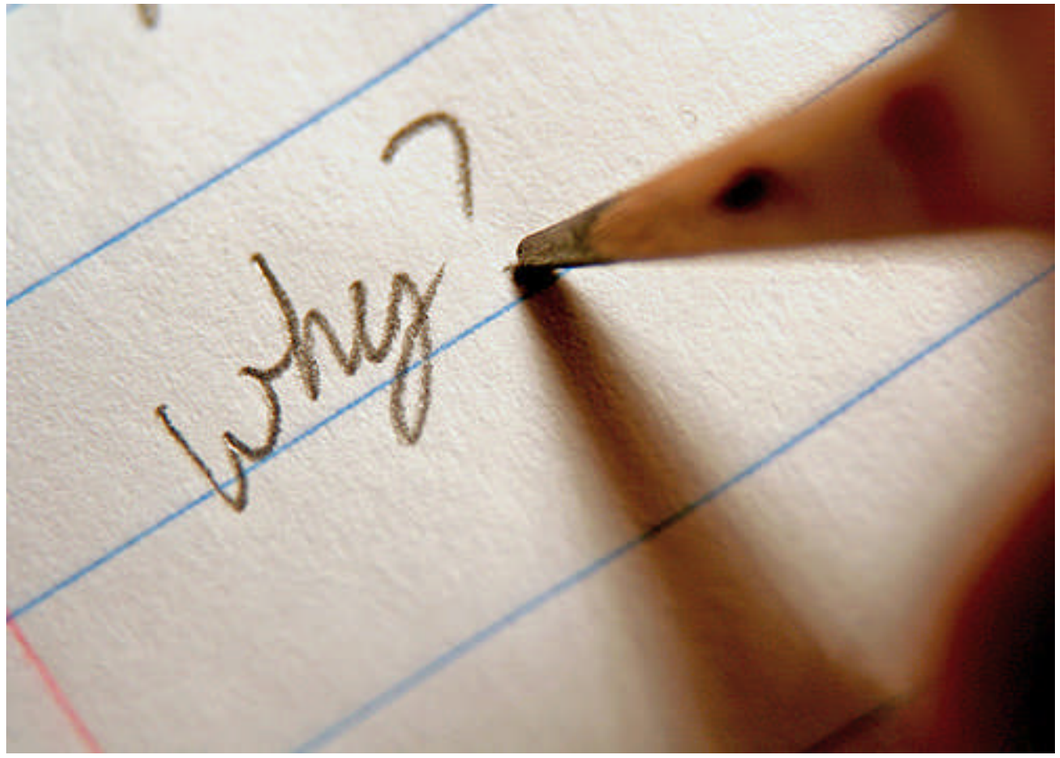
稽核方法與執行技巧（續）

- Why：遵法性目標
- What：業務流程及範圍
- Who：保護責任
- When：持續不斷
- Where：保護管控層級



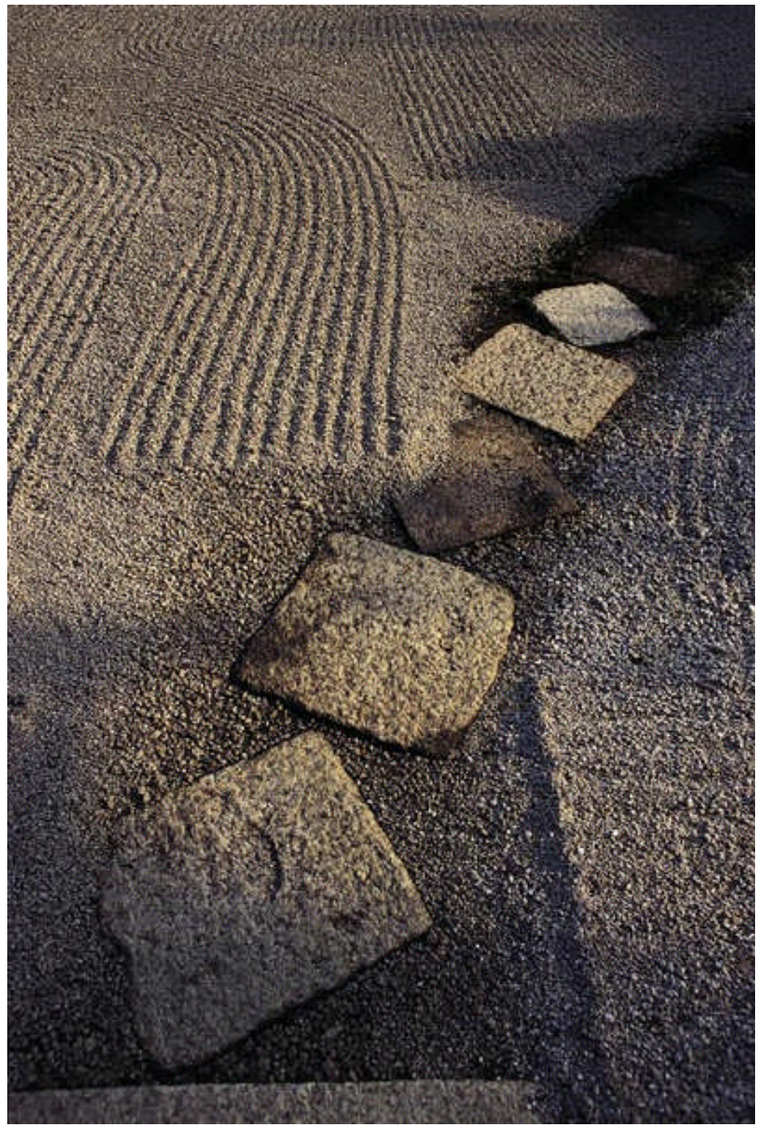
稽核方法與執行技巧（續）
Why

- 確保資訊的機密性、完整性、可用性
- 避免資訊資產被誤用或損壞
- 避免資訊資產被竊取或竄改



稽核方法與執行技巧（續）
What

- 資料和程式的保護
- 實體環境的保護
- 管理是否落實
- 存取控制是否適當
- 特殊權限管理
- 遠端存取
- 實體安全
- 緊急應變措施



稽核方法與執行技巧（續）
Who

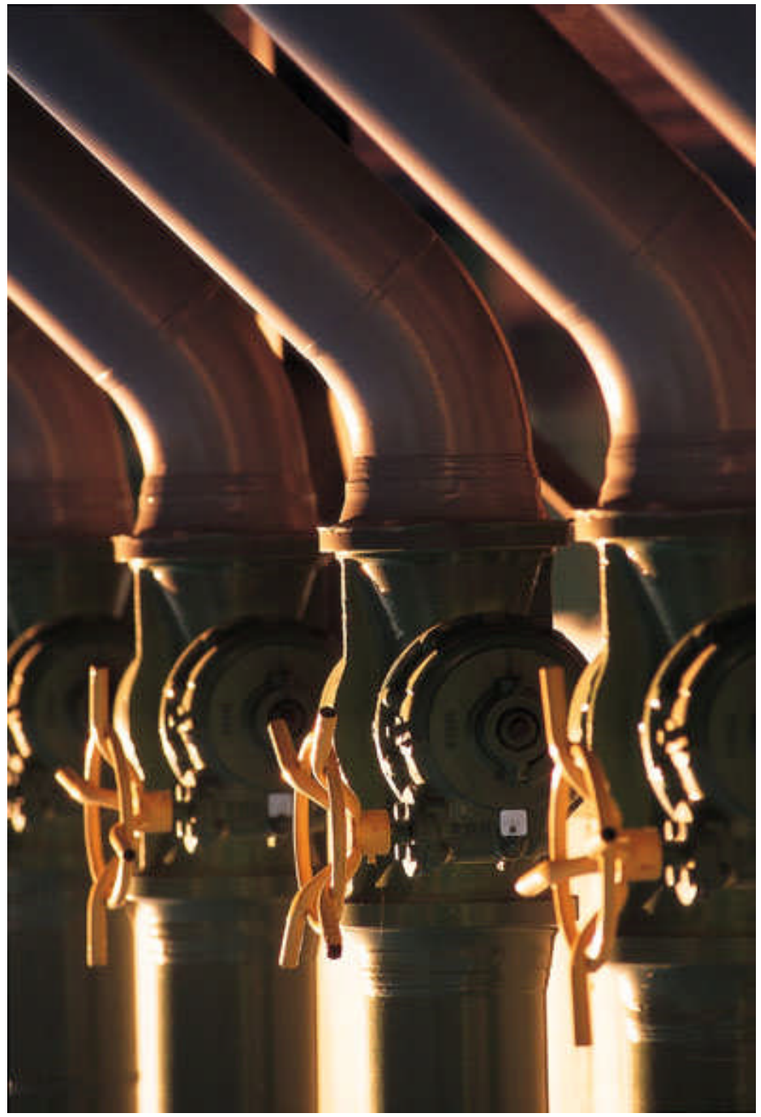
- 資訊安全主管
- 資料擁有者
- 系統管理者
- 資料使用者

稽核方法與執行技巧（續）
When

- 何時可以使用系統
- 系統使用時間
- 系統自動簽出機制
- 紀錄保存期限

稽核方法與執行技巧（續）
Where

- 實體層級 Physical Level
- 系統層級 System Level
- 應用層級 Application Level
- 功能層級 Function Level
- 欄位層級 Field Level



了解受稽方(被稽核對象)

取得被稽核單位現有之作業流程文件

- 可能遇到之情況：
  - ✓ 被稽核單位作業流程有書面文件，但不符實際作業流程
  - ✓ 被稽核單位作業流程無書面文件
- 如何回應

了解受稽方(被稽核對象)(續)

與被稽核單位人員進行訪談

- 訪談之目的：
  - ✓ 確認被稽核單位人員熟知作業流程，且控制點有確實被執行
  - ✓ 確認被稽核單位人員熟知之作業流程與書面文件一致
- 訪談之技巧：

  與被稽核單位人員進行訪談應保持專業的懷疑態度，適時地請對方提供相關文件（報表、作業手冊、表單等）以證明其所敘述。
- 在確認訪談的有效性中，時時保持專業的懷疑態度是很重要的。
  - ✓ 合理的懷疑並不表示要假設管理當局的正直性。
  - ✓ 進一步了解不一致的資訊（例如同一控制，但不同單位的說法不一；或稽核人員依所取得的文件得知的資訊與訪談者不同）。
  - ✓ 對於任何企圖阻止或防礙稽核的情況應保持警覺。

了解受稽方(被稽核對象)(續)

- 訪談後應注意事項：

若在訪談過程中，依訪談者及相關文件得知，從來沒有發現任何錯誤，則應評估其可能原因係：

因為有良好的預防控制，

OR

因為作業執行者缺乏執行控制的能力

稽核結果討論及報告撰寫

- 建立共識
- 專業知識與證據
- 建議解決方案
- 持續追蹤

不符合事項定義

<u>改善機會 (Opportunity For Improvement)</u>

- 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

<u>觀察事項 (Observation)</u>

- 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

不符合事項定義

次要缺失 (Minor nonconformity)

- 單獨違反系統/程序要求事件，且不會引起顯著資訊安全損失的風險。

主要缺失 (Major nonconformity)

- 系統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
- 違犯系統/程序要求事件，且會引起顯著資訊安全損失的風險
- 存在明顯立即資訊安全損失的風險
- 重大資訊安全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

追蹤及確認

追蹤

- 可由缺失發生單位主管自行追蹤辦理狀況，後回報稽核小組
- 或由管理單位進行追蹤有效性。

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。

追蹤改善

- 將缺失狀況與管理階層進行討論
- 與管理階層研議改善時程與複檢之計畫
- 對於缺失狀況與改善計畫，向上級報告
- 執行後續改善狀況之追蹤
- 追蹤後的風險評估
- 將缺失狀況匯交人資單位，以作為績效評量之參考

稽核過程中可能發生的狀況：

受稽者
態度強悍

人員不見

預先準備
好樣本

怕生的
受稽者

文件遺失

單元 3

查核重點介紹

查核程式

受稽核單位					
稽核項目	符合	部分符合	不符合	不適用	執行現況
◯資訊安全管理制度					

ISO27001內稽作業流程

稽核程序

- 資訊安全管理推動小組作業流程訪談
- 驗證範圍內各相關單位及人員作業流程稽查
- 風險評鑑作業稽查
- 實體安全(機房安全)控管稽查
- 系統開發環境稽查
- 營運持續管理
- 日常作業環境稽查
- 備份與備援稽查

資訊安全管理推動小組作業流程訪談

1. 查看適用性聲明書(SOA)
2. 查閱上次外稽矯正預防單
3. 查閱上次內稽矯正單 (➔今年內稽的矯正單)
4. 矯正效果的查核
5. 詢問如何識別有關利益相關團體（利害關係人）、法令、法規、契約等的 ISMS要求(內外部議題)及範圍，以及如何履行這些要求及訂定ISMS驗證範圍?
6. 詢問最高管理階層如何更積極的展現領導和承諾?是否成立跨部門之資訊安全小組？
7. 詢問資訊安全政策及資訊安全目標如何適合於組織之目的?
8. 確認關鍵績效指標的內容及執行的狀況
9. 詢問資訊安全政策是否有提供給有關利益相關團體（利害關係人)? 若有，作法為何?
10. 詢問資訊安全政策是否有依規劃之期間或發生重大變更時審查?
11. 詢問與有關利益相關團體（利害關係人）的相關溝通方式及聯絡窗口是否有文件化記載(例如溝通計畫或是溝通名單與對應窗口)?
12. 詢問資訊安全管理推動小組是否有向高階管理階層報告關鍵績效指標的執行狀況?
13. 詢問是否有相關工作職掌及工作說明書?
14. 如何證明資訊安全稽核人員、新進人員、在職人員有足夠勝任之能力及資格條件?

資訊安全管理推動小組作業流程訪談（續）

15. 詢問是否有公告對於違反資訊安全之員工的懲處原則及內容
16. 詢問是否有公告聘用責任終止後的資訊安全責任及義務?
17. 查看教育訓練計畫、課程表、簽到紀錄、成績紀錄
18. 查閱資訊安全稽核計畫及瞭解施行狀況
19. 詢問外來文件的管理方式?
20. 查閱管理審查會議紀錄，確認資訊安全績效的趨勢狀況
21. 詢問公司如何針對控制措施進行有效性量測?
22. 詢問目前資訊安全政策核可層級?
23. 詢問最近一次修改資訊安全政策之時間與相關修改情況?
24. 詢問目前如何確認資訊安全政策上 KPI 的達成率?
25. 詢問資訊安全管理審查委員會成員編制?
26. 查閱單位 ISMS 文件一覽表並審視文件發行情形及定期審查及修訂紀錄
27. 文件核可及發布機制?文件版本的控管(如何確保使用文件為最新版本)?
28. 詢問專案的定義及確認專案的資安控制措施執行狀況? 確認資訊安全目標是否有納入專案目標?

驗證範圍內各相關單位及人員作業流程稽查

1. 審視人員晉用辦法、離職流程、違反相關規定懲戒辦法及人員保密協議書及相關切結書
2. 實地觀察實體辦公環境(含媒體管理、資料生命週期相關紀錄、資料遞送相關紀錄與重要資料安全保管方式、媒體報廢方式…等)
3. 審視單位相關業務職掌及權限、組織系統密碼原則、強制變更密碼週期、人事異動、文件保存年限、有無違反相關法規要求
4. 審視機密等級文件之歸檔方式及借閱方式
5. 審視紙本資料保存及銷毀方式
6. 審視媒體資料保存及銷毀方式

風險評鑑作業稽查

1. 審視目前風險評鑑的做法
2. 人員是否均熟悉單位所採用的風險評估及管理辦法
3. 風險發生可能性及衝擊的評估標準及合理性?
4. 詢問哪裡可以識別資產所有者及風險所有者?
5. 詢問風險處理計畫的做法 ?決定風險所有者的方式?
6. 確認計算風險能力（Risk Capacity）及風險胃納（Risk Appetite）的方式
7. 詢問風險擁有者對風險處理計畫的核准程序及對剩餘風險接受的原則?
8. 詢問風險處理的優先順序之原則為何?
9. 確認適用性聲明書是否有參考風險評鑑之結果? 若有，納入及由附錄A排除之理由為何?
10. 詢問風險值是如何計算出的?風險管理措施的合理性?
11. 中心是否有實作資訊安全風險處理計畫?

風險評鑑作業稽查（續）

9. 詢問目前組織可接受之風險值為多少？可接受風險值是如何訂定？是否有決議之會議紀錄？
10. 詢問資訊資產價值清單如何審核？審核層級？
11. 詢問矯正措施執行的方法
12. 詢問如何確認高風險清單之完整性
13. 抽樣風險改善計畫，對照風險評估表
14. 詢問資訊資產分級及標示的方式?
15. 詢問資訊資產清冊如何更新？頻率為何？
16. 各項資訊資產是否設有適當之保管人，並適當標示管理?
17. 最近有做任何的設備更新嗎？資訊資產清單是否一併更新？
18. 人員是否均瞭解資訊資產評價之標準及分類辨識之方法?

實體安全(機房安全)控管稽查

1. 實地了解門禁管制做法
2. 實地了解重要場所與機房出入之權限授與及監控措施
3. 消防設備維護紀錄
4. 審視保全委外合約
5. 了解門禁監控影片品質之維護情況
6. 審視機房空調及UPS維運紀錄
7. 了解單位發電機測試週期與情形
8. 審視設備停機處理機制
9. 了解機房門禁的權限授與情形
10. 主機群、門禁及錄影等設備有關時間準確性之審視(含定期紀錄)
11. 核心設備可用性之監控審視 (例： HD Size 、CPU 、Memory)
12. 機房交接班表檢視(例：依出現重大事項來反查該單位處理情形)
13. 檢視單位設備、人員進出安控紀錄

系統開發環境稽查

1. 審查系統開發資安政策及系統工程資安原則
2. 確認資訊安全需求是否有納入新資訊系統或既有資訊系統強化的要求事項中
3. 詢問系統變更控制程序的作法
4. 確認開發之委外廠商運作機制，並確認是否有監督及監視委外系統開發活動
5. 確認委外廠商是否有遵守組織訂的系統開發資安政策及系統工程資安原則
6. 審視使用者及資訊安全需求驗收狀況
7. 委外廠商使用軟體的合法性審視 (例：合約有無載明)及可攜式媒體管控
8. 審視測試系統和正式機的權限授與情形(例：有無職能衝突)(測試與上線人員不可一樣)
9. 審視程式源碼之管理(版本控管及存取控制)
10. 程式從測試機移轉正式機之相關紀錄(LOG)
11. 確認針對測試用資料是否有做相對應的保護
12. 確認組織針對委外廠商可存取之資產的保護及控管方式
13. 確認與委外廠商之合約是否有議定相關資訊安全要求事項及包含因應供應鏈之資訊安全風險
14. 確認是否有定期稽核委外廠商有關資訊安全要求事項的執行狀況

營運持續管理

1. 詢問 BCP 演練分工與落實情形?
2. 詢問關鍵性業務流程之資訊處理設備及設施是否有相對應的備援機制?
3. 詢問判定為關鍵性業務之標準為何? 抽檢關鍵業務備援機制的建立狀況

日常作業環境稽查

1. 審視 DB 及相關 SERVER 存取帳號授與情形 (是否有共用帳號的狀況)
2. 審視 OA 環境密碼變更週期
3. 查閱帳號申請單 (例：抽檢離職人員的表單進行比對)
4. 查閱 AP /DB Root User 帳號申請單
5. 了解 網路環境監控情形
6. 審視存取權限之移除或調整的狀況
7. 實際系統帳號和 紙本申請表單進行比對
8. 審視 Root 密碼變更情形
9. 審視主機相關紀錄(有無重大事件與變動紀錄)
10. 審視上 Patch/Service Pack 之嚴謹程度(是否有做測試)
11. 資產歸還及報廢流程
12. 詢問 BCP 演練分工與落實情形
13. 審視單位網路架構圖(例:了解網段分隔情況或設備的 HA)
14. 審閱行動裝置政策

日常作業環境稽查（續）

14. 審視 E-mail帳號申請/移除之嚴謹程度
15. 審視P2P或即時通軟體申請使用程序與嚴謹程度
16. 審視訪客權限控管之嚴謹程度
17. 審視 Client 瀏覽器安全性管控措施(例:Active-X)
18. 審視防火牆設定變更有無紀錄
19. 審視防火牆設定變更時有無進行 Config 備份
20. 詢問期間有無中毒或駭客事件
21. 發生資安事件時有無落實矯正預防通報機制
22. 詢問 OA 營運 BCP 演練情形
23. 詢問弱點掃描相關紀錄及改善情形(含矯正預防機制)
24. 詢問 Web 防駭防範及通報處理機制
25. 詢問 IPS 的運作通報機制(含日常韌體更新機制)

日常作業環境稽查（續）

26. 是否建立資安事故、個資外洩事故之通報程序
27. 是否建立資安事件及事故管理之責任與程序
28. 針對緊急事故，是否建立緊急應變機制與反應管道
29. 是否要求資訊系統及服務的使用者，如：所有員工、約聘員工或第三方人員，注意並通報任何觀察到的或可疑的有關系統或服務方面的安全弱點或威脅
30. 是否建立對安全或失效事故之管理機制，並從事故中學習
31. 組織是否有定義相關程序以識別、蒐集、取得及保存可用作證據之資訊

簡報完畢 謝謝指教