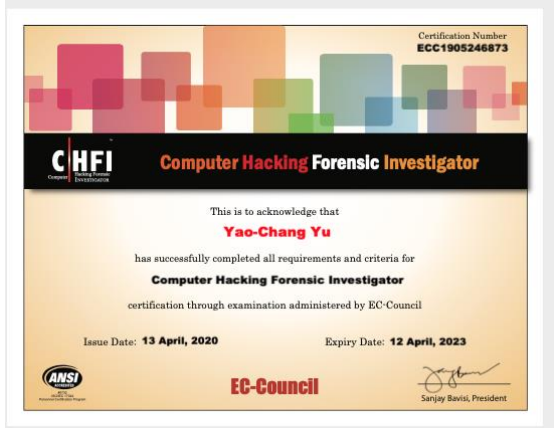
資安及個資管理規範導入作業實務

于燿彰 博士

2023/08/10

講師簡介



- 學歷:
  1. 國立成功大學 工程科學所 博士
  2. 密蘇里大學堪薩斯城校區 資訊工程所 碩士
- 經歷：
  1. 財團法人電信技術中心 資通安全組 副組長
  2. Hermes-Infortech Inc. 資深資安顧問/講師
  3. 鼎智國際技術服務有限公司 技術長/資深資安顧問
  4. USIS INC. 創辦人/技術長/資深資安顧問 （現任）
  5. 鑑智實相科技股份有限公司 協同創辦人/執行長（現任）
  6. 鑑智實相科技股份有限公司（馬來西亞分公司）協同創辦人/技術長（現任）
  7. 國立成功大學工程科學所 兼任助理教授 （現任）
- 專長:
  1. 網路通訊協定安全
  2. 資訊安全
  3. 管理系統(資訊安全、IT服務、營運持續)
  4. 資安產品測試 (ISO/IEC 15408)
  5. 密碼模組測試(FIPS 140-2)
  6. 實體環境安全
  7. 密碼學
- 稽核員資格：
  1. ISO/IEC 27001稽核員
  2. ISO/IEC 17025稽核員
  3. BS10012稽核員
- 聯絡資訊:

  Email: avis.y@ustar-is.com

大綱

- 業務持續管理
- 內部稽核
- D051_個人電腦設定與軟體安裝查核表操作簡介

業務持續管理

修復要7天！南韓電信龍頭KT火災成「國難」　醫院、店家全癱瘓

南韓電信龍頭KT位於首爾忠正路的阿峴分公司地下通訊室24日驚傳大型火災，消防人員持續打火長達10小時才終於撲滅火勢，但由於內部電纜受損嚴重，使許多地區家用電話、無線通信、行動網路全部斷線，各地也傳出ATM、地下鐵置物櫃等民生需求設備受到影響，生活機能大倒退，火災儼然上升至國家級災難。

綜合韓媒報導，火災起火點所在的通訊室有多達16.8萬條有線電話線路、220條光纖線路，使用這些線路的首爾西大門區、恩平區、麻浦區、中區一帶鬧區和京畿道高陽市部分區域民眾的日常生活彷彿靜止了，顯示出過度依賴資訊和通訊技術的IT強國可能因為一次火災便陷入癱瘓的弱點。

全美海關電腦大當機 旅客塞爆出入境

美國移民官員的電腦系統16日下午突然全面當機，導致旅客無法正常入境美國，各大城市的國際機場都受害，由於正值暑期出入境高峰期，海關塞滿排隊人潮，直到稍早才逐漸回復正常，根據官方表示目前未掌握到系統遭到惡意攻擊，詳細故障原因仍待調查。

綜合外電報導，此次全美海關大當機，包括西雅圖、費城、舊金山、休士頓、芝加哥、紐約甘迺迪國際機場（JFK）及華盛頓的杜勒斯國際機場（Dulles International Airport）出入境作業一度緊急加派人手以人工作業方式進行查驗，但仍難減緩排隊人潮，民眾紛紛上傳影片至社群媒體網站，顯示海關辦理檢查站出現長長排隊人龍。

這不是系統首次面臨問題，許多乘客2017年1月2日要結束耶誕假期時，系統也曾停擺4小時。國土安全部（DHS）督察長辦公室（OIG）2017年11月發布的報告發現，「CBP軟體容量測試不足，讓處理錯誤可能再度發生。」

電腦「死機」致停市半天 香港首次 金融中心蒙羞

因衍生產品交易系統軟件出現問題而須破天荒停市半天的香港期貨交易市場，今早如常開市，運作正常。不過，因軟件程序錯誤而令電腦死機以致須要停市、死機約四小時後才宣布停市等決定，卻受到不少人批評。香港交易所總裁李小加對事件表示遺憾，承諾日後會儘力防止事件重演。

受期貨交易系統「死機」及「停市」影響，九月份恆生指數期貨及國企指數期貨周四的成交量大減九成至只有3.1萬張。

受事故影響，昨日股市、窩輪及牛熊證的成交都減少。及至下午停市，投資者需沽貨對衝，令恆生指數由半日原先升逾100點，在下午一度倒跌逾200點。不過，有業內人士表示，由於昨日股市並非太波動，預料本港投資者整體損失不大。

標準的要求

A.17 營運持續管理之資訊安全層面		
A.17.1 資訊安全持續		
目標：資訊安全持續應嵌入組織之營運持續管理系統中。		
A.17.1.1	規劃資訊安全持續	控制措施 組織應決定其對資訊安全之要求事項，以及於不利情況下(例：危機或災難期間)，對資訊安全管理之持續性要求事項。

標準的要求

A.17.1.2	實作資訊安全持續	控制措施 組織應建立、文件化、實作及維持過程、程序及控制措施，以確保不利情況期間所要求之資訊安全持續等級。
A.17.1.3	查證、審查並評估資訊安全持續	控制措施 組織應定期查證所建立及實作之資訊安全持續控制措施，以確保其於不良情況期間係生效及有效。
A.17.2 多重備援		
目標：確保資訊處理設施之可用性。		
A.17.2.1	資訊處理設施之可用性	控制措施 應對資訊處理設施實作充分之多重備援，以符合可用性要求。

NIST Cybersecurity Framework: 復原階段

復原計畫 Recovery Planning

- 具有復原規劃方案與具體計畫，作為資通安全事件發生當下與後續的執行依據。

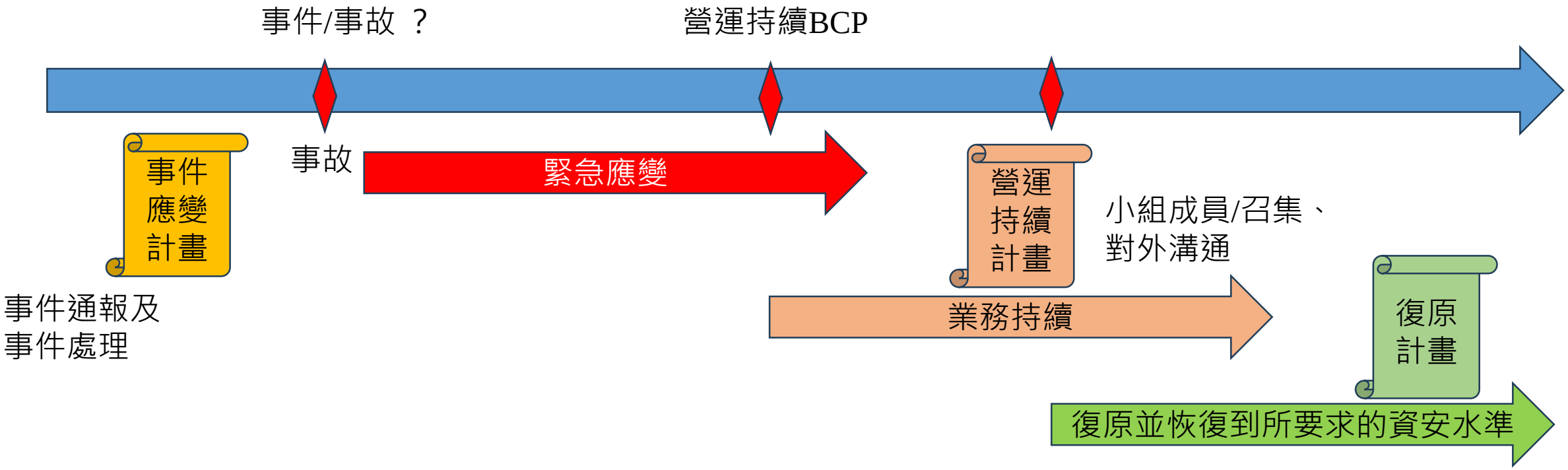
持續強化 Improvements

- 於復原計畫內容，加入事件過程中學習的經驗。
- 復原策略應隨之更新強化。

溝通 Communications

- 應管理與公眾的關係。
- 於事件發生後修復聲譽。
- 復原活動除內部管理層及執行團隊掌握情況外，應同時傳達予利害關係團體。

事件管理與營運持續


事件/事故 ？
營運持續BCP
事件
應變
計畫
事故
緊急應變
營運
持續
計畫
小組成員/召集、
對外溝通
事件通報及
事件處理
業務持續
復原
計畫
復原並恢復到所要求的資安水準

以恢復業務目標/功能為主軸，訂定系統復原計畫

- 恢復資訊系統的目的在於恢復業務功能; 恢復步驟應考量業務優先順序、時間點要求（ MTPD, RTO, RPO)
- 除復原資料與資訊系統外，於系統運行相對應的監控機制、權限管控等也應一並恢復。
- 應預期事故期間相關資源性能下降，須納入容量管理。

業務流程	單位名稱	負責人	最大可容忍中斷時間 (MTPD)	復原時間目標 (RTO)	資料復原時間目標 (RPO)	重要分級	備註

內部稽核

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

- 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

- 定義ISMS範圍
- 風險評估
- 確認控制目標
- 選擇控制點

- 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

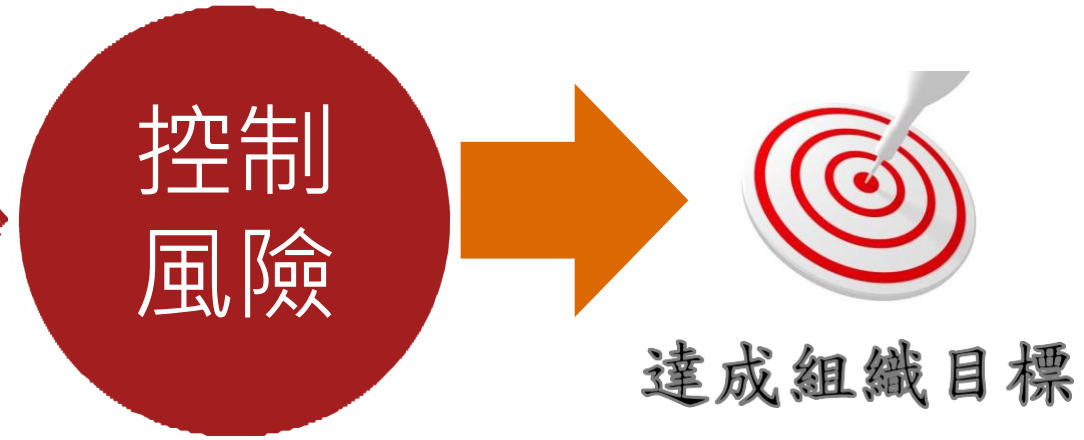
覆核控管程序是否落實

評估管理成效

協助發現缺失

提供改善方案

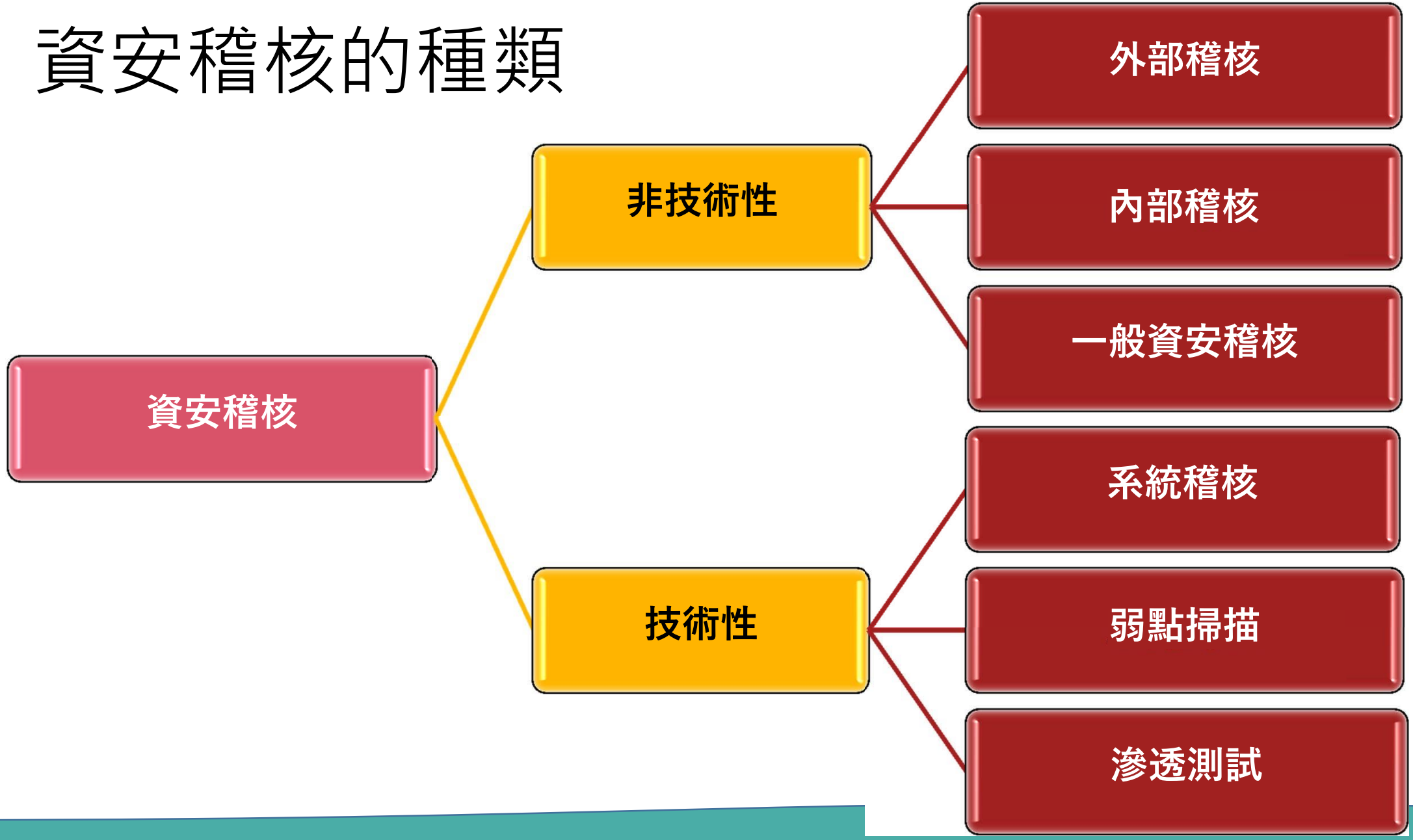
針對特殊目的之驗證性稽核



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：

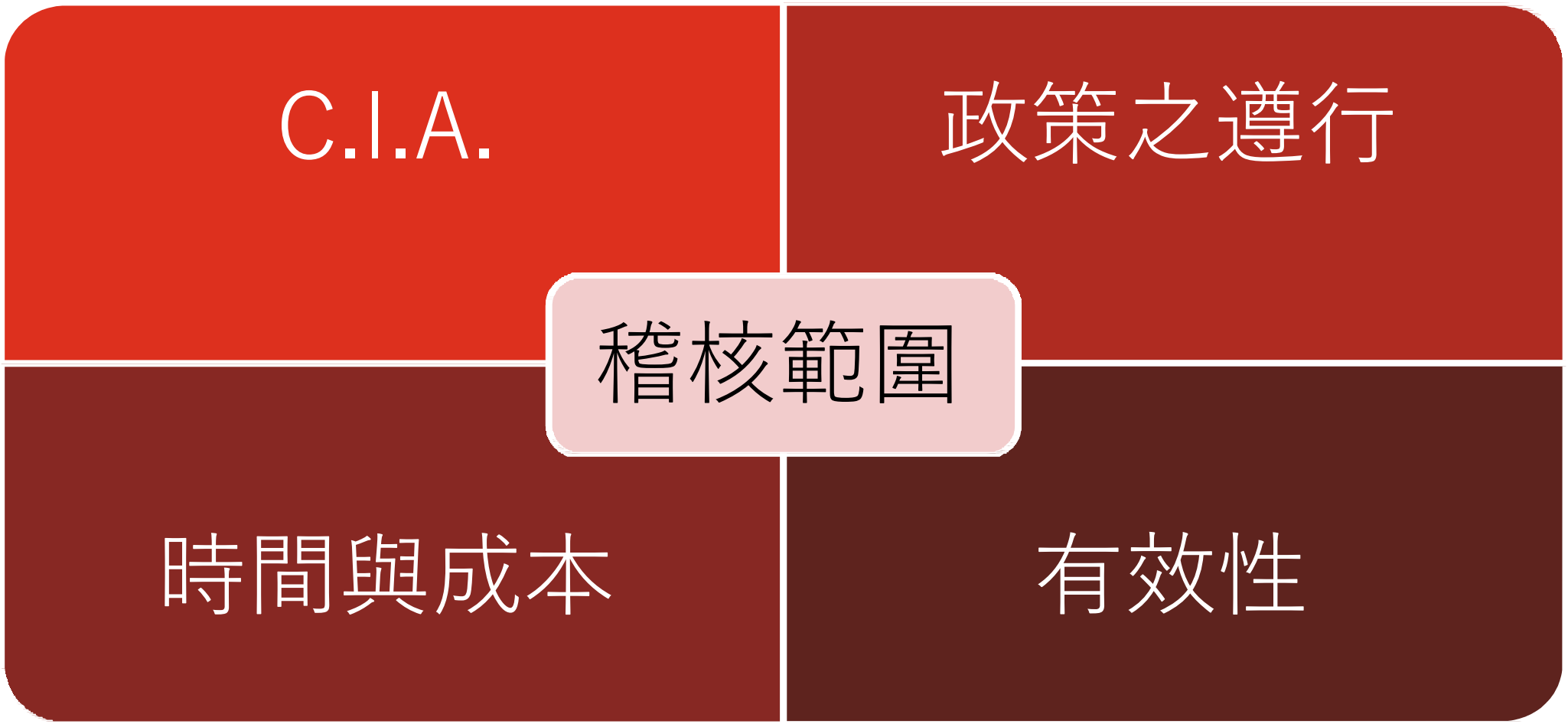
- 可於貴校程序書裡面要求。

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。

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」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）

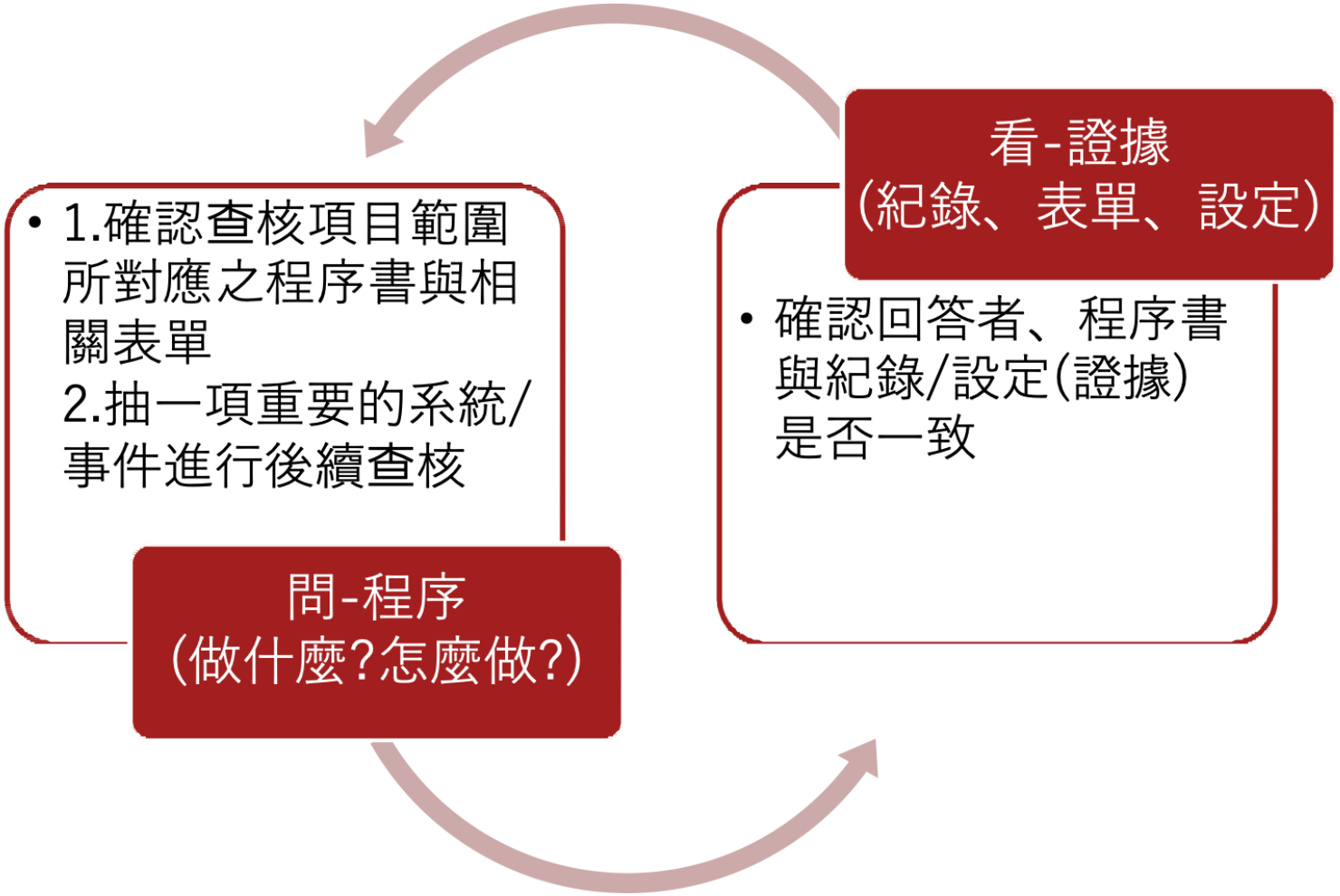
- 執行稽核

➢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況。

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。

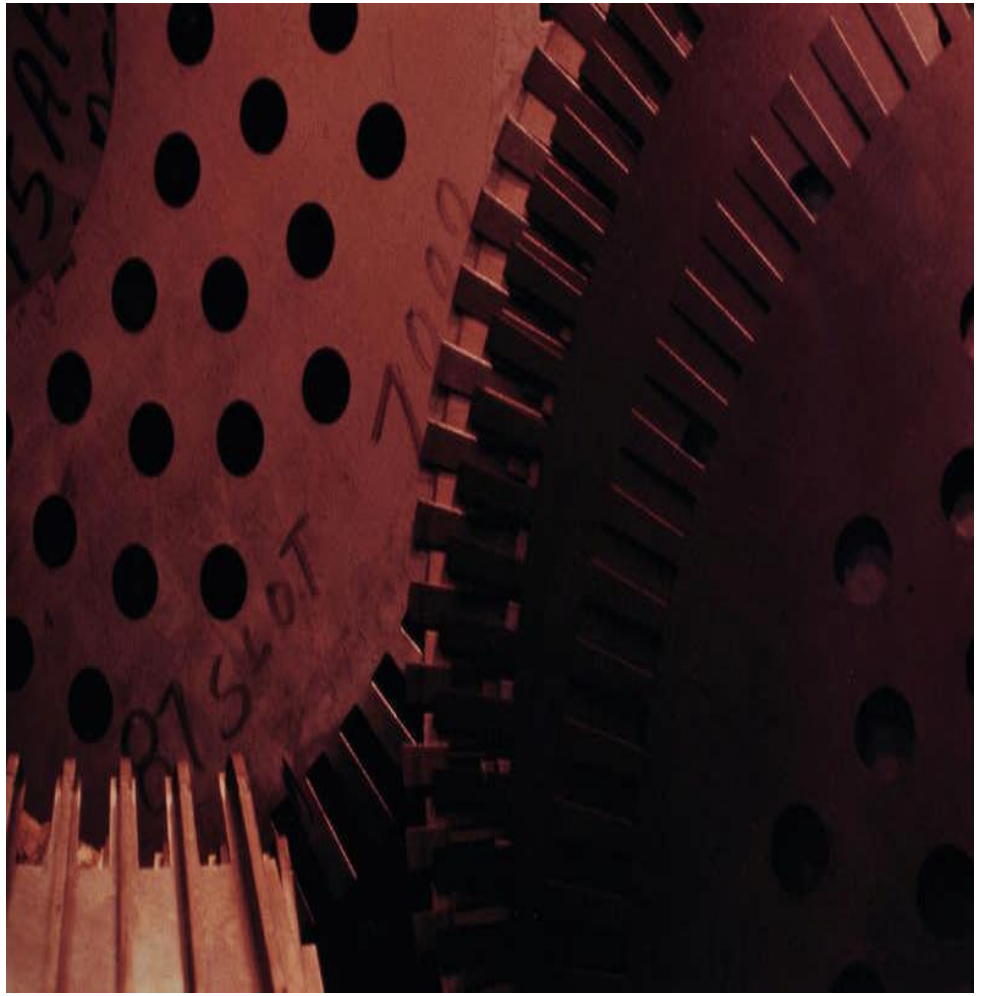
➢稽核小組成員依據已確認之「稽核查檢表」彙整為「稽核報告」。

➢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措施，後續改善追蹤及確認由資訊安全小組負責。

資安查核技巧分享

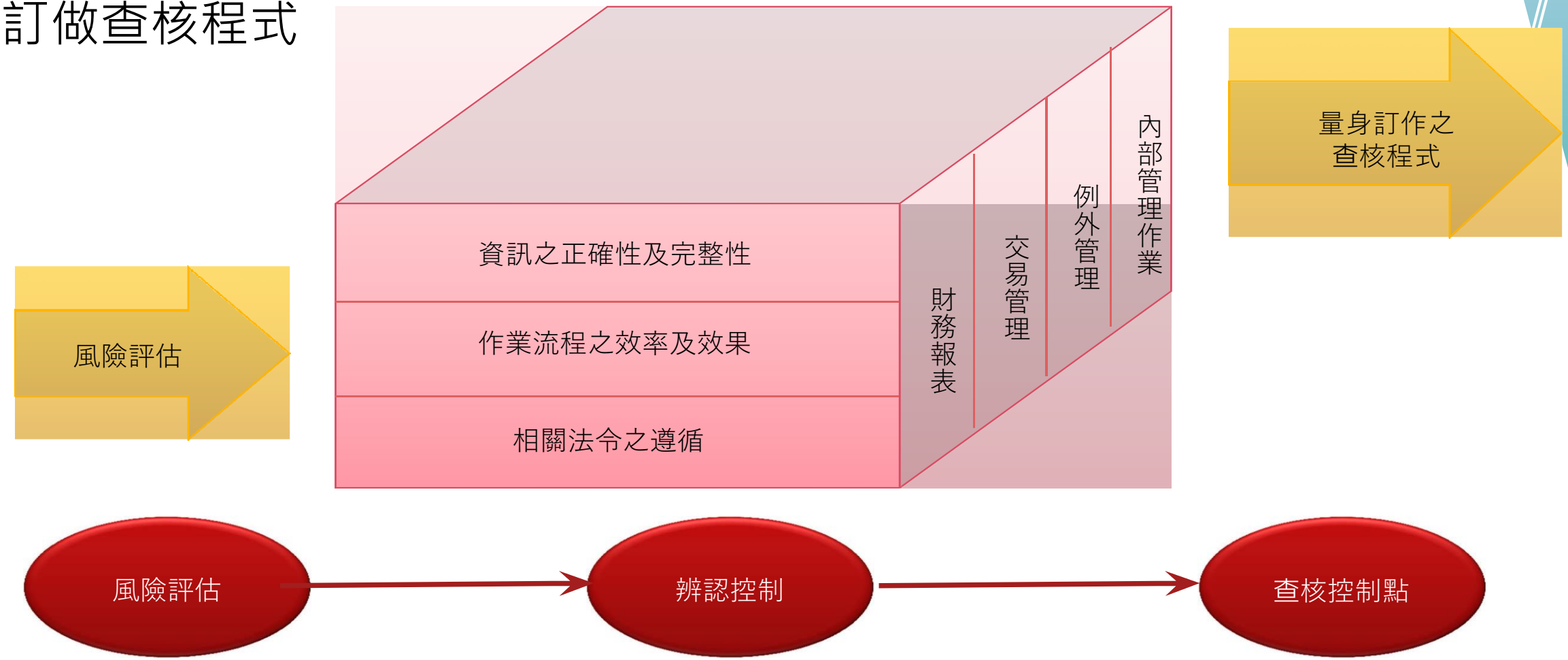
稽核計畫應考量...

- 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

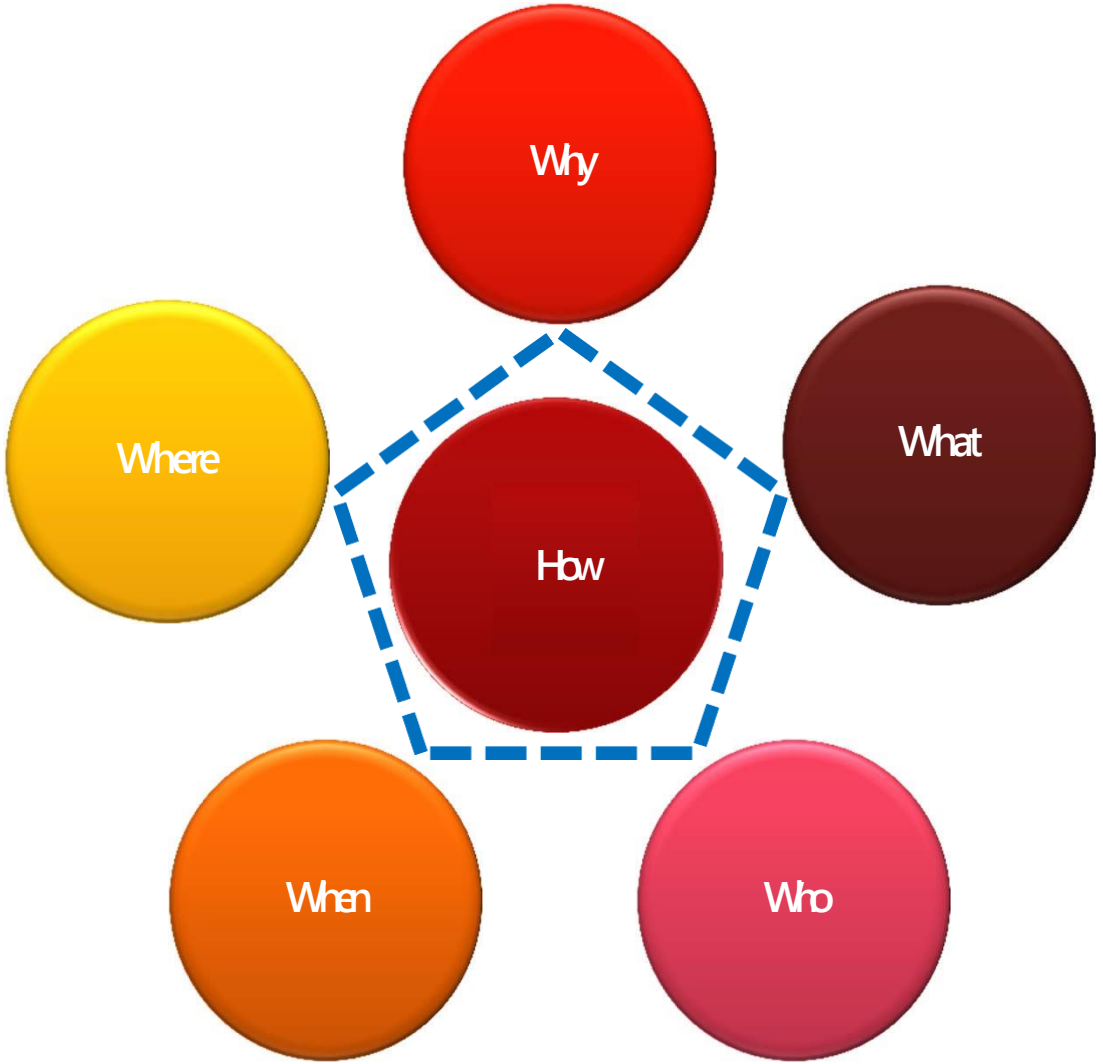
量身訂做查核程式



稽核方法與執行技巧

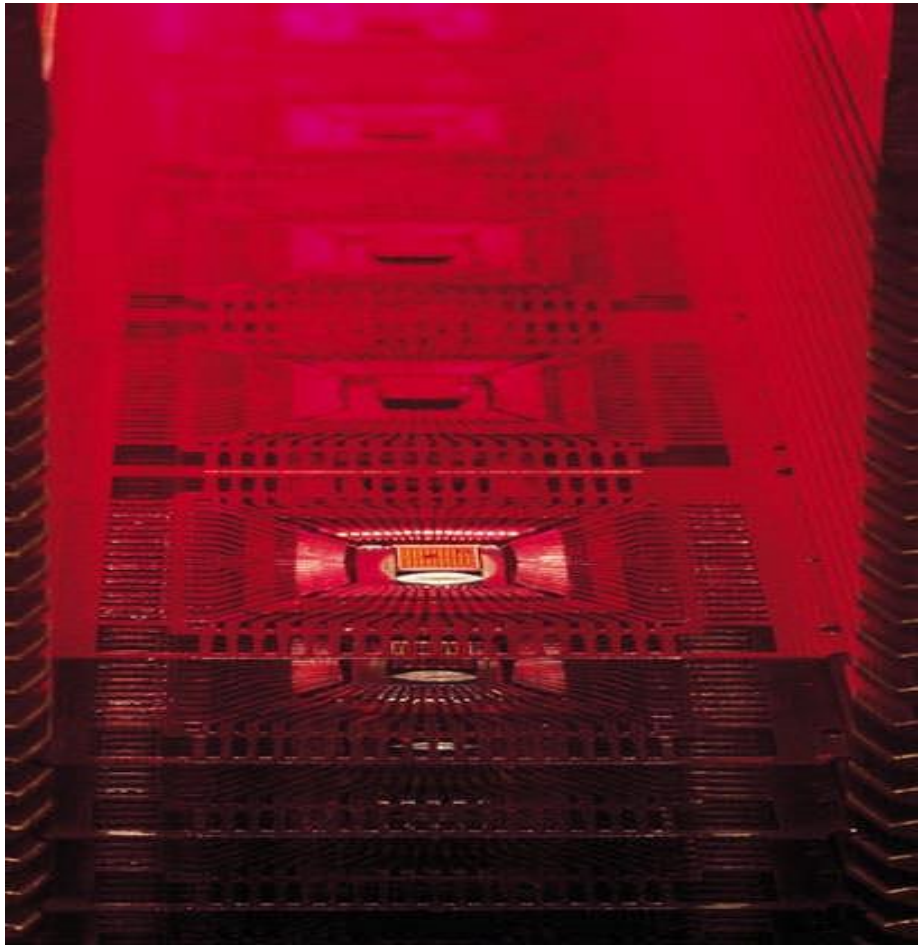
- 文件檢視。
- 訪談。
- 抽樣。
- 觀察。
- 使用電腦輔助查核。
- 選擇和測試控制點。

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。

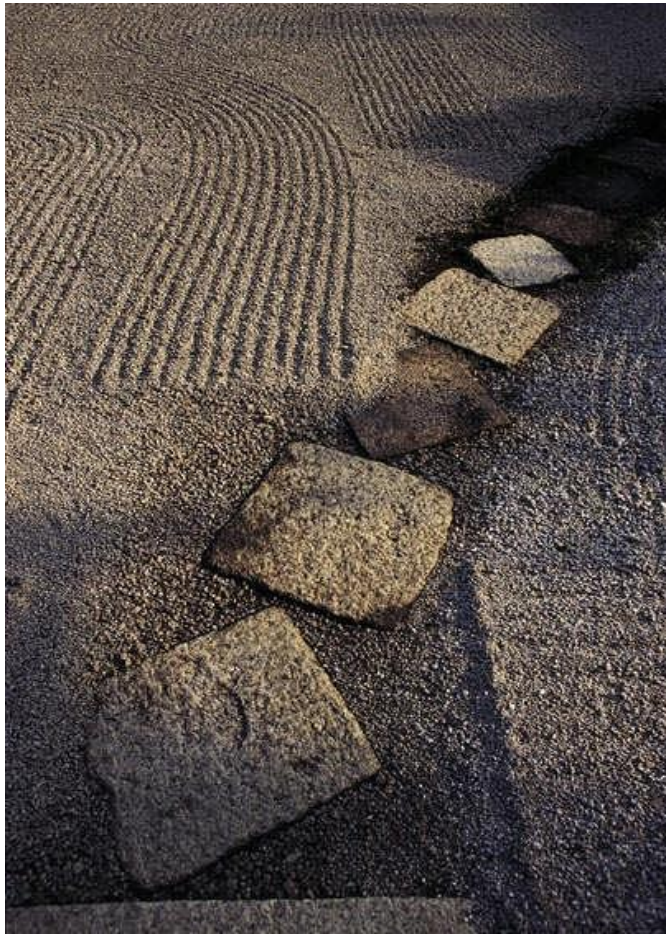
➢存取控制是否適當。

➢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）

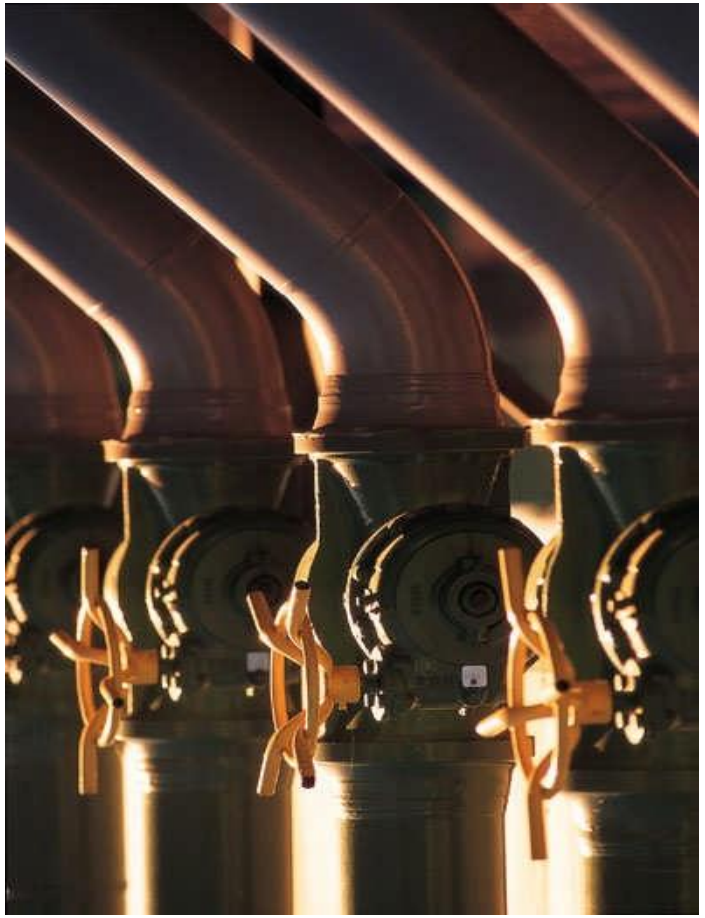
- Who
  - 資訊安全主管。
  - 資料擁有者。
  - 系統管理者。
  - 資料使用者。

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

- 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。

不符合事項定義（續）

- 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

D051_個人電腦設定與軟體安裝查核表操作簡介

D051_個人電腦設定與軟體安裝查核表

個人電腦設定與軟體安裝查核表		
文件編號：NUTN-ISMS-D051	版次：1.4	機密等級：限閱
紀錄編號：	填表日期：　　年　　月　　日	

管理人員	
設備資料	1. 資訊資產名稱：＿＿＿＿＿＿＿＿＿＿財產序號：□□□□□□ 2. 作業系統：□Windows＿＿＿＿(請填寫版本) □其他＿＿＿＿＿＿

	查　核　項　目	結果	檢查說明
1	電腦系統帳號密碼設定	□是□否	系統重新開機查看是否需要登入帳號
2	完成稽核原則設定	□是□否	執行 CMD：gpedit.msc 電腦設定→Windows 設定→安全性設定→本機原則→稽核原則→每個項目的「成功/失敗」全部開啟
3	完成密碼原則設定	□是□否	執行 CMD：gpedit.msc ✓ 電腦設定→Windows 設定→安全性設定→帳戶原則→密碼原則→密碼最長有效期=180天、密碼最小長度=8 ✓ 電腦設定→Windows 設定→安全性設定→帳戶原則→帳戶鎖定原則→帳戶設定閥值=3、帳戶鎖定/重設時間=10 分鐘
4	刪除/關閉不必要帳號。	□是□否	如關閉 Guests
5	完成鐘訊校時設定	□是□否	鐘訊同步主機 140.133.2.81 或 time.windows.com
6	關閉自動播放(CD-ROM、USB)	□是□否	✓ 方法一：執行 CMD：gpedit.msc→電腦設定→系統管理範本→Windows 元件→自動播放原則 ✓ 方法二：左下角 Windows 設定→裝置→自動播放→為所有媒體與裝置使用自動播放功能→關閉
7	帳號密碼無置於顯而易見之處	□是□否	桌面上無任何可見易得的帳號密碼資訊
8	完成螢幕保護程式設定	□是□否	10 分鐘以內啟動，並點選「密碼保護」
9	安裝防毒軟體，防毒軟體病毒碼已更新至最新版。	□是□否	□Kaspersky □Windows Defender □其他＿＿＿＿＿＿
10	防毒軟體設定定期掃描	□是□否	完整掃描及弱點掃描，並修復掃描到的問題。
11	開啟 WINDOWS 系統自動更新程式	□是□否	確實進行軟體更新，修補漏洞，保持更新至最新狀態。
12	無非法及未經授權軟體。	□是□否	✓ 查看控制台→新增/移除程式、查看程式集。 ✓ 如有發現來路不明或未授權檔案，請立即移除。例如 winrar、teamviewer、AnyDesk ✓ 如有 P2P 分享軟體，請立即移除。
13	其他軟體之更新	□是□否	Office 應用程式、Adobe Acobat Reader、Java 更新、其他合法軟體的更新狀況
14	電腦檔案及 Mail2000 郵件之刪除	□是□否	電腦檔案及 Mail2000 郵件刪除後，務必立即清理資源回收桶(垃圾桶)。

管理人	檢核人	單位主管	資通安全官

1.電腦系統帳號密碼設定

- 檢查說明：
  - 系統重新開機查看是否需要登入帳號。

2.完成稽核原則設定

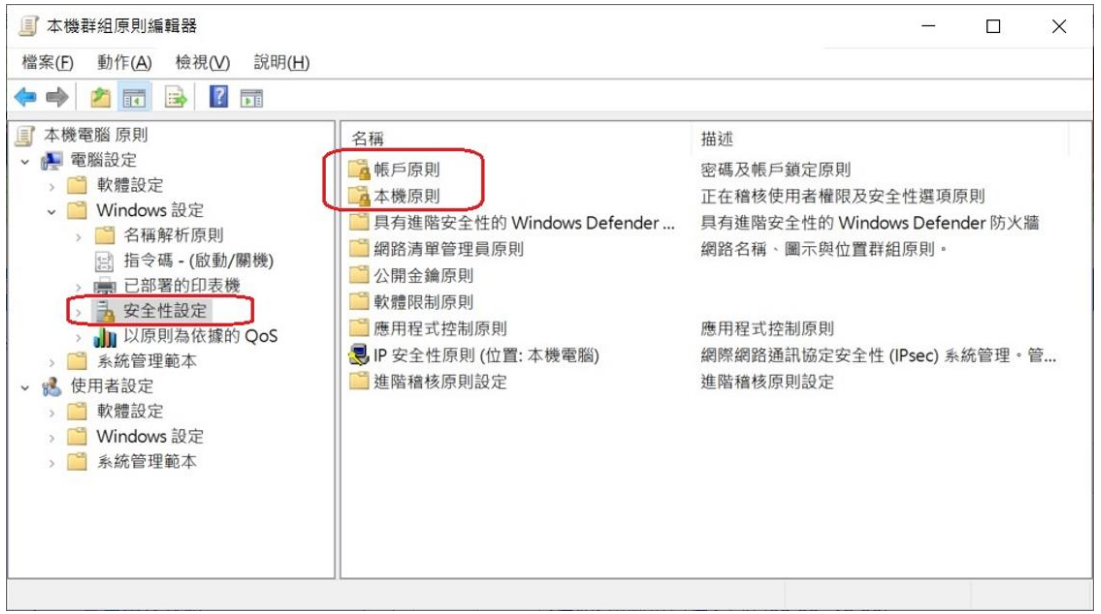
- 檢查說明：
  - 執行CMD：gpedit.msc
  - 電腦設定→Windows設定→安全性設定→本機原則→稽核原則→每個項目的「成功/失敗」全部開啟。

3.完成密碼原則設定

- 檢查說明：
  - 執行CMD：gpedit.msc
  - 電腦設定→Windows設定→安全性設定→帳戶原則→密碼原則→密碼最長有效期=180天、密碼最小長度=8 。
  - 電腦設定→Windows設定→安全性設定→帳戶原則→帳戶鎖定原則→帳戶設定閥值=3、帳戶鎖定/重設時間=10分鐘。

◆項次2、3執行步驟說明

- 於Windows視窗「搜尋列」輸入gpedit.msc後按enter鍵。
- 出現「本機群組原則編輯器」畫面，點選『電腦設定→Windows設定→安全性設定』進行變更設定 。

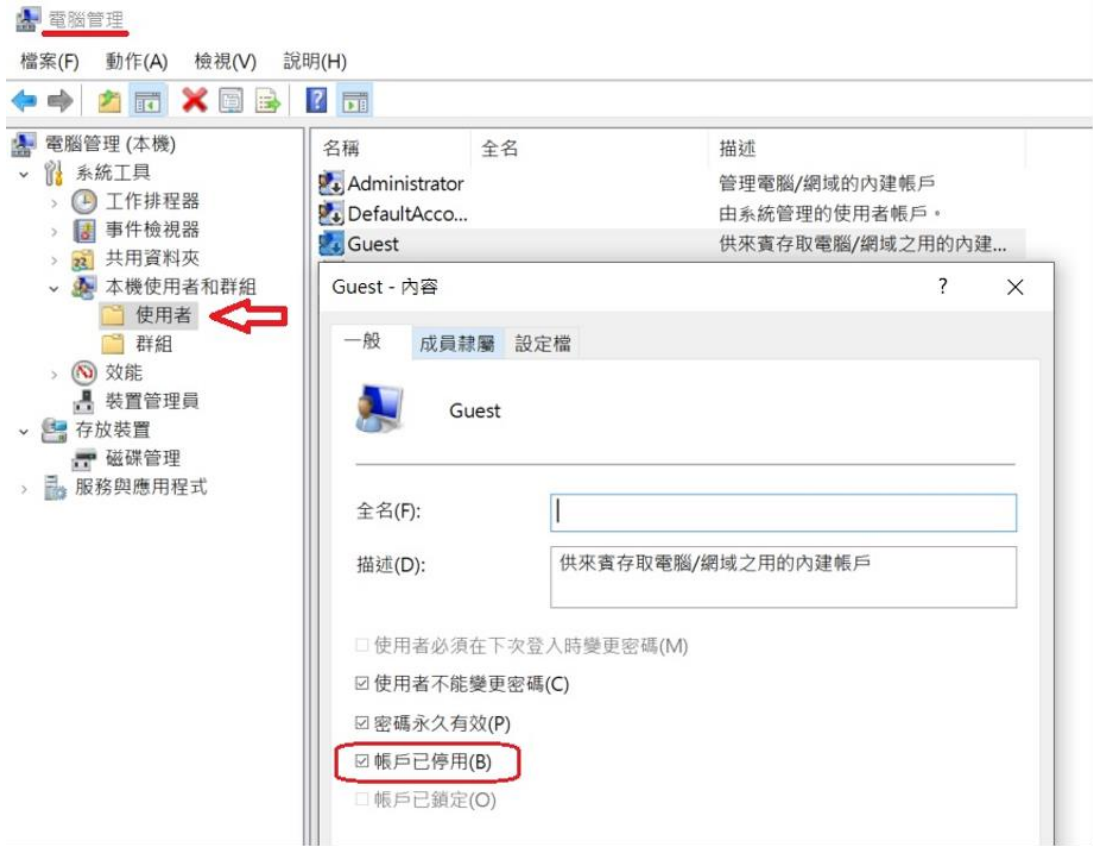


4.刪除/關閉不必要帳號

- 檢查說明：
  - 如關閉Guests。

◆項次4執行步驟說明

- 點選執行「開始 / Windows系統管理工具 / 電腦管理」。
- 出現右方畫面，點選本機使用者和群組之使用者，點選Guest帳號，確認Guest帳號已停用。



5.完成鐘訊校時設定

- 檢查說明：
  - 鐘訊同步主機140.133.2.81或time.windows.com。

◆項次5執行步驟說明

- 開啟控制台，點選在「日期和時間」，切換至「網際網路時間」。
- 點選「變更設定」，設定網際網路時間時間伺服器。（140.133.2.81或time.windows .com）。

6.關閉自動播放（CD-ROM、USB）

- 檢查說明：
  - 方法一：執行CMD：gpedit.msc→電腦設定→系統管理範本→Windows元件→自動播放原則（參考項次2、3之步驟）。
  - 方法二：左下角Windows設定  →裝置→自動播放→為所有媒體與裝置使用自動播放功能→關閉。

7.帳號密碼無置於顯而易見之處

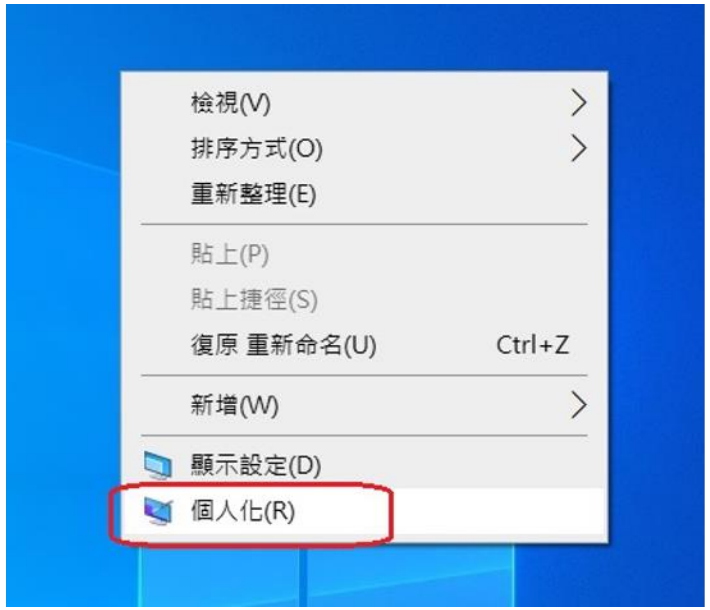
- 檢查說明：
  - 桌面上無任何可見易得的帳號密碼資訊。

8.完成螢幕保護程式設定

- 檢查說明：
  - 10分鐘以內啟動，並點選「密碼保護」。

◆項次8執行步驟說明（1/2）

- 於電腦桌面點按滑鼠右鍵，出現選單點選「個人化」。
- 點選「鎖定畫面」，再點選「螢幕保護設定」。設定等候時間為10分鐘，並勾選「繼續執行後，顯示登入畫面」。



◆項次8執行步驟說明（2/2）

9.安裝防毒軟體，防毒軟體病毒碼已更新至最新版

- 檢查說明：
  - 啟動Windows Defender

◆項次9執行步驟說明

- 點選執行「設定 / 更新與安全性 / Windows安全性 / 防火牆與網路保護」。
- 確認防火牆已開啟。

10.防毒軟體設定定期掃描

- 檢查說明：
  - 完整掃描及弱點掃描，並修復掃描到的問題。

◆項次10執行步驟說明

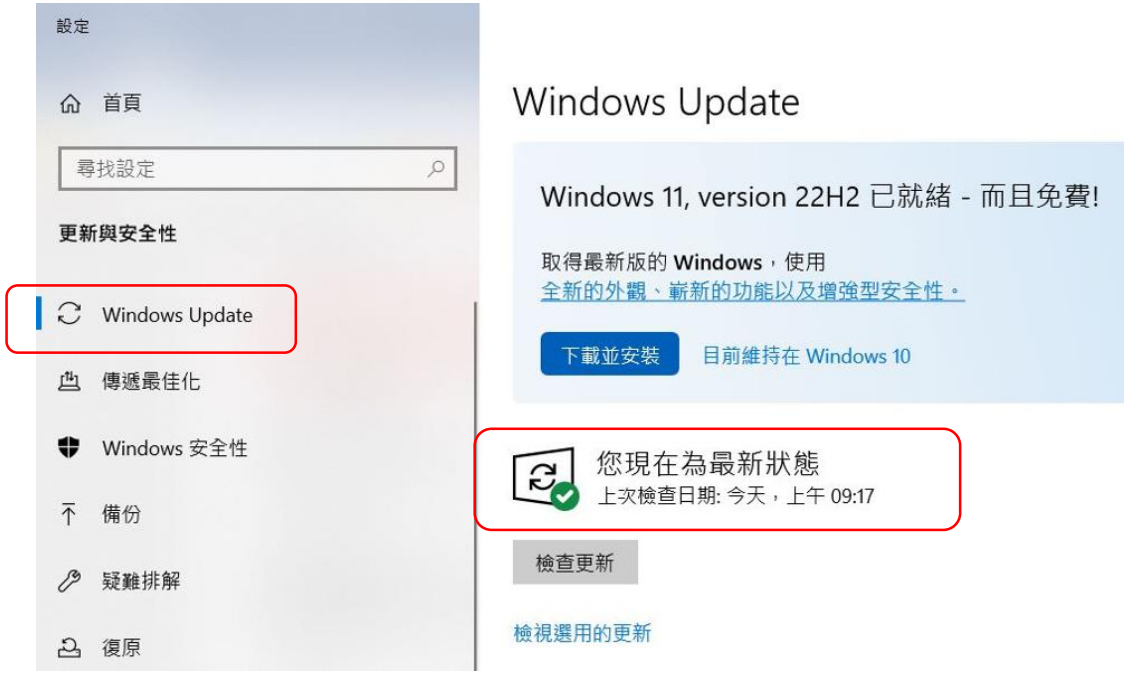
- 點選執行「設定 / 更新與安全性 / Windows安全性 / 病毒與威脅防護」。
- 確認「沒有目前的威脅」。

11.開啟WINDOWS系統自動更新程式

- 檢查說明：
  - 確實進行軟體更新，修補漏洞，保持更新至最新狀態。

◆項次11執行步驟說明

- 點選執行「設定 / 更新與安全性 / WindowsUpdate。
- 點選「檢查更新」，確認「現在為最新狀態」。



12.無非法及未經授權軟體

- 檢查說明：
  - ➢ 查看控制台→新增/移除程式、查看程式集。
  - ➢ 如有發現來路不明或未授權檔案，請立即移除。例如winrar、teamviewer、AnyDesk
  - ➢ 如有P2P分享軟體，請立即移除。

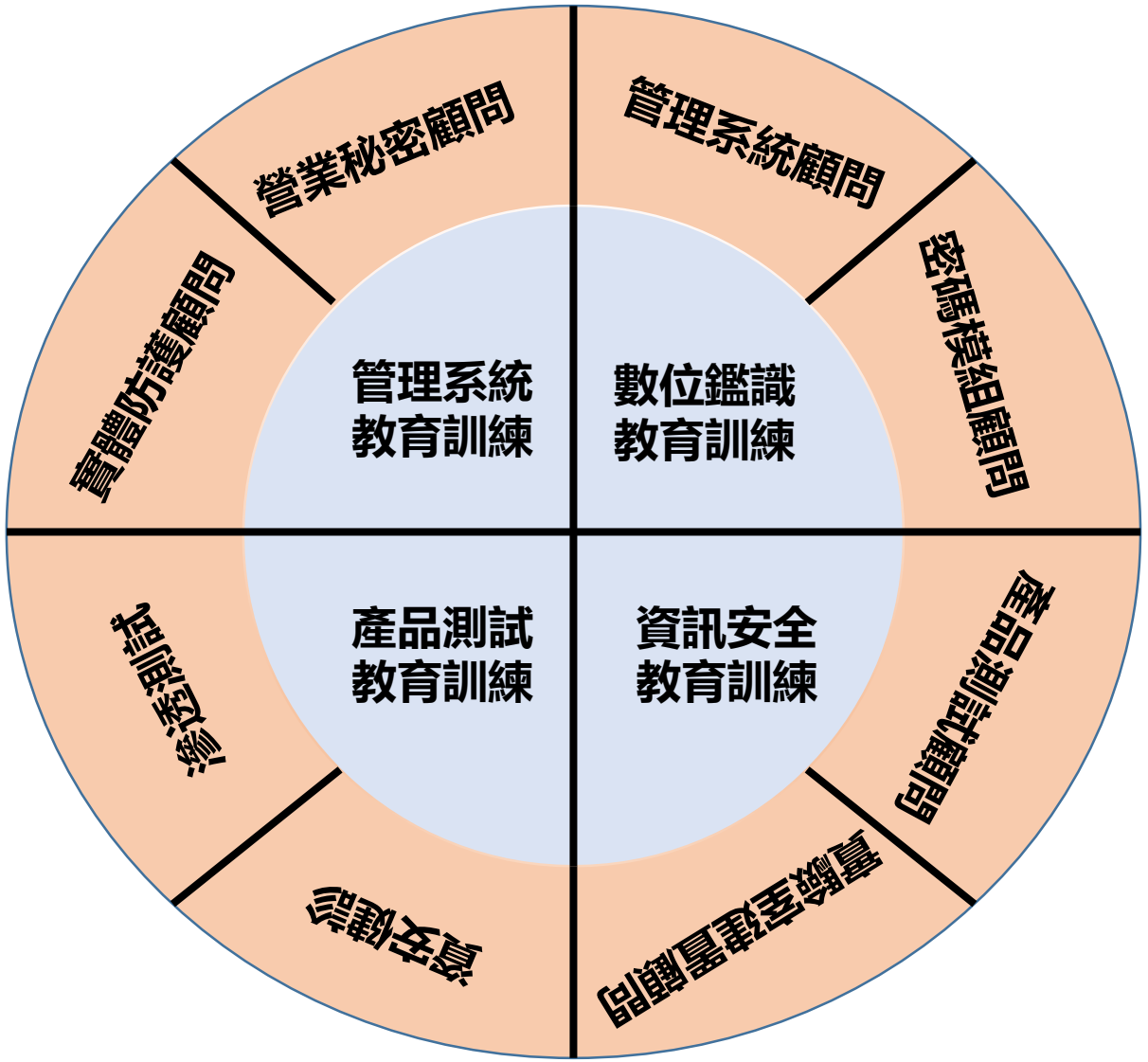
✓ 著作權法第91-1條...侵害他人之著作財產權者，處三年以下有期徒刑、拘役，或科或併科新臺幣五十萬元以下罰金。

13.其他軟體之更新

- 檢查說明：
  - Office應用程式、Adobe Acobat Reader、Java更新、其他合法軟體的更新狀況。

14.電腦檔案及Mail2000郵件之刪除

- 檢查說明：
  - 電腦檔案及Mail2000郵件刪除後，務必立即清理資源回收桶（垃圾桶）。


營業秘密顧問
管理系統顧問
密碼模組顧問
產品測試顧問
資訊安全顧問
資安健診
管理系統
教育訓練
數位鑑識
教育訓練
產品測試
教育訓練
資訊安全
教育訓練

優士創造您的資安優勢