數位發展部資通安全署
Administration for Cyber Security, moda

稽核常見待改善事項及建議作法

數位發展部資通安全署

111年11月

110年稽核作業
共通發現宣導事項

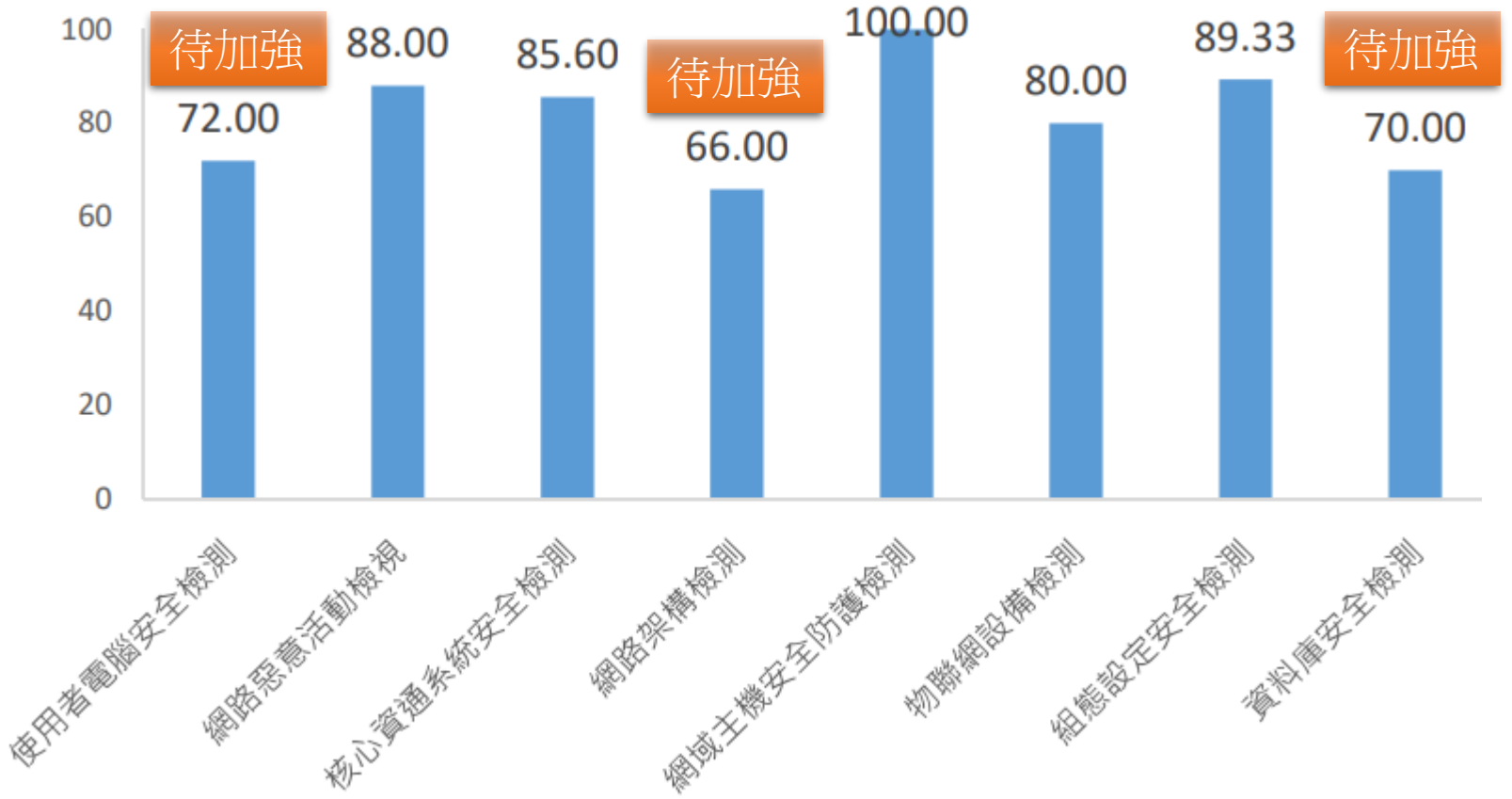
資通安全稽核

- **稽核準則**
  - 資通安全管理法及其子法、國家資通安全發展方案、受稽機關之資通安全維護計畫、CNS 27001:2014(ISO 27001:2013)、ISO 20000-1:2018
- **稽核小組**
  - 領隊1人、稽核委員至少7人(策略面2人、管理面2人、技術面3人)
- **稽核範圍**
  - 受稽機關資通安全維護計畫所含之全機關及核心資通系統各項資通安全管理政策、程序等
- **稽核方式**

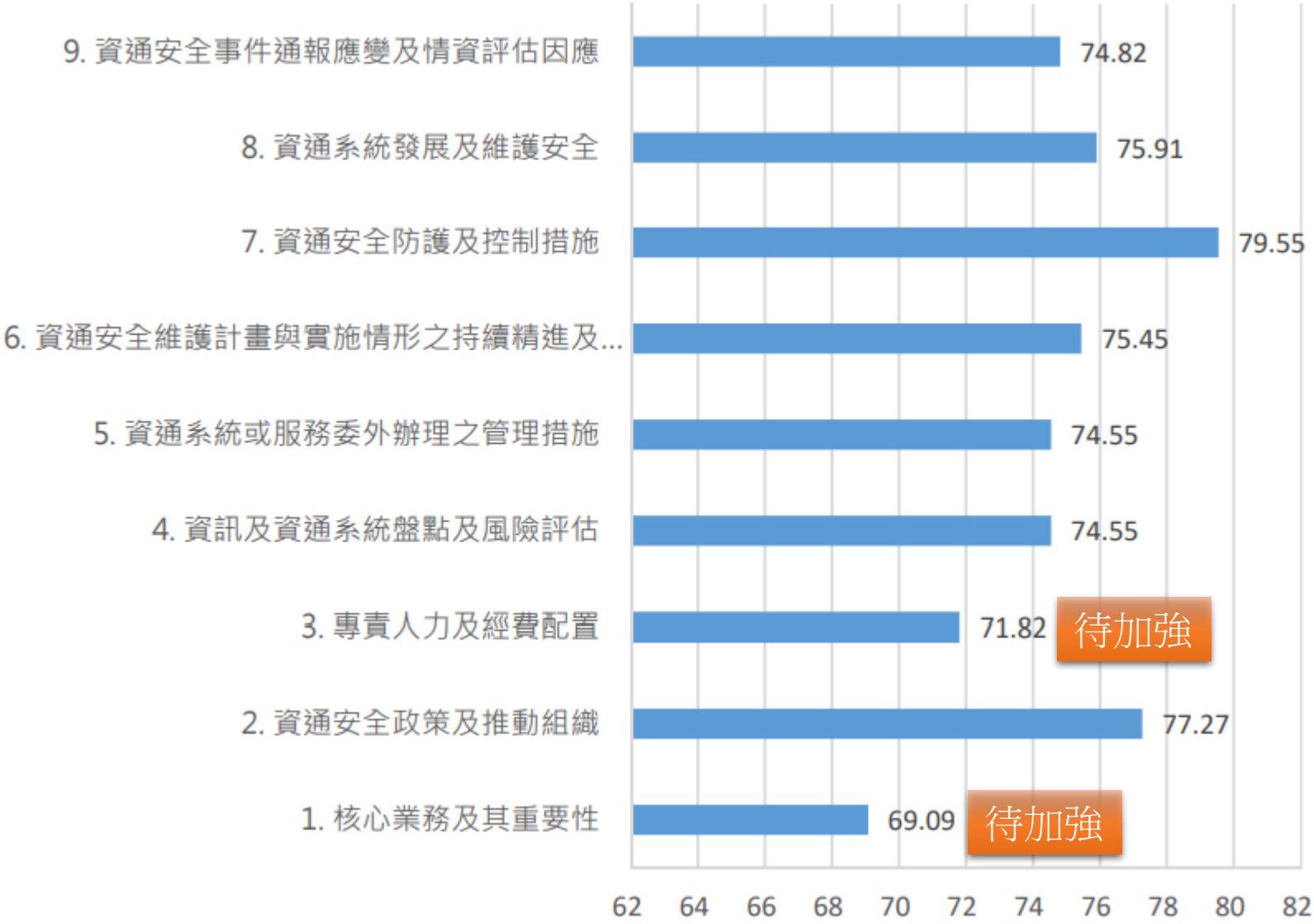
稽核分組	公務機關	特定非公務機關
技術檢測	√	
實地稽核	√	√

- **辦理稽核實務作法可參考e等公務園「111年第一次政府資通安全防護巡迴研討會」**https://elearn.hrd.gov.tw/info/10027719

資通安全稽核結果-技術檢測



資通安全稽核結果-實地稽核



策略面

核心業務/系統界定(1/3)

稽核發現

- 未落實核心業務及核心系統之界定

案例

1. 機關未列核心業務或辨識核心業務為某資通系統
2. 機關未依組織法之法定職務，評估核心業務相關使用之系統，納入資通安全維護計畫之核心系統防護中
3. 依機關資通安全維護計畫之「核心業務及重要性」，有關OO產業管理資通系統屬於核心資通系統，卻列於該計畫非核心業務及說明項目中，未落實核心業務及核心業務之界定
4. 雖已完成資通系統盤點與分級，有核心資通系統RTO(復原時間目標)達24小時，大於非核心資通系統RTO 4小時情形，其合理性待審酌

策略面

核心業務/系統界定(2/3)

稽核發現

- 未落實核心業務及核心系統之界定

法遵規定

資通安全管理法施行細則§7

核心業務範圍

①依其組織法規，該業務為核心權責所在。例如：稅務機關核心業務為稅捐稽徵、戶政機關掌理戶籍登記

②維運、提供關鍵基礎設施必要業務。例如：商港、漁港管理

③須注意非資訊相關業務亦須界定。例如：稅務機關為民服務、戶政機關戶口調查

核心資通系統

①支持核心業務持續運作必要之系統。例如：戶政機關戶役政系統

②系統防護需求分級為高等級之系統，系統機密性、完整性、可用性、法律遵循性任一構面為「高」者，為核心系統

策略面-核心業務/系統界定(3/3)

稽核發現

- 未落實核心業務及核心系統之界定

參考作法

1. 應全面盤點機關資通系統/網站，包含資訊、業務及輔助單位
2. 將所有核心業務使用之系統，納入資通安全維護計畫範圍內
3. 核心業務或核心系統如有變更，除修正維護計畫外，其實施情形亦應確實填報
4. 系統管理單位(資訊、業務或輔助單位)如有系統新增、調整等變更事宜，應主動告知系統盤點彙整單位；系統盤點彙整單位應定期檢視盤點資料是否有系統名稱或數量不一致等情形，適時提報資安長知悉
5. 整體規劃系統整併或集中管理機制，使用量低之網站評估下架，避免系統/網站數量過多，致維運難以負荷造成資安破口

策略面

維護計畫與實施情形不一致(1/2)

稽核發現

- 資通安全維護計畫與實施情形填報內容有所差異

案例

1. 110年稽核時提供之資通安全維護計畫為108年訂定，其中資安責任等級、資通系統盤點名稱及資通安全目標等，與實際執行情形不儘一致
2. 已提報資通安全維護計畫實施情形，但填報內容與執行情形有不一致情形，如：資安推動小組會議出席情形、內部稽核及技術檢測發現改善辦理期限等

策略面

維護計畫與實施情形不一致(2/2)

稽核發現

- 資通安全維護計畫與實施情形填報內容有所差異

法遵規定

資通安全管理法§10、§12

1. 公務機關應訂定、修正及實施資通安全責任等級要求之資通安全維護計畫
2. 並每年向上級或監督機關提出資通安全維護計畫實施情形

資通安全管理法§16、§17

1. 特定非公務機關應訂定、修正及實施資通安全責任等級要求之資通安全維護計畫
2. 並依中央目的事業主管機關所定特定非公務機關管理辦法提出資通安全維護計畫實施情形

參考作法

1. 資通安全維護計畫應定期檢視修正並提報資安長核定
2. 資通安全維護計畫實施情形應確實依實際執行情形提報

策略面

資通安全目標設定

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 資通安全目標設定未儘妥適，將資安事件發生次數納為量測指標

案例

1. 資通安全維護計畫目標納入資安事件不得發生之數量
2. ISMS有效性量測表訂定「資安事件發生次數上限」為量測方式，且以「每月檢視資通安全事件通報紀錄，整年不得超過目標」為其檢核方式

說明及參考作法

1. 將資安事件發生次數設為資通安全目標恐影響通報
2. 參考「數位發展部資通安全署官網/資安法規專區/範本文件/資通安全維護計畫範本」，訂定合宜之資通安全量化型目標，例如核心資通系統可用性達**9x.xx%**以上(或中斷時數/總運作時數≤0.x%)、電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於**a%**及 **b%**等、資安事件通報皆符法遵時效

策略面

資安專職/責人力

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 機關囿於資安人力資源，未妥善配置資安專職/責人力

案例

資安責任等級A級機關應配置4名資安專職人員，查資安專業證照及職能證書尚未符合法遵要求，且1位人員非專職辦理資安業務

規定

資通安全責任等級分級辦法-附表一至六

A級：至少4名資安專職/責人員

B級：至少2名資安專職/責人員　分別各自持有證照及證書各1張以上

C級：至少1名資安專職/責人員

參考作法

適度引入具資訊或資安經歷之人力協助相關作業

如暫無缺額人力可支配，得先以約聘僱或委外人員擔任

策略面

代理出席管審會議

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 管審會議常有委員代理出席情形，難以彰顯管理階層之支持及重視

案例

1. 資通安全處理小組辦理會議時，約有1/3~1/2委員由代理人出席
2. 資通安全推動組織成員僅列資訊單位，未涵蓋全機關

規定及參考作法

依資通安全管理法施行細則§6，應設置資通安全推動組織

1. 資安是全機關作業(非僅資訊單位的事)，資通安全推動組織應涵蓋全機關各單位(包含業務單位)，並由單位主管擔任成員
2. 組織成員應親自參與，避免代理出席會議，並由資安長督導出席情形及會議事項執行進度，顯示高階管理階層重視與支持
3. 管理審查會議可評估以實體與線上會議併行方式辦理

策略面

利害關係人清單

稽核發現

- 未完整建立機關內、外部利害關係人清單，並定期檢討其適宜性

案例

機關已識別內、外利害關係人，但未建立聯絡清單且無定期更新、檢討機制

規定及參考作法

ISO 27001:2013本文4及7.4

1. 利害關係人指機關資通系統維運、資安推動所涉及的內外部對象，包含上級 / 監督機關、所屬 / 所管機關、IT/OT、軟硬體或資通服務(含SOC)供應商，及與機關連線作業單位等
2. 機關應建立並即時更新內、外部利害關係人清單，以落實情資分享、事件通報的需求
3. 機關應每年向利害關係人宣導資安政策及目標，並滾動修正機關ISMS導入或通過公正第三方驗證範圍，檢視執行情形

管理面

委外管理(1/2)

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 資訊服務委外作業未於契約或建議書徵求文件明確規範防護基準需求

案例

廠商的技術與能力要求、服務水平、安全控制措施(含保密、處理人員之管理)及績效監控(稽核)與報告機制等，未明訂於管理程序及合約規範中，或未落實執行

規定

資通安全管理法施行細則§4

委外作業安全應建立相關管理程序

資通系統籌獲各階段資安強化措施(行政院院臺護字第1110174630號函)

廠商資安管理作業自我評估表(範例)

管理面

委外管理(2/2)

稽核發現

- 資訊服務委外作業未於契約或建議書徵求文件明確規範防護基準需求

參考作法

1. 公告招標時即應說明系統防護需求等級，俾據以納入履約要求
2. 可參考「技服中心網站/資安業務與服務/資安服務」各項資安服務RFP範本
3. 確保SOC營運符合合約服務水準協定(SLA)
   - ①資通安全威脅偵測管理(SOC)服務RFP範本(v5.0)
   - ②政府資訊作業委外資安參考指引
   - ③資訊服務採購契約範本

管理面

資通系統及資訊之盤點(1/2)

稽核發現

- 已辦理資訊資產盤點作業，惟盤點範圍與內容完整性不足

案例

1. 部分機關(構)之業務單位個人電腦並未納入資產清冊，資產清冊僅被動接受各單位異動通知
2. 核心系統所使用之資料庫版本已停止支援，且其主機作業系統授權已過期，無法進行安全性更新

規定

資通安全管理法施行細則§6

1. 委外作業應建立相關管理措施
2. 辦理資訊資產盤點並建立資產清冊

管理面

資通系統及資訊之盤點(2/2)

稽核發現

- 已辦理資訊資產盤點作業，惟盤點範圍與內容完整性不足

參考作法

1. 資訊資產盤點範圍須包含機關全部單位，非僅限資訊單位
2. 應掌握各單位資料，並定期比對盤點資料是否有落差(如系統名稱及整體數量不一致)，建議強化資訊資產清冊即時異動機制
3. 運用計畫經費所籌獲之資通系統亦應納入盤點
4. 進行資產價值鑑別及風險評估，對於已停止服務或移轉他機關之系統，應落實資產異動管理程序
5. 建議於資產盤點發現軟、硬體設備老舊問題時，應及早規劃系統更新作業，以免問題持續累積，增加處理困難

管理面

受託者資通安全稽核(1/2)

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 機關辦理委外廠商稽核作業無記錄相關查核證據，且無追蹤管考機制

案例

1. 查有機關之系統維運未落實資通安全管理施行細則規定，部分系統於〇年營運至今，未定期對委外廠商辦理資安稽核
2. 機關已對核心資通系統之委外廠商進行稽核，並規劃每年完成所有資通系統委外廠商之稽核作業，惟未確認所有廠商均已完成稽核

規定

資通安全管理法施行細則§4

落實定期或於知悉受託者發生可能影響受託業務之資通安全事件時，對受託者辦理稽核或其他適當方式，以確認受託業務之執行情形

管理面

受託者資通安全稽核(2/2)

稽核發現

- 機關辦理委外廠商稽核作業無記錄相關查核證據，且無追蹤管考機制

參考作法

1. 辦理委外廠商稽核作業時，建議將開發維運環境，如專案辦公室等納入稽核查檢表，並逐年將非核心系統納入委外廠商稽核範圍，以落實委外管理
2. 機關應將對受託者之稽核機制、對稽核結果之追蹤管考機制，納入契約中，並完整記錄查核證據，落實執行
3. 建議機關可再查核委外廠商稽核作業之完成度，以確認作業之有效性

參考e等公務園「111年第一次政府資通安全防護巡迴研討會」
https://elearn.hrd.gov.tw/info/10027719

管理面

內部資通安全稽核(1/2)

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 機關已規劃執行內部資通安全稽核作業，惟稽核計畫內容不完整

案例

1. 部分機關2次法定內部稽核間隔過近
2. 內部稽核應明確訂定年度稽核計畫，部分機關僅以其上級機關之資安內部稽核計畫，以抽樣方式辦理內部稽核，稽核對象未涵蓋全機關。另有發現總公司與分處(分公司)分別為不同資通安全責任等級，惟僅總公司訂有110年資通安全內部稽核計畫，對分處(分公司)則採抽樣方式辦理內部稽核
3. 部分機關(構)稽核範圍過於簡略，應包括稽核之依據與目的、期間、稽核團隊組成方式、保密義務、稽核方式、基準與項目及受稽單位協助事項，並應將前次稽核結果納入稽核範圍

管理面

內部資通安全稽核(1/2)

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 機關已規劃執行內部資通安全稽核作業，惟稽核計畫內容不完整

規定

資通安全管理法施行細則§6

應訂定資通安全維護計畫，包括資通安全推動組織

資通安全管理法§ 13與資通安全責任等級分級辦法應辦事項

辦理內部資通安全稽核作業

參考作法

1. 建議事前擬定年度稽核計畫(包括內稽頻率、時程、準則、檢核項目、方式、範圍等) ，每年2次稽核宜間隔半年
2. 建議所屬(管)機關(構)宜訂定內部資通安全稽核計畫，包含稽核目標、範圍、時間、程序及人員等，且須落實執行
3. 建議依實際分組查核方式，詳細列出稽核項目，並檢視範圍之合宜性

技術面

安全性檢測及資通安全健診(1/3)

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 已進行資通系統安全性檢測及資通安全健診等作業，惟後續修補作業未落實執行，且無訂定相關作業程序進行後續追蹤

案例

1. 機關雖已定期辦理弱點掃描，惟未針對弱點進行修補作業，針對不進行修補之中高風險弱點，亦未有評估與審核機制
2. 核心系統中含有Broken Access Control問題，該系統在近2年屢次出現相同弱點，代表過往緩解措施無效，應儘速修補
3. 針對安全性檢測及資通安全健檢結果修補作業，查有高風險弱點已逾年未完成修補

技術面

安全性檢測及資通安全健診(2/3)

稽核發現

- 已進行資通系統安全性檢測及資通安全健診等作業，惟後續修補作業未落實執行，且無訂定相關作業程序進行後續追蹤

法遵規定

資通安全責任等級分級辦法-資通系統防護基準

1. 系統與服務獲得：於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務與埠口
2. 系統與資訊完整性：系統之漏洞修復應測試有效性與潛在影響，並定期更新
3. 系統與資訊完整性：定期確認資通系統相關漏洞修復之狀態

技術面

安全性檢測及資通安全健診(3/3)

稽核發現

- 已進行資通系統安全性檢測及資通安全健診等作業，惟後續修補作業未落實執行，且無訂定相關作業程序進行後續追蹤

參考作法

1. 修訂相關程序文件(維護計畫、查檢表)，訂定標準化程序，例如針對不同等級風險訂定修補期限，落實執行，並適時提報資安長及資安推動小組會議知悉
2. 建議可自「技服中心網站/資安防護訊息/共通規範/參考指引」下載「資通系統防護基準驗證實務參考指引」，參考安全性檢測、滲透測試等各項作業之驗證確認實務

技術面

系統與服務獲得(1/2)

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 已訂定系統開發、測試、驗收、上線等相關程序，惟內容未臻完善，且未完整保留版本更新過程與紀錄，另系統分析與設計文件未及時更新與納管

案例

1. 資通系統發展應留存相關文件，查OOO資料庫於OOO年O月OO日更新之程式無相關紀錄文件，應予以改善
2. 應進行資訊處理設備安全管理，查OOO系統未追蹤系統版本更新狀態，僅被動等待廠商更新，恐致資安風險

法遵規定

資通安全責任等級分級辦法-資通系統防護基準

系統與服務獲得(SSDLC)

技術面

系統與服務獲得(2/2)

稽核發現

- 已訂定系統開發、測試、驗收、上線等相關程序，惟內容未臻完善，且未完整保留版本更新過程與紀錄，另系統分析與設計文件未及時更新與納管

參考作法

1. 所有系統(包含業務單位管理之系統)皆應落實SSDLC各階段作業，保留各版本及更新過程與紀錄
2. 參考「資通系統委外開發RFP資安需求範本(V2.0)-附件1資通系統資安需求項目查檢表」，設計發展系統安全需求檢核表，供相關人員在發展系統安全需求時運用
3. 應透過機關資安推動小組會議(管審會)、內部稽核等方式確認各單位系統籌獲各階段辦理及相關規定落實情形
4. 針對全機關之資安規定(含SSDLC)，可適時提報資安長知悉，有助於跨單位協調，以加強推動力道及機關整體落實度

技術面

系統與資訊完整性(1/2)

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 針對資通系統所使用之外部元件或軟體，缺乏更新、管控機制

案例

1. 應建立外部元件或軟體安全通告更新與修補機制，並定期評估更新，查並未落實執行，應儘速修正
2. 目前核心系統使用外部元件OOO版本為OOO已存在弱點且版本過舊，應改善之

法遵規定

資通安全責任等級分級辦法-資通系統防護基準

系統與資訊完整性

技術面

系統與資訊完整性(2/2)

稽核發現

- 針對資通系統所使用之外部元件或軟體，缺乏更新、管控機制

參考作法

1. 定期追蹤相關軟硬體設備EOS(End of Service，停止支援)情形，並提早預為因應
2. 確認採用之軟體與元件，已使用最新之穩定版本或該版本已排除所有已知安全漏洞，並納入驗收程序
3. 針對相關元件或軟體之安全性漏洞通告(透過CVE Details網站、廠商安全通告等)，應落實評估更新，並關閉資通系統不必要之服務及埠口，如以WSUS定期派送安裝Windows作業系統更新

技術面

網路架構安全性

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

- 網路架構安全性仍顯不足，如網段區隔、存取控管未確實

案例

1.機關未依需求設定使用者與內部伺服器網段間之存取控制，避免使用者存取不需要之資源
2.機關未針對使用者與外點人員對伺服器與資料庫網段間，依需求設定存取控制及防火牆規則

規定與參考作法

資通安全責任等級分級辦法應辦事項
資通安全健診-網路架構檢視

1.不同作業需求(開發、測試及正式環境)，區隔不同的設備及網段
2.應依最小權限原則，限制能存取的資源(來源/目的IP、連線埠等)
3.一角色對應一帳號，避免同帳號擁有多重角色

技術面

資安事件通報及應變 (1/3)

稽核發現

- 辦理資安事件通報及應變演練，惟未納入事件通報環節
- 機關自訂之通報應變程序，與通報應變辦法不符

案例

1. 演練情境以災害復原演練為主，著重於設備故障判斷與復原能力
2. 演練範圍僅以資訊單位為主
3. 機關自訂之通報應變程序，將中毒定義為非資安事件，不符通報應變辦法規定
4. 機關自訂之通報應變程序，未納入事後矯正預防追蹤機制
5. 機關收到EWA警訊，查證後確有符合資安事件定義情形，但未通報

技術面

資安事件通報及應變 (2/3)

數位發展部資通安全署
Administration for Cyber Security, moda

稽核發現

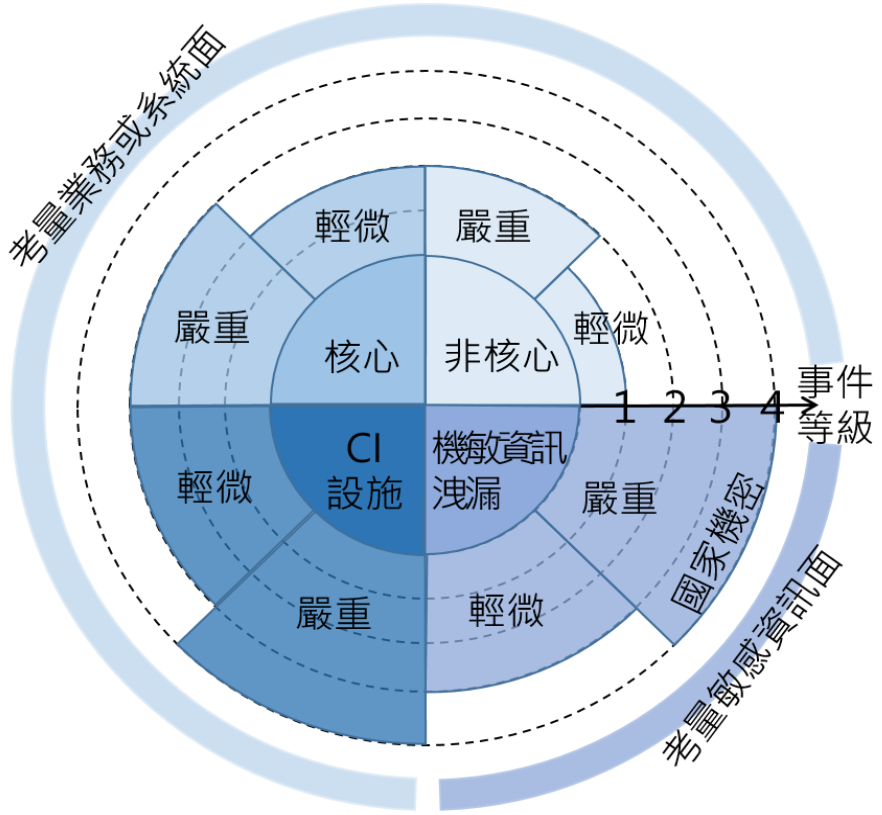
- 辦理資安事件通報及應變演練，惟<u>未納入事件通報環節</u>
- 機關自訂之通報應變程序，與通報應變辦法不符

規定

<u>資通安全通報及應變辦法</u>

事件輕微或嚴重-考慮C,I,A三面向

- 機密性(C)
  - 業務資訊遭洩漏
- 完整性(I)
  - 業務資訊遭竄改
  - 資通系統遭竄改
- 可用性(A)
  - 資通系統受影響或停頓
  - 是否於可接受時間內回復



技術面

資安事件通報及應變 (3/3)

稽核發現

- 辦理資安事件通報及應變演練，惟未納入事件通報環節
- 機關自訂之通報應變程序，與通報應變辦法不符

參考作法

1. 以業務為導向，演練情境並可參考資安威脅趨勢，納入複合式情境，如：天然災害、勒索軟體、DDoS攻擊、個資外洩處理及資安事件通報等
2. 擴大演練範圍至相關業務單位，而非僅限資訊單位

技術面

資料庫安全檢測

稽核發現

- 未設定使用加密傳輸，或已啟用TLS 1.2傳輸協定，但資料庫未啟用「強制加密」設定
- 未針對資料庫主機定期執行弱點掃描
- 備份檔案未進行加密保護
- 未限制僅授權對象可對資料庫進行存取

參考作法

1. 設定資料庫帳號鎖定機制
2. 強化帳號安全性，針對未使用之預設管理帳號，應變更帳號名稱並停用
3. 資料庫應採用適當保護與安全傳輸機制，強化資料儲存與傳輸安全性，並定期進行資料庫主機校時，確保稽核軌跡之時間正確性
4. 建議定期執行資料庫主機弱點掃描，掌握風險現況

近期重要宣導事項

DNS安全強化

DNS安全強化

1. 確認已將DNS快取主機設定指向GSN Cache DNS(210.69.1.1 與 210.69.2.1)
2. 為避免誤使用DNS快取服務，請設定防火牆限制TCP 53埠及853埠的連線對象
3. 採自建DNS權威主機(Authoritative DNS)提供服務者，請評估其必要性及關閉不必要的DNS開放解析(open DNS resolver)，並請妥為防護以降低該主機遭受攻擊(如DDoS)之影響
4. 啟用DNS分析紀錄功能，至少保存6個月，並定期檢視

主機或系統安全強化

主機或系統安全強化

1. 確認無使用弱密碼，密碼長度及複雜度應符合政府組態基準(GCB)

係指容易被猜出來的密碼
例如身分證字號/生日/電話等個人資訊
或是1234567等具簡單規則的密碼

2. 避免使用明文傳輸協定，應關閉SSLv2協定

3. 落實軟硬體韌體更新及漏洞修補(技服中心網站/資安防護訊息/漏洞警訊公告、重大漏洞專區)

定期更新
惡意中繼站清單

定期更新惡意中繼站清單

- 於防火牆等資安防護設備定期(至少每週)更新惡意中繼站清單，以技服中心提供惡意中繼站清單為基礎，增列機關自有防護規則，確保資安防護即時有效

黑名單下載方式

- 登入通報網站，在資安訊息公告之重要公告事項
- 每週四之公告事項，會提供完整版惡意中繼站清單(其餘日期公告事項內容僅註記增加/刪除之DN/IP)

強化資安弱點通報機制(VANS)

資通安全弱點通報機制(VANS)

數位發展部資通安全署
Administration for Cyber Security, moda

法遵事項

資安責任等級B級以上之公務機關及關鍵基礎設施提供者應於**111年8月23日**前導入資通安全弱點通報機制，C級之公務機關及關鍵基礎設施提供者應於112年8月23日前導入

宣導事項

每日：應注意弱點通知，當發現CVSS 7分以上之弱點，應儘速確認處置方式，並於1週內填寫改善措施**(尚未修補前應有控制措施並加強監控)**

每月：更新資訊資產，如接獲重大弱點通報或大量資產異動，應即時進行資訊資產更新作業

- 完整教材：請至「技服中心網站/資安業務與服務/資通安全弱點通報機制(VANS)專區/教育訓練教材」

  111年資通安全弱點通報機制(VANS)實作訓練課程

資通安全弱點通報機制(VANS)-常見問題

4.14. 應辦事項列表中VANS導入範圍為何？建議之上傳頻率？

(1)公務機關VANS導入範圍以全機關之資訊資產為原則

(2)有關資訊資產上傳頻率，除重大弱點通報或大量資產異動外建議每個月至少定期上傳1次，並應針對發現弱點設定修補期限

4.15.應辦事項列表中VANS所稱「資訊資產」為何？如何執行盤點作業？是否有相關參考資料供導入參考？

(1)「資訊資產」係指伺服器主機及使用者電腦之作業系統及應用程式等軟體資訊

(2)導入VANS之資訊資產盤點資料， 為彙總性之盤點資料，僅含比對所需之必要欄位資訊，包含「資產名稱」、「資產版本」及「數量」等

(3)提交作業流程，可參考技服中心網站/資安業務與服務/資通安全弱點通報機制(VANS)專區

資通安全弱點通報機制(VANS)-上傳資料檢查

- 請於上傳資訊資產前，先行檢視欲上傳資產內容之合理性，如利用CPE條目或資產名稱，檢視上傳作業系統數與實際導入電腦數量之差異，以評估資產盤點之合理性

步驟2.將欲上傳資產之作業系統加總

步驟1.利用關鍵字「:o:」進行篩選

機關OID	機關名稱	資產數量	資產名稱	資產廠商	資產版本	CPE 2.3	CPE完整名稱
NCCST	技服中心	1	Windows Server 2012 R2 St	Microsoft Corparation	N/A	cpe:2.3:o:microsoft:windows_server_2012:r2:*:*	Microsoft Windows Server 2012 R2 Standard
NCCST	技服中心	1	Windows Server 2019 Datac	Microsoft Corparation	1809	cpe:2.3:o:microsoft:windows_server_2019:-:*:*	Microsoft Windows Server 2019 Datacenter
NCCST	技服中心	1	Microsoft Visual C++ 2008 R			N/A	
NCCST	技服中心	2	Microsoft Silverlight			N/A	
NCCST	技服中心	1	VMware Tools			N/A	
NCCST	技服中心	1	Microsoft Visual C++ 2008 R			N/A	
NCCST	技服中心	1	Apache Tomcat 9.0 Tomcat9			cpe:2.3:a:apache:tomcat:9.0.16:*:*:*:*:*:*:*	Apache Software Foundation Tomcat 9.0.16
NCCST	技服中心	1	Microsoft Office 專業增強版			cpe:2.3:a:microsoft:office:2019:*:*:*:*:-:*:*	Microsoft Office 2019
NCCST	技服中心	1	MySQL Workbench 8.0 CE			N/A	N/A
NCCST	技服中心	1	Java 8 Update 202 (64-bit)	Oracle Corporation	8.0.2020.8	cpe:2.3:a:oracle:jre:1.8.0:update_202:*:*:*:*:*:*	Oracle JRE 1.8.0 Update 202

部分作業系統可能有未比對到CPE條目之情形，則可用資產名稱進行搜尋

cpe:2.3:o:microsoft:

產品類別

產品類別為「o」表示為作業系統

步驟3.比較實際導入電腦數量與欲上傳作業系統數之差異，以評估資產盤點之合理性

禁止使用或採購
大陸廠牌資通訊產品

禁止使用或採購大陸廠牌資通訊產品

- 行政院109.12.18函各公務機關禁止使用及採購大陸廠牌資通訊產品(含硬體、軟體及服務)
- 近期有大陸產品以非大陸廠牌方式，參與採購情形(如監視器、智慧黑板)。建議各機關採購資通訊產品時，在招標文件中要求投標廠商聲明產品組成資訊，作為採購參考，以避免誤採購具高風險危害安全之資通訊產品
- 各機關自行或委外營運，提供公眾活動或使用之場地，不得使用大陸廠牌資通訊產品(含軟體、硬體及服務)。機關應將前段規定事項納入委外契約或場地使用規定中，並督導辦理；如已簽約，則須調整契約或執行風險管制措施

行動裝置資安防護

行動裝置資安防護

- 現行公務處理多依賴手機裝置，需更重視其機密性、完整性及可用性之資安防護議題
- 針對美國眾議院議長來訪期間，發現有機關業務主管手機門號遭盜用

行動裝置防護建議

- 現行作法：依行政院國家資通安全會報技術服務中心「**行動裝置資通安全注意事項**」，如不開啟藍牙、密碼、軟體安裝注意事項等**資安防護**作為

技服中心網站/資安防護訊息/共通規範

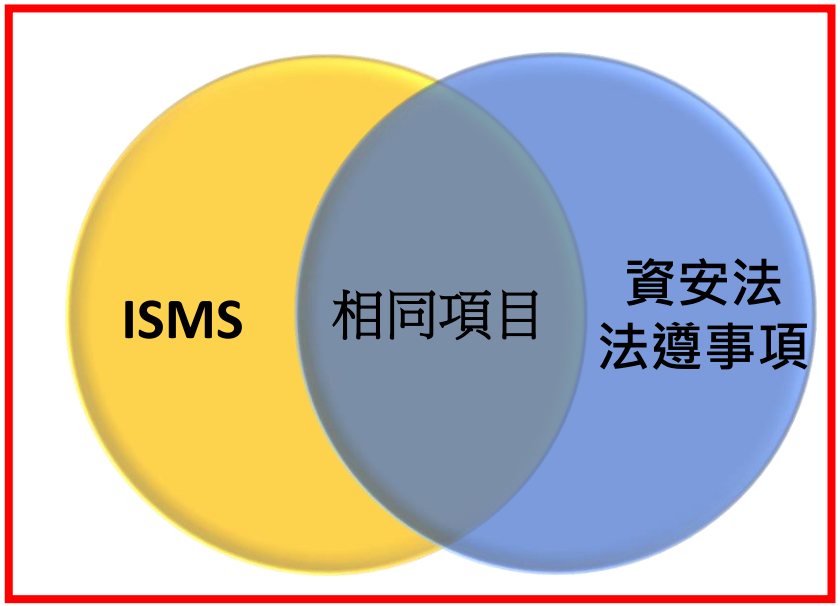
- 精進建議

方法	保護對象	特色
安裝防毒軟體	重要幕僚之行動裝置	操作簡便，可快速導入，並防範手機病毒
納入機關防毒機制，或進一步納入機關資訊安全監控中心(SOC)保護	公務手機/平板(行動裝置)	可自動派送更新病毒碼，惟裝置持有者所安裝軟體須經申請並接受偵測
安裝裝置管理軟體(MDM)	國安/軍事單位之行動裝置	相對嚴謹，但行動裝置可安裝的所有軟體均嚴格管制，使用限制多(如鎖定照相、網路連線等功能)

資通安全管理法
驗證方案特定要求

資通安全管理法驗證方案特定要求

- 為加速推動資安法法遵落實，刻正規劃於「資訊安全管理系統認證領域」項下(ISMS)，增加「資通安全管理法驗證方案特定要求」，由公正第三方驗證機構進行驗證



資安法特定要求驗證之驗證範圍
原ISMS驗證項目+資安法規定項目

資安法驗證方案追加稽核項目

- 資安維護計畫實施情形
- 資安責任等級應辦事項
- 資通系統防護基準

資通安全管理法驗證方案特定要求

- 請各機關於辦理ISMS驗證時，納入驗證方案特定要求
- 本項要求將規劃納入資通安全管理法修法

最後更新日期： 2022/04/30 點閱次數： 80

本會自111年5月1日起，開放受理「資通安全管理法驗證方案」之認證服務。

一、行政院資安處制定「資通安全管理法」，以期積極推動國家資通安全政策，加速建構國家資通安全環境，以保障國家安全，維護社會公共利益。因應國家推動「資通安全管理法」之政策，落實公務機關與特定非公務機關之法令遵循義務。

二、本會制定「管理系統驗證機構資通安全管理法驗證方案特定要求」，並自111年5月1日起正式開放「資通安全管理法驗證方案」之認證服務。

三、本會認證服務之相關資訊，請參見本會網站https://www.taftw.org.tw/文件專區/認證方案/管理系統驗證機構文件。

資安長設置

資安長異動更新

- **設置依據**：資通安全管理法第11條
- **資安長出缺之因應作為**：於機關資安長職務出缺、尚未派員遞補時，應依「各機關職務代理應行注意事項」，由法定代理人職務代理，確保相關資安業務順暢運行
- **即時更新**：至「國家資通安全通報應變網站」更新資安長資訊，以利資安事件即時通報，並適時掌握資安重點政策

數位發展部資通安全署

Administration for Cyber Security, moda

資安是持續精進的風險管理