108 年政府機關(構)資通安全稽核作業

共同發現事項

108 年稽核結果共同發現事項分從策略面、管理面及技術面說明如下：

一、策略面

(一)資通系統分級

1、說明：未有效落實核心業務及核心資通系統之界定。

2、建議：應依據資通安全管理法施行細則第 7 條，確實界定機關核心業務及核心資通系統，並依據資通安全責任等級分級辦法完成資通系統分級，及完成相對應之控制措施。

(二)資安維護計畫

1、說明：資安維護計畫與內部 ISMS 規範文件不一致，且未納入資安法規要求。

2、建議：因應資通安全管理法之施行，各機關應重新檢討機關內部資安規範與資通安全管理法之合規性，並配置資源確實執行。

(三)資安推動組織

1、說明：資通安全相關法遵及技術知能要求與日俱增，惟受稽機關常因資安人力資源缺乏未配置專職/責人力。

2、建議：機關應依資通安全管理法規定，重新檢視目前資安人力配置與運用情形，於機關總員額範圍內，優先調配資安專職人員，並結合資安專業訓練，培養機關所需之資安專職人力。

二、管理面

(一)資安法規認知

1、說明：受稽機關人員與委外廠商對於資安相關法規認知仍顯不足。

2、建議：各機關應配合資通安全管理法施行，透過教育訓練、內部會議、張貼公告等方式，落實並宣導資通安全管理法之法遵事項。

(二)委外管理

1、說明：未依資通安全管理法等規範事項規劃與落實資訊委外作業。

2、建議：各機關應強化監督及管理委外廠商之權責，加強自身管理能力，並依據資通安全管理法規定及參考「政府資訊作業委外安全參考指引」辦理資訊委外管理作業。

(三)上級機關監督管理

1、說明：上級機關未依所屬或監督機關之資通安全責任等級，規劃適當之稽核整體計畫(包含明訂受稽機關遴選原則、依機關資安責任等級需求規劃檢核表等)，以致影響稽核執行成效。

2、建議：公務機關對於所屬或監督機關之第二方稽核作業，建議訂定整體稽核計畫，包含期間、重點領域、稽核方式、基準及項目等，以落實對所屬或監督機關之監督管理。

三、技術面

(一)網路架構安全

1、說明：網路架構安全性仍顯不足，未確實進行網段區隔及存取控管。

2、建議：各機關應針對網路架構建立定期檢視政策，透過網路架構全面性檢視，持續強化網路架構相關安全防護。

(二)資訊系統開發安全

1、說明：資通系統安全開發程序未納入資通系統防護需求且未落實。

2、建議：各機關應依資通安全責任等級分級辦法附表十資通系統防護基準「系統與服務獲得」構面之各項措施內容重新檢視機關內部在安全系統發展生命週期(SSDLC)之機制，確保軟體系統在開發過程中可以採行相應之安全防護措施。

(三)安全防護

1、說明：未針對核心資通系統定期進行弱點掃描、系統滲透測試，機關資安健診作業應訂定內部資安作業程序，且應確實改善追蹤。

2、建議：依資通安全責任等級分級辦法之應辦事項規定，各

機關應針對核心資通系統定期進行弱點掃描、系統滲透測試，並且對於全機關進行資安健診作業，並訂定後續改善追蹤機制，以確保機關之資通安全防護。

(四)GCB 導入

1、說明：未就 GCB 套用之例外管理，提出可行方式及改善時程，並定期追蹤改善情形。

2、建議：各機關應確實導入 GCB，除因技術限制、個別資通系統之設計、結構或性質等因素之例外管理，應提出方式及改善時程，並且定期檢視追蹤改善情形。

(五)物聯網安全

1、說明：未將物聯網設備納入資訊資產盤點範圍，並建立適當防護措施。

2、建議：各機關應將物聯網設備納入資通訊資產盤點範圍，並建立適當防護管理措施，另設備應通過資安檢測規範或標準，以降低資安風險。