113年度資安稽核共同發現事項及建議

經綜整113年之稽核發現，就待改善事項彙整較具重要性可提供各級機關借鏡之事項，分別就策略面、管理面及技術面說明如下：

一、策略面

(一) 業務持續運作演練及備份復原

1. 說明：部分機關業務持續運作演練未切合實際，且未妥適規劃備份資料之復原程序。

2. 建議：依資通安全責任等級分級辦法應辦事項及資通系統防護基準規定，核心資通系統應辦理持續運作演練，及辦理系統備份備援作業。機關應對整體資訊服務進行營運衝擊分析（BIA），明確訂定資通系統之系統復原時間目標（RTO）及資料復原時間點目標（RPO），並訂定備份資料之復原程序及定期執行回復測試，以確保備份資料之有效性。另建議評估納入複合式及資安新興議題演練情境，以切合實際。

(二) 資通安全政策及目標

1. 說明：部分機關資通安全政策及目標未臻妥適，或目標、指標設定過低。

2. 建議：依資通安全管理法施行細則第6條規定，機關資通安全維護計畫應訂定資通安全政策及目標，目標宜有量化型及質化型指標，且應考量合宜性（例如不應納入資安事件發生次數）並有一致性的量測頻率及衡量基準，定期依實際執行及指標達成情形，檢討調修資通安全維護計畫。

(三) 資通安全持續精進及績效管理機制

1. 說明：部分機關資通安全維護計畫與實施情形之持續精進及績效管理機制未確實執行。

2. 建議：依資通安全管理法第10條、第12條、第16條、第17條、資通安全管理法施行細則第6條及資通安全責任等級分級辦法應辦事項規定，機關應訂定且每年滾動式調修資安維護計畫，並確實辦理內部資通安全稽核及稽核發現之後續改善追蹤管考作業，以落實 PDCA 管理循環流程並持續精進以達績效管理目

標。

二、管理面

(一) 資通系統或服務委外辦理之管理措施

1. 說明：部分機關未落實監督及管理委外廠商工作。

2. 建議：依資通安全管理法第9條、資通安全管理法施行細則第4條及第6條規定，對資通系統或服務之委外，應依資通系統分級將 SSDLC 安全及資通系統防護基準需求納入招標文件，並落實辦理 ISMS 程序書、維護計畫等委外管理要求，且定期以稽核或其他適當方式，確認受託業務執行情形。另應依「各機關對危害國家資通安全產品限制使用原則」規定，落實相關資通安全產品管制。

(二) 資通系統與資訊資產盤點

1. 說明：部分機關未完整盤點資通系統及資訊資產、未妥適界定核心系統及系統分級。

2. 建議：依資通安全管理法施行細則第6條規定，應落實盤點完整掌握全機關之資通系統及相關資產。盤點範圍應涵蓋全機關，包含業務單位、輔助單位，納入 OT、IoT、連網及未連網設備，並落實資產異動管理程序，及依規定進行後續資安風險評估及資通系統分級等作業。

(三) 內部資通安全稽核

1. 說明：部分機關之內部稽核辦理範圍、頻率及稽核項目規劃未臻妥適。

2. 建議：依資通安全管理法施行細則第6條及資通安全責任等級分級辦法應辦事項規定，機關應實施內部資安稽核，稽核範圍應涵蓋全機關，非僅限資訊單位，並建議擬定整體稽核計畫，規劃各單位之稽核頻率、稽核委員組成及稽核發現之後續追蹤管考機制。

三、技術面

(一) 弱點修補或緩解措施

1. 說明：部分機關未完成全部高風險弱點之修補，或完成修補前未加強管控或採行緩解措施。

2. 建議：依資通安全責任等級分級辦法應辦事項及資通系統防護基準規定，應定期辦理安全性檢測、導入弱點通報機制及定期進行軟體元件漏洞修復與更新，倘發現軟體或元件具有安全漏洞，或經安全性檢測所檢出之系統漏洞，應依機關風險評估及處理原則，修復並定期追蹤修補進度，妥適規劃複測作業。發現高風險以上之弱點，應即時完成修補，未能如期修補時，應於完成修補前規劃緩解措施。

(二) 資安事件通報應變

1. 說明：部分機關資安事件通報作業仍有未符規定情形。

2. 建議：依資通安全管理法第14條及第18條、資通安全事件通報及應變辦法第9條及第15條規定，應訂定資通安全事件通報作業規範並進行相關演練，於發生資安事件時方能確實依相關作業流程規範，執行等級判定等作業，並依時限完成通報。

(三) 資通安全防護及控制措施

1. 說明：部分機關資安防護控制措施之執行未完備。

2. 建議：依資通安全責任等級分級辦法應辦事項及資通系統防護基準規定，並得參考國家資通安全研究院訂定之參考文件，如資通系統防護基準驗證實務規範、安全控制措施參考指引等，持續落實技術面各應辦事項及控制措施。並建議加強確認遠端連線原則禁止例外允許、高權限帳號控管、無線 AP 管理檢查機制、SOC 監控範圍並持續維運、防火牆規則定期檢視、資訊機房消防區隔及監視設備等事項。