111年度公務機關資安稽核作業
共同發現事項

111年資安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) 資通安全目標

1. 說明：部分機關所訂資通安全目標，未有一致性客觀衡量指標，或與機關實際作業所訂目標不一致、將資安事件發生次數納入量化型目標等。

2. 建議：依資安法施行細則第6條規定，應制定資通安全政策、目標，其中資通安全目標宜有量化型與質化型指標，量化型指標並應考量合宜性。各機關可依對應資通安全責任等級分級辦法附表一至八之應辦事項及資通系統分級結果所對應之防護需求等，審酌機關業務屬性、系統特性及資料持有情形等，訂定較客觀及量化之衡量指標，據以一致性評估機關資通系統之防護需求。請勿納入資安事件發生次數，以免影響資安事件通報意願。

二、管理面

(一) 資通系統或服務委外管理

1. 說明：部分機關辦理資訊委外作業未訂定安全管理措施及受託者應辦理之安全維護事項，建議書徵求文件亦未明確規範防護基準需求及資通安全防護水準。

2. 建議：依資安法施行細則第4條及資通系統籌獲各階段資安強化措施規定，應對委外作業資通安全建立相關管理程序，包含選商(技術與能力要求)、服務水平、安全控制措施(包括保密與人員之管理)、績效管控及對廠商稽核等監督管理機制，皆應明訂於機關管理程序；且資通系統取得前即應評估並標註所需之資通系統防護需求等級，並納入與廠商之契約規範中落實執行。

(二) 受託者稽核作業

1. 說明：部分機關辦理委外廠商稽核作業未訂定委外廠商稽核之相關管理規範，且未明確訂定廠商稽核之挑選原則及家數。

2. 建議：依資安法施行細則第4條規定，委託機關應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，以稽核或其他適當方式確認受託業務之執行情形；並完整記錄查核證據，訂定改善追蹤管考機制並納入與廠商之契約規範；且應落實執行，以維稽核之有效性。

(三) 資訊及資通系統之盤點

1. 說明：已辦理資訊資產盤點作業，惟盤點範圍與內容完整性不足，盤點範圍未包含全機關。

2. 建議：依資安法施行細則第6條規定，應完整盤點資通系統及資產，明確標示核心資通系統及相關資產，盤點範圍為全機關，不應侷限於資訊單位維管或資訊經費採購者。盤點後應進行資產價值鑑別及風險評估，對於老舊軟、硬體、已停止之服務，或已移轉他機關之資產，應更新及落實資產異動管理程序。

三、技術面

(一) 事件通報、應變及演練

1. 說明：部分機關資安事件通報及應變程序，未訂定資安事件相關證據資料保護規範、事件調查復原與後續矯正改善追蹤機制。

2. 建議：依資安法第14條規定，應訂定通報及應變機制，內容除知悉資通安全事件後之通報及應變，應包含資安事件相關跡證保護、事件調查復原與後續矯正改善追蹤機制，並應定期演練。

(二) 存取控制—遠端存取

1. 說明：部分機關允許以遠端方式維護資通系統，且未有相應管理作為。

2. 建議：依行政院資通安全處110年3月2日院臺護字第1100165761號函規定，各機關對於遠端維護資通系統，除應採「原則禁止、例外允許」，並應強化相關管理作為，及至少辦理以下防護措施：

(1) 如開放委外廠商遠端存取，應要求委外廠商依資安法施行細則第4條，辦理受託業務之相關程序及環境，須具備完善之資通安全管理措施。

(2) 資通安全責任等級分級辦法附表十「存取控制」構面下「遠端存取」相關規定。

(3) 遠端存取開放原則應以短天期為限，並建立異常行為管理機制。

(4) 遠端存取開放期滿，應即確實關閉網路連線，並更換遠端存取通道(如 VPN 等)登入密碼等。