110 年政府機關(構)資通安全稽核作業

共同發現事項

110 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：依資通安全管理法(以下簡稱資安法)施行細則第 7 條規定，

(1)核心業務為公務機關依組織法規足認該業務為核心權責所在、公營事業及財團法人之主要服務或功能、機關維運、提供關鍵基礎設施必要業務、依資通安全責任等級分級辦法第四條第一至五款或第五條第一至五款涉及之業務。

(2)完整盤點全機關之資通系統，包括業務單位之資通系統、營運技術 (OT) 系統等，就支持核心業務持續運作必要之系統，或資通系統防護需求等級為高者，列為機關之核心資通系統，並依不同安全等級之資通系統施予適當之安全控制措施。

(二)資通安全推動組織

1、說明：召開管審會議常有委員係代理出席，難彰顯管理階層之支持及重視。

2、建議：依資安法施行細則第 6 條規定，應設置資通安全推動組織，推動資通安全相關政策、落實資通安全事件通報及相關應變處理，建議組織成員親自參與，避免代理出席會議，以顯示管理階層對資安作業之重視與支持。

(三)資通安全目標

1、說明：機關資通安全目標之量測指標仍納入資安事件發生次數，未考量合宜性。

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，量化型指標應考量合宜性，為免影響資安事

件通報，勿納入資安事件發生次數。

二、管理面

(一)委外管理

1、說明：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。

2、建議：依資安法施行細則第 4 條規定，對於委外作業安全應建立相關管理程序，從廠商選擇(技術與能力要求)、服務水平、安全控制措施(包括保密、處理人員之管理)及廠商績效監控(稽核)與報告機制等，皆應明確制訂於管理程序，並落實於與廠商之契約規範中。

(二)資通系統及資訊之盤點

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。

2、建議：依資安法施行細則第 6 條規定，

(1)應完整盤點全機關各單位資通系統及資訊，明確標示核心資通系統及相關資產。

(2)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；另如發現軟、硬體老舊問題時，及早規劃更新作業。

(三)受託者資通安全稽核

1、說明：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。

2、建議：依資安法施行細則第 4 條規定，

(1)委託機關應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，以稽核或其他適當方式確認受託業務之執行情形。

(2)並應注重稽核作業之有效性，如完整記錄查核證據，並訂定機制落實對稽核結果之追蹤管考。

(四)內部資通安全稽核

1、說明：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。

2、建議：依資通安全責任等級分級辦法應辦事項規定，對於資通安全內部稽核作業，應注意稽核範圍是否涵蓋全機關、1 年 2 次內部稽核是否適當區隔時間、稽

核項目是否完整納入資安法法遵事項，及內部稽核發現事項之改善追蹤情形。

三、技術面

(一)安全性檢測及資通安全健診

1、說明：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。

2、建議：依資通安全責任等級分級辦法應辦事項規定，應針對資通系統定期進行弱點掃描、系統滲透測試及資通安全健診，並應追蹤檢測結果修補情形，以確實降低機關之資安風險。

(二)系統與服務獲得

1、說明：已訂定資通系統開發、測試、變更及上線等相關程序，惟其內容未臻完善，且未完整保留資通系統之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。

2、建議：依資通安全責任等級分級辦法防護基準規定，

(1)應落實系統發展生命週期各階段作業，保留各系統之版本及更新過程與紀錄。

(2)除資訊單位外，各業務單位委外之系統亦應注意辦理本項作業。

(三)系統與資訊完整性

1、說明：針對資通系統所使用之外部元件或軟體，缺乏明確管理規範。

2、建議：依資通安全責任等級分級辦法防護基準規定，

(1)機關針對資通系統所使用之外部元件或軟體，應建立系統化管理機制，並納入驗收程序。

(2)針對外部元件或軟體之安全性漏洞通告，應落實評估更新,並關閉資通系統不必要之服務及埠口。