109 年政府機關(構)資通安全稽核作業

共同發現事項

109 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：機關應依資通安全管理法施行細則第 6 條及第 7 條規定，明確界定應保護之標的，且依不同防護需求等級之資通系統施予防護控制措施，相關作業包含界定機關核心業務，盤點各單位之資通系統，並包括業務營運之資通系統、輔助系統等。支持核心業務持續運作必要之系統，及資通系統防護需求等級為高者，皆應列為機關之核心資通系統並達成法規要求之防護作業。

(二)資安事件通報應變

1、說明：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。。

2、建議：依資通安全事件通報及應變辦法第 9 條規定，應完善資通安全事件通報窗口及聯繫方式資訊，包含機關內部、外部利害關係人(如上級／監督機關、所屬／所管機關、合作機關、IT 服務供應商及民間等)。

(三)資安專責人員

1、說明：資通安全相關法遵、資安威脅趨勢及技術知能要求與日俱增，惟部分機關受限資安人力資源，未配置資安專職/責人力。

2、建議：機關應依資通安全責任等級分級辦法應辦事項規定，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，優先調配資安專責人員，並結合資安專業訓練、證照及職能訓練證書，培養機關所需之資安專業人力。

二、管理面

(一)資訊及資通系統盤點

1、說明：已辦理資訊資產盤點並建立資產清冊，惟盤點範圍與內容完整性不足。

2、建議：依資通安全管理法施行細則第 6 條規定，機關應落實盤點資訊及資通系統，並標示核心資通系統及相關資產。

(二)委外管理

1、說明：未規劃與落實資訊委外作業(如委外廠商選任要求、防護基準納入 RFP、安全檢測、通報程序等)

2、建議：依資通安全管理法施行細則第 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，皆應於管理程序明確制訂，並落實於與廠商之合約規範。

(三)內部資安稽核

1、說明：已規劃並執行資通安全內部稽核作業，惟部分機關稽核對象未涵蓋全機關，且稽核項目未完整納入資安法應辦事項。

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，應注意稽核頻率、時程、準則、檢核項目、方式、範圍等是否妥適，如範圍是否涵蓋全機關、稽核項目是否完整納入資安法法遵事項，及有效管考內部稽核發現事項之改善情形。

三、技術面

(一)網路架構安全

1、說明：部分機關網路架構安全性仍顯不足，如網段區隔與存取控管未確實。

2、建議：依資通安全責任等級分級辦法應辦事項規定，機關網路架構應清楚界定並規劃不同需求屬性之區域，且依業務屬性設定內部人員可存取網段，並定期檢視網路架構安全及存取授權。

(二)安全防護

1、說明：已進行網站安全性檢測、滲透測試及資通安全健診等作業，惟未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，包括何人實施、實施標的(涵蓋範圍)、何時實施、如何實施(工具、方法等)、及實施結果之改善(改善機制、改善時程)，以確保機關之安全防護。

(三)資訊系統開發安全

1、說明：未將資通系統安全開發程序納入資通系統防護需求。

2、建議：應依資通安全責任等級分級辦法資通系統防護基準之「系統與服務獲得」構面，重新檢視系統發展生命週期(SSDLC)於需求、設計、開發、測試、部署與維運等階段之各項安全要求，並落實資通系統防護需求等級對應之防護基準。

(四)資安事件通報應變演練

1、說明：已辦理資安事件通報與應變演練，惟未納入事件通報環節，另建議將新興資安議題或事件納入演練情境。。

2、建議：依資通安全事件通報及應變辦法規定，應訂定資安事件通報/應變作業規範，公務機關每年應辦理1次之資安事件通報及應變演練。