

104 年政府機關（構）資通安全稽核作業

共同發現事項及建議

104 年稽核結果共同發現事項及建議分策略面、管理面、技術面及技術檢測等項，分別說明如下：

一、策略面

（一）導入資訊安全管理系統範圍適切性

機關（構）資安推動組織成員大多為資訊部門，業務部門較少參與，難以確保相關資安控制措施有效落實。

建議：資安推動組織關係機關（構）整體資安管理，宜由各部門主管（或副主管）共同組成，訂定適當之資安管理指標與有效之量測方式，並透過定期召開資安推動會議，追蹤與檢討相關資安控制措施的適切性及有效性。

（二）資源投入資安業務狀況

機關（構）資訊（安）人員人力不足或遇缺不補，造成人力不足，對一般人員資安風險亦缺乏有效管理。

建議：宜妥適解決資訊（安）人力問題，或將資訊（安）業務向上集中，以為因應，並依員工及業務屬性，辨識可能資安風險後，透過內、外部稽核及教育訓練等妥適控管。

（三）業務運作規劃與落實

1. 機關（構）對營運持續計畫之規劃、演練與情境設定過於簡化，且未確實進行營運衝擊分析評估。

建議：宜增強營運持續計畫之規劃深廣度及演練效度，

除測試系統運作層面外，更應深入瞭解備份資料回復後的完整性與可用性。

2. 微軟 Windows XP 與 Windows Server 2003 業已終止支援服務，機關（構）尚未完成汰換或採取有效之管控作業，資安風險未減。

建議：應確實評估仍需繼續使用 Windows XP 與 Windows Server 2003 之必要性，並積極進行汰換作業或採取有效之管理。

二、管理面

（一）個人資料保護與管理

機關（構）對於個人資料盤點內容尚欠周延。

建議：以個人資料之作業流程進行盤點，採流程圖方式繪製資料生命週期，並呈現相關利害關係者。

（二）風險評鑑、資訊資產清查與管理

機關（構）已對資訊資產進行盤點，惟資訊資產之風險評鑑仍未臻完善。

建議：在完成資訊資產盤點後，應進行後續之風險評鑑，以確認每項資訊資產均具妥適之安全保護，並依組織及業務變動適時調整。風險評鑑之風險評估方法論，亦應適時加以檢討，以符合機關（構）之實際需求。

（三）人力資源管理

機關（構）於委外契約訂有資安稽核條款，惟較少落實，亦缺乏對委外廠商資安要求的有效性管理。

建議：應落實執行委外廠商之資安稽核及資安相關要求，以盡監督管理之責任，另委外廠商駐點人員之權責亦應

明確劃分，由機關（構）同仁負責管理與稽核，廠商駐點人員則負責執行。

三、技術面

(一)通訊與作業管理適切性與落實執行狀況

1. 機關（構）未有效管理委外廠商之資安服務作業，對其（駐點）人員之日常作業與存取權限未妥善管控。

建議：應針對委外廠商詳訂作業程序與管理規範，限縮其遠端存取功能，並強化機關（構）自身監督管理權責，加強管理能力。

2. 網路服務安全控制措施之適切性及落實度較不足，且應於網路或系統存取時，啟用相關日誌設定或建立相關保護機制。

建議：應強化網路服務設定之安全強度，檢討外部遠端連線內部系統之必要性，並訂定檢視週期落實執行；此外，於軌跡紀錄的保存、管理與分析，宜依系統容量及日誌之屬性，規劃日誌管理機制。

3. 對於行動裝置缺乏有效之管理。

建議：如因業務需要必須開放使用行動裝置時，宜在需求面及安全性同時兼顧下啟用，並妥善管理行動裝置存取權限，以確保資訊安全。

(二)應用系統開發及維護安全管理

1. 應用系統開發上線前，機關（構）未進行弱點掃描等必要性之資安檢測，致系統或軟體易遭駭客入侵。

建議：應用系統開發或更新上線前，應進行版本控管，對系統或軟體進行原始碼檢測及弱點掃描，並定

期辦理滲透測試，以降低系統遭入侵之風險。

2. 機關（構）針對弱點掃描結果，未進行適當修補作業。

建議：弱點掃描等資安檢測作業所發現之漏洞為立即性之風險，機關（構）應建立修補管控機制，落實安全性檢測與修補作業，以降低資安風險。

四、技術檢測

經行政院國家資通安全會報技術服務中心（105 年 1 月 20 日改制為行政法人國家資通安全科技中心）針對受稽機關（構）於實地稽核前進行使用者電腦弱點掃描、使用者電腦安全防護檢測、組態設定安全防護檢測、惡意中繼站連線阻擋檢測、核心資訊系統內網滲透測試、網路架構檢測及 AD 主機安全防護檢測等。共同發現事項如下：

（一）使用者電腦弱點掃描

機關（構）啟用不必要或未使用之應用服務，導致使用者電腦存在弱點，如遠端桌面、遠端操作軟體或 FTP 等。

建議：機關（構）定期執行電腦弱點掃描，並落實執行弱點修補管控，以及限制使用者自行下載或安裝未經授權之應用服務項目。

（二）使用者電腦安全防護

機關（構）之電腦安全性更新有缺漏情形。

建議：機關（構）對於安全性更新管理，除落實 Windows 與 Office 之安全性更新外，應將電腦所安裝之其他軟體之安全性更新納入管控，如 Java 與 Adobe 等。