

# 第十一條附表一修正規定

附表一 資通安全責任等級 A 級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級及其防護基準之妥適性。
	資訊安全管理系統之導入及通過公正第三方之驗證		全部核心資通系統導入 CNS 27001 或 ISO 27001 等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，完成公正第三方驗證，並持續維持其驗證有效性。
	資通安全專職人員		配置四人以上。
	內部資通安全稽核		每年辦理二次。
	營運持續計畫演練		全部核心資通系統每年辦理一次。
	資安治理成熟度評估		每年辦理一次。
技術面	安全性檢測	弱點掃描	全部核心資通系統每年辦理二次。
		滲透測試	全部核心資通系統每年辦理一次。
	資通安全健診	網路架構檢視	每年辦理一次。
		網路惡意活動檢視	
		使用者端電腦惡意活動檢視	
		伺服器主機惡意活動檢視	
		目錄服務系統設定及防火牆連線設定檢視	
		核心資通系統資料庫安全檢視	
	資通安全監控管理機制		完成監控管理機制建置，並持續維運及依主管機關指定之方式提交監控管理資料。其監控範圍應包括本表所定「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與核心資通系統之日誌紀錄及資通設備紀錄。
	政府組態基準		依主管機關公告之項目，完成政府組態基準

			導入作業，並持續維運。
	資通安全弱點管理		一、知悉資通安全弱點時，應適時修補或採行緩解措施。 二、依主管機關指定方式導入弱點管理作業，並持續維運。
	端點偵測及應變機制		完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。
	資通安全防護	防毒軟體	完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系統者，應備應用程式防火牆	
認知與訓練	資通安全教育訓練	進階持續性威脅攻擊防禦措施	
		資通安全專職人員	
		資通安全專職人員以外之資訊人員	
	資通安全專業證照及職能訓練證書	一般使用者及主管	每人每年接受三小時以上之資通安全通識教育訓練。
			資通安全專職人員各自持有證照及證書各一張以上，並持續維持證照及證書之有效性。

備註：

- 一、資通系統之性質為共用性系統者，由該資通系統之主責設置、維護或開發機關判斷是否屬於核心資通系統。
- 二、「公正第三方驗證」所稱第三方，指通過我國標準法主管機關委託機構認證之機構；第三方核發之驗證證書應有前開委託機構之認證標誌。
- 三、資通安全專職人員，指應全職執行資通安全業務者，亦即資通安全為其主要核心業務，且應優先辦理。資通安全專職人員以外之資訊人員，指其他實際從事資通安全業務或資訊業務之人員。
- 四、公務機關辦理本表「資通安全健診」時，除依本表所定項目、內容及時限執行外，亦得採取經主管機關認可之其他具有同等或以上效用之措施。

五、資通安全弱點管理，指結合資訊資產管理與弱點管理，掌握整體風險情勢，並協助機關落實本法有關資產盤點及風險評估應辦事項之作業。

六、端點偵測及應變機制，指具備對端點進行主動式掃描偵測、漏洞防護、可疑程式或異常活動行為分析及相關威脅程度呈現功能之防護作業。

七、資通安全專業證照，指經主管機關公告之資通安全專業證照。

八、資通安全職能訓練證書，指通過主管機關資通安全職能評量所核發之證書。

九、應辦事項辦理期限

(一)資通系統分級及防護基準：應於初次受核定或等級變更後之一年內完成；資通系統新增、系統分級變更或其適用防護基準有異動情形時，亦同。

(二)資訊安全管理系統之導入及通過公正第三方之驗證：應於初次受核定或等級變更後之二年內，全部核心資通系統導入資訊安全管理系統，並於三年內完成公正第三方驗證。

(三)資通安全監控管理機制、政府組態基準、資通安全弱點管理、端點偵測及應變機制：應於初次受核定或等級變更後之一年內，完成導入作業；主管機關公告新增政府組態基準項目，亦同。

(四)資通安全防護：應於初次受核定或等級變更後之一年內完成啟用，並持續使用。

(五)配置資通安全專職人員、資通安全教育訓練、資通安全專業證照及職能訓練證書：應於初次受核定或等級變更後之一年內完成；人員異動時，亦同。

(六)其餘應辦事項應於初次受核定、等級變更或核心資通系統異動後之次年度起，依附表規定辦理。