## 附表二 資通安全責任等級 A 級之特定非公務機關應辦事項

管理面 資內業安 資診 資 資 資 通 部務 全 通	施理石口	<b>辦</b> 珊石口伽石	施理 內 宏
管理面 資內業 安 資診 資 資 資 通 部務 全 通 通 通 通	辦理項目	辨理項目細項	辦理內容
管理面 資內業 安 資診 資 資 資 通 部務 全 通 通 通 通			初次受核定或等級變更後之一年內,針
管理面 資內業 安 資診 資 資 資 通 部務 全 通 通 通 通			對自行或委外開發之資通系統,依附表
過資內業安資診 資資 資資	迪系統分級	及防護基準	九完成資通系統分級,並完成附表十之
過資內業安資診 資資 資資			控制措施;其後應每年至少檢視一次資
過資內業安資診 資資 資資			通系統分級妥適性。
過資內業安資診 資資 資資	資訊安全管理系統之導入及通 過公正第三方之驗證		初次受核定或等級變更後之二年內,全
過資內業安資診 資資 資資			部核心資通系統導入 CNS 27001 資訊安
過資內業安資診 資資 資資			全管理系統國家標準、其他具有同等或
資內業安資診 資資 資			以上效果之系統或標準,或其他公務機
內業 安 資診 資 資 資			關自行發展並經主管機關認可之標準,
內業 安 資診 資 資 資			於三年內完成公正第三方驗證,並持續
內業 安 資診 資 資 資			維持其驗證有效性。
內業 安 資診 資 資 資	資通安全專責人員		初次受核定或等級變更後之一年內,配
業 安 資診 技術面 資 資			置四人。
業 安 資診 技術面 資 資	內部資通安全稽核		每年辦理二次。
資診 技術面 資 資	務持續運作		全部核心資通系統每年辦理一次。
資診 技術面 資 資	安全性檢測	網站安全弱點	
資診 技術面 資 資		檢測	全部核心資通系統每年辦理二次。
技術面 資通		系統滲透測試	全部核心資通系統每年辦理一次。
技術面 資通	資通安全健 診	網路架構檢視	每年辦理一次。
技術面 資通		網路惡意活動	
技術面 資通		檢視	
技術面 資通		使用者端電腦	
技術面 資通		展意活動檢視 思意活動檢視	
技術面資通		伺服器主機惡	
資通		意活動檢視	
資通			
資通		目錄伺服器設	
資通		定及防火牆連	
資通		線設定檢視	2. 1. 在12 户上 林 加 坳 五 4 、
	資通安全威脅偵測管理機制		初次受核定或等級變更後之一年內,完
			成威脅偵測機制建置,並持續維運。
	資通安全 防護	防毒軟體	初次受核定或等級變更後之一年內,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	
		禦機制 具有對外服務	

		4 七、	
		統者,應備應用	
		程式防火牆	
		進階持續性威	
		脅攻擊防禦措	
		施	
		資通安全及資 訊人員	每年至少四名人員各接受十二小時以上
	次区户入		之資通安全專業課程訓練或資通安全職
	資通安全		能訓練。
認知	教育訓練練	一般使用者及	每人每年接受三小時以上之一般資通安
與訓練		主管	全教育訓練。
	資通安全專業證照		初次受核定或等級變更後之一年內,資
			通安全專責人員總計應持有四張以上,
			並持續維持證照之有效性。

## 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。
- 三、特定非公務機關辦理本表「資通安全健診」時,除依本表所定項目、內容及時限執行外,亦得採取經中央目的事業主管機關認可之其他具有同等或以上效用之措施。
- 四、特定非公務機關之中央目的事業主管機關得視實際需求,於符合本辦法規定之範圍內,另行訂定其所管特定非公務機關之資通安全應辦事項。
- 五、資通安全專業證照,指由主管機關認可之國內外發證機關(構)所核發之資通安全證照。