

項目	(七)資通安全防護及控制措施		
7.1	是否依法規定定期辦理安全性檢測及資通安全健診?1.全部核心資通系統辦理弱點掃描 (A 級機關：每年 2 次；B 級機關：每年 1 次；C 級機關：每 2 年 1 次) 2.全部核心資通系統辦理滲透測試 (A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次) 3.資通安全健診，包含網路架構檢視、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、目錄伺服器設定及防火牆設定檢視等？ (A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次)		
稽核 依據	資通安全責任等級分級辦法應辦事項：技術面之安全性檢測之弱點掃描		N2010
	資通安全責任等及分級辦法資通系統防護基準/系統與資訊完整性/漏洞修復		C0701
	1. 資通安全責任等級分級辦法第 11 條第 1 項應辦事項：全部核心資通系統弱點掃描，A 級每年 2 次；B 級每年 1 次；C 級每 2 年 1 次 2. 資通安全責任等級分級辦法第 11 條第 1 項應辦事項：全部核心資通系統滲透測試，A 級每年 2 次；B 級每年 1 次；C 級每 2 年 1 次 3. 資通安全責任等級分級辦法第 11 條第 1 項應辦事項：資通安全健診二、A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次)		
稽核 重點	檢視機關執行弱點掃描、滲透測試及資安健診情形。	佐證 資料	機關核心系統清冊 (或維護計畫內所載或所填報實施情形中的系統清冊)、弱點掃描報告、執行修補作業與驗證改善
稽核 參考	1. 機關全部核心資通系統之弱點掃描、滲透測試、資安健診頻率、至少近 2 次檢測時間、檢測方式、內容、結果。 2. 資安健診各項範圍皆應為全機關，倘為抽測，母數範圍應為全機關。 3. 是否依機關風險評估及處理原則執行弱點修補 (例如機關風險處理原則為中風險以上弱點皆須修補，就須檢視是否有中風險以上未修補也未有經核定之評估紀錄)。 4. 比較近 2 次結果，相同弱點存在時，可探其內容及原因，改善追蹤機制及落實情形。 5. 漏洞修復應測試有效性 (例如複測) 及潛在影響，並定期更新。		

FQA	