

項目	(八)資通系統發展及維護安全		
8.12	是否針對資通系統所使用之外部元件或軟體、韌體，注意其安全漏洞通告，且定期評估更新？系統之漏洞修復是否測試有效性及潛在影響？		
稽核 依據	資通安全責任等級分級辦法附表十資通系統防護基準：系統與資訊完整性之漏洞修復		C0701
	1. 資通安全責任等級分級辦法第 11 條第 2 項：資通系統防護基準之系統與資訊完整-漏洞修復，系統之漏洞修復應測試有效性及潛在影響，並定期更新（普）。定期確認資通系統相關漏洞修復之狀態（中高）		
稽核 重點	外部元件或軟體之安全漏洞通告，應有評估、更新及確認機制	佐證 資料	資通系統所使用的外部元件或軟體清單、漏洞修補程序及相關紀錄、設備型號等
稽核 參考	1. 宜建立資通系統所使用的外部元件或軟體清單，注意其安全漏洞通告，且定期評估更新，評估及更新均留下紀錄。 2. 宜參考美國 CISA KEV 目錄(Known Exploited Vulnerabilities Catalog)，其所列之 CVE 漏洞已被積極利用，應優先排入修補期程。 3. 於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。 4. 漏洞修補應有測試及覆核機制（如於測試環境套用更新程式，確認不會對系統服務造成危害後，始於正式環境進行更新，並留有相關紀錄）。		
FQA			