

項目	(八)資通系統發展及維護安全		
8.5	資通系統開發階段，是否針對安全需求實作必要控制措施並避免常見漏洞（如OWASPTop10等）？且針對防護需求等級高者，執行源碼掃描安全檢測？		
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：系統與服務獲得之系統發展生命週期開發階段、系統文件		C0503、C0508
	<p>一、資通系統開發階段，避免常見漏洞及源碼掃描</p> <ol style="list-style-type: none"> 1. 資通安全責任等級分級辦法第 11 條第 2 項：應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表 10 所定資通系統防護基準執行控制措施 2. 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服務獲得-系統發展生命週期開發階段，應注意避免軟體常見漏洞及實作必要控制措施，執行「源碼掃描」安全檢測（資通系統高等級者）。 3. 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服務獲得-系統發展生命週期開發階段，應注意避免軟體常見漏洞及實作必要控制措施（普中高），執行「源碼掃描」安全檢測（高）。 		
稽核 重點	應針對安全需求實作必要控制措施	佐證 資料	資通系統源碼存取之相關管理程序、相關紀錄（掃描報告、修補紀錄及複測紀錄）
稽核 參考	<ol style="list-style-type: none"> 1. 應注意避免軟體常見漏洞及實作必要控制措施，安全需求可能包含機關規定之組態設定，以明確說明允許之功能、埠口、協定及服務等，或是提供必要資安防護能力，如密碼強度要求、加密強度要求、實作存取控制、身分驗證及授權機制等資安功能實作。 2. 發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息，以免系統架構被拼湊得知全貌。 3. 針對防護需求等級高者之資通系統，應執行「源碼掃描」安全檢測，檢具掃描報告、修補紀錄及複測紀錄，且具備系統嚴重錯誤之通知機制。 4. 採用之源碼檢測工具宜具備常見安全弱點（如OWASPTop10、跨站腳本攻擊及注入攻擊等）檢測能力。 		

FQA	