<table>
<tr><td>項目</td><td colspan="3">(八) 資通系統發展及維護安全</td></tr>
<tr><td>8.5</td><td colspan="3">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？另是否執行安全性功能測試，且檢討執行情形？</td></tr>
<tr><td rowspan="2">稽核依據</td><td>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</td><td colspan="2">C0503、C0508</td></tr>
<tr><td colspan="3">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（普中高），執行「源碼掃描」安全檢測（高）。</td></tr>
<tr><td>稽核重點</td><td>應針對安全需求實作必要控制措施</td><td>佐證資料</td><td>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）</td></tr>
<tr><td>稽核參考</td><td colspan="3">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。
5. 安全性功能測試包含但不限於邏輯及安全性驗測、機敏資料存取、 用戶登入資訊檢核及用戶輸入輸出之檢查過濾測試及在各種使用者環 境端皆可更新成功並正常執行之測試，並檢討執行情形。</td></tr>
<tr><td>FQA</td><td colspan="3"></td></tr>
</table>
