<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>8.6</td><td colspan="3">資通系統測試階段，是否執行弱點掃描安全檢測？且針對防護需求等級高者，執行滲透測試安全檢測？</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">C0504、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-系統發展生命週期測試階段，執行弱點掃描安全檢測（普中），以及滲透測試安全檢測（高）。</td></tr>
<tr><td>稽核重點</td><td>資通系統測試階段應執行安全性檢測</td><td>佐證資料</td><td>系統測試管理程序、系統測試計畫、審查紀錄、弱點掃描報告、滲透測試報告、執行修補作業與驗證改善</td></tr>
<tr><td>稽核參考</td><td colspan="3">測試階段即應執行安全性檢測
1. 皆應執行「弱點掃描」安全檢測，應注意所採用之弱點掃描工具需具備基本之安全弱點（包含但不限於 OWASP Top10、軟體元件版本弱點、通訊協定弱點等）檢測能力。
2. 針對防護需求等級高者之資通系統，除弱點掃描外，須另執行「滲透測試」安全檢測。</td></tr>
<tr><td rowspan="2">FQA</td><td colspan="3"></td></tr>
<tr><td colspan="3"></td></tr>
</table>