<table>
<tr><td>項目</td><td colspan="3">(五) 通系統或服務委外辦理之管理措施</td></tr>
<tr><td>5.8</td><td colspan="3">委外客製化資通系統開發者，若屬核心資通系統或委託金額達新臺幣一千萬元以上者，委託機關是否自行或另行委託第三方進行安全性檢測？</td></tr>
<tr><td rowspan="3">稽核依據</td><td>資通安全管理法施行細則第 6 條：資通系統或服務委外辦理之管理措施</td><td colspan="2">P11</td></tr>
<tr><td>資通安全管理法施行細則第 4 條</td><td colspan="2">L1110082304</td></tr>
<tr><td colspan="3">1. 資通安全管理法第 9 條：應考量、選任受託者，並監督其資通安全維護情形。
2. 資通安全管理法施行細則
(1) 第 4 條第 1 項第 5 款：受託業務包括客製化資通系統開發者，受託者應提供該資通系統之安全性檢測證明；該資通系統屬委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測；涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。
(2) 第 6 條第 1 項第 11 款：資通系統或服務委外辦理之管理措施
3. 資通安全責任等級分級辦法第 11 條第 2 項：附表 10 資通系統防護基準之系統與服務獲得-SSLDC 開發階段及測試階段-執行弱點掃描安全檢測(資通系統普/中/高等級者)、源碼掃描及滲透測試安全檢測(資通系統高等級者）</td></tr>
<tr><td>稽核重點</td><td>符合條件者，除要求廠商要提供安全性檢測證明外，機關應自行或另外委託第三方進行安全性檢測</td><td>佐證資料</td><td>契約書、委外開發系統之驗收程序、檢視廠商提供之安全性檢測紀錄、機關自行或委託第三方執行的安全性檢測紀錄（符合條件者）、資訊作業委外安全管理程序文件</td></tr>
<tr><td>稽核參考</td><td colspan="3">一、委外客製化資通系統開發者，若為委託機關之核心資通系統，或委託金額達新臺幣一千萬元以上者
1. 要求廠商提供安全性檢測證明，且機關應自行或另外委託第三方進行安全性檢測。</td></tr>
</table>

	2. 委託機關宜評估是否導入獨立驗證與認證機制（IV&V），評估結果宜經委託機關資通安全長確認。 3. 可參考行政院 111 年 5 月 26 日院臺護字第 1110174630 號函訂定「資通系統籌獲各階段資安強化措施」[工程會資訊服務採購契約範本，請委員依實際狀況檢視機關契約內容] 二、資通安全責任： 1. 涉及利用非受託者自行開發之系統或資源者，並應標示非自行開發之內容與其來源及提供授權證明。廠商於上線前應清除正式環境之測試資料與帳號及管理資料與帳號。 2. 本案金額達新臺幣一千萬元以上，廠商交付之軟硬體及文件，應接受委託機關或其所委託之第三方進行安全性檢測
FQA	