<table>
<tr><td>項目</td><td colspan="3">(五) 資通系統或服務委外辦理之管理措施</td></tr>
<tr><td>5.14</td><td colspan="3">是否訂定委外廠商系統存取程序及授權規定（如限制其可接觸之系統、檔案及資料範圍等）？委外廠商專案人員調整及異動，是否依系統存取授權規定，調整其權限？</td></tr>
<tr><td rowspan="3">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：存取控制</td><td colspan="2">C0101、C0102、C0103</td></tr>
<tr><td>行政院 110 年 3 月 2 日院臺護字第 1100165761 號通函各機關委外廠商進行遠端維護資通系統，應採「原則禁止、例外允許」方式辦理</td><td colspan="2">O01</td></tr>
<tr><td colspan="3">1. 行政院資通安全處 110 年 3 月 2 日院臺護字第 1100165761 號函
(1) 依資通安全管理法施行細則第 4 條及資通安全責任等級分級辦法附表十中有關遠端存取相關規定辦理，並建立及落實管理機制。
(2) 開放遠端存取期間原則以短天期為限，並建立異常行為管理機制。
(3) 於結束遠端存取期間後，應確實關閉網路連線，並更換遠端存取通道(如 VPN)登入密碼。
2. CNS27002：2023
8.2 特殊存取權限、8.3 資訊存取限制、8.4 對原始碼之存取</td></tr>
<tr><td>稽核重點</td><td>機關應定有系統存取控管相關規範，並應包含委外廠商之系統存取及授權規定，且原則應禁止委外廠商遠端維護，例外允許應採短天期並應經權責人員核可。</td><td>佐證資料</td><td>系統存取控管相關規範、申請核可紀錄、異動紀錄</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 委外廠商存取機關各項資源（網路、系統等）之作業程序應符合系統防護基準，另建議不開放遠端連線維護系統，及例外允許相應之控制措施。
2. 了解其必要性，給予最小權限（權限限制、登入時段等）。
3. 對於廠商專案人員異動之管控時，系統權限是否一併調整。
4. 定期監督管理，有檢視妥適性並滾動調整機制。
5. 抽樣檢視。</td></tr>
<tr><td>FQA</td><td colspan="3"></td></tr>
</table>