<table>
<tr><td>項目</td><td colspan="4">(四)資訊及資通系統盤點及風險評估</td></tr>
<tr><td>4.7</td><td colspan="4">是否針對資通系統或資訊處理設施之變更訂定適當之變更管理程序，且落實執行，並定期檢視、審查及更新程序？</td></tr>
<tr><td rowspan="2">稽核依據</td><td colspan="3">資通安全管理法施行細則第 6 條：資通安全維護計畫應包含資通安全防護及控制措施</td><td>P8</td></tr>
<tr><td colspan="4">1. 資通安全管理法施行細則第 6 條第 1 項第 8 款：資通安全防護及控制措施<br>2. 資通安全責任等級分級辦法第 11 條第 1 項：應辦事項之 ISMS 導入及通過公正第三方驗證，ISMS 須符合 CNS 27001 或 ISO 27001<br>3. CNS 27001：<br>（1）7.5.2 制訂及更新：於制訂及更新文件化資訊時，應確保合宜性及適切性之審查及核准<br>（2）表 A.1 控制目標及控制措施：A.12 運作安全-A.12.1 運作程序及責任-A.12.1.2 變更管理：控制措施應控制對影響資訊安全之組織、營運過程、資訊處理設施及系統的變更</td></tr>
<tr><td>稽核重點</td><td colspan="2">訂定資通系統或資訊處理設施之變更管理程序，並定期檢視因應</td><td>佐證資料</td><td>變更管理相關文件</td></tr>
<tr><td>稽核參考</td><td colspan="4">1. 新系統之引進及對既有系統的重大變更，宜遵循議定之規則，以及文件製作、規格、測試、品質控制及受管理的實作之正式過程。宜備妥管理責任及程序，以確保對所有變更進行令人滿意之控制。<br>2. 宜書面記錄並實施變更控制程序，以確保資訊處理設施及資訊系統中資訊之機密性、完整性及可用性，針對由初期設計階段直至所有後續維護工作的整個系統開發生命週期。</td></tr>
<tr><td>FQA</td><td colspan="4"></td></tr>
</table>