<table>
<tr><td>項目</td><td colspan="3">(四) 資訊及資通系統盤點及風險評估</td></tr>
<tr><td>4.4</td><td colspan="3">是否訂定風險處理程序，選擇適合之資通安全控制措施，且相關控制措施經權責人員核可？是否妥善處理剩餘之資通安全風險？</td></tr>
<tr><td rowspan="2">稽核依據</td><td>資通安全管理法施行細第 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 colspan="2">P8</td></tr>
<tr><td colspan="3">1. 資通安全責任等級分級辦法第 11 條第 1 項應辦事項：ISMS 導入及通過公正第三方驗證，ISMS 符合 CNS27001 或 ISO27001
2. CNS27001：20236.1.3 資訊安全風險處理-組織應定義並用用風險處理過程（即程序），以達成下列事項。(b)決定所有必要實作之控制措施，(f)取得對資訊安全風險處理計畫之核准，以及對剩餘資訊安全風險之接受。</td></tr>
<tr><td>稽核重點</td><td>依據所訂風險處理程序，選擇適當之控制措施，並妥善處理剩餘資安風險</td><td>佐證資料</td><td>程序文件、風險評估結果、風險處理措施及時程規劃、改善追蹤、對於剩餘風險之處理</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 辦理風險評估及結果（報告）之審核。
2. 訂定風險處理程序、風險處理計畫。
3. 依風險評估結果，訂定相應之安控措施、時程、權責人員等。
4. 就相應之安控措施有效性之驗證機制。
5. 風險處理選擇
（1）風險修改（風險降低）：藉由施行、移除或改變安全控制措施，已修訂或降低風險等級，使殘餘風險得被重新評定為可接受。
（2）風險保留：根據風險評估結果，確認無進一步行動，而保留風險之決策。如風險等級符合風險接受準則，則不虛實做額外之控制措施。
（3）風險避免：風險避免係藉由從已規劃或現有活動或一組活動中退出，或變更活動運作的情況，做出完全避免風險的決定。如社交工程攻擊，除進行演練作業外，強化認知訓練及宣導，才是防範社交工程攻擊或進階持續攻擊最有效控制措施。</td></tr>
</table>

	（4）風險分擔：依據風險評估結果，將部分風險分擔至能有效管理該特定風險之另一方。如資訊硬體損害之風險可利用保險方案加以分擔，於重大事件發生後，可經由理賠以降低損失之程度，包含人員與資產。
FQA	