<table>
<tr><td>項目</td><td colspan="4">(二) 資通安全政策及推動組織</td></tr>
<tr><td>2.5</td><td colspan="4">是否訂定內部資通安全稽核計畫，包含稽核目標、範圍、時間、程序、人員等？是否規劃及執行稽核發現事項改善措施，且定期追蹤改善情形？</td></tr>
<tr><td rowspan="3">稽核依據</td><td colspan="2">資通安全責任等級分級辦法應辦事項：管理面之內部資通安全稽核(A 級每年 2 次、B 級每年 1 次、C 級每 2 年 1 次)</td><td colspan="2">N10400</td></tr>
<tr><td colspan="2">資通安全管理法施行細則第 6 條：資通安全維護計畫與實施情形之持續精進及績效管理機制</td><td colspan="2">P13</td></tr>
<tr><td colspan="4">1. 通安全責任等級分級辦法第 11 條第 1 項應辦事項：內部資通安全稽核
2. 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 須符合 CNS27001 或 ISO27001
3. CNS27001：20239.2 內部稽核-組織應規劃、建立、實作及維持稽核計畫</td></tr>
<tr><td>稽核重點</td><td>機關應實施內部資安稽核，並應有後續追蹤改善機制。</td><td>佐證資料</td><td colspan="2">內部稽核計畫、內部稽核報告、相關執行紀錄、後續管考紀錄、向資安長報告之紀錄</td></tr>
<tr><td>稽核參考</td><td colspan="4">1. 機關實施內部稽核應以全機關為原則，倘以抽測，應自機關所有內部單位抽測。
2. A 級機關一年需執行至少 2 次內部稽核，考量內部稽核後之改善措施，需執行一定時間方可足夠紀錄顯示其有效性，爰 2 次之間宜間隔至少半年以上。
3. 稽核人員適切性、獨立性、勝任度等。
4. 建議可檢視至少最近 2 次之內稽紀錄，並實際檢視改善情形、久未結案的原因、後續管考方式及改善紀錄。</td></tr>
<tr><td rowspan="2">FQA</td><td colspan="4">[FAQ4.9</td></tr>
<tr><td colspan="4">機關內部資安稽核應涵蓋全機關，非僅限資訊單位，另建議先擬定整體稽核計畫，確認各單位之稽核頻率、稽核委員組成及稽核發現之後續追蹤管考機制等。]</td></tr>
</table>