<table>
<tr><td>項目</td><td colspan="2">(六) 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></tr>
<tr><td>6.3</td><td colspan="2">是否針對所屬/監督之公務機關及所管之特定非公務機關稽核其資通安全維護計畫實施情形，包含訂定稽核計畫及提出稽核報告等？是否規劃及執行對所屬/監督機關稽核發現事項改善措施，且定期追蹤改善情形？
【不適用特定非公務機關】</td></tr>
<tr><td rowspan="5">稽核依據</td><td>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>P13</td></tr>
<tr><td>資通安全管理法第 13 條：應稽核其所屬或監督機關</td><td>L0107060613</td></tr>
<tr><td>資通安全管理法第 16 條：應稽核所管關鍵基礎設施提供者</td><td>L0107060616</td></tr>
<tr><td>資通安全管理法第 17 條：得稽核所管關鍵基礎設施提供者以外之特定非公務機關（即公營事業及財團法人）</td><td>L0107060617</td></tr>
<tr><td colspan="2">1. 資通安全管理法第 13 條第 1 項：公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形。
2. 資通安全管理法第 13 條第 2 項：受稽核機關之資通安全維護計畫實施有缺失或待改善者，應提出改善報告，送交稽核機關及上級或監督機關。
3. 資通安全管理法第 16 條第 4 項：中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形。
4. 資通安全管理法第 17 條第 3 項：中央目的事業主管機關得稽核所管第一項特定非公務機關之資通安全維護計畫實施情形，發現有缺失或待改善者，應限期要求受稽核之特定非公務機關提出改善報告。
5. 資通安全管理法施行細則第 3 條：公務機關或特定非公務機關提出改善報告，應針對資通安全維護計畫實施情形之稽核結果提出下列內容，並依主管機關、上級或監督機關或中央目的事業主管機關指定之方式及時間，提出改善報告之執行情形
6. 資通安全管理法施行細則第 6 條第 1 項第 13 款：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></tr>
<tr><td>稽核重點</td><td>所屬/監督之公務機關及所管特定非公務機關稽核實施情形及後續追蹤改善</td><td>佐證資料</td><td>稽核計畫、稽核報告、相關執行紀錄、後續管考紀錄</td></tr>
</table>

稽核參考	1. 公務機關應稽核其所屬或監督機關之資通安全維護計畫實施情形,稽核對象應包含所有所屬或所監督之機關，無規定要在一年內稽核全部，惟應有整體之規劃，且年份不宜過長。 2. 中央目的事業主管機關應稽核所管關鍵基礎設施提供者之資通安全維護計畫實施情形,稽核對象應包含所有所管 CI 提供者，無規定要在一年內稽核全部，惟應有整體之規劃，且年份不宜過長。 3. 中央目的事業主管機關得稽核所管關鍵基礎設施提供者以外特定非公務機關（財團法人及公營事業）之資通安全維護計畫實施情形，非所有 CI 提供者以外的特定非公務機關皆須稽核，惟宜有評估不實施稽核之準則及記錄。 4. 對所屬之稽核計畫（如時程、頻率、機關遴選原則、領隊&稽核員、稽核方式等）是否合適。 5. 對所屬或所管之資安稽核，應有管考機制。 6. 建議參考 ISO27001 之精神，機關原則於 3 年內完成所屬或監督之公務機關及所管之特定非公務機關稽核（可採分層分批稽核方式），資通安全責任等級 A、B、C 級機關建議以實地稽核方式辦理，資通安全責任等級 D、E 級機關可採書面查核方式辦理。
FQA	