<table>
<tr><td>項目</td><td colspan="2">(七)資通安全防護及控制措施</td></tr>
<tr><td>7.14</td><td colspan="2">資通系統重要組態設定檔案及其他具保護需求之資訊是否加密或其他適當方式儲存（如實體隔離、專用電腦作業環境、資料加密等）？是否針對資訊之交換，建立適當之交換程序及安全保護措施，以確保資訊之完整性及機密性（如採行識別碼通行碼管制、電子資料加密或電子簽章認證等）？是否針對重要資料的交換過程，保存適當之監控紀錄？</td></tr>
<tr><td rowspan="4">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：系統與通訊保護之傳輸之機密性與完整性</td><td>C0601</td></tr>
<tr><td>資通安全責任等級分級辦法附表十資通系統防護基準：系統與資訊完整性之軟體及資訊完整性</td><td>C0703</td></tr>
<tr><td>資通安全責任等級分級辦法附表十資通系統防護基準：系統與通訊保護之資料儲存之安全</td><td>C0602</td></tr>
<tr><td colspan="2">一、機密及敏感性資料處理及儲存之防護措施
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
2. 資通安全責任等級分級辦法第 11 條第 2 項：資通系統防護基準之存取控制、系統與通訊保護-資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。(資通系統高等級者)
二、法規未明訂，其他參考依據：
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
2. 資通安全責任等級分級辦法第 11 條第 2 項：
(1)資通系統防護基準之系統與通訊保護-傳輸之機密性與完整性(資通系統高等級者)
(2)資通系統防護基準之系統與資訊完整性-軟體及資訊完整
3. CNS27002：20238.技術控制措施 8.26 應用系統安全要求事項(b)對所交換或處理之資訊要求之完整性信任等級，以及識別缺乏完整性的機制(例：循環備援核對、雜湊、數位簽章)。</td></tr>
</table>

稽核重點	了解機關是否針對系統與資料傳輸之機密性與完整性建立適當之防護措施	佐證資料	作業規定、組態設定文件、資料傳輸規定、完整性檢查執行紀錄、機關自訂之資料交換之規範、程序、資料交換項目、交換方式清單、保護措施、監控紀錄、資通系統加密連線之測試報告（如 Nmap 檢測結果）
稽核參考	1. 資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。[資通系統防護基準驗證實務 2.6.1.2]如資通系統啟用 SSLV3、TLS1.0 及 TLS1.1 等通訊協定，或所使用演算法包含 RC2、RC4、DES、3DES、MD5 及 SHA 等安全性不足之加密或雜湊演算法，則未符合此控制措施。 2. 高防護需求等級資通系統重要組態設定檔案及其他具保護需求之資訊應加密或其他適當方式儲存。 3. 使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。 4. 使用者輸入資料合法性檢查應置放於應用系統伺服器端。 5. 發現違反完整性時，資通系統應實施機關指定之安全保護措施。 6. 資通系統至少應加密保護資料庫連線位址資訊與連線帳號密碼等機密資訊。 7. 了解系統組態設定檔儲存方式，並可檢視系統組態設定檔，不得以明文呈現資料庫連線資訊及帳號密碼等機敏內容，須使用適當加密方式（如檔案加密、組態欄位加密等）確保機密性。 8. 若組態設定值僅透過簡單編碼（如 Base64 編碼等），因無法有效保護機密性，原則上未符合此控制措施。 9. 資訊交換相關程序及安控措施，若機關為其他機關之資料領用者（例如機關有向內政部取得戶役政資料等），應配合資料提供機關（例如內政部）之規定，並宜將資料提供機關之規定納入自身之資料交換規範。 10. 機關應掌握資料交換項目、交換方式，並應對交換資料的完整性及機密性實施安控措施。		

	11. 資料交換過程應留存相關監控記錄，並有查核機制。
FQA	