<table>
<tr><td>項目</td><td colspan="3">(七)資通安全防護及控制措施</td></tr>
<tr><td>7.26</td><td colspan="3">機關是否對雲端服務應用進行相關資安防護管理?</td></tr>
<tr><td rowspan="2">稽核依據</td><td>資通安全管理法施行細則第 6 條：資通安全防護及控制措施</td><td colspan="2">P8</td></tr>
<tr><td colspan="3">1. 參考國家資通安全研究院網站之共通規範專區所公布「政府機關雲端服務應用資安參考指引」，其內容包括共通資安管理規劃、IaaS、PaaS、SaaS以及自建雲端服務等資安控制措施。
2. ISO/IEC27017：基於 ISO/IEC27002 的雲端服務資訊安全控制之作業規範確保雲端環境中的資料及服務的安全性，其重要控制措施：
(1) 資料隔離及分割
(2) 身分及存取管理
(3) 監控及日誌紀錄
(4) 供應商管理</td></tr>
<tr><td>稽核重點</td><td>雲端服務應用應應針對安全需求實作必要控制措施</td><td>佐證資料</td><td>雲端服務部署規劃、雲端資源配置、更新管理、虛擬防火牆管理、身分存取控制、認證管理、雲端資料備份、清除相關紀錄</td></tr>
<tr><td>稽核參考</td><td colspan="3">下列安全措施提供參考：(參考資安院_政府機關雲端服務應用資安參考指引)
1. 雲端服務部署規劃：機關應依業務需求、欲達成目標及風險評鑑結果，評估採自建或租用方式籌獲雲端服務，並對於資料遷移、資通系統遷移、資料保留及退場機制進行詳細規劃。
2. 當機關發現所建置或租用之雲端服務發生資安事件或營運中斷時，應備有資安事件管理機制與營運持續計畫，進行雲端服務相關損害控管與業務持續運作之管理程序。
3. 可查看虛擬機器資源配置、更新管理、虛擬防火牆管理、身分存取控制、認證管理、雲端資料備份、清除等是否落實管理。</td></tr>
<tr><td>FQA</td><td colspan="3">[資安法 FAQ8.7]</td></tr>
</table>

	1. 政府機關於建置或使用雲端服務時，請參考國家資通安全研究院之共通規範專區所公布「政府機關雲端服務應用資安參考指引」，其內容包括共通資安管理規劃、IaaS、PaaS、SaaS 以及自建雲端服務等資安控制措施。 2. 為使政府機關於建置或使用雲端服務時，降低可能之風險，相關資安要求事項如下： （1）應禁止使用大陸地區（含香港及澳門地區）廠商之雲端服務運算提供者。 （2）提供機關雲端服務所使用之資通訊產品（含軟硬體及服務）不得為大陸廠牌，執行委外案之境內團隊成員（含分包廠商）亦不得有陸籍人士參與，就境外雲端服務之執行團隊成員，至少應具備相關國際標準之人員安全管控機制，並通過驗證。另，雲端服務提供者自行設計之白牌設備暫不納入限制。 （3）機關應評估機敏資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區（含香港及澳門地區），且不得跨該等境內傳輸相關資料。