<table>
<tr><td>項目</td><td colspan="3">(九)資通安全事件通報應變及情資評估因應</td></tr>
<tr><td>9.9</td><td colspan="3">【A、B 級機關適用】是否依指定方式提交 SOC 監控管理資料？</td></tr>
<tr><td rowspan="4">稽核依據</td><td>資通安全責任等級分級辦法應辦事項：管理面之資通安全威脅偵測管理機制</td><td colspan="2">N20300</td></tr>
<tr><td>政府領域聯防監控作業規範</td><td colspan="2">O01</td></tr>
<tr><td>行政院資通安全處 108 年 8 月 23 日院臺護字第 1080186464 號函</td><td colspan="2">O01</td></tr>
<tr><td colspan="3">一、SOC 監控管理資料
1. 資通安全責任等級分級辦法第 11 條第 1 項：應辦事項之資通安全威脅偵測管理機制(A 級及 B 級機關者)，初次受核定或等級變更後之一年內，完成威脅偵測機制建置，並持續維運及依主管機關指定之方式提交監控管理資料</td></tr>
<tr><td>稽核重點</td><td>確認 A、B 級機關是否依主管機關指定之方式提交其 SOC 監控管理資料之情形。</td><td>佐證資料</td><td>SOC 監控管理資料、提交紀錄等。</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 不論自行或委外監控，在 SOC 觸發並記錄事件資料時，即需依「政府領域聯防監控作業規範」回傳下列 3 項 SOC 監控管理資料至聯防監控平台：
(1) 監控設備狀況單（每月 5 日前回傳上月資訊）:納入監控設備之狀況資訊，如設備名稱、型號、資安防護類型及上月觸發次數等，其資安防護類型應包含「端點偵測及應變機制」與「資通安全防護」之辦理內容、目錄服務系統與機關核心資通系統。
(2) 資安監控單（即時回傳）:有監控紀錄即須回傳，其回傳情資須可明確辨識威脅種類（如入侵攻擊、惡意程式等）。
(3) 情資分析單（即時回傳）:為 SOC 分析人員對「資安監控單」進行影響性評估、驗證及關聯分析資訊之情資，如機關綜整評估後無可用情資即無分享。
2. 機關可登入資通安全作業管考系統，查詢自身及所屬機關 SOC 回傳情</td></tr>
</table>

	況。
FQA	