<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>9.8</td><td colspan="3">【A、B 級機關適用】是否建置資通安全威脅偵測管理（SOC）機制？監控範圍是否包括「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之資通設備紀錄及資訊服務或應用程式紀錄？SOC 是否有委外供應商？SOC 供應商是否依契約規範（包含 SLA 水準）確實履約？</td></tr>
<tr><td rowspan="3">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>資通安全管理法施行細則第 6 條：資通系統或服務委外辦理之管理措施</td><td colspan="2">P11</td></tr>
<tr><td colspan="3">一、資通安全威脅偵測管理(SOC)機制及監控範圍
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)，其監控範圍應包括本表所定「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之資通設備紀錄及資訊服務或應用程式紀錄。</td></tr>
<tr><td>稽核重點</td><td>了解機關是否依資通安全責任等級分級辦法 A、B 級機關應辦事項落實情形。</td><td>佐證資料</td><td>機關訂定之監控作業程序、機關訂定之通報應變作業程序、監控規範及相關紀錄（資安事件分析紀錄）、日誌保存機制、契約書</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 了解機關 SOC 是屬於自建或者委外，其建置、管理機制及執行情形。如為委外，契約書之 SLA 應可對應法遵內容。
2. SOC 監控對象、範圍應至少包括「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之資通設備紀錄及資訊服務或應用程式紀錄。
3. SOC 運作機制應包含監控機制、監控原則、通報及事件處理之程序</td></tr>
<tr><td>FQA</td><td colspan="3"></td></tr>
</table>