<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>9.13</td><td colspan="3">是否監控資通系統以偵測攻擊與未授權之連線?是否辦理系統軟體及資訊完整性之控制措施?</td></tr>
<tr><td rowspan="2">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：系統與資訊完整性之資通系統監控、軟體及資訊完整性</td><td colspan="2">C0702、C0703</td></tr>
<tr><td colspan="3">1. 資通安全責任等級分級辦法第 11 條第 2 項：應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表 10 所定資通系統防護基準執行控制措施?
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系統與資訊完整性之資通系統監控–、監控資通系統，以偵測攻擊與未授權之連線（中高）。
3. 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系統與資訊完整性之軟體及資訊完整性–、軟體及資訊完整性之 4 項控制措施（中高）。</td></tr>
<tr><td>稽核重點</td><td>確認機關是否依資通安全責任等級分級辦法附表十「系統與資訊完整性」及系統防護需求等級落實辦理相關法遵作業。</td><td>佐證資料</td><td>資安事件分析紀錄、完整性驗證工具、相關紀錄</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 應建立資通安全通報機制，當發現資通系統遭不當存取、竄改、毀損等疑似入侵攻擊跡象時，可透過當面告知、電話、簡訊、電子郵件訊息等適當聯絡方式，通知相關人員進行適當處理。
2. 驗證已監控防護需求等級中級以上資通系統之連線行為（可使用 WAF、IPS、IDS、惡意程式防護工具、日誌監控及網路監控軟體等），確認已具備必要偵測能力，發現潛在惡意攻擊及未授權使用行為，並留有相關紀錄。
3. 防護需求等級中級以上系統應驗證其完整性，完整性檢查技術如使用密碼雜湊函數、同位元檢查及循環冗餘檢查等，亦可評估採用目錄檔案監控工具，可自動偵測應用程式與網站目錄或檔案之異動事件，並留有紀錄及示警。</td></tr>
</table>

FQA	