<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>9.11</td><td colspan="3">是否依日誌儲存需求，配置所需之儲存容量，並於日誌處理失效時採取適當行動及提出告警？</td></tr>
<tr><td rowspan="3">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：事件日誌與可歸責性之日誌儲存容量、日誌處理失效之回應</td><td colspan="2">C0203、C0204</td></tr>
<tr><td>數位發展部 111 年 11 月 23 日數授資通字第 1112000033 號函修訂各機關資通安全事件通報及應變處理作業程序</td><td colspan="2">O01</td></tr>
<tr><td colspan="3">一、日誌之儲存容量及處理失效之行動與告警
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事件日誌與可歸責-日誌儲存容量依據日誌儲存需求，配置所需之儲存容量，以及日誌處理失效之回應。</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「事件日誌與可歸責性」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>系統備份紀錄與控管文件</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 依據日誌儲存需求（至少保留 6 個月），配置所需之儲存容量。
2. 亦可實作其他控制措施以維持可用之儲存空間：
（1）定期檢查剩餘容量。
（2）超過容量警戒值時通知相關人員。
（3）定期壓縮或歸檔日誌。
（4）定期刪除超過保存期限之日誌。
3. 資通系統於日誌處理失效時，應採取適當之行動。
4. 機關規定需要即時通報之日誌處理失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。</td></tr>
<tr><td>FQA</td><td colspan="3"></td></tr>
</table>
