<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>9.10</td><td colspan="3">是否訂定應記錄之特定資通系統事件（如身分驗證失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為等）、日誌內容、記錄時間週期及留存政策，且保留日誌至少 6 個月？是否有啟用 DNS 及內部網路之相關紀錄日誌日誌時戳是否對應世界協調時間（UTC）或格林威治標準時間（GMT）或相關校時主機?</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記錄事件、日誌紀錄內容、時戳及校時</td><td colspan="2">C0201、C0202C0205</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">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-日誌紀錄內容，資通系統產生之日誌，應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，訂定日誌並保留日誌至 6 個月。
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事件日誌與可歸責-資通系統應使用系統內部時鐘產生日誌需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。</td></tr>
<tr><td>稽核重點</td><td>機關應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辦理相關法遵作業。</td><td>佐證資料</td><td>日誌保存紀錄、相關程序文件。</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 訂定日誌之記錄時間週期及留存政策，並保留日誌至少 6 個月。
（1）範圍：A 級：全部資通系統與各項資通及防護設備、B 級：核心資通系統與相連之資通及防護設備、C 級核心資通系統。
（2）保存項目：作業系統日誌（OSeventlog）、網站日誌（weblog）、應用程式日誌（APlog）、登入日誌（logonlog）。
2. 確保資通系統有記錄特定事件之功能，並決定應記錄之特定資通系統事</td></tr>
</table>

	件。 3. 應記錄資通系統管理者帳號所執行之各項功能。 4. 應定期審查機關所保留資通系統產生之日誌。 5. 資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。 6. 資通系統應使用系統內部時鐘產生日誌所需時戳，並可以對應到世界協調時間（UTC）或格林威治標準時間（GMT）。 7. 系統內部時鐘應定期與基準時間源進行同步。 8. 各機關於日常維運資通系統時，應依自身資通安全責任等級保存日誌（log），並建議定期備份至與原稽核系統不同之實體系統。
FQA	