<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>9.14</td><td colspan="3">知悉資通安全事件後，是否於規定時間內完成損害控制或復原作業，並持續進行調查及處理(包含根因分析、跡證保存及防範措施等)，於 1 個月內送交調查、處理及改善報告，且落實執行？（第一級或第二級事件：72 小時內完成損害控制或復原作業；第三級或第四級事件：36 小時內完成損害控制或復原作業）</td></tr>
<tr><td rowspan="4">稽核依據</td><td colspan="2">資通安全管理法施行細則第 6 條：資通安全事件通報、應變及演練相關機制</td><td>P9</td></tr>
<tr><td colspan="2">資通安全事件通報及應變辦法第 6 條</td><td>L3110082306</td></tr>
<tr><td colspan="2">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>O01</td></tr>
<tr><td colspan="3">一、知悉資通安全事件後之損害控制或復原作業，以及調查、處理及改善報告
1. 資通安全管理法施行細則
（1）第 6 條第 1 項第 9 款：資通安全事件通報、應變及演練相關機制
（2）第 8 條第 1 項：本法第十四條第三項及第十八條第三項所定資通安全事件調查、處理及改善報告
2. 資通安全事件通報及應變辦法
（1）第 6 條第 2 項：公務機關依前項規定完成損害控制或復原作業後，應持續進行資通安全事件之調查及處理，並於一個月內依主管機關指定之方式，送交調查、處理及改善報告。</td></tr>
<tr><td>稽核重點</td><td>確認機關是否落實辦理資通安全事件通報及應變辦法第 6 條法遵及第三級或第四級資通安全事件，應另以密件公文將該報告送交主管機關及上級或監督機關規定。</td><td>佐證資料</td><td>資通安全事件處理紀錄、資通安全事件調查、處理及改善報告</td></tr>
</table>

稽核參考	1. 了解機關資通安全事件管理情形，檢視機關最近之資通安全事件是否於規定時間內（第 1、2 級事件 72 小時，第 3、4 級事件 36 小時）完成損害控制或復原作業並依主管機關指定之方式及對象辦理通知事宜，且持續進行調查及處理，於 1 個月內送交調查、處理及改善報告。 2. 資通安全事件調查、處理及改善報告應包括： (1) 事件發生、完成損害控制或復原作業之時間。 (2) 事件影響之範圍及損害評估。 (3) 損害控制及復原作業之歷程。 (4) 事件調查及處理作業之歷程。 (5) 事件根因分析。 (6) 為防範類似事件再次發生所採取之管理、技術、人力或資源等層面之措施。 (7) 前款措施之預定完成時程及成效追蹤機制（機關應評估短、中、長期資安管理改善策略及追蹤管理）。
FQA	