<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>9.4</td><td colspan="3">是否建立資安事件相關證據資料保護措施，以作為問題分析及法律必要依據？</td></tr>
<tr><td rowspan="4">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 10 條：資通安全事件應變規範應包含事件相關紀錄之保全</td><td>L3110082310</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">1. 資通安全管理法施行細則第 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. 資通安全事件通報及應變辦法
(1) 第 10 條第 1 項第 5 款：公務機關資通安全事件應變作業規範應包含事件相關紀錄之保全
(2) 第 16 條第 1 項第 5 款：特定非公務機關資通安全事件應變作業規範應包含事件相關紀錄之保全
3. 範本_壹拾、資通安全事件通報、應變及演練相關機制</td></tr>
<tr><td>稽核重點</td><td>機關應變相關作業規範應包含事件發生後之復原、鑑識、調查及改善機制。</td><td>佐證資料</td><td>程序書、相關佐證資料。</td></tr>
<tr><td>參考</td><td colspan="3">1. 資安事件相關證據資料保護規範。
2. 資安事件證據資料保護程序。[各機關資通安全事件通報及應變處理作業程序四、跡證保存]
3. 發生資通安全事件時，機關應依下列原則進行跡證保存：
(1) 機關進行跡證保存時，應優先採取隔離機制，包含設備關機、網路連線中斷或隔離、關閉服務、限制連線、限制權限、有限度修補漏洞等方式，以降低攻擊擴散。
(2) 若系統無備援機制，應備份受害系統儲存媒介（例如硬碟、虛擬機映像檔）後，以乾淨儲存媒介重建系統，於完成系統測試後提供服務。</td></tr>
</table>

	(3) 若系統有備援機制，應將服務切換至備援系統提供服務，並保留受害系統及設備，於完成事件根因分析或完整備份後重建系統，經系統測試後切換至原系統提供服務。 (4) 若備援設備亦為受害範圍，於重建受害系統時應以維持最低限度對外運作為原則，保存受害跡證。
FQA	