<table>
<tr><td>項目</td><td colspan="2">(九)資通安全事件通報應變及情資評估因應</td></tr>
<tr><td>9.2</td><td colspan="2">是否訂定資安事件應變作業規範，包含應變小組組織、事前之演練作業、事中之損害控制機制、事後之復原、鑑識、調查及改善機制、相關紀錄保全等，且落實執行？</td></tr>
<tr><td rowspan="4">稽核依據</td><td>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>資通安全事件通報及應變辦法第 10 條：應就資通安全事件之應變訂定作業規範</td><td>L3110082310</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>O01</td></tr>
<tr><td colspan="2">一、資安事件應變作業規範
1. 資通安全管理法：
(1) 第 14 條第 1 項：公務機關為因應資通安全事件，應訂定通報及應變機制。
(2) 第 18 條第 1 項：特定非公務機關為因應資通安全事件，應訂定通報及應變機制。
2. 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，應包括下列事項
3. 資通安全事件通報及應變辦法
(1) 第 10 條第 1 項：公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：包含應變小組組織、事前之演練作業、事中之損害控制機制、事後之復原、鑑識、調查及改善機制、相關紀錄保全等
(2) 第 16 條第 1 項：特定非公務機關應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：包含應變小組組織、事前之演練作業、事中之損害控制機制、事後之復原、鑑識、調查及改善機制、相關紀錄保全等</td></tr>
</table>

稽核重點	機關應依資通安全事件通報應變辦法第 10 條事項辦理相關應辦事項。	佐證資料	資安事件應變作業規範、規範內容之落實紀錄
稽核參考	1. 應就資通安全事件之應變訂定作業規範，其內容應包括下列事項：(１) 應變小組之組織。 (1) 事件發生前之演練作業。 (2) 事件發生時之損害控制機制。 (3) 事件發生後之復原、鑑識、調查及改善機制。 (4) 事件相關紀錄之保全。 (5) 其他資通安全事件應變相關事項。 2. 視事件需要成立編組，並因應資安事件訂定通報應變機制。 3. 檢視機關所訂資通安全事件之應變作業規範，其中對於演練之規定是否落實執行。 4. 檢視駭侵類資安事件，後續事件調查及根因釐清是否落實辦理。		
FQA	5.		