<table>
<tr><td>項目</td><td colspan="3">(六) 資通安全維護計畫與實施情形之持續精進及績效管理機制</td></tr>
<tr><td>6.5</td><td colspan="3">【本項僅總統府與中央一級機關之直屬機關及直轄市、縣（市）政府適用】是否對於其自身、所屬或監督之公務機關，每年辦理 1 次資安事件通報及應變演練?是否針對表現不佳者有強化作為？是否將新興資安議題、複合式攻擊或災害納入演練情境，以驗證各種資安事件之安全防護及應變程序？</td></tr>
<tr><td rowspan="2">稽核依據</td><td>資通安全事件通報及應變辦法第 8 條</td><td colspan="2">L3110082308</td></tr>
<tr><td colspan="3">1. 資通安全事件通報及應變辦法第 8 條：
總統府與中央一級機關之直屬機關及直轄市、縣（市）政府，對於其自身、所屬或監督之公務機關...應規劃及辦理資通安全演練作業，並於完成後一個月內，將執行情形及成果報告送交主管機關。</td></tr>
<tr><td>稽核重點</td><td>機關演練情境是否足以驗證各種資安事件之應處機制</td><td>佐證資烙</td><td>演練計畫、報告及成果、至管考系統填報紀錄。</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 上級 / 監督機關（總統府與中央一級機關之直屬機關及直轄市、縣市政府）應規劃及辦理資通安全演練作業，並於完成後 1 個月內，將執行情形及成果報告送交主管機關。
2. 完成演練後 1 個月逕至管考系統填報演練結果（依行政院秘書長 108 年 4 月 8 日院臺護字第 1080171277 號函）。
3. 了解上級 / 監督對於所屬 / 所監督之機關之資安事件通報及應變演練規劃（時程、規模、方式、內容、追蹤改善管考等）。
4. 機關資安事件通報及應變演練規劃應可與扣合機關資安事件通報及應變作業規範。
5. 資安新興議題，包括但不限於針對雲端應用、行動裝置、巨量資料以及物聯網應用等新興應用所驅動之資安議題。
6. 複合式攻擊（全災害）情境演練，包括但不限於系統遭駭侵致敏感性資料外洩、機房火災致核心系統失能、DNS 遭 DDoS 攻擊且網頁遭駭侵置換等。
7. 演練結果應有相關持續精進及績效管理機制。</td></tr>
</table>

	8. 本項適用範圍請參考附件。
FQA	