<table>
<tr><td>項目</td><td colspan="3">(二)資通安全政策及推動組織</td></tr>
<tr><td>2.2</td><td colspan="3">是否訂定資通安全之績效評估方式（如績效指標等），且定期監控、量測、分析及檢視？</td></tr>
<tr><td rowspan="2">稽核
依據</td><td>資通安全管理法施行細則第 6 條：資通安全政策及目標、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><td colspan="2">P2、P13</td></tr>
<tr><td colspan="3">一、資通安全之績效評估方式
1. 資通安全管理法施行細則第 6 條第 1 項第 13 款：資安全維護計畫與實施情形之持續精進及績效管理機制
2. 資通安全責任等級分級辦法第 11 條第 1 項：應辦事項之 ISMS 導入及通過公正第三方驗證，ISMS 須符合 CNS 27001 或 ISO 27001
3. CNS27001：20239.績效評估-組織應評估資訊安全績效及資訊安全管理系統之有效性-(b)監督、量測、分析及評估之適用方法，以確保有效的結果。組織應保存適切之文件化資訊，作為監督及量測結果的證據</td></tr>
<tr><td>稽核
重點</td><td>檢視機關所訂定資安績效指標之適切性</td><td>佐證
資料</td><td>績效指標、定期檢視紀錄</td></tr>
<tr><td>稽核
參考</td><td colspan="3">1. 應訂定資通安全目標，設定量化與質性指標
2. 績效指標訂定適切性、可行性
3. 定期監控、量測、分析及檢視之方式（何時、方式、依據資訊）
4. 機關資通安全目標應與其資通安全政策一致，並考量適用之資安要求事項及風險評鑑、風險處理之結果，針對是否可以設定為法遵事項無特別限制。
5. 量化型目標（範例）:
（1）核心資通系統可用性達 99.99%以上。(中斷時數/總運作時數 <=0.1%)
（2）知悉資安事件發生，能於規定的時間完成通報、應變及復原作業。
（3）電子郵件社交工程演練之郵件開啟率及附件點閱率分別低於 5%及 2%。
6. 質化型目標（範例）:</td></tr>
</table>

	（1）適時因應法令與技術之變動，調整資通安全維護之內容，以避免資通系統或資訊遭受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他侵害，以確保其機密性、完整性及可用性。 （2）達成資通安全責任等級分級之要求，並降低遭受資通安全風險之威脅。 （3）提升人員資安防護意識、有效偵測與預防外部攻擊等。 7. 不適當的資通安全目標及績效指標。 （1）納入資安事件發生數。 （2）目標或指標設定太低，無精進效益（如近 3 年社交工程演練點閱率皆低於 3%，惟機關資通安全目標設定為點閱率不超過 10%）。
FQA	