<table>
<tr><td>項目</td><td colspan="3">(四) 資訊及資通系統盤點及風險評估</td></tr>
<tr><td>4.1</td><td colspan="3">是否確實盤點全機關資訊資產建立清冊（如識別擁有者及使用者等），且鑑別其資產價值?</td></tr>
<tr><td rowspan="3">稽核依據</td><td>資通安全管理法施行細則第 6 條：資訊及資通系統之盤點，並標示核心資通系統及相關資產</td><td colspan="2">P6</td></tr>
<tr><td>資通安全責任等級分級辦法應辦事項：對自行或委外開發之資通系統，依附表 9 完成系統分級，並完成附表 10 之控制措施；每年至少檢視 1 次資通系統分級妥適性。</td><td colspan="2">N10100</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 6 款：資訊及資通系統之盤點，並標示核心資通系統及相關資產。
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 CNS27001 或 ISO27001
3. CNS27001：本標準各項要求事項，包括 CNS27005(資訊安全風險管理)
4. CNS27005：本標準支援 CNS27001 所規定之一般概念。
附錄 B 資產之識別與估價及衝擊評鑑-B.2 資產估價（估價指鑑別）
CNS27002：20235.9 資訊及其他相關聯資產之清冊</td></tr>
<tr><td>稽核重點</td><td>1. 資訊資產宜包含與資通訊、資安正常維運相關者，包含硬體、軟體、系統或服務。
2. 資訊資產盤點範圍應為全機關及各核心業務與各資訊資產之對應情形。
3. C 級以上機關應每年檢視一次資通系統清冊及分級之妥適性，並應有核可紀錄。</td><td>佐證資料</td><td>資產價值鑑別及分級紀錄、資通系統清單及分級結果核可紀錄</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 資通系統之盤點範圍應涵蓋全機關（含業務單位、輔助單位），建議檢視資通安全維護計畫「資通系統及資訊之盤點」。
2. 資訊資產之盤點應涵蓋全機關（含業務單位、輔助單位），不侷限於 IT（即 OT 也應盤點）、不侷限於連網設備（即不連網設備也應盤點）。[資通系統風險評鑑參考指引]機關可藉由資通系統所提供的業務流程活動，識別該資通系統之資訊及資通系統資產，包括業務流程活動中之資源保</td></tr>
</table>

	管人、所需使用之資源與規範、執行關鍵活動中所產生的紀錄與最後之輸出及度量標準等。 3. 各核心業務與各資通系統或資訊資產之對應情形，核心業務無對應資通系統或資訊資產者之妥適性。 4. 依據資通系統防護需求分級原則進行適當分級（支持核心業務持續運作必要系統列為中級以下之妥適性）。 5. 核心資通系統：指支持核心業務持續運作必要之系統，或系統防護需求等級為高者，是否有不符情形（例如，系統防護需求等級為高，卻沒有被列為核心資通系統）。 6. 機關核心資通系統清單，應經權責人員核定。核定人員建議為資安長或其指派之適階人員。 7. 定期檢視的方式及相關紀錄。 8. 為執行風險評估，故需識別核心資通系統與資訊資產之關聯，可確認機關是否有相關文件足以描述前開關聯，例如但不侷限於將核心資通系統標示於資訊資產盤點結果，或於系統清冊上標示對應之資訊資產。
FQA	