<table>
<tr><td>項目</td><td colspan="3">(七) 資通安全防護及控制措施</td></tr>
<tr><td>7.4</td><td colspan="3">【A、B 級公務機關應於 111 年 8 月 24 日前或核定後 1 年內完成；C 級公務機關應於 112 年 8 月 24 日前或核定後 2 年內完成】
是否完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定方式提交資訊資產盤點資料？是否針對高風險弱點進行修補或執行其他控制措施?
【特定非公務機關：A、B、C 級關鍵基礎設施提供者】</td></tr>
<tr><td rowspan="2">稽核依據</td><td>資通安全責任等級分級辦法應辦事項：技術面之資通安全弱點通報機制</td><td colspan="2">N20500</td></tr>
<tr><td colspan="3">1. 資通安全責任等級分級辦法第 11 條第 1 項應辦事項：
資通安全弱點通報機制導入作業：
初次受核定或等級變更後之一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。
2. 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後一年內，完成資通安全弱點通報機制導入作業，並持續維運及依主管機關指定之方式提交資訊資產盤點資料。</td></tr>
<tr><td>稽核重點</td><td>資通安全弱點通報機制導入作業及持續有效情形</td><td>佐證資料</td><td>VANS 系統（如上傳歷程紀錄查詢、資訊資產列表、資產風險狀態等）、高風險以上弱點修補紀錄、資訊資產清冊、工控系統相關評估紀錄</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. A、B、C 級公務機關皆應依限完成 VANS 導入及提交資訊資產盤點資料。另因等級變更而新增 VANS 應辦事項者，係自資安責任等級核定後起算辦理期限；如等級變更前已有 VANS 應辦事項者，仍依原等級之法遵期限完成。
2. 導入範圍：
(1) 公務機關：以全機關之資訊資產為原則，有關支持核心業務持續運作相關之資通系統主機與電腦應於規定時限內完成導入。
(2) 建議可請機關登入 VANS 系統，並查閱機關 ISMS 資訊資產清冊，自該清冊抽查部分項目是否確實完成上傳。
3. 資訊資產上傳頻率：
(1) 除重大弱點通報或大量資產異動外，每個月至少定期上傳 1 次。</td></tr>
</table>

	(2) 建議可請機關登入 VANS 系統，並透過資訊查詢功能檢視機關近 12 個月的上傳歷程紀錄。 4. 弱點處置： (1) 機關發現高風險以上之弱點，應即時完成修補；於完成修補前，應規劃緩解措施及管理作為，相關弱點處置方式應於 1 週內至 VANS 系統填寫，並納入機關內部稽核與管理審查等機制進行管理，確認弱點改善措施之有效性。 (2) 建議確認機關弱點管理相關規定，並瞭解機關針對 VANS 比對出之高風險弱點是否訂定修補期限；於弱點完成修補前，是否訂定相關防護及管理措施。 (3) 建議可請機關登入 VANS 系統，並檢視機關風險狀態列表（包含資通系統、使用者電腦等 2 類），且優先查看高風險弱點（風險指數 CVSS>=7.0）資產項目之弱點處置填報情形。 (4) 屬工控系統之實務建議：工控系統以能持續運作為首要目標，若 VANS 導入作業會影響相關系統運作，建議先評估是否導入。若導入，則自行開發之程式需盤點至 VANS 系統上進行資產管理。
FQA	