<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>7.5</td><td colspan="3">【A、B 級公務機關應於 112 年 8 月 24 日前或核定後 2 年內完成】
是否完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定方式提交偵測資料？是否偵測異常事件判定為資安事件後有回傳相關資料?
【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：技術面之端點偵測及應變機制</td><td colspan="2">N20600</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：端點偵測及應變機制導入作業(A 級級 B 級機關)
初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。
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，應於修正施行後二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。</td></tr>
<tr><td>稽核重點</td><td>A、B 級機關應依資通安全責任等級公務機關應辦事項辦理「端點偵測及應變機制」相關作業。</td><td>佐證資料</td><td>EDR 相關檢視或執行紀錄</td></tr>
<tr><td>稽核參考</td><td colspan="3">1. 了解機關之端點偵測及應變機制導入現況，施行範圍是否妥當，是否有提交偵測資料。
（1）確認其端點偵測及應變機制。
（2）了解 A、B 級機關是否依照主管機關指定方式提交偵測資料。
（3）辦理內容，如目錄服務系統與機關核心資通系統之資通設備紀錄及資訊服務或應用程式紀錄等。
2. 機關導入 EDR 以全機關為目標，如機關囿於經費，可就從事核心業務之主機與電腦、資安風險程度及資訊資產重要性等，逐步完成導入作業。
3. 機關 EDR 偵測到異常活動，並確認成為資安事件時，即須依律定之 STIX 格式，透由機關 SOC 回傳管道提交偵測資料。
4. 了解近 1 年機關通報資安事件若屬於非法入侵（如植入惡意程式、系統遭</td></tr>
</table>

	入侵等)，其 EDR 回傳情形。
FQA	