<table>
<tr><td>項目</td><td colspan="3">(一)核心業務及其重要性</td></tr>
<tr><td>1.3</td><td colspan="3">是否將全部核心資通系統納入資訊安全管理系統（ISMS）適用範圍？</td></tr>
<tr><td rowspan="2">稽核
依據</td><td colspan="2">資通安全責任等級分級辦法應辦事項：管理面之資訊安全管理系統之導入及通過公正第三方驗證</td><td>N10200</td></tr>
<tr><td colspan="3">一、全部核心資通系統
1. 資通安全管理法施行細則第 7 條第 2 項：核心資通系統指支持核心業務持續運作必要之系統，或依資通安全責任等級分級辦法附表九資通系統防護需求分級原則，判定其防護需求等級為高者為核心資通系統
二、ISMS 之導入或驗證
1. 資通安全責任等級分級辦法第 11 條第 1 項應辦事項：ISMS 導入及通過公正第三方驗證
2. A 級及 B 級機關：全部核心資通系統 2 年內完成 ISMS 導入，3 年內通過公正第三方驗證
3. C 級機關：全部核心資通系統 2 年內完成 ISMS 導入
4. 無 TAF 標誌之處理，請參考資通安全管理法 FAQ_1110523_4.17.</td></tr>
<tr><td>稽核
重點</td><td>全部核心資通系統都應納入 ISMS 適用範圍，A、B 級機關並應通過公正第三方驗證（通過我國標準法主管機關委託機構認證之機構：TAF）。</td><td>佐證
資造</td><td>ISMS 驗證證書、資安政策、核心資通系統清單、相關執行（會議）紀錄</td></tr>
<tr><td>稽核
參考</td><td colspan="3">1. A、B 級機關：全部核心資通系統 2 年內完成 ISMS 導入，3 年內通過公正第三方驗證，第三方驗證機構核發之驗證證書應有 TAF 認證標誌，證書驗證範圍應包括全部核心資通系統，且應為有效之證書。
（1）核心資通系統發生異動後，建議規劃相關 ISMS 導入（驗證）計畫，ISMS 導入範圍應於 2 年內完成更新；ISMS 驗證範圍應於 3 年內完成更新。
（2）證書有效性的判定原則：A.證明文件於機關維運核心資通系統時應在有效期內。B.證明文件須顯示出全部核心資通系統在驗證範圍內。C.ISO27001：2013 證書認列至 114 年 10 月 31 日為止，各機關應於該</td></tr>
</table>

	期限內完成轉版。 2. C 級機關：全部核心資通系統 2 年內完成 ISMS 導入。 3. 是否定期檢視範圍的適切性。(ISMS 導入範圍係機關維運之全部核心資通系統，依「資通安全責任等級分級辦法應辦事項：管理面之資通系統分級及防護基準」規定，每年至少檢視一次資通系統分級妥適性，爰建議機關於每年盤點核心資通系統時同時檢視 ISMS 範圍之妥適性。)
FQA	[FAQ4.3]
	核心資通系統不論是委外或自行維運，皆須導入 CNS27001 或 ISO27001 等資訊安全管理系統標準，並相關安全性檢測。