項目	(一)核心業務及其重要性	
1.1	是否盤點全機關業務，並進行營運衝擊分析，以識別核心及非核心業務，且盤點對應之資通系統，亦依資通系統防護需求分級原則完成資通系統分級，以及依資通安全管理法施行細則識別核心資通系統？每年是否至少檢視 1 次分級之妥適性？	
稽核依據	資通安全管理法施行細則第 6 條：核心業務及其重要性、資訊及資通系統之盤點	P1、P6
	資通安全管理法施行細則第 7 條：核心業務定義 1.公務機關依其組織法規，足認該業務為機關核心權責所在。 2.各機關維運、提供關鍵基礎設施所必要之業務。 3.各機關依資通安全責任等級分級辦法第四條第一款至第五款或第五條第一款至第五款涉及之業務。	L1110082307
	資通安全責任等級分級辦法應辦事項：初次核定或等級變更後之一年內，針對自行或委外開發之資通系統，依附表九完成資通系統分級，並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。	N10100
	1. 資通安全管理法施行細則第 6 條第 1 項第 7 款：資通安全風險評估。（資通安全風險評估包含鑑別可能造成營運中斷事件之機率及衝擊影響，且進行營運衝擊分析(BIA)） 2. 資通安全管理法施行細則 (1) 第 6 條第 1 項第 1 款：核心業務及其重要性。 (2) 第 6 條第 1 項第 6 款：資通系統及資訊之盤點，並標示核心資通系統及相關資產。 (3) 第 7 條第 1 項：核心業務範圍 (4) 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(CIA)，判定其防護需求等級為高者為核心資通系統 3. CNS27001：20236.1.2-組織應定義及應用資訊安全風險評鑑過程於下列事項中：(1)建立風險準則(2)識別風險：依 CIA(3)分析風險：潛在結	

	果及可能性、等級(4)評估風險：風險準則與分析結果比較、處理優先序		
稽核重點	機關應於資通安全維護計畫中，界定其核心業務	佐證資料	核心及非核心業務檢視紀錄、對應之資通系統清冊、資通系統(含核心及非核心資通系統)之盤點及分級清單、分級結果核可紀錄
稽核參考	1. 機關於界定核心業務及非核心業務時，宜辦理營運衝擊分析，並確認所對應之資通系統。 2. 核心業務，其範圍如下： （1）公務機關依其組織法規，足認該業務為機關核心權責所在。 （2）各機關維運、提供關鍵基礎設施所必要之業務。 （3）各機關依資通安全責任等級分級辦法第 4 條第 1 款至第 5 款或第 5 條第 1 款至第 5 款涉及之業務。 3. 機關應於資通安全維護計畫中界定其核心業務，C 級以上機關應每年檢視一次資通系統盤點及分級妥適性 4. 定期檢視的方式及相關紀錄。 5. BIA 分析結果應能呼應資安風險評鑑之結果與核心資通系統之關鍵性。 6. 核心資通系統：支持核心業務持續運作必要之系統、或防護需求等級為高者之資通系統；機關涉及核心業務之資訊系統皆須納入核心系統，再依資通安全責任等級分級辦法附表 9 進行分級（核心系統資通安全防護等級不一定為高）。 7. 依資通安全責任等級分級辦法應辦事項，A、B、C 級機關，針對自行或委外開發之資通系統，依附表九完成資通系統分級（CIAL），並完成附表十之控制措施；其後應每年至少檢視一次資通系統分級妥適性。 8. 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	[資安法 FAQ8.4] Q：若系統資料含特種個資，該系統防護需求等級是否一定要列為「高」？若含一般個資，系統防護需求等級是否一定要列為「中」以上？或是依系統所含個資種類、數量等，是否有建議的系統防護需求分級參考？
	A：各機關應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，就機關業務屬性、系統特性及資料持有情形等，訂定較客觀及量化之衡量指標，據以一致性評估機關資通系統之防護需求。