項目	(一)核心業務及其重要性	
1.5	核心資通系統是否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）？是否明確訂定核心資通系統之系統復原時間目標（RTO）及資料復原時間點目標（RPO）？是否訂定備份資料之復原程序，且定期執行回復測試，以確保備份資料之有效性？復原程序是否定期檢討及修正？	
稽核依據	資通安全責任等級分級辦法附表十資通系統防護基準：營運持續計畫之系統備份	C0301
	一、資通系統之備份作業及異地存放 1. 資通安全責任等級分級辦法第 11 條第 2 項：應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表 10 所定資通系統防護基準執行控制措施 2. 資通安全責任等級分級辦法附表 10 資通系統防護基準之營運持續計畫系統備份：應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份（資通系統等級高等級者）執行系統源碼與資料備份（資通系統等級普/中/高等級者）	
	二、進行 BIA 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))二、訂定 RTO 及 RPO 2. 資通安全責任等級分級辦法第 11 條第 2 項：附表 10 資通系統防護基準之營運持續計畫： （1）系統備份：訂定系統可容忍資料損失之時間要求。(RPO) （2）系統備援：訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。(RTO)	
	1. 資通安全責任等級分級辦法第 11 條第 2 項：應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表 10 所定資通系統防護基準執行控制措施 2. 資通安全責任等級分級辦法第 11 條第 2 項：附表 10 資通系統防護基準	

	之營運持續計畫系統備份：應將備份還原，作為營運持續計畫測試之一部分。(高）應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。(中/高）		
稽核重點	檢視機關所訂定的 BIA、RTO、RPO 之適切性檢視核心資通系統資料備份復原程序、有效性及其落實情形	佐證資料	備份機制相關程序或文件、備份復原測試及程序調修改善紀錄、營運衝擊分析結果、營運持續演練成果及滾動調整記錄
稽核參考	1. 核心資通系統 BIA 分析結果。 2. 核心資通系統 RTO 及 RPO 之適切性（建議與契約規定相符），宜以業務流程角度評估，評估人員宜包含業務單位、資訊單位，且評估結果應經權責人員核定，核心資通系統之 RTO 亦不宜大於非核心資通系統之 RTO。 3. RTO 與 RPO 無直接關係。 4. 確認備分週期不可大於 RPO 設定。 5. 中、高等級系統應依系統分級定期執行各類的備份媒體之可靠性、完整性及可還原性測試，確認是否符合 RTO 及 RPO，並留存相關測試紀錄。 6. 檢視回復測試程序（如頻率、方式、測試環境等）及相關紀錄。 7. 依回復測試情形或結果，定期檢視及修正復原程序。 8. MTPD(最大可容忍中斷時間)=RTO+WRT(了解機關 RTO 定義是否包含 WRT;工作恢復時間)，需確認設定之合理性，RTO 不可大於 MTPD。		
FQA			