<table>
<tr><td>項目</td><td colspan="3">(一)核心業務及其重要性</td></tr>
<tr><td>1.2</td><td colspan="3">是否至少針對核心業務訂定最大可容忍中斷時間(MTPD)，並至少針對防護需求為中等級以上之資通系統，訂定從中斷後至重新恢復服務之可容忍時間要求(RTO)，及可容忍資料損失之時間要求(RPO)？是否依 RPO 訂定資料及系統之備份頻率？</td></tr>
<tr><td rowspan="3">稽核依據</td><td>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。(防護需求為中等級以上者)</td><td colspan="2">C0301</td></tr>
<tr><td>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：(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)</td><td colspan="2">C0301、
C0302</td></tr>
<tr><td colspan="3">1. 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)
2. 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
3. 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)</td></tr>
<tr><td>稽核重點</td><td>檢視機關所訂定的 MTPD、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</td><td>佐證資料</td><td>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</td></tr>
</table>

稽核參考	1. 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。 2. 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。 3. RTO 與 RPO 無直接關係。 4. 確認備份週期不可大於 RPO 設定。
FAQ	