

項目	(一) 核心業務及其重要性
1.1	是否 <b>盤點</b> 全機關業務，並進行營運衝擊分析，以 <b>識別</b> 核心及非核心業務，且 <b>盤點</b> 對應之資通系統，亦依資通系統防護需求分級原則 <b>完成</b> 資通系統分級，以及依資通安全管理法施行細則 <b>識別</b> 核心資通系統？每年是否至少 <b>檢視</b> 1 次分級之妥適性？
1.2	是否至少針對核心業務 <b>訂定</b> 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， <b>訂定</b> 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 <b>訂定</b> 資料及系統之備份頻率？
1.3	所有資通系統是否 <b>定期執行</b> 系統源碼與資料備份？防護需求為高等級之資通系統，其軟體與其他安全相關資訊是否 <b>儲存</b> 於與運作系統不同地點之獨立設施或防火櫃中？防護需求為中等級以上資通系統之備份資訊，是否 <b>定期測試</b> 備份資訊，以 <b>驗證</b> 備份媒體之可靠性及資訊之完整性？
1.4	防護需求為中等級以上之資通系統是否 <b>設置</b> 系統備援，原服務中斷時，於可容忍時間內，由備援設備或其他方式 <b>取代</b> 並提供服務？
1.5	是否至少對全部核心資通系統 <b>訂定</b> 營運持續計畫，營運持續計畫內容至少包含人員職責應變、作業程序、資源調度機制及檢討改善措施等，並 <b>定期辦理</b> 業務持續運作演練？(A 級機關：每年 1 次；B、C 級機關：每 2 年 1 次)
1.6	資安治理成熟度 <b>評估</b> 等級為何？並依評估結果 <b>檢討</b> 相關策進作為？評估等級是否經內部 <b>簽核</b> 程序、 <b>召開</b> 會議或其他適當方式確認？(A、B 級機關適用，以達到 3 級為目標)
1.7	是否將全部核心資通系統 <b>納入</b> 資訊安全管理系統 (ISMS) 適用範圍？