

項目	(四)資訊及資通系統盤點及風險評估		
4.3	是否 建立 風險準則且 執行 風險評估作業，並針對重要資訊資產及委外業務項目 鑑別 其可能遭遇之風險， 分析 其喪失機密性、完整性及可用性之衝擊？		
稽核 依據	資通安全管理法施行細則第 6 條：資通安全維護計畫應包含資通安全風險評估		P7
	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，ISMS 符合 CNS27001 或 ISO27001 2. 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	訂定風險準則，並依據可能遭遇風險鑑別重要資訊資產喪失 CIA 之衝擊。	佐證 資料	資產清冊、資訊安全風險列表、風險管理程序
稽核 參考	1. 了解機關所 訂定 之風險管理程序文件、機關風險評估準則、衝擊準則及風險接受準則等風險管理基本準則，建議檢視機關資通安全維護計畫「資通安全風險評估」。 2. 界定 風險評估範圍，並清查 盤點 該範圍內所有相關的資通系統。 3. 委外 業務項目之風險評估，對於現有資產、流程、作業環境或特殊對機關之威脅造成可能影響。 4. 風險評估 成員 宜包含施政業務與支援該業務之資通系統相關人員，不宜只交由資訊或資安人員負責，以避免產出結果過於主觀，不符合該機關的真實現況。 5. 抽樣 檢視風險評估適切性。 6. 不可接受 之風險等級及風險評估結果（包含不可接受風險之資產清單）宜經機關管理層級審查並核定。 7. 下列方法提供參考： [資通系統風險評鑑參考指引]		

- (1) CNS31010 提供**風險評鑑方法**：A.企業衝擊分析 (BIA)：高階風險評鑑。B.後果/機率矩陣:詳細風險評鑑。
- (2) **風險值**=資訊及資通系統**資產**價值 x **脆弱性**利用難易度 x **威脅**發生可能性。
- (3) 資通系統**風險管理**過程：風險溝通及諮詢、建立全景、風險評鑑、風險處理、風險監控與審查。
- (4) **高階**風險評鑑方法：如資通安全責任等級分級辦法附表九，安全等級分為 3 級 (普、中、高)、4 大影響構面 (機密性、完整性、可用性、法律遵循性)，**評定**資通系統安全等級。
- (5) **詳細**風險評鑑方法：詳細風險評鑑對於**資產**進行深度之識別與鑑別作業，並針對資產詳細列出其可能面臨之威脅與可能存在之脆弱性，以做為評鑑其風險與風險處理方法之依據，詳細之步驟需考慮時間、耗費程度及專家意見等。
- A.**風險識別**：資產識別、威脅與脆弱性識別、現有控制措施識別、後果識別。
- B.**風險分析**：後果評鑑 (含資訊及資通系統資產價值評鑑)、事件可能性評鑑、決定風險等級。
- C.**風險評估**：決定風險可接受等級。

FQA