

項目	(八) 資通系統發展及維護安全		
8.4	資通系統設計階段，是否依系統功能及要求，識別可能影響系統之威脅，進行風險分析及評估？		
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：系統與服務獲得之系統發展生命週期設計階段系統文件		C0502、C0508
	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：資通系統防護基準之系統與服務獲得-系統發展生命週期設計階段：根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。		
稽核 重點	應識別可能影響系統之威脅，進行風險分析及評估	佐證 資料	風險評估及處理文件、資通系統安全檢視表、資通系統安全需求修正紀錄
稽核 參考	針對防護需求等級中、高者，於資通系統設計階段，根據系統功能與要求，應識別可能影響系統之威脅，包含偽冒、竄改、否認行為、機敏資訊外洩、拒絕存取服務及權限提升等，足以危害系統機密性、完整性及可用性之系統存取行為，進行風險分析及評估，且將風險評估結果（風險評估執行紀錄或報告）回饋需求階段之檢核項目，並提出安全需求修正（資通系統安全需求修正紀錄）。		
FQA			