

項目	(八) 資通系統發展及維護安全		
8.2	資通系統開發程序是否依安全系統發展生命週期 ( Secure Software Development Life Cycle, SSDLC ) 納入資安要求？並是否有檢核機制？		
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需求階段、系統文件		C0501~C0508
	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		
稽核 重點	自行或委外開發之資通系統各階段應遵循 SSDLC	佐證 資料	資通系統盤點清冊、資通系統安全發展程序、各階段落實相關紀錄、契約書
稽核 參考	1. SSDLC 各階段安全需求 ( 需求確認、風險評估、修正需求、源碼檢測、滲透測試、弱掃、版控、環境區隔、系統文件 ) 皆應納入資通系統安全發展程序。 2. 各階段的安全需求達成情形應有檢核機制。		
FQA			