

項目	(八) 資通系統發展及維護安全		
8.10	資通系統測試如使用正式作業環境之測試資料，是否針對測試資料建立保護措施，且留存相關作業紀錄？		
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：系統與通訊保護		C0602
	1. 資通安全管理法施行細則第 6 條第 1 項第 8 款：資通安全防護及控制措施 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：資通系統防護基準之系統與服務獲得-系統發展生命週期測試階段，執行源碼掃描安全檢測，以及滲透測試安全檢測（資通系統高等級者）。 4. 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-獲得程序，開發、測試及正式作業環境應為區隔。(中高) 5. CNS27002：2023 技術控制：8.33 測試資訊		
稽核 重點	測試資料如使用正式資料，應有保護措施	佐證 資料	測試資料來源、測試資料刪除紀錄。
稽核 參考	1. 測試資料應以不使用正式資料為原則，倘需使用正式資料，並應有保護機制（例如遮罩等，並應特別注意敏感測試資料之保護）。 2. 測試資料於使用後應即移除並有覆核機制，並留存紀錄。		
FQA			