

項目	(五)通系統或服務委外辦理之管理措施		
5.13	委外廠商專案成員進出機關範圍是否被限制？對於委外廠商駐點人員使用之資訊設備（如個人、筆記型、平板電腦、行動電話及智慧卡等）是否建立相關安全管控措施？是否定期檢視並分析資訊作業委外之人員安全、媒體保護管控、使用者識別及鑑別、組態管控等相關紀錄？		
稽核 依據	資通安全管理法第 9 條：選任適當之受託者，並監督其資通安全維護情形	L0107060609	
	資通安全管理法施行細則第 4 條：受託者應採取之其他資通安全相關維護措施	L1110082304	
	一、法規未明訂，其他參考依據： 1. CNS27002：20237.2 實體進入之控制措施 指引：對諸如交付及裝卸區，以及其他未經授權人員可進入之作業場所的進出點，宜加以控管；若可能宜與資訊處理設施隔離，以避免未經授權之存取(e)進出時，檢視及檢查人員及關注方之個人物品。		
稽核 重點	機關應對廠商駐點人員有相關管理規範，包含實體進出、設備管理及存取控管等要求。	佐證 資料	相關管理規範、相關監督及分析紀錄
稽核 參考	1. 委外廠商專案人員經核可後始可進出限定場域及時段。 2. 委外廠商專案人員攜帶之設備，是否有經核可後始可使用之規定，並應遵守機關相關安控規範。 3. 機關是否監督管理委外業務相關紀錄，並應進行檢視與分析（如人員安全管控、媒體與設備安全管控、存取安全、組態管控），並應包含委外廠商專案人員所用機關所有或自攜之設備，降低委外廠商對機關資通安全造成影響。 4. 就委外業務監督管理機制，是否有檢視妥適性並滾動調整機制。 5. 抽樣檢視。		
FQA			

