項目	(八) 資通系統發展及維護安全
8.1	針對自行或委外開發之資通系統是否依資通系統防護需求分級原則完成資通系統分級，且依資通系統防護基準執行控制措施？
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?
8.3	資通系統開發前，是否設計安全性要求，包含機敏資料存取、用戶登入資訊檢核及用戶輸入輸出之檢查過濾等，且檢討執行情形？
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？
8.5	資通系統開發階段，是否針對安全需求實作必要控制措施並避免常見漏洞（如OWASPTop10 等）？且針對防護需求等級高者，執行源碼掃描安全檢測？另是否執行安全性功能測試，且檢討執行情形？
8.6	資通系統測試階段，是否執行弱點掃描安全檢測？且針對防護需求等級高者，執行滲透測試安全檢測？
8.7	資通系統開發如委外辦理，是否將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入契約書？
8.8	是否將開發、測試及正式作業環境區隔，且針對不同作業環境建立適當之資安保護措施？
8.9	是否儲存及管理資通系統發展相關文件？儲存方式及管理方式為何？
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？
8.11	是否針對資通系統所使用之外部元件或軟體、韌體，注意其安全漏洞通告，且定期評估更新？系統之漏洞修復是否測試有效性及潛在影響?