

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

既有系統功能後續擴充						
類型	項目	子項	資料或系統類型			說明：
			高	中	普	
既有系統功能後續擴充	資通安全項目	提供服務商	●	●	◎	說明： 1. 依資通安全責任等級分級辦法第11條第2項，各機關自行或委外開發之資通系統應依該辦法所定資通系統防護需求分級原則完成資通系統分級(高、中、普)，並依「附表十、資通系統防護基準」執行各項控制措施。如涉及關鍵資訊基礎設施CII之資料或系統建議至少符合中級以上。 2. 圖示：●-建議辦理，◎-經機關評估個案有必要辦理時，▲-依委託機關資通安全責任等級辦理，導入方式應依機關要求及個案需求辦理，得納入本案或另於他案採購(經確認納入他案辦理者，本案免辦)。 3. 中央目的事業主管機關就特定類型資通系統之防護基準另有規定者，依其規定辦理。
			◎	◎	◎	資通安全管理法施行細則第4條第1項第1款規定：「受託者辦理受託業務之相關程序及環境，應具備完善之資通安全管理措施或通過第三方驗證。」
			◎	◎	◎	提請機關資安長確認廠商所開發之系統是否有導入必要。
			◎	◎	◎	採購涉及國家安全事項，得限制第三地區含陸資廠商不得參加，工程會107年12月20日工程企字第1070050131號函請參考。
			◎	◎	◎	依資通安全責任等級分級辦法附表一至六應辦事項規定，委託機關認定為核心資通系統時必選。
	符合國際標準規範	機關提供IEC 62443規範要求，廠商符合機關ISO 27701或同級規範	◎	◎	◎	
			◎	◎	◎	
			◎	◎	◎	
	程式碼安全	程式來源不得為來自大陸或港澳地區	●	●	●	若因業務需求且無其他替代方案，仍需使用危害國家資通安全產品時，應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關(數位部)核定，產品未汰換前，並應加強相關資安強化措施

各類資訊(服務)採購之共通性資通安全基本要求參考一覽表

112年9月25日

第三方檢測	廠商提供之應用程式不能有植入後門或木馬程式	●	●	●	●
	於更新程式時提供軟體物料清單 (Software Bill of Materials, SBOM) 及安全測試報告，並於每季提供軟體物料清單及安全測試報告	●	●	●	◎
	原始碼檢測	●	◎	◎	◎
	程式功能上線前主機弱點掃描	●	●	●	●
	程式功能上線前網站弱點掃描	●	●	●	●
	程式功能上線前滲透測試掃描	●	◎	◎	◎
	主機弱點掃描	▲	▲	▲	▲
	網站弱點掃描	▲	▲	▲	▲
	滲透測試掃描	▲	▲	▲	▲
	廠商需參加機關資安規範教育訓練	●	●	●	●
資安教育訓練					
核心資通系統或委託金額達新臺幣一千萬元以上者，委託機關應自行或另行委託第三方進行安全性檢測。					