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

雲端微服務（SaaS）套裝型							
類型		項目	子項	資料或系統類型			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。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 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。
				高	中	普	
		提供服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	●	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。」
			須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準	◎	◎	◎	提供服務項目涉及個資時應納入要求。
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	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。
		身分鑑別/傳輸機密性與完整性	廠商提供機關帳號控管措施	◎	◎	◎	
			廠商提供機關資料傳輸措施	◎	◎	◎	
		事件日誌保存與可歸責性	應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求	●	●	●	

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

雲端微服務（SaaS）套裝型	資通安全項目	供應商及產品安全要求	針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險 1.供應商安全：符合以下任一條件。 (1)廠商有公開漏洞回報應變機制 (2)廠商有第三方檢測團隊執行檢測 2.產品安全：符合以下任一條件。 (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告 (2)提供經商用弱點檢測軟體未含___等級風險之掃描報告 (3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證	●	●	●	2.產品安全：(2)提供經商用弱點檢測軟體未含___等級風險之掃描報告，掃描報告風險接受等級視各機關資安規範要求。
			廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification,CMMC)	◎	◎	-	
		資料安全	未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	●	●	●	
			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	●	●	●	
			廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	●	●	◎	

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

雲端微服務（SaaS）辦公室生產力工具
（含郵件、行事曆、雲端硬碟、即時通訊等）

類型		項目	子項	資料或系統類型 高	中	普	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。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 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。
		提供服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	●	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。」
			須通過CNS 27701或ISO 27701等隱私資訊管理標準、其他具有同等或以上效果之系統或標準	◎	◎	◎	提供服務項目涉及個資時應納入要求。
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	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。
		傳輸機密性與完整性	廠商提供機關資料傳輸措施	●	●	●	
		事件日誌保存與可歸責性	應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求	●	●	●	

雲端微服務（SaaS）辦公室生產力工具	資通安全項目	供應商及產品安全要求	針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險 1.供應商安全：符合以下任一條件。 (1)廠商有公開漏洞回報應變機制 (2)廠商有第三方檢測團隊執行檢測 2.產品安全：符合以下任一條件。 (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告 (2)提供經商用弱點檢測軟體未含___等級風險之掃描報告 (3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證	●	●	●	2.產品安全：(2)提供經商用弱點檢測軟體未含___等級風險之掃描報告乙項，掃描報告風險接受等級視各機關資安規範要求。
			廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification,CMMC)	◎	◎	-	
		防惡意軟體	靜態分析	●	●	●	
			動態沙箱分析	●	●	◎	
		防惡意連結	靜態分析	●	●	●	
			動態沙箱分析	●	●	◎	
		防釣魚郵件	釣魚郵件過濾	●	●	●	
			身分偽冒辨識(anti-spoofing)	●	●	◎	
		資料與個資安全	資料分類與標籤	●	●	●	
			資料加密與存取控制	●	●	◎	
			資料外洩防護	●	●	◎	
			未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	●	●	●	
			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	●	●	●	
			廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	●	●	◎	
		身分驗證與存取控制	多因子認證	●	●	●	
			零信任：身分鑑別/設備鑑別/信任推斷	●	●	◎	

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

既有雲端微服務（SaaS）客製化需求更版							
類型		**項目**	**子項**	**資料或系統類型**			**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。** **2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時** **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。**
				高	**中**	**普**	
既有雲端微服務（SaaS）客製化需求更版	資通安全項目	供應商及產品安全要求	針對供應商、產品之下列要求提出佐證資料，若無符合條件者提請機關資安長確認風險 1.供應商安全：符合以下任一條件。 (1)廠商有公開漏洞回報應變機制 (2)廠商有第三方檢測團隊執行檢測 2.產品安全：符合以下任一條件。 (1)產品經第三方檢測單位未含OWASP TOP 10弱點之報告 (2)提供經商用弱點檢測軟體未含___等級風險之掃描報告 (3)取得第三方認可實驗室認證,如：行動應用App基本資安標章（Mobile Application Basic Security,MAS）、Common Criteria或其他同等級認證	●	●	●	2.產品安全：（2)提供經商用弱點檢測軟體未含___等級風險之掃描報告乙項，掃描報告風險接受等級視各機關資安規範要求。
			廠商通過網路安全成熟度模型認證(Cybersecurity Maturity Model Certification,CMMC)	◎	◎	-	
		資料安全	未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	●	●	●	
			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	●	●	●	

			廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	●	●	◎	

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

雲端平台(PaaS或IaaS)

類型		項目	子項	資料或系統類型			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。
				高	中	普	
		提供平台服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	●	
			廠商不得為大陸地區廠商第三地區含陸資成分廠商	●	●	●	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。
		弱點管理	雲端應用系統平台具備定期檢視PaaS 之應用、組件或 Web服務是否存在漏洞並進行更新修補	●	●	●	
		存取控制	雲端應用系統平台提供帳號安全認證、權限管理、網路安全傳輸及遠端存取控管佐證	●	●	◎	
			須針對維運管道建立基於零信任(ZTA)控管基礎之防護機制，並導入同等(AAL2)或更高等級的多因子身份鑑別機制	●	●	◎	
		事件日誌保存與可歸責性	應提供日誌保存，包括記錄帳號與權限變更、登入名稱、時間、IP 位址、資料存取及重要安全性事件等，應確保其完整與正確性並符合機關保存年限(建議至少六個月)要求	●	●	●	
		營運持續計畫	檢視廠商平台營運持續、資料復原計畫及執行情形	●	●	●	

雲端平台(PaaS或IaaS)	資通安全項目	變更管理/安全管理	雲端應用系統平台具備變更管理制度	●	●	◎	
			雲端應用系統平台具備設定安全管理制度	●	●	●	
		資料安全	未經機關審查同意，不得將雲端資訊系統或儲存資料移至本國以外地區	●	●	●	
			資料於雲端服務之存取、備份及備援之實體所在地不得位於大陸地區(含香港及澳門地區)，且不得跨該等境內傳輸相關資料。	●	●	●	
			廠商對於虛擬主機平台內之虛擬主機映像檔，應強化其儲存與使用安全並提供佐證	●	●	◎	
			雲端應用系統平台內如存有機密或個人資料應依相關法令強化資料安全防護措施	●	●	●	
		資安防護建置持續監控	資安監控(SOC)機制，廠商須提供 7x24 小時全天候監控	▲	▲	▲	
			須提供資安事件應變服務(Emergency Response Service)	▲	▲	▲	
			具備相關網路入侵防護、實體入侵防護、監測活動管理或防毒機制(DDoS 防護服務、防毒、防火牆、IPS/IDS、WAF、APT等)	▲	▲	▲	
			導入端點偵測與回應機制(Endpoint Detection and Respons, EDR)	▲	▲	▲	
			導入VANS (Vulnerability Alert and Notification System, VANS)	▲	▲	▲	
			導入GCB(Government Configuration Baseline)	▲	▲	▲	如有不適用規則，應擬具管理或替代作為，並提請機關資安長確認風險。
		資安演練	DDoS (Distributed Denial of Service)攻防演練	◎	◎	◎	涉及重要對外服務之系統建議評估辦理。
			入侵與攻擊模擬 (Breach and Attack Simulation)演練	◎	◎	◎	涉及關鍵資訊基礎設施之系統建議評估辦理。
			紅藍隊演練	◎	◎	◎	
		資安檢測	主機弱點掃描	●	●	●	該服務屬委託機關之核心資通系統，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。
			網站弱點掃描	●	●	●	
			滲透測試掃描(由檢測人員測試雲端服務是否具備TLS v1.2以上安全通訊協定)	●	◎	◎	
			雲端服務之APP取得行動應用 App 基本資安標章	●	●	◎	
			資安健診	●	●	●	依委託機關需求執行資安檢測，或依機關規劃另案配合執行。

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

<table>
<tr><th colspan="8">資訊系統規劃服務</th></tr>
<tr><th rowspan="2">類型</th><th rowspan="2"></th><th rowspan="2">項目</th><th rowspan="2">子項</th><th colspan="3">資料或系統類型</th><th rowspan="2">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。
2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時
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。</th></tr>
<tr><th>高</th><th>中</th><th>普</th></tr>
<tr><td rowspan="2">資訊系統規劃服務</td><td rowspan="2">資通安全項目</td><td>提供服務商</td><td>不得為大陸地區廠商或第三地區含陸資成分廠商</td><td>●</td><td>●</td><td>●</td><td>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。</td></tr>
<tr><td>資訊服務類規劃標需納入資安政策</td><td>符合機關資訊安全要求規範
1.政府機關：資通安全管理法含子法
2.關鍵基礎設施提供者：國家關鍵基礎設施安全防護指導綱要、關鍵資訊基礎設施資安防護建議
3.金融機構：參照金融監督管理委員會針對銀行、壽險、產險、證券、期貨、保險經紀人、保險代理人相關資安規範
4.教育單位：教育部資通安全管理實施要點、教育體系資通安全責任等級分級作業規定(草案)、教育體系資通安全暨個人資料管理規範、教育部所屬機關及各級公私立學校資通安全工作事項、國立大專校院資通安全維護作業指引、教育部所管特定非公務機關資通安全管理作業辦法
5.醫療院所：基層醫療院所資安防護參考指引</td><td>●</td><td>●</td><td>●</td><td></td></tr>
</table>

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

資訊安全類規劃服務							
類型		項目	子項	資料或系統類型			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。 2.圖示：●-建議辦理，◎-經機關評估個案有必要辦理時 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。
				高	中	普	
資訊安全類規劃服務	資通安全項目	提供服務商	不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	
		審視機關資安規劃	機關已有無法修復之高風險或發生資通安全事件第三級級第四級時，依據機關現況及限制，參考NIST Cybersecurity Framework協助機關規劃資安整體強化措施	●	●	●	

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

應用軟體或系統開發服務

類型		項目	子項	資料或系統類型：高	資料或系統類型：中	資料或系統類型：普	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。
		提供服務商	具備完善之資通安全管理措施	●	●	●	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。」
			須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	◎	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。」
			須具備IEC 62443 資安檢測實驗室（CBTL）資格	◎	◎	◎	
			須具備發佈CVE的資格及能力	◎	◎	◎	
			開發系統導入安全軟體發展生命週期(Secure Software Development Life Cycle,SSDLC)	◎	◎	◎	提請機關資安長確認廠商所開發之系統是否有導入必要。
			不得為大陸地區廠商或第三地區含陸資成分廠商	●	●	●	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。
		符合國際標準規範	協助系統導入及取得CNS27001及ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準驗證	◎	◎	◎	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。

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

			機關提供ISO 27701或同級規範要求，廠商協助系統符合機關ISO 27701制度或同級規範	●	●	●	提供服務項目涉及個資時應納入要求。
		應用程式安全	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
			廠商提供之應用程式不能有植入後門或木馬程程式	●	●	●	
			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	●	●	◎	
		存取控制	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準存取控制控制措施，包含帳號管理、採最小權限原則及遠端存取	●	●	●	
			須針對維運管道建立基於零信任(ZTA)控管基礎之防護機制，並導入同等(AAL2)或更高等級的多因子身份鑑別機制	●	●	◎	
		事件日誌保存與可歸責性	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準事件日誌保存與可歸責性控制措施，應建立日誌保存，包含記錄事件、日誌記錄內容、日誌儲存容量、日誌處理失效之回應、時戳及校時、日誌資訊之保護	●	●	●	
		營運持續計畫	依據系統防護需求分級，本系統為_____級，需依據_____級系統制定系統營運持續計畫控制措施，包含系統備份及系統備援	●	●	●	
		身分識別與鑑別	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準識別與鑑別控制措施，包含內部使用者識別與鑑別、身分驗證管理、鑑別資訊回饋、加密模組鑑別及非內部使用者之識別與鑑別	●	●	●	有關帳號安全如：密碼複雜度、多因子認證等原則，可參考資通安全責任等級分級辦法(附表十，https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030304)
		系統與服務獲得	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準系統與服務獲得控制措施，包含系統發展生命週期需求階段、設計階段、開發階段、測試階段、部署與維運階段、委外階段、獲得程序及系統文件	●	●	●	

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

應用軟體或系統開發服務	資通安全項目	系統與通訊保護	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準系統與通訊保護控制措施，包含傳輸之機密性與完整性及資料儲存之安全	●	●	●	
			資料庫存取及管理操作資料庫之稽核軌跡紀錄，至少包含使用者ID、存取時間、存取之資料庫物件及執行的完整指令	◎	◎	◎	
		系統與資訊完整性	依據系統防護需求分級，本系統為_____級，需符合_____級系統資通系統防護基準系統與資訊完整性控制措施，包含漏洞修復、資通系統監控及軟體、資訊完整性	●	●	●	
			廠商應整體考慮實體、軟體與資料安全，及系統運作的正確性，相關流程應規劃妥適的安全性協定(如TLS保密協定等)，以完整的保護資料不被盜取、竄改，並杜絕發生系統入侵之事件	◎	◎	◎	
		與其他平台系統API介接	其他平台系統介接之網路連線間資料通訊應加密	●	●	◎	
			不得使用管理人員帳號介接資料庫，應另行建立最小(必要)權限的帳號提供應用程式介接資料庫使用	●	●	◎	
			機敏資料的新增、刪除、修改及讀取，應有稽核紀錄	●	●	◎	
			應用系統之資料匯出或介接其它系統，如有去識別化之需求，廠商應配合本機關要求處理	●	●	◎	
		資安防護建置持續監控	資安監控(SOC)機制，廠商須提供 7x24小時全天候監控	▲	▲	▲	
			須提供資安事件應變服務(Emergency Response Service)/IR	▲	▲	▲	
			DDoS 防護服務	▲	▲	▲	
			導入端點偵測與回應機制(Endpoint Detection and Respons, EDR)	▲	▲	▲	
			協助機關就委託案範圍內導入資安弱點通報機制(Vulnerability Alert and Notification System,VANS)	▲	▲	▲	
			導入政府組態基準(Government Configuration Baseline,GCB)	▲	▲	▲	如有不適用規則，應擬具管理或替代作為，並提請機關資安長確認風險。
			導入防毒軟體	▲	▲	▲	

				導入網路防火牆	▲	▲	▲	
				導入入侵偵測及防禦機制	▲	▲	▲	
				導入應用程式防火牆	▲	▲	▲	
				導入進階持續性威脅攻擊防禦措施	▲	▲	▲	
				導入網路流量全時側錄分析	◎	◎	◎	
			資安維運服務	專案建置範圍之系統軟體或硬體設備，發現之安全漏洞，定期完成更新、修補或進行緊急之應變	●	●	●	
			資安演練	分散式阻斷服務(Distributed Denial of Service,DDoS)攻防演練	◎	◎	◎	涉及重要對外服務之系統建議評估辦理。
				入侵與攻擊模擬 (Breach and Attack Simulation)演練	◎	◎	◎	涉及關鍵資訊基礎設施之系統建議評估辦理
				紅/藍隊演練	◎	◎	◎	
			資安檢測	原始碼檢測	●	◎	◎	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。
				程式應用軟體或系統上線前主機弱點掃描	●	●	●	
				程式應用軟體或系統上線前網站弱點掃描	●	●	●	
				程式應用軟體或系統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	▲	▲	▲	
				資安健診	▲	▲	▲	
				取得行動應用 App 基本資安標章	●	●	◎	
				外部攻擊面管理(External Attack Surface Management,EASM)檢測	◎	◎	◎	
			資安治理成熟度評	由專業顧問協助完成標案資安治理成熟度評估	◎	◎	◎	
			資安專責人員	廠商提供資安駐點人員	◎	◎	◎	
			資安教育訓練	提供機關資安及資訊人員 12小時以上	◎	◎	◎	
				提供機關一般人員與主管3小時	●	●	●	
				提供機關資安專責人員取得專業證照	◎	◎	◎	
				廠商需參加機關資安規範教育訓練	●	●	●	

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： 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。
				高	中	普	
既有系統功能後續擴充	資通安全項目	提供服務商	須具備完善資通安全管理措施或通過CNS 27001或ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準	●	●	◎	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。」
			導入安全軟體發展生命週期(Secure Software Development Life Cycle,SSDLC)	◎	◎	◎	提請機關資安長確認廠商所開發之系統是否有導入必要。
			不得為大陸地區廠商或第三地區含陸資成分廠商	◎	◎	◎	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。
		符合國際標準規範	協助系統導入及取得CNS27001及ISO 27001等資訊安全管理系統標準、其他具有同等或以上效果之系統或標準驗證	◎	◎	◎	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。
			機關提供IEC 62443規範要求，廠商符合機關IEC 62443規範	◎	◎	◎	
			機關提供ISO 27701或同級規範要求，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

			廠商提供之應用程式不能有植入後門或木馬程程式	●	●	●	
			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	●	●	◎	
		第三方檢測	原始碼檢測	●	◎	◎	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。
			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	▲	▲	▲	
		資安教育訓練	廠商需參加機關資安規範教育訓練	●	●	●	

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

應用軟體或系統維運服務

類型		項目	子項	資料或系統類型			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。
				高	中	普	
應用軟體或系統維運服務	資通安全項目	提供服務商	不得為大陸地區廠商或第三地區含陸資成分廠商	◎	◎	◎	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。
		符合機關資安政策	機關提供資安規範要求，廠商須符合機關資訊安全要求規範 1.政府機關：資通安全管理法含子法 2.關鍵基礎設施機關：國家關鍵基礎設施安全防護指導綱要、關鍵資訊基礎設施資安防護建議 3.金融機構：參照金融監督管理委員會針對銀行、壽險、產險、證券、期貨、保險經紀人、保險代理人相關資安規範 4.教育單位：教育部資通安全管理實施要點、教育體系資通安全責任等級分級作業規定(草案)、教育體系資通安全暨個人資料管理規範、教育部所屬機關及各級公私立學校資通安全工作事項、國立大專校院資通安全維護作業指引、教育部所管特定非公務機關資通安全管理作業辦法 5.醫療院所：基層醫療院所資安防護參考指引	●	●	●	

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

		應用程式安全	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	●	●	◎	
		資安檢測	主機弱點掃描	▲	▲	▲	
			網站弱點掃描	▲	▲	▲	
			滲透測試掃描	▲	▲	▲	
			資安健診	▲	▲	▲	