資通系統籌獲各階段資安強化措施執行檢核表填寫說明書

<table>
<tr><th>階段</th><th>編號</th><th>檢核項目</th><th>備註</th></tr>
<tr><td rowspan="4">需求階段</td><td>1-1</td><td>依資通安全責任等級分級辦法所定資通系統防護需求分級原則評估等級。</td><td></td></tr>
<tr><td>說明</td><td>請下載 安全等級評估表評估等級，並依照機密性、完整性、可用性及法律遵循性， 選出各系統防護分級(普、中、高)中最高等級。
附表九 資通系統防護需求分級原則
<table>
<tr><th>防護需求等級 / 構面</th><th>高</th><th>中</th><th>普</th></tr>
<tr><td>機密性</td><td>發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。</td><td>發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響。</td><td>發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響。</td></tr>
<tr><td>完整性</td><td>發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。</td><td>發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響。</td><td>發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響。</td></tr>
<tr><td>可用性</td><td>發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響。</td><td>發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響。</td><td>發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響。</td></tr>
<tr><td>法律遵循性</td><td>如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任。</td><td>如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處。</td><td>其他資通系統設置或運作於法令有相關規範之情形。</td></tr>
</table>
備註：資通系統之防護需求等級，以與該系統相關之機密性、完整性、可用性及法律遵循性構面中，任一構面之防護需求等級之最高者定之。</td><td></td></tr>
<tr><td>1-2</td><td>標示資通系統之資通系統防護需求等級供廠商知悉。</td><td></td></tr>
<tr><td>說明</td><td>完成評估系統防護分級後，將對應等級(含以下)的控制措施(如為中，應納入中、普)納入契約書或規格書等相關文件。</td><td></td></tr>
</table>

		(請於檢核表上**備註欄**詳述列於 OO 文件第幾頁)	
	1-3	資通系統資安防護需求等級評估結果應經機關資通安全長確認。	
	說明	請需求單位詳閱後勾選，並於全校資訊資產及資通系統盤點時，一併將該系統盤入。	
	1-4	評估訂定廠商應配置之資通安全專業人員數量及所需能力等相關需求。	
	說明	請依照專案規模大小，於契約書或規格書等相關文件註明廠商應配置資安專責人員數目及參考資安法施行細則第4條第1項第二款規定訂定所需能力。 (廠商應配置至少1名資通安全專業(責)人員且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗。) (請於檢核表上**備註欄**詳述列於 OO 文件第幾頁)	
	1-5	以資通系統籌獲案中資訊經費之5%以上估算資安經費」(請參考招商廠商估價單)為原則，如因實務作業無法達成，應敘明原因及資安作為，依執行方式依下列作法辦理： (1) 採購：應敘明原因及資安作為，報請機關資通安全長核准後辦理。 (2) 委任、行政委託及行政協助：應敘明原因及資安作為，報請委任、委託或請協助機關核准後辦理。	
	說明	**請以資訊經費的5%以上來估算資安經費。** (1) **資訊經費**為採購資訊相關產品之費用； (2) **資安經費**為採購資安設備、服務之費用(如：安全軟體發展生命週期(SSDLC)設計及檢核作業、系統資安防護基準符規作業、系統資安檢測及弱點修補、系統備份還原及持續營運演練、資通安全教育訓練等)。	

		招商估價單如下： **（標的名稱）案第（招標次數）次招標** **廠商估價單（資安作業經費分析範例）** **總標價(含稅)：新臺幣　元整** 1. ※請使用中文大寫(壹、貳、參、萬、仟、佰) 2. 廠商名稱：　（公司印鑑） 3. 負 責 人：　（負責人印鑑）	
	1-6	於資通系統籌獲案之內部成本分析及請廠商提報之估價單等投標文件(請參考招商廠商估價單)中**明列資安經費**。	不限

項次	標的名稱、規格及型號	單位	單 價	000 年	
				數量	總價
1	系統開發				
1-1	安全軟體發展生命週期(SSDLC)設計及檢核作業				
1-2	系統資安防護基準符規作業				
2	系統及設備維運				
2-1	系統資安檢測及弱點修補				
2-2	系統備份還原及持續營運演練				
3	資通安全教育訓練				
小　　計					
合　　計					

<table>
<tr><td></td><td>說明</td><td>請檢附招商廠商估價單或廠商估價單。

（標的名稱）案第（招標次數）次招標
廠商估價單（資安作業經費分析範例）

<table><tr><td rowspan="2">項次</td><td rowspan="2">標的名稱、規格及型號</td><td rowspan="2">單位</td><td rowspan="2">單 價</td><td colspan="2">000 年</td></tr><tr><td>數量</td><td>總價</td></tr><tr><td>1</td><td>系統開發</td><td></td><td></td><td></td><td></td></tr><tr><td>1-1</td><td>安全軟體發展生命週期(SSDLC)設計及檢核作業</td><td></td><td></td><td></td><td></td></tr><tr><td>1-2</td><td>系統資安防護基準符規作業</td><td></td><td></td><td></td><td></td></tr><tr><td>2</td><td>系統及設備維運</td><td></td><td></td><td></td><td></td></tr><tr><td>2-1</td><td>系統資安檢測及弱點修補</td><td></td><td></td><td></td><td></td></tr><tr><td>2-2</td><td>系統備份還原及持續營運演練</td><td></td><td></td><td></td><td></td></tr><tr><td>3</td><td>資通安全教育訓練</td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td></td><td></td><td></td><td></td><td></td><td></td></tr><tr><td colspan="4">小 計</td><td colspan="2"></td></tr><tr><td colspan="4">合 計</td><td colspan="2"></td></tr></table>
總標價(含稅)：新臺幣 元整
1. ※請使用中文大寫(壹、貳、參、萬、仟、佰)
2. 廠商名稱： （公司印鑑）
3. 負 責 人： （負責人印鑑）</td><td>金額大小皆須填寫估價單</td></tr>
<tr><td></td><td>1-7</td><td>廠商資安作業應納入評選項目，如屬依採購法規定無須辦理評選/評審之採購，則仍應以適當方式檢視廠商條件。</td><td></td></tr>
<tr><td></td><td>說明</td><td>資安作業項目請參考資安管理作業自我評估表，</td><td></td></tr>
</table>

或依照資安法施行細則第4條第1項相關規定檢視廠商條件。

（廠商名稱）參與（招標機關）辦理（標的名稱）案之

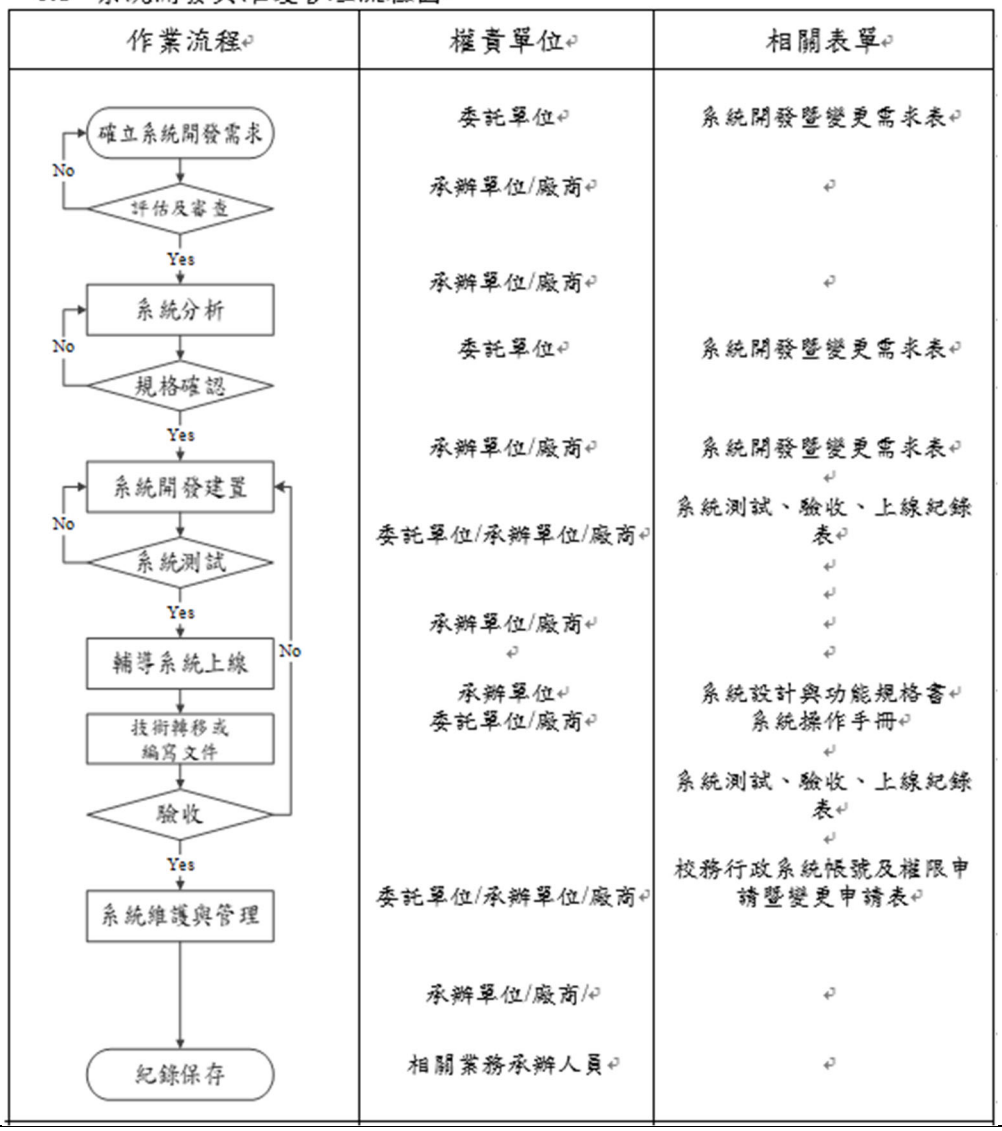
相關資安管理作業自我評估表（範例）

日期： 年 月 日

評估項目	辦理情形
1.管理面	
1.1辦理本專案受託業務相關程序及環境之資通安全管理措施或通過第三方驗證	□辦理本專案受託業務之相關程序及環境已(將)通過_____認(驗)證並持續有效，驗證公司為_____ □辦理本專案受託業務之相關程序及環境已具備完善資安管理措施，詳_____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □本專案受託業務之相關程序及環境未導入適當資安管理措施 備註：_____
1.2本專案之資安負責人、資安專責主管或其他資安人員之人力配置規劃	□本專案之資安負責人(專案主管)為____ □本專案之資安人員為____ □本專案未指派資安負責人、資安專責主管或其他資安人員 備註：_____
1.3本專案之資安風險評估，包含可能之資通系統機密性、完整性、可用性風險，及採取之對應控制措施	□本專案受託業務相關程序及環境之資安風險評估結果已(將)載明於____文件，已(將)採取對應之控制措施詳____文件(如未載明於既有文件內，請於備註欄內說明相關措施) □未就本專案進行資安風險評估 備註：_____
1.4本專案範圍內之資安事件通報應變程序，包含知悉資安事件發生或有發生之虞之相關通報時效規定、通報方式、資安事件調查、處理及改善流程	□本專案受託業務相關程序及環境之資安事件通報應變程序已(將)載明於_____文件(如未載明於既有文件內，請於備註欄內說明相關措施)，知悉資安事件或發現有事件發生之虞時，應於__小時內向甲方等相關利害關係人通報，通報對象包含____ □未就本專案訂定相關資安事件通報及應

1-8	以採適用或準用最有利標，不訂底價為原則，將委託案之相關資安作業納入評選項目(參附件2)，至少佔總分10%；如籌獲案中之資通系統或服務佔比低於10%，至少佔總分5%	非招標案免填
說明	評分比須符合規定。	

	1-9	評選時應要求廠商說明履約之資安作為(請參考相關資安管理作業自我評估表)。	非招標案免填
	說明	請欲參與採購之廠商填寫相關資安管理作業自我評估表，並於評選時請廠商說明公司履約之資安作為。	
	1-10	可參考「資通系統防護基準驗證實務」指引，於規劃(招標)階段訂定對應之廠商專業能力需求資格，俾選任合適廠商。	非招標案免填
	說明	請將資通系統之**資通系統防護需求等級之控制措施**納入契約書或規格書等相關文件，作為訂定廠商專業能力的需求資格要項。(請於檢核表上**備註欄**詳述列於 OO 文件第幾頁)	
	1-11	涉**核心**資通系統籌獲作業且採用**評選**方式選任廠商時，應包含至少1位資安專業評選委員，並符合下列資格之一(如不採用評選方式選任廠商時，則委託機關辦理資通系統籌獲案之團隊應至少包含一位資安專業人員，協助廠商選任作業)： (1) 至少取得資安主管機關認可之國內外發證機關(構)所核發之資通安全專業證照。 (2) 從事資安實務作業3年以上。 (3) 資安教學經驗6年以上。 (4) 公共工程委員會公告之評選委員會專家學者建議名單資料庫中的資訊安全委員。	資通系統防護需求分級普、中級免填
	說明	1. 使用評選方式辦理採購核心系統評選廠商時，應有至少1位資安專業評選委員，並符合上述(1)~(4)的任一條件。 2. 其他方式辦理採購核心系統選任廠商時，應請資安種子人員協助選任廠商作業。	
	1-12	可參考本院110年7月13日院臺護字第1100177483號函「資訊服務採購案之資安檢核事項」(請參考資訊服務採購案之資安檢核事項)辦理，據以確認採購案各項資安要求。	非招標案免填
	說明	請依「資訊服務採購案之資安檢核事項」之**說明**欄位勾選所需項目。	

	1-13	對廠商及其所供應之財物(軟硬體設備)或勞務之資料存取、儲存、備份及備援等作業，其實體所在地及資料傳輸是否跨境相關議題，得要求廠商以書面方式揭露，並納入採購評估參考。	
	說明	請廠商於報價單等文件上，註明實體所在地及資料傳輸是否跨國，以做為採購評估參考。 (請於檢核表上**備註欄**詳述列於 OO 文件第幾頁)	
建置階段	2-1	委託機關之資通安全專責人員應以適當方式協助資通系統籌獲需求單位要求、監督及確認開發團隊於系統開發時遵循安全軟體開發生命周期(SSDLC) 。	
	說明	請依照本校規定，於契約書或規格書等相關文件上註明應**繳交相關階段產生之文件。** (請於檢核表上**備註欄**詳述列於 OO 文件第幾頁) **註：相關文件請資安種子人員至協同平台/ISMS 專區/ISO27001/四階文件表單下載。** 6.1 系統開發與維護管理流程圖  	

	2-2	資通系統籌獲案於採購及驗收時，應有單位之資安窗口協助資通系統籌獲各表單內容確認。	
	說明	請需求單位詳閱後勾選。	
	2-3	**核心**資通系統籌獲案，應聘請外部資安專家為顧問或委員，協助機關於專案重點里程碑中，檢視履約程序與成果之相關資安管理作為。	資通系統防護需求分級普、中級免填
	說明	1. 請需求單位詳閱後勾選。 2. 專案重點里程碑為**採購及驗收**等階段。	
	2-4	受託業務包括委託機關之**核心**資通系統且委託金額達一千萬元以上者，機關應評估導入獨立驗證與認證機制(IV&V)，評估結果應經機關資通安全長確認。	資通系統防護需求分級普、中級免填
	說明	請需求單位詳閱後勾選。	

維運階段	3-1	單位之資安窗口應協助確認資通系統維運作業確實依委託機關之資安管理措施落實辦理。	
	說明	請需求單位詳閱後勾選。	
	3-2	廠商應配置適當之資通安全專責人員，確認履約階段作業符合學校及廠商雙方之資安管理規範。	
	說明	請於契約書或規格書等相關文件上，依照資安法施行細則第4條第1項第二款規定註明「廠商應配置至少1名資通安全專業(責)人員且經適當之資格訓練、擁有資通安全專業證照或具有類似業務經驗。，**確認履約階段作業符合學校及廠商雙方之資安管理規範**」。(請於檢核表上**備註欄**詳述列於 OO 文件第幾頁)	
	3-3	得依資通系統籌獲案之規模及性質，要求廠商應就受委託範圍自行辦理資安稽核作業。	
	說明	請需求單位詳閱後勾選。	
	3-4	資通系統防護需求等級為「高級」之資通系統籌獲，委託機關應以適當方式定期或不定期對廠商辦理資安稽核；「中級」之資通系統，得視需求以適當方式定期或不定期對廠商辦理資安稽核。	
	說明	請需求單位詳閱後勾選。	
	3-5	廠商執行受託業務知悉資安事件，且經**審核為重大資安事件時**，單位**應**辦理資安稽核，並應將稽核結果送交主管機關。	
	說明	請需求單位詳閱後勾選。	
	3-6	可依本院110年12月14日院臺護字第1100194960號函「受託者資通安全聯合查核指引」辦理，集結相關委託機關之查核資源與能量，監督受託者(廠商)之資通安全維護情形，並減少受託者(廠商)受機關查核之頻率。	
	說明	請需求單位詳閱後勾選。	