附件 2　政府資訊作業委外安全檢核表

1. 計畫作業階段

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
1	涉及國家機密業務委外，執行廠商之相關人員應接受適任性查核，並依國家機密保護法之規定，管制其出境		3.1.2.1政府採購資訊安全考量
2	涉及機密性或敏感性資訊之專案，承商的背景是否加強限制？(不允許外國、大陸地區廠商或第三地區含陸資成分廠商，且不得分包給對我國不友善國家之廠商)		3.1.2.1政府採購資訊安全考量
3	是否明示承商必須遵守資安與個資法之要求，及其相關義務與責任		3.1.3.3.1.契約書
4	是否提示承商應注意違反個資法致個資外洩所造成的損害，應負擔損害賠償責任		3.1.3.3.1.契約書
5	是否規定牽涉到甲乙雙方相關資料、專業技術及應用軟體等所有權的歸屬		3.1.3.3.1.契約書
6	專案如係由第三方協助驗收或稽核服務，相關之職掌與作業程序等是否納入RFP之中		3.1.3.3.1.契約書
7	機關是否制定資訊作業委外安全管理政策？是否定期(至少每年一次)檢視		3.1計畫作業階段
8	機關依據前述檢查結果，是否因應缺失、系統及機關的異動或資安事件，更新委外安全政策與程序		3.1計畫作業階段
9	預定委外業務項目是否經檢討分析適合委託辦理		3.1.1委外可行性分析

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
10	預定委外業務項目是否有將資安工作內容列入成本，進行效益分析(包括量化與非量化指標)		3.1.1委外可行性分析
11	委外業務項目是否進行資訊風險評估作業，以強化委外安全。評估風險範圍包含可能影響資產、流程、作業環境或特殊對機關之威脅		3.1.2資訊風險評估
12	機關是否依據資訊作業委外安全管理政策，規劃成立資安組織，並完成相關單位資訊安全權責之分配		3.1.3.1專案編成
13	機關是否依據資訊作業委外安全管理政策與計畫，制定委外作業人員的合法使用規則與相關管理程序		3.1.3.1專案編成
14	機關是否針對各項資訊安全需求，分別在徵求建議書文件(RFP)、委外契約書及服務水準協議(SLA)中明確表達		3.1.3.3資安需求項目規劃
15	機關是否依據資訊作業委外安全政策建立相關安全計畫，並實施管控措施供管理階層檢視與核准		3.1.3.3.2徵求建議書文件(RFP)
16	是否參照資安管理法及相關子法規定，依據系統安全等級說明適當的安全控制措施需求，並舉出驗證方式		3.1.3.3.2徵求建議書文件(RFP)
17	是否明示承商必須遵守資安與個資法之要求，及其相關義務與責任		3.1.3.3.2徵求建議書文件(RFP)
18	承商專業資格是否予以限制或訂定基本要求		3.1.3.3.2徵求建議書文件(RFP)
19	是否依據資訊作業委外安全管理政策與計畫，於徵求建議書文件中要求委外作業人員簽署保密切結書		3.1.3.3.2徵求建議書文件(RFP)

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
20	徵求建議書文件評分表是否將資安列入評選項目		3.1.3.3.2徵求建議書文件(RFP)
21	是否提示承商應遵守個資法中對公務機關與非公務機關之規定		3.1.3.3.2徵求建議書文件(RFP)
22	是否於事前研提資訊安全需求，明訂廠商之資訊安全責任與保密規定		3.1.3.3.2徵求建議書文件(RFP)
23	是否提示承商應注意違反個資法致個資外洩所造成的損害，應負擔損害賠償責任		3.1.3.3.2徵求建議書文件(RFP)
24	是否要求執行稽核作業，請承商提供異常報告，以利後續追蹤與管理		3.1.3.3.2徵求建議書文件(RFP)
25	是否要求承商提出資訊安全管理計畫		3.1.3.3.2徵求建議書文件(RFP)
26	是否要求承商提供人員安全管理規劃是否含專案人員異動之安全管理規劃		3.1.3.3.2徵求建議書文件(RFP)
27	受託業務涉及國家機密其執行廠商之相關人員應接受適任性查核		3.1.3.3.2徵求建議書文件(RFP)
28	參與人員或分包商人員，必須接觸到機密性或敏感性資料者，是否要求其接受素行調查		3.1.3.3.2徵求建議書文件(RFP)
29	當任何一方終止服務時，是否規範應遵循的處理程序？		3.1.3.3.2徵求建議書文件(RFP)
30	是否要求承商配合機關內相關安控措施之協調、推動及督導等事項		3.1.3.3.2徵求建議書文件(RFP)
31	是否要求承商之工作團隊，須遵守各機關有關資訊安全的規範與適時接受資訊安全的規範相關教育訓練		3.1.3.3.2徵求建議書文件(RFP)
32	是否要求承商完成新系統建置時，必須配合訂定緊急應變與回復作業程序		3.1.3.3.2徵求建議書文件(RFP)

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
33	是否要求承商提供新應用程式與系統的開發建置應有之資安積極作為		3.1.3.3.2徵求建議書文件(RFP)
34	是否要求承商提供符合資安要求的系統開發作業程序規劃		3.1.3.3.2徵求建議書文件(RFP)
35	是否明確訂定承商顧問服務達到資訊系統的保密性與可用率等整體安全性的指標		3.1.3.3.3. 服務水準協議(SLA)
36	是否明確訂定承商達到資訊系統的保密性與可用率等整體安全性的指標		3.1.3.3.3. 服務水準協議(SLA)
37	是否根據資安需求項目(如：安全漏洞檢測、承載力檢測、壓力測試及無障礙檢測等)，依專案規模、專案人天及程式行數，列出各種可能計價方式		3.1.3.3.4資安檢測預算
38	涉及國家機密、機密性或敏感性資訊之專案，承商的背景是否加強限制？(不允許外國、大陸地區廠商或第三地區含陸資成分廠商，且不得分包給對我國不友善國家之廠商)		3.1.3.3.1. 契約書
39	涉及與國家安全與機密等相關之特殊業務者，是否禁止專案成員不得有來自大陸地區者		3.1.3.3.1. 契約書
40	是否依據工程會、投審會陸資企業辦理採購		3.1.2.1.4 陸資企業之規範
41	辦理採購涉及簽訂 WTO 政府採購協定對我輸美貿易之影響，如有特殊安全需求，是否應用政府採購法第 22 條採限制性招標，第 16 款「其他經主管機關認定者」事由處理		3.1.3.3.1 契約書

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
42	如需引進與啟用新資訊科技(如軟體、硬體、通信及管理措施等)，是否於事前進行安全評估，了解新資訊科技之安全保護措施與水準，並依行政程序經權責主管人員核准		3.1.2.1.2. 資訊科技保護考量

2. 招標、決標階段

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
1	廠商資格審查是否依 RFP 與契約書規定辦理（含外國、大陸地區廠商或第三地區含陸資成分廠商）		3.2 招標階段
2	遴選評選委員時，是否考量其學經歷、相關領域實務經驗及利益迴避等條件		3.2 招標階段
3	評選廠商投標建議書時，評選委員是否將資安列入評選項目		3.3 決標階段

3. 履約管理階段

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
1	機關是否成立專責單位負責執行相關安控措施之協調、推動及督導等事項		3.4.1 資訊安全組織

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
2	機關與委外廠商是否皆已指定專案管理人員，負責推動、協調及督導資訊安全管理事項？如為大型或複雜的專案是否成立跨部門資訊安全推行小組		3.4.1 資訊安全組織
3	在資訊軟硬體、通訊系統建置時，是否對承商之專案成員規範與限制其可接觸之系統、檔案及資料範圍		3.4.2 委外相關風險識別
4	承商專案成員進出機關範圍是否被限制		3.4.2 委外相關風險識別
5	承商專案成員進出機關，所攜帶之設備與儲存媒體是否被管制		3.4.2 委外相關風險識別
6	是否建立承商專案成員使用者註冊管理制度		3.4.2 委外相關風險識別
7	機關是否訂定承商專案成員系統存取政策與授權規定		3.4.2 委外相關風險識別
8	是否基於實際作業需要，核發短期性與臨時性之系統辨識與通行碼，供承商專案成員使用		3.4.2 委外相關風險識別
9	承商專案成員人員調整與異動，是否依系統存取授權規定，限期調整其權限		3.4.2 委外相關風險識別
10	重要資料委外建檔，不論在機關內外執行，是否採取適當與足夠之安全管制措施		3.4.2 委外相關風險識別
11	是否拒絕提供長期性之系統辨識與通行碼供承商專案成員使用		3.4.2 委外相關風險識別
12	機關是否依據委外作業人員的合法使用規則，並取得對此聲明的簽署，以表示他們在授權存取資訊系統及裡面的資料前，已經閱讀、了解並同意遵守這些行為規範		3.4.3 與廠商協議中之安全說明

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
13	因委外作業所有衍生對應之內部控制措施的安全要求，是否反映在與委外廠商協議中		3.4.3 與廠商協議中之安全說明
14	是否協調完成辦理使用者與行政管理人員在方法、程序及安全上的訓練？辦理委外作業人員對資訊安全責任與事宜的訓練		3.4.3 與廠商協議中之安全說明
15	協議是否敘明委外廠商如何保證維持由風險評鑑所定義之充分安全性，安全如何調適與識別，並因應風險的變更		3.4.3 與廠商協議中之安全說明
16	機關是否有針對資訊作業委外人員之任用制定相關管理政策		3.4.4 委外人力資源安全
17	是否已訂定程序以確保委外承商於合約中止時受到管理，並完成歸還設備、資訊資產及應移交的所有作業程序		3.4.4 委外人力資源安全
18	委外作業人員如違反資訊安全，是否執行正式的懲處		3.4.4 委外人力資源安全
19	是否對所有委外作業人員(含分包與轉包廠商)之背景進行查證檢核		3.4.4 委外人力資源安全
20	機關是否針對資訊作業委外時應對委外承包廠商作業人員、分包廠商及轉包廠商的安全角色與責任予以區分		3.4.5.1 角色與責任 3.4.7.3 職務的區隔
21	機關是否於同意委外作業人員授權存取資訊系統前，針對個人需求完成審查		3.4.5.1.1 篩選
22	委外作業人員是否在機關檢視或更新存取授權前，完成簽署機密性或保密協議		3.4.5.1.2 僱用條款與條件
23	機關是否定期或不定期檢視並分析資訊委外作業之人員安全相關紀錄		3.4.5.2.1 管理階層責任

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
24	機關依前述檢查結果，若發現稽核事件有違反政策，或因系統與組織的異動或資安事件的發生，是否制定因應流程改善或矯正措施		3.4.5.2.1 管理階層責任
25	機關是否依據機關資安政策，發展資訊作業委外安全認知與訓練的政策		3.4.5.2.2 資訊安全認知、教育及訓練
26	機關是否定期或不定期針對委外作業人員開課，訓練其正確使用資訊作業委外及安全的系統操作？		3.4.5.2.2 資訊安全認知、教育及訓練 3.4.9 委外資訊安全事件管理
27	機關是否依據上述管理政策，制定相關的管理程序		3.4.5.2.2 資訊安全認知、教育及訓練
28	機關於執行委外作業時，在授權存取到系統前組織是否對委外作業人員提供基準的安全認知訓練		3.4.5.2.2 資訊安全認知、教育及訓練
29	機關是否檢視委外人員完成資訊作業委外安全訓練課程後的成果(如運用安全演練與系統操作測驗等方式)		3.4.5.2.2 資訊安全認知、教育及訓練
30	機關是否定期或不定期檢視並分析資訊委外作業之安全認知與訓練紀錄		3.4.5.2.2 資訊安全認知、教育及訓練
31	機關依前述檢查結果，若發現稽核事件違反政策,或因系統/組織的異動與資安事件的發生，是否制定因應流程改善或矯正措施		3.4.5.2.2 資訊安全認知、教育及訓練

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
32	是否已訂定程序以確保委外作業人員於離開機關時受到管理，歸還所有相關資訊資產與移除所有的存取權限，並由專人保管離職人員系統紀錄		3.4.4 委外人力資源安全 3.4.5.2.5 終止責任
33	機關於委外作業人員重新指派或轉換工作時，應重新檢視資訊系統與設施授權存取權限		3.4.5.2.4 僱用終止或變更
34	機關是否因應資訊委外作業建立正式且文件化的實體與環境安全管理政策		3.4.6 委外實體與環境安全
35	機關是否依據上述管理政策，制定相關的管理程序		3.4.6 委外實體與環境安全
36	機關是否使用安全周界，以區隔委外作業與內部資訊處理設施的區域		3.4.6 委外實體與環境安全
37	機關是否定期或不定期檢視並分析資訊委外作業之實體與環境安全管控紀錄		3.4.6 委外實體與環境安全
38	機關依前述檢查結果，若發現稽核事件違反政策,或因系統/組織的異動或資安事件的發生，是否制定因應流程改善或矯正措施		3.4.6 委外實體與環境安全
39	機關對於委外使用之資訊設備是否有相關安全管控措施，包括個人電腦、個人數位助理、行動電話及智慧卡等		3.4.6.2 設備安全
40	機關是否妥善管理資訊作業委外產製之相關文件		3.4.7 委外之作業管理 3.4.7.1 文件化作業程序
41	機關內操作程序是否已文件化並維持，且讓有需要的委外作業人員，可隨時或經由要求取得資訊處理與通信設施相關系統活		3.4.7 委外之作業管理 3.4.7.1 文件化

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
	動已文件化之程序，以供委外作業人員遵循使用		作業程序
42	機關資訊作業委外開發或維護是否制定相關系統組態管理政策		3.4.7.2 變更管理
43	機關是否依上述管理政策，制定相關管理程序		3.4.7.2 變更管理
44	機關是否為委外開發或管理之資訊系統發展與維護一套現行之基準組態，並製作相關文件		3.4.7.2 變更管理
45	機關是否對資訊系統之異動進行授權、記錄與控制		3.4.7.2 變更管理
46	機關是否監控資訊系統之異動並實施安全影響分析以確定異動造成之影響		3.4.7.2 變更管理
47	機關是否定期或不定期檢視並分析資訊委外作業之組態管控紀錄		3.4.7.2 變更管理
48	機關依前述檢查結果，若發現稽核事件違反政策,或因系統/組織的異動或資安事件的發生，是否制定因應流程改善或矯正措施		3.4.7.2 變更管理
49	機關是否對於資訊系統異動其個別存取特權需獲得批准、並強制實體與邏輯的存取限制		3.4.7.2 變更管理
50	對於委外職務與責任領域宜加以區隔，以降低機關資產遭未經授權或非意圖的修改或誤用產生，並注意無任何人員可未經授權或未受偵測的存取、修改或使用資產		3.4.7.3 職務的區隔
51	規模較小的機關或委外專案可能認為職務區隔難以達成時，是否考慮其他控制措施，諸如活動的監視、稽核存底及管理監		3.4.7.3 職務的區隔

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
	督等		
52	機關是否訂定資訊作業委外系統開發或維護之相關規範，以落實系統與資訊完整		3.4.7.4 委外開發、測試及運作
53	機關是否依據前述安全管理政策，制定相關程序		3.4.7.4 委外開發、測試及運作
54	機關是否定期或不定期檢視並分析資訊委外作業之系統與資訊整合紀錄		3.4.7.4 委外開發、測試及運作
55	機關依前述檢查結果，若發現稽核事件違反政策,或因系統/組織的異動或資安事件的發生，是否制定因應流程改善或矯正措施		3.4.7.4 委外開發、測試及運作
56	機關是否要求資訊系統開發廠商製作管理計畫，以控制系統於開發階段之變更，追蹤安全缺點，要求任何變更之適當授權，以及計畫與實作之相關文件		3.4.7.4 委外開發、測試及運作
57	機關是否要求資訊系統開發廠商製作一套資安測試與評估計畫，實作此計畫，並將結果文件化		3.4.7.4 委外開發、測試及運作
58	機關是否制定資訊委外作業相關系統與服務取得之管理政策		3.4.7.5 廠商服務交付管理
59	機關是否依據上述管理政策，制定相關的管理程序		3.4.7.5 廠商服務交付管理
60	機關為維持系統與資訊完整，資訊作業委外時是否執行惡意程式防護措施		3.4.7.7 防範惡意碼與行動碼
61	機關是否因應資訊委外作業訂定正式且文件化的媒體保護政策		3.4.7.8 委外媒體的處置
62	機關是否依據上述管理政策，制定相關的管理程序		3.4.7.8 委外媒體的處置

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
63	機關是否定期或不定期檢視並分析資訊委外作業之媒體保護管控紀錄		3.4.7.8 委外媒體的處置
64	機關依前述檢查結果，若發現稽核事件違反政策缺失,或因系統/組織的異動或資安事件的發生，是否制定因應流程改善或矯正措施		3.4.7.8 委外媒體的處置
65	機關各項委外作業所需存取之資訊媒體是否依程序管制並記錄		3.4.7.8.1 可攜式媒體的管理 3.4.7.8.2 系統文件的安全
66	機關是否妥善保存資訊作業委外產製之相關文件		3.4.7.8.2 系統文件的安全
67	機關委外作業使用之儲存媒體宜依製造商規格儲存在安全、受保護及受控制的環境		3.4.7.8.1 可攜式媒體的管理 3.4.7.8.2 系統文件的安全
68	機關是否將機關資訊作業委外安全存取識別與鑑別管理政策納入資安政策？		3.4.8 委外使用者存取管理
69	機關是否依照資訊作業委外安全政策與相關設備的存取識別與鑑別政策，制定相關管理程序		3.4.8 委外使用者存取管理
70	機關是否透過帳號、識別證及卡片等機制，區分委外作業人員具有「唯一」的識別符並可以驗證每一位使用者的身分		3.4.8 委外使用者存取管理
71	機關是否定期或不定期檢視並分析資訊委外作業之使用者識別與鑑別紀錄		3.4.8 委外使用者存取管理
72	機關依前述檢查結果，若發現稽核事件違反政策,或因系統/組織的異動或資安事件的發生，是否制定因應流程改善或矯正措施		3.4.8 委外使用者存取管理

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
73	機關是否依照組織政策而制定資訊作業委外相關存取控制管理政策		3.4.8 委外使用者存取管理
74	機關是否依上述管理政策，制定相關管理程序		3.4.8 委外使用者存取管理
75	機關是否管理委外作業人員相關管理系統的帳號(包括帳號的建立、啟動、修改、定期審查、停用及移除)		3.4.8 委外使用者存取管理
76	機關是否定期或不定期檢視並分析資訊委外作業存取控制管控紀錄		3.4.8 委外使用者存取管理
77	機關依前述檢查結果，若發現稽核事件違反政策,或因系統/組織的異動或資安事件的發生，是否制定因應流程改善或矯正措施		3.4.8 委外使用者存取管理
78	機關是否因應資訊委外作業訂定正式且文件化的事件反應政策		3.4.9 委外資訊安全事件管理
79	機關是否依據上述管理政策，制定相關的管理程序		3.4.9 委外資訊安全事件管理
80	機關委外作業人員是否定期實施事件反應訓練，使委外作業人員了解其角色與責任		3.4.9 委外資訊安全事件管理
81	機關委外作業人員是否具備資安事件處理或反應能力		3.4.9 委外資訊安全事件管理
82	機關委外作業人員於資安事件發生時，是否依程序向機關業務承辦人或主管提出報告		3.4.9 委外資訊安全事件管理
83	機關是否定期或不定期檢視並分析資訊委外作業之事件反應組態管控紀錄		3.4.9 委外資訊安全事件管理
84	機關依前述檢查結果，若發現稽核事件違反政策,或因系統/組織的異動或資安事件的發生，是否制定因應流程改善或矯正措施		3.4.9 委外資訊安全事件管理

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
85	機關是否要求委外資訊系統服務之提供者採用適當的資安控制措施，並遵循政府法律、政策、規章、標準及服務等級協議(SLA)		3.4.10 遵循適法性要求

4. 驗收階段與保固作業

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
1	機關(構)是否有定期或不定期檢視並分析資訊委外作業之系統和服務取得相關紀錄？		3.5 驗收階段
2	廠商於簽約後是否如期提交「專案工作計畫書」		3.5 驗收階段
3	廠商於簽約後是否如期提交「驗收計畫書」		3.5 驗收階段
4	廠商是否定期召開工作進度報告會議，並提交工作報告		3.5 驗收階段
5	配合各階段需求，規劃並實施充足之教育訓練，推動並提昇委外作業人員資安知識與技能		3.5 驗收階段
6	廠商是否依機關要求格式，交付契約內要求之各項文件		3.5 驗收階段
7	廠商是否負責製作專案進行過程中每次會議之紀錄，交由機關確認		3.5 驗收階段
8	是否完成程式源碼檢測，執行程式弱點掃描		3.5.1 資安檢測

參考指引名稱	政府資訊作業委外安全參考指引	指引版本	V4.0
項次	查核項目	是否完成	備考(對照章節)
9	是否定期執行系統弱點掃描		3.5.1 資安檢測
10	發現資安弱點與可能面臨的威脅，是否請原設計廠商提供變更計畫		3.6.1 異常管理
11	執行中之資訊系統發生異常或系統漏洞時，機關對是否詳細評估承商所提之變更計畫對系統的影響並獲得批准		3.7.1 異常管理

註：備考欄內有( )說明者，指僅與該類服務有關，未標明者表示與三類服務均有關。