附表三

國軍委外廠商資安自我查核項目表

專案名稱（契約編號）：

受託單位名稱：

資通系統名稱：

填表日期：

填寫人員：

註 1：
適用範圍：表示屬於此服務類之受託單位應填寫該項查核內容
註 2：
符合：受託單位依據查核內容之要求已辦理
不符合：受託單位未辦理或未規劃查核內容之要求
不適用：受託單位不適用查核內容之要求

查核項目	查核內容	適用範圍(註1)	自我查核結果(註2)			自我查核佐證
			符合	不符合	不適用	
1.配置適當之資通安全專業人員及適當之資源	1.1 是否配置資安人力？(請說明目前公司有配置多少資安人力)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	
2.資訊及資通系統之盤點及風險評估	2.1 各項資產(如 NAS 主機、版控軟體、版控主機、監控主機、儲存主機、各類伺服器等)是否造冊列管並說明各項資產之管理者及使用者？(請說明多久更新造冊內容及各項資產之管理者及使用者)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	

查核項目	查核內容	適用範圍(註1)	自我查核結果(註2)			自我查核佐證
			符合	不符合	不適用	
	2.2 對於上述所提及之資產項目當發生異常狀態時(如設備異常、空間不足…等)，處理機制為何？(請說明處理機制，如設備有備品、設備採用 HA 架構…等)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	
3.資通安全管理措施之實施情況	3.1 人員進入廠商之重要實體區域是否訂有安全控制措施？(請說明實體區或機房區管理文件名稱並說明管理方式) **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	
	3.2 電腦機房及重要地區，對於進出人員是否作必要之限制及監督其活動？(請說明人員進出管理方式及 CCTV 保留影像) **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	
	3.3 電腦機房操作人員是否隨時注意環境監控系統，掌握機房溫度及溼度狀況？(請說明機房溫溼度範圍) **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	
	3.4 電腦機房之環控設備(消防、空調、UPS、發電機)是否定期檢查？(請說明環控設備多久檢查) **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	
	3.5 第三方支援服務人員進入重要實體區域是否經過授權並陪同或監視？(請說明人員進入實體區之管理方式) **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	

查核項目	查核內容	適用範圍(註1)	自我查核結果(註2)			自我查核佐證
			符合	不符合	不適用	
	3.6 重要資通設備之設置地點是否檢查及評估火、煙、水、震動、化學效應、電力供應、電磁幅射或民間暴動等可能對設備之危害？(請說明有機房內設置有哪些安全管控，如偵煙系統、漏水偵測) **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	
	3.7 電腦機房或重要區是否制定可攜式媒體(如筆電、磁帶、磁片、光碟片、隨身碟及報表等)管理方式？(請說明攜帶可攜式媒體進入電腦機房或重要區時管理方式) **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	
	3.8 電源之供應及備援電源是否配置發電機或 UPS 等機制？ **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） SOC 監控服務之受託單位	□	□	□	

查核項目	查核內容	適用範圍(註1)	自我查核結果(註2)			自我查核佐證
			符合	不符合	不適用	
	3.9 對於本專案之重要、機密、敏感、版控等相關資料儲存於廠商內部之設備(如 Storage、NAS、版控主機…等)是如何管理？ (1)資料文件存放於那些設備？ (2)是否定期保養、設備送場外維修？ (3)報廢管理方式？ (4)多久備份一次？ (5)備份資料是否定期回復測試？ (6)是否制訂使用者存取權限註冊及註銷之作業流程？ (7)是否定期審查存取權限之合宜性？(多久審查一次) (8)登入帳號是否設定密碼原則為長度超過 8 位字元(特權帳號 12 位字元)，並啟用密碼複雜度原則(大小寫字母、數字及符號至少 3 種以上組成) (請說明以上(1)~(8)項目內容,建議可多寫其他管理機制) (9)網路及系統設備是否建立實體、邏輯架構圖 **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	☐	☐	☐	
	3.10專案系統開發區及系統測試區是否區隔在不同之作業環境？(請說明系統開發區及系統測試區之網段或區隔方式) **【專案屬單位駐點、人力派遣性質得不適用】**	AP 服務之受託單位（系統規劃、設計、建置、維護及代管）	☐	☐	☐	

查核項目	查核內容	適用範圍(註1)	自我查核結果(註2)			自我查核佐證
			符合	不符合	不適用	
	3.11專案工作人員之個人電腦或伺服器是否全面使用防毒軟體並即時更新病毒碼及設定密碼原則為密碼長度超過 8 位字元(特權帳號 12 位字元)並啟用密碼複雜度原則(大小寫字母、數字及符號至少 3 種以上組成？(請說明防毒名稱、多久掃描、多久更新、個人電腦密碼原則設定值)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	
	3.12專案工作人員之個人電腦是否要求電子郵件附件及下載檔案在使用前需檢查有無惡意軟體(含病毒、木馬或後門等程式)？(請說明相關電子郵件管理文件及內容)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	
	3.13所使用的網路是否依網路型態(Internet、Intranet、Extranet)制定適當的管理方式？(請說明公司內容使用網路之管理機制及公司網路配置)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	
	3.14對於重要特定網路服務(FTP 等)，是否制訂管理控制措施，如身份鑑別、資料加密或網路連線控制？(請說明管理特定網路服務之管理方法)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	
	3.15如需辦理程式變更是否經甲方（或其代理人）管理人員確認系統變更？(請說明如何通知甲方（或其代理人）管理人員)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管）	□	□	□	

查核項目	查核內容	適用範圍(註1)	自我查核結果(註2)			自我查核佐證
			符合	不符合	不適用	
	3.16系統開發環境（內部開發區或開發工程師之本機）是否有適當的保護？(如作業系統更新、防毒軟體安裝、掃描等)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管）	□	□	□	
	3.17於測試作業是否避免以真實資料進行？(如有使用真實資料則如何管制，如測試環境實體隔離或存取權限限制)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管）	□	□	□	
	3.18於內部之開發環境及測試環境取得程式原始碼之機制為何？且是否經主管或其授權人核可後使用？(請說明內部之開發環境及測試環境取得原始碼管理方式)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管）	□	□	□	
	3.19對自己公司內部之版控程序如何管理？（如程式版本控管、版控軟體權限管控、舊的程式版本管理及避免使用到舊的程式版本、版控存取紀錄留存….等，包含但不限於以上內容)。	AP 服務之受託單位（系統規劃、設計、建置、維護及代管）	□	□	□	
4.訂定資通安全事件通報及應變之程序及機制	4.1 是否制定資通安全事件發生之通報應變程序？(請說明廠商之通報應變管理文件及內容)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	
	4.2 專案成員如何知悉資通安全事件通報應變程序並依規定辦理？(請說明如何讓專案成員知悉)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	

查核項目	查核內容	適用範圍(註1)	自我查核結果(註2)			自我查核佐證
			符合	不符合	不適用	
	4.3 發生資安事件時是否留有資通安全事件處理之記錄文件，記錄中並有改善措施？(請說明如發生事件時之措施為何，如發生事件，處理方式、包含紀錄留存、改善措施做法等)	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	
5.定期辦理資通安全認知宣導及教育訓練	5.1 是否定期舉辦資通安全教育訓練、資通安全認知宣導或具備相關專業資安證照、認證課程，而每位專案成員是否都有參加並留存簽到記錄？	AP 服務之受託單位（系統規劃、設計、建置、維護及代管） ISMS 服務之受託單位 SOC 監控服務之受託單位	□	□	□	

計畫申購單位審查意見

資訊(安)部門審查意見