

國軍委外辦理資通系統服務資安管控指導要點

111 年 7 月 1 日國通資安字第 1110163215 號令

112 年 10 月 30 日國通資戰字第 1120297940 號令

一、為確保國軍各單位辦理資通系統服務委外之受託業者或委外服務具備完善資通安全管理措施、專業技術、維運計畫及資安驗證等要求事項，明定資通專案委外安全查核規範，並遂行實質查核督管作為，確保國軍資通委外安全，特訂定本要點。

二、適用範圍

- (一) 國軍各單位計畫申購品項涉及資通系統服務規劃、設計、建置、維護及代管，均適用本要點。
- (二) 公告金額十分之一（新臺幣十萬元）以下採購案，仍應依本要點之規定進行查核督管。但計畫申購單位得依委外性質、範圍等項，經資通（安）單位審查後，採部分納入。

三、作業權責

- (一) 國防部參謀本部通信電子資訊參謀次長室(以下簡稱國防部通次室)：
 - 1. 策頒指導要點，規劃資通系統服務委外管控全般事宜。
 - 2. 訂定委外資通安全查核及系統防護基準範本。
 - 3. 指導各級計畫申購單位律定委外資通安全防護基準及查核表。
- (二) 國防部國防採購室：
 - 1. 協助將「委外資通安全管控項目查核表」納入採購招標文件。
 - 2. 提供各級單位遂行委外資通專案相關採購諮詢。

(三) 各級計畫申購單位：

1. 檢核委外資通安全管控項目，依專案需求納入採購契約（協議書）資通安全需求規範，並將相關表單納入契約附加條款。
2. 依採購契約（協議書）審驗委外廠商資安自我查核項目。
3. 納編單位資通及資安人力，於履約期間得對委外廠商進行實質資通安全查核。

(四) 各級採購單位：

1. 協助計畫申購單位將資通安全管控項目納入採購契約（協議書）。
2. 協助計畫申購單位遂行資通專案委外履約作業。

(五) 各級資通（安）單位：

1. 協助計畫申購單位律定委外資通安全防護基準及查核表。
2. 協助計畫申購單位審查委外查核表、廠商自評表及防護基準表。
3. 配合計畫申購單位資安稽核需求，依採購契約（協議書）對委外廠商進行實質資通安全查核。

四、作業要領

(一) 國軍資通系統委外專案，依國軍資通安全責任等級分級作業指導之資通系統防護需求分級原則，區分普、中、高級（如附表一），計畫申購單位應訂定資通安全查核及系統防護基準，並將下列書表納入採購契約（協議書）規範

1. 委外資通系統服務之安全管控項目查核表（如附表二）：
 - (1) 計畫申購單位完成資通系統分級，並依適用分級訂

定查核表，經資訊（安）部門審查確認後，將表內相關資通要求納入採購相關文件，並於合約內明定廠商應配合執行資安管控事項。

(2) 適用分級為普、中、高級全部等級者，所有系統均應列入；另計畫申購單位考量預算限制等因素，且經資訊(安)部門評估為可接受之風險後，得於備註欄註明原因，選擇不予納入。

2. 委外廠商資安自我查核項目表（如附表三）：

(1) 得標廠商應依採購契約要求完成資安自我查核，計畫申購單位及資通（安）部門應於履約期間依項目表進行資安查核作業（專案期間至少一次；另專案期程如超過一年以上者，每年至少一次）。

(2) 專案如屬單位駐點、人力派遣性質，且系統發展未在委外廠商本身公司環境者（非在委外廠商公司環境發展、維護），檢核內容屬廠商公司環境項目，得納入不適用範圍。

3. 資通系統防護基準確認書（如附表四）：

(1) 計畫申購單位依專案性質及適用分級之資安防護需求填載確認書，納入採購文件，於系統建置完畢，採購驗收或上線啟用前進行自我檢核，經確認安全無虞後，納入履約驗收文件，驗收合格始上線運行。

(2) 確認書之填載，得依專案屬性（如系統發展、系統維護等）刪減不適用項目。

（二）本要點依採購流程分成前、中、後三作業階段如附表五：

1. 採購作業前期：於計畫編製階段，由計畫申購單位將委外資通系統服務之安全管控項目查核表，依專案需求完成查核表自檢，審查確認後納入採購相關文件，

律定廠商應須配合執行資安管控事項。

2. 採購作業中期：得標廠商依「委外廠商資安自我查核項目表」完成自檢後，提供計畫申購單位，於專案執行階段由計畫申購單位偕同單位資通(安)單位於履約期間對委外廠商（含分包商）進行資安查核作業。
3. 採購作業後期：計畫申購單位於系統建置完畢，專案採購驗收或上線啟用前，依防護基準進行自我檢核，經確認安全無虞後，納入履約驗收文件，驗收合格始上線運行。

（三）採購需求文件載明服務水準及資安要求：

1. 計畫申購單位得依「政府資訊服務採購作業指引」所定「常用資訊服務等級協議(SLA)之參考項目」，按個案採購類型及需求，妥適選擇必要項目，並於招標文件載明，以利廠商合理估價及遵循。
2. 計畫申購單位得參考「各類資訊(服務)採購共通性資通安全基本要求參考一覽表」，擇定涉及資安之履約項目，並於招標文件中載明；資訊財物採購亦得參考上開一覽表擇定須符合之資安項目。

五、督導與考核

- （一）各級計畫申購單位應落實執行委外廠商資安管控及稽核驗證等事項，經查未依本要點執行相關管制作業之情事，國防部通次室除主動要求限期改正外，並列入年度資通（安）定期督檢成績加重扣分。
- （二）國軍各單位應配合年度資通安全定（突）檢時機，檢查所屬資通專案委外資安管控及查核執行現況，查有未符本要點執行事項或委外廠商缺失，應要求立即改正並實施複查；委外廠商未執行或未改正之資安管控項目，計畫申購單位應將相關罰則納入採購計畫，並

依採購契約（協議書）相關罰則辦理。

（三）因委外資安管控不善，肇致資安事件者，單位應依國軍資安事件通報應變指導要點進行事件應處，國防部通次室依陸海空軍懲罰法及國軍資通安全獎懲規定，對違失人員檢討究責，以確保國軍資通委外作業安全。

（四）國防部通次室將運用年度稽核或不定期稽核時機，驗證各單位執行情形。

六、各單位辦理委外辦理資通系統服務作業時，確依行政院訂定之「資通系統籌獲各階段資安強化措施」及「政府資訊服務採購作業指引」，強化籌獲各階段資安措施。

附表一：資通系統防護需求分級原則

防護需求等級 構面	高	中	普
機密性	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。	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。	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。
完整性	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。	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。	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。
可用性	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。	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。	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。
法律遵循性	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。	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。	其他資通系統設置或運作於法令有相關規範之情形。

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、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。

附表二

國軍委外資通系統服務安全管控項目查核表

填表日期： 年 月 日

防護需求分級：☐普 ☐中 ☐高

系統名稱					
計畫申購單位		承辦人		單位主管	

※計畫申購單位應依防護需求分級將相應之資通安全管控措施項目納入契約規範，非相應分級之項目毋須填列；其中適用分級為普、中、高級全部等級者，所有系統均須列入或選擇【部分列入】。

※計畫申購單位若基於預算限制等因素，可接受資安風險而選擇【部分列入】，則需於備註欄註明原因。

資通安全管控措施項目	適用分級	列入 RFP (依需求修訂) 標明頁數	備註欄
<p>1. 委外廠商應具備以下要求與資格：</p> <p>(1) 廠商辦理委外業務之相關程序及環境，應具備完善之資通安全管理措施(需提供證明文件供甲方審認)或通過第三方驗證(如：CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準)。</p> <p>※參考資通安全管理法施行細則第四條第一點。</p> <p>(2) 廠商應配置至少 1 位擁有資通安全專業證照(可參照行政院【https://nicst ey.gov.tw】公告之證照列表)或具有_____業務經驗(需提供證明文件供甲方審認)之資通安全專業人員。</p> <p>(3) 委外業務複委託情形：</p> <p>○不得複委託。</p> <p>○得複委託，廠商應於企劃書說明複委託之範圍與對象，同時廠商對於複委託之受託者應至少有下列要求：(依需求擇項)</p> <p><input type="checkbox"/> 資通安全專業證照或具有_____業務經驗之資通安全專業人員</p> <p><input type="checkbox"/> 履約期間內，專案成員至少由甲方(或其代理人)完成____小時資安教育訓練</p> <p>(4) 涉及利用非廠商自行開發之系統或資源者，廠商應標示非自行開發之內容與其來源及提供授權證明。</p>	全部	<p><input type="checkbox"/> 列入採購評選(審)評分表</p> <p><input type="checkbox"/> 未辦理採購評選(審)之籌獲案(如小額採購)，由計畫申購單位於選商前自行評估廠商資格。</p>	本項目應納入 <u>企劃書及採購評選評分表(依需求修訂)</u>

資通安全管控措施項目	適用分級	列入 RFP (依需求 修訂) 標明頁數	備註欄
2. 針對承包國軍委外專案業務之相關人員(含分包商)應經單位保防部門完成安全調查,並不得為陸(港、澳)籍人士,經保防部門安全查核未通過者,及大陸地區與港澳地區人民,嚴禁參與專案;另應於相關規定及合約中,規範外部組織設資安管制編組及遵守國防部相關資訊安全管理規定。	全部	第__頁	
3. 廠商應依契約要求提出「專案管理工作計畫書」(含光碟及書面文件),內容應包括資安防護管控作業之工作項目、參與人員、執行敘述、作業時程交付甲方(或其代理人)審查。人員、工作項目如有異動時,需於3個工作天前主動將異動資料以書面函報甲方(或其代理人)審查。	全部	第__頁	
4. 廠商須於決標次日起14個工作天內簽署甲方(或其代理人)「保密切結書」,若須提前參與本案,須於實際參與專案前完成簽署。	全部	第__頁	
5. 應遵循行政院資安管理法及本部資安管控規範等相關規定與要求,強化資訊安全管理,確保資料傳送、儲存及流通之安全。	全部	第__頁	
6. 合約規範或保固期內,定期及不定期配合甲方(或其代理人)實施網站與主機之弱點掃描作業所提之弱點掃描報告,廠商須於甲方(或其代理人)通知日起____個日曆天內完成弱點改善(完成風險修正或降低至甲方可接收之風險)。	全部	第__頁	
7. 應用系統開發測試階段及版本更新時,應執行原始碼檢測(1次),廠商須於甲方(或其代理人)通知日起____個日曆天內完成弱點改善(完成風險修正或降低至甲方可接收之風險)。	全部	第__頁	
8. 合約規範或保固期內,定期及不定期配合甲方(或其代理人)實施之資安檢測(資通系統屬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,機關應自行或另行委託第三方進行安全性檢測)、本部及行政院網路攻防演練等作業所提之檢測報告,廠商須於甲方(或其代理人)通知日起14個日曆天內完成弱點改善(完成風險修正或降低至甲方可接收之風險)。	全部	第__頁	
9. 原則禁止廠商透過網際網路(民網)遠端維護系統。	全部	第__頁	
10. 系統發生資通安全事件或資安弱點檢測驗證成功(如行政院網路攻防演練、資料外洩、被竊取、	全部	第__頁	

資通安全管控措施項目	適用分級	列入 RFP (依需求 修訂) 標明頁數	備註欄
駭客入侵等情事)，須主動通報甲方（或其代理人）。另接獲甲方（或其代理人）通知資安事件時，須 24 小時內協助甲方（或其代理人）完成系統修復及損害管制，並於 7 日曆天內提供改善情形及建議報告書。			
11. 系統之測試及正式作業環境應作區隔；正式作業及測試系統，應採用不同的登入程序。	全部	第__頁	
12. 程式變更須於測試環境測試無誤並保留變更前後差異之紀錄，並由甲方（或其代理人）管理人員確認後，於甲方（或其代理人）指定時間安裝程式變更於正式作業，如程式變更後無法正常運作，則須立即恢復原狀。廠商應於更新完成後____個日曆天(或工作天，不得逾 10 個工作天)內提供相關說明文件，如有必要需安排教育訓練。如程式變更涉及系統文件修正，應於系統變更完成後一個月內修正完成送交甲方(或其代理人)。	全部	<input type="checkbox"/> 列入 第__頁 <input type="checkbox"/> 部分列入 第__頁	
13. 程式變更正式作業前應依「國軍軟體發展管理作業規定」針對系統做相關資訊安全檢測，並提交甲方（或其代理人）指定之檢測報告格式，檢測報告須證明系統無中、高風險之弱點。(廠商需於初次檢測時提出檢測軟體能偵測 OWASP TOP 10 項目的檢測報告)。 ※如系統屬單位核心系統，則此項須全數列入	全部	<input type="checkbox"/> 列入 第__頁 <input type="checkbox"/> 部分列入 第__頁	
14. 配合本部資訊安全風險評估及安全管理需求，機敏資料存於資料庫或其他儲存媒體時，採用對稱式或其他加密方式，將機敏資料加密成密文後儲存，若有傳輸機敏資料時，採用 HTTPS 等加密協定，確保機敏資料以密文方式傳輸。	全部	第__頁	
15. 系統須將存於資料庫內之使用者密碼以加密(不可逆)處理儲存，以防止使用者密碼為使用者以外人員知悉。	全部	第__頁	
16. 系統加密方式，應採用公開、國際機構建議安全且未遭破解之演算法(如 AES 對稱式加密、RSA 非對稱式及 SHA-2 安全雜湊等演算法)。並使用該演算法支援的最大金鑰長度，以減少被暴力破解解密之可能及弱點。	全部	第__頁	
17. 系統採用之加密金鑰或憑證，應配合加密金鑰或憑證週期，於到期前進行更換。	全部	第__頁	
18. 系統應具備帳號管理相關功能，包含帳號之新	全部	第__頁	

資通安全管控措施項目	適用分級	列入 RFP (依需求 修訂) 標明頁數	備註欄
增、停用、刪除及使用者權限建立控制機制，且帳號權限應以最小權限為原則，以確保系統安全；資訊系統應具備唯一識別及鑑別使用者，不應有共用帳號之行為並應識別及鑑別非機關使用者。			
19. 若應用 ActiveX 與 Java applet，應採取相關防護措施(如：加註警語提醒使用者將下載之相關元件為何)。	全部	第__頁	
20. 系統發生錯誤時，使用者頁面僅顯示簡短訊息及代碼不包含詳細的錯誤訊息，且系統管理者介面需限制存取來源。	全部	<input type="checkbox"/> 列入 第__頁 <input type="checkbox"/> 部分列入	
21. 系統檢核使用者產生之密碼，系統應確保一般使用者密碼長度至少 8 位字元、特權帳號密碼長度至少 12 為字元，且均應包含大寫英文字母、小寫英文字母、阿拉伯數字及特殊符號等至少 3 種組合，系統須提供密碼最短及最長之效期限制，且要求密碼最短效期限限制為 1 天，最長之效期限限制要求使用者至少 3 個月修改一次密碼，且密碼不可與前 3 次相同，並於畫面上提示使用者如何產生強化密碼。	全部	<input type="checkbox"/> 列入 第__頁	
22. 系統須建立將使用者異動情形記錄於稽核日誌之功能，且系統應提供查詢系統帳號之建立、修改、啟用、禁用及刪除動作、授予權限功能及異動紀錄。廠商非經甲方（或其代理人）同意不得新增或刪除系統帳號及異動權限。另系統須提供資訊系統管理者帳號所執行之各項功能稽核日誌，稽核日誌不得由管理者刪除，須由特定授權之人員才得以進行稽核檔之異動、刪除作業，並留軌跡紀錄。	全部	<input type="checkbox"/> 列入 第__頁 <input type="checkbox"/> 部分列入 第__頁	
23. 應用系統伺服器上之應用程式不可以賦予資料庫及作業系統最高權限帳號，應給予最小需用權限，以免惡意人員透過資料庫管理系統破壞內部資訊作業。	全部	第__頁	
24. 廠商如接獲系統異常無法正常運作通知，應配合甲方（或其代理人）訂定系統可容忍中斷時間，於 4 個小時內（依合約規範調整）做緊急處理，並於系統可容忍中斷時間（ ）內回復系統運作。 ※（ ）內請填入可容忍中斷時間（含時間單位）	全部	第__頁	
25. 廠商應配合甲方（或其代理人）訂定之可容忍資	全部	第__頁	

資通安全管控措施項目	適用分級	列入 RFP (依需求 修訂) 標明頁數	備註欄
料損失時間()，建立執行系統源碼和資料 備份機制。 ※()內請填入可容忍中斷時間(含時間單位)			
26.廠商應配合甲方(或其代理人)主機移機或汰 換，將系統原主機資料(包含應用系統、資料庫 及檔案等)移轉至新環境，進行相關網路連線設 定和系統測試，以確保系統運作正常。	全部	第__頁	
27.開發或維護系統時，廠商應配合甲方(或其代理 人)要求，對於所開發(維護)之應用系統之系統 運作環境(如：作業系統版本、資料庫系統版本 或軟體版本...等)之更動，協助進行事前評估及 協助轉置，且於前述更動前、後，須進行系統測 試，以確保系統運作正常及符合甲方(或其代理 人)伺服器端及用戶端構型相容性。	全部	第__頁	
28.維護(保固)期間內甲方(或其代理人)因軟硬體 設備異動，因而涉及原系統環境變更時(如版本 變更或安裝 Patch)，廠商應提供技術服務及辦理 變更前、後系統測試，並依甲方(或其代理人) 需求協助關閉軟硬體中不必要之服務及埠口。	全部	第__頁	
29.維護期間內如因故終止服務，廠商應於甲方(或 其代理人)要求或合約規範之期限內，將甲方(或 其代理人)存在於委外廠商處的資料或設備移轉 至甲方處或甲方(或其代理人)指定單位。	全部	第__頁	
30.系統需符合 IPV4 與 IPV6 協定。	全部	第__頁	
31.配合甲方(或其代理人)委外稽核作業之查核， 廠商(含分包商)應配合接受甲方(或其代理人) 或委託單位之稽核或查核等業務，其範圍包括本 專案開發環境、設備、人員及系統之管理機制 等；另專案如有允許複委託項目，廠商應針對複 委託項目督管分包商資安檢核。 ※開發、測試及正式環境均須符合本部「專網專 用、實體隔離」政策，且開發人員活動區域(空 間)應有明確限制。	全部	第__頁	
32.資訊系統應就涉及機敏資料部分建立稽核日 誌，並確保資訊系統有稽核特定事件(至少包含 更改密碼、登入成功及失敗、資訊系統存取成功 及失敗)之功能，採用單一日誌紀錄機制，確保 輸出格式的一致性，且僅限特定授權之使用者能 存取稽核日誌。	全部	第__頁	
33.稽核日誌需具備以下項目：	全部	第__頁	

資通安全管控措施項目	適用分級	列入 RFP (依需求 修訂) 標明頁數	備註欄
(1)識別使用者之 ID，不可為個資類型。 (2)時間應記錄至秒等級。 (3)執行的功能或存取資源名稱。 (4)執行結果或事件描述。 (5)網路來源與目的位址。 (6)其他本部要求之項目。			
34. 廠商應評估及配置適切之稽核日誌所需之儲存容量，並至少保留 1 年（含）以上之稽核紀錄，如發生稽核日誌處理失效時(如儲存容量不足)，應自動採取適當之因應措施，如覆寫最舊的稽核日誌或經甲方（或其代理人）同意之措施，並於()小時內主動通報系統管理者及其指定人員。 ※含個人資料之應用系統紀錄資料應至少保存 5 年以上；未含個人資料之應用系統紀錄資料應至少保存 1 年以上。	全部	第__頁	
35. 應用系統主機須建立時間同步機制。	全部	第__頁	
36. 本部監控資訊系統如偵測到攻擊或異常情形，廠商須協助對事件進行分析和說明，以釐清不尋常之活動。 針對資訊系統所使用的外部元件或軟體(含開源軟體)，廠商應注意其相關安全漏洞通告(如技服中心公告訊息)，定期評估更新，且不得使用預設密碼。	全部	第__頁	
37. 系統除允許匿名存取的功能外，所有功能都必須於已通過身分驗證後才允許存取。網站除公開區域外，其他網頁皆需於身分驗證登入成功後，才得以存取。系統傳遞身分驗證相關資訊(如：帳號、密碼等)應採用加密傳輸，不以明文傳輸，以避免資訊被攔截或監聽竊取。	全部	第__頁	
38. 系統需提供稽核日誌查詢介面，供特定授權之人員得以進行稽核檔查詢作業；甲方(或其代理人)有審查稽核事件需求時，應依需求協助產出稽核事件之紀錄，供承辦人員審查。	中高	第__頁	
39. 廠商應提供應用系統重要程式完整性定期驗證機制，偵測未授權變更特定軟體及資訊，如採用版本管控程式(如 SVN)比對機制或其他同等效益之替代方式。當發現違反完整性時，應協助進行資料回復作業。	中高	第__頁	
40. 系統應禁用閒置帳號。亦即使用者帳號連續	中	第__頁	

資通安全管控措施項目	適用分級	列入 RFP (依需求 修訂) 標明頁數	備註欄
()日未登入，系統即予以鎖定或禁用。 ※ () 內請填入系統可容許未登入時間	高		
41. 系統應設計連線閒置時自動登出或自動連線中斷(Session Timeout)功能，其中含敏感資料之系統不得超過 15 分鐘。	中高	第__頁	
42. 稽核資訊應運用雜湊或其他適當方式確保其完整性	中高	第__頁	
43. 身份驗證機制應防範自動化程式之登入或密碼更換嘗試。	中高	第__頁	
44. 密碼重設機制應對使用者重新身分確認後，發送一次性及具有時效性符記。	中高	第__頁	
45. 廠商應協助建置備援設備以取代原服務中斷時，可於容忍時間內提供服務。	中高	第__頁	
46. 系統應配合甲方 (或其代理人) 所定之情況及條件(如上班時間或指定 IP 來源)，限制使用系統。	高	第__頁	
47. 系統應提供監控系統帳號違反正常使用狀況之記錄功能(如：半夜連線執行特定功能)，並於發現違常使用或嚴重錯誤時提供回報機制(如：email 或簡訊通知)。	高	第__頁	
48. 廠商應建立機制每日備份稽核日誌到與原系統不同之實體系統，並運用加密機制，保護稽核資訊之完整性。	高	第__頁	
49. 廠商應配合提供重要資訊系統軟體與其他安全相關資訊之備份資料，以便甲方 (或其代理人) 儲存在與運作系統不同地點之獨立設施或防火櫃中。	高	第__頁	
50. 對帳號之網路存取，應採取多重認證技術(如：鎖 IP、採用動態密碼認證)；在使用者建立連線前，應識別允許存取之特定來源(如：IP)。	高	第__頁	
51. 加密金鑰應採取安全管理措施。	高	第__頁	
52. 系統之服務水準，經甲方 (或其代理人) 評估須滿足高可用性需求者，應採取分散式或叢集伺服器架構，以使當系統發生錯誤情況或硬體毀損時，服務仍能正常運作。	高	第__頁	
53. 系統應定期執行軟體與資訊完整性檢查(如：同位元檢查、循環冗餘檢查、密碼雜湊函數)。	高	第__頁	

資通安全管控措施項目	適用分級	列入 RFP (依需求 修訂) 標明頁數	備註欄
54. 應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	高	第__頁	
資訊(安)部門審查意見			

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
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)是否造冊列管並說明各項資產之管理者及使用使用者？(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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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	
	<p>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?</p> <p>(1)資料文件存放於那些設備?</p> <p>(2)是否定期保養、設備送場外維修?</p> <p>(3)報廢管理方式?</p> <p>(4)多久備份一次?</p> <p>(5)備份資料是否定期回復測試?</p> <p>(6)是否制訂使用者存取權限註冊及註銷之作業流程?</p> <p>(7)是否定期審查存取權限之合宜性?(多久審查一次)</p> <p>(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)</p> <p>(請說明以上(1)~(8)項目內容,建議可多寫其他管理機制)</p> <p>(9)網路及系統設備是否建立實體、邏輯架構圖</p> <p>【專案屬單位駐點、人力派遣性質得不適用】</p>	<p>AP 服務之受託單位(系統規劃、設計、建置、維護及代管)</p> <p>ISMS 服務之受託單位</p> <p>SOC 監控服務之受託單位</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	<p>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)</p> <p>【專案屬單位駐點、人力派遣性質得不適用】</p>	<p>AP 服務之受託單位(系統規劃、設計、建置、維護及代管)</p>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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）	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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制）	AP 服務之受託單位（系統規劃、設計、建置、維護及代管）	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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）	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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）	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

計畫申購單位審查意見

資訊(安)部門審查意見

附表四

國軍資通系統防護基準確認書

資通系統防護需求等級：☐普 ☐中 ☐高

填表日期： 年 月 日

本系統是否含有個人資料：☐是 ☐否

系統名稱					
計畫申購單位		承辦人		單位主管	

※本表單依「資通安全責任等級分級辦法」第十一條第二項「各機關自行或委外開發之資通系統應依附表九所定資通系統防護需求分級原則完成資通系統分級，並依附表十所定資通系統防護基準執行控制措施」之要求，確認附表十所訂各項措施符合情形。

※本確認書以符合資安法要求為原則，爾後有需要再滾動修正。

※計畫申購單位應依系統安全等級將相應之資通安全管控措施項目提出說明：

1. 等級為「普」之系統，須填寫等級「普」之項目。
2. 等級為「中」之系統，須填寫等級「普、中」之項目。
3. 等級為「高」之系統，須填寫全部項目。

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
1.存取控制	1-1.帳號管理	1	建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統帳號申請、開通、停用及刪除機制採用（複選）： <input type="checkbox"/> 填寫紙本申請單流程(如：帳號權限申請表(SSO)、XXX 應用系統使用者帳號異動申請單) <input type="checkbox"/> 系統線上申請流程 <input type="checkbox"/> 其他，程序說明_____
		2	已逾期之臨時或緊急帳號應刪除或禁用。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序，皆採最小權限原則。 2. 系統最近一次帳號清查：____年__月__日
		3	資通系統閒置帳號應禁用。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	
		4	定期審核資通系統帳號之建立、修改、啟用、禁用及刪除。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
1.存取控制	1-1.帳號管理	5	逾越機關所定預期間置時間或可使用期限時，系統應自動將使用者登出。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統閒置時間設為_____分鐘後系統會自動登出。 2. 是否有限制使用者登入時段(如:上班時): <input type="checkbox"/> 有 限制時段:_____ <input type="checkbox"/> 無
		6	應依機關規定之情況及條件，使用資通系統。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統配合本部所定之情況及條件(如指定IP 來源)，限制使用說明:_____
		7	監控資通系統帳號，如發現帳號違常使用時回報管理者。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統回報方式:_____
	1-2.最小權限	8	採最小權限原則，僅允許使用者(或代表使用者行為之程序)依機關任務及業務功能，完成指派任務所需之授權存取。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 建立帳號管理機制，包含帳號之申請、開通、停用及刪除之程序，皆採最小權限原則。 2. 系統最近一次帳號清查:____年__月__日
	1-3.遠端存取	9	自單位內採連線存取，應先取得授權，建立使用限制、組態需求、連線需求及文件化，使用者之權限檢查作業應於伺服器端完成。 ※依本部資安政策，不允許遠端(自單位外連入)存取	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	<input type="checkbox"/> 本系統未開放遠端存取及單位內連線存取功能 <input type="checkbox"/> 本系統廠商可於單位內以連線存取方式連至後台管理頁面，管控機制:_____(如:限定連接電腦 IP)

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
2.稽核與可歸責性	2-1.稽核事件	10	依規定時間週期及紀錄留存政策，保留稽核紀錄。(應用系統稽核紀錄保存至少1年、含個人資料者保存至少5年)	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統目前保留最早之應用系統稽核紀錄為____年____月____日之稽核紀錄；本系統保留最近一筆應用系統稽核紀錄為____年____月____日之稽核紀錄
		11	確保資通系統有稽核特定事件之功能，並決定應稽核之特定資通系統事件。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統至少包含更改密碼、登入成功及失敗、資訊系統存取成功及失敗等功能之稽核紀錄
		12	應稽核資通系統管理者帳號所執行之各項功能。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統提供資訊系統管理者帳號所執行之各項功能稽核日誌
		13	應定期審查稽核事件。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統最近一次審核稽核事件日期：____年____月____日
	2-2.稽核紀錄內容	14	資通系統產生之稽核紀錄應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	稽核日誌已具備以下項目： (1)識別使用者之ID，不可為個資類型。 (2)時間應記錄至秒等級。 (3)執行之功能或存取資源名稱。 (4)執行結果或事件描述。 (5)網路來源與目的位址。
		15	資通系統產生之稽核紀錄，應依需求納入其他相關資訊。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	除事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊外，本系統是否有納入其他相關資訊之需求： <input type="checkbox"/> 無 <input type="checkbox"/> 有，已納入其他相關資訊
	2-3.稽核儲存容量	16	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已配置稽核紀錄所需之儲存容量，儲存容量超過警示值將以e-mail通報應用系統承辦人員。

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
2.稽核與可歸責性	2-4.稽核處理失效之回應	17	資通系統於稽核處理失效時，應採取適當之行動。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統稽核處理失效(註4)時處理方式為： <input type="checkbox"/> 關閉資訊系統 <input type="checkbox"/> 覆寫最舊的稽核紀錄 <input type="checkbox"/> 停止產生稽核紀錄 <input type="checkbox"/> 通知管理者進行故障排除 <input type="checkbox"/> 其他 _____
		18	機關規定需要即時通報之稽核失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統稽核失效(註1)時的通報機制採用： <input type="checkbox"/> email <input type="checkbox"/> 簡訊 <input type="checkbox"/> 其他_____ 2. 通報人員：_____
	2-5.時戳及校時	19	資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統稽核紀錄時戳，_____(系統內部時鐘或本部 NTP 伺服器)產生，可對應至_____(UTC 或 GMT)
		20	系統內部時鐘應依機關規定之時間週期與基準時間源進行同步。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統主機時間與應用系統管理人員個人電腦時間相符
	2-6.稽核資訊之保護	21	對稽核紀錄之存取管理，僅限於有權限之使用者。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	稽核日誌僅特定授權之人員：_____(如：系統管理人員)才得以存取。
		22	應運用雜湊或其他適當方式之完整性確保機制。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	稽核紀錄運用雜湊或其他適當方式確保其完整性，管控機制：_____(如：異機備份稽核紀錄、稽核紀錄匯出時提供 Hash 值)

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
2.稽核與可歸責性	2-6.稽核資訊之保護	23	定期備份稽核紀錄至與原稽核系統不同之實體系統。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統定期備份稽核紀錄到與原系統不同之實體系統
3.營運持續計畫	3-1.系統備份	24	訂定系統可容忍資料損失之時間要求。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統可容忍資料損失時間(RPO)_____小時
		25	執行系統源碼備份。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	<input type="checkbox"/> 定期備份最新版本之系統源碼 <input type="checkbox"/> 其他_____ (套裝軟體/租賃系統可不備份系統源碼)
		26	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統最近一次備份還原測試日期：____年__月__日
		27	應將備份還原，作為營運持續計畫測試之一部分。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統最近一次營運持續演練：____年__月__日，並已包含備份還原程序
		28	應在與運作系統不同處之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已將資通系統軟體與其他安全相關資訊之備份置於不同處之獨立設施
		29	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統可容忍中斷時間(RTO)_____小時
	3-2.系統備援	30	原服務中斷時，於可容忍時間內，由備援設備取代提供服務。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已建置備援機制(包含 VM 備份與資料備份)，可於可容忍時間內，由備援設備取代提供服務

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
4.識別與鑑別	4-1.內部使用者之識別與鑑別	31	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統具備唯一識別及鑑別使用者，無共用帳號之行為
		32	對帳號之網路或本機存取採取多重認證技術。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統使用之多重認證技術： _____ (如：鎖定 IP 或使用自然人憑證)
	4-2.身分驗證管理	33	使用預設密碼登入系統時，應於登入後要求立即變更。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統帳號預設密碼機制：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 系統無使用預設密碼，系統開通帳號程序：_____ <input type="checkbox"/> 本系統使用者以預設密碼登入系統時，於登入後要求立即變更密碼
		34	身分驗證相關資訊不以明文傳輸。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統傳遞身分驗證相關資訊(如：帳號、密碼等)採用加密傳輸，加密傳輸方式： _____ (如：採用 Https 傳輸)，不以明文傳輸
		35	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達三次後，至少三十分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統帳戶鎖定機制：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 本系統執行帳號登入進行身分驗證失敗超過 5 次後即暫停_____分鐘(至少三十分鐘)使用者登入 <input type="checkbox"/> 其他自建登入失敗驗證機制： _____

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
4.識別與鑑別	4-2.身分驗證管理	36	基於密碼之鑑別資通系統應強制最低密碼複雜度；強制密碼最短及最長之效期限制。 五、使用者更換密碼時，至少不可以與前三次使用過之密碼相同。 六、第四點及第五點所定措施，對非內部使用者，可依機關自行規範辦理。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	《內部系統》(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 非採用 SSO 登入機制： 1. 本系統通行碼長度至少 8 位字元(特權帳號 12 位字元)且包含大寫英文字母、小寫英文字母、阿拉伯數字及特殊符號等至少 3 種組合 2. 強制____個月應變更密碼(不得大於 3 個月) 3. 本系統使用者更換密碼時，不與前三次使用過之密碼相同
		37	身分驗證機制應防範自動化程式之登入或密碼更換嘗試。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統防範自動化程式之登入或密碼更換嘗試機制：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 本系統防範自動化程式之登入方式：_____(如：圖形驗證)
		38	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統具有密碼重設機置：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 系統確認身分後，發送一次性及具有時效性符記 <input type="checkbox"/> 以人工確認身分，人工重設機制 <input type="checkbox"/> 其他_____
	4-3.鑑別資訊回饋	39	資通系統應遮蔽鑑別過程中之資訊。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統遮蔽在輸入過程中之資訊(如密碼於輸入時顯示為*****)

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
4.識別與鑑別	4-4.加密模組鑑別	40	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統密碼加密機制：(可複選) <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 非採用 SSO 登入機制： 本系統存於資料庫內之使用者密碼以加密方式(不可逆)處理儲存，以防止使用者密碼為使用者以外人員知悉。
	4-5.非內部使用者之識別與鑑別	41	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統識別及鑑別非機關使用者方式：(可複選) <input type="checkbox"/> 本系統未提供外部人員使用 <input type="checkbox"/> 採 SSO 登入機制 <input type="checkbox"/> 本系統具備識別及鑑別非機關使用者之機制，管控機制：_____ (如：帳號資訊包含使用者機關/單位) <input type="checkbox"/> 其他_____
5.系統與服務獲得	5-1.系統發展生命週期需求階段	42	針對系統安全需求(含機密性、可用性、完整性)，以檢核表方式進行確認。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已填寫「資通系統防護需求分級表」完成資通系統分級作業
	5-2.系統發展生命週期設計階段	43	根據系統功能與要求，識別可能影響系統之威脅，進行風險分析及評估。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已填寫「防護需求等級評估表」完成資通系統分級作業
		44	將風險評估結果回饋需求階段之檢核項目，並提出安全需求修正。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已依本系統「防護需求等級評估表」結果於委外需求中納入各項安全需求
	5-3.系統發展生命週期開發階段	45	應針對安全需求實作必要控制措施。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已依本系統安全等級需求進行資安法要求之控制措施

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
5.系統與服務獲得	5-3.系統發展生命週期開發階段	46	應注意避免軟體常見漏洞及實作必要控制措施。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已於開發階段避免軟體常見漏洞及實作必要控制措施，並於變更時進行驗證： <input type="checkbox"/> 本系統本年度最近一次程式變更並執行弱點掃描(檢測軟體能檢測 OWASP TOP 10)確認已無中高風險之時間:____年__月__日 <input type="checkbox"/> 本年度無進行程式變更作業，惟已於____年__月__日由資訊處協助執行弱點掃描並確認已無中高風險
		47	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	系統發生錯誤時，使用者頁面僅顯示簡短訊息及代碼不包含詳細的錯誤訊息
		48	應執行原始碼安全檢測，確認程式無安全漏洞或邏輯錯誤等風險。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已於____年__月__日完成原始碼安全檢測，檢測結果： <input type="checkbox"/> 檢測結果通過 <input type="checkbox"/> 檢測結果未通過，惟已完成程式碼修正，並於____年__月__日複測通過
	5-3.系統發展生命週期開發階段	49	執行「源碼掃描」安全檢測。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已於開發階段執行源碼掃描的時間:____年__月__日
		50	具備系統嚴重錯誤之通知機制。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統嚴重錯誤(如：使系統營運中斷)之通知機制： <input type="checkbox"/> email <input type="checkbox"/> 簡訊 <input type="checkbox"/> 其他_____
	5-4.系統發展生命週期測試階段	51	執行「弱點掃描」安全檢測。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已執行「弱點掃描」，並確認已無中高風險或已接受無法修補風險之時間:____年__月__日(掃描時間須驗收前 1 個月內)
		52	執行「滲透測試」安全檢測。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統最近一次依滲透測試結果修補並確認已無中高風險或已接受無法修補風險之時間:____年__月__日(至少每年須辦理 1 次)
	5-5.系統發展生命週期部署與維運階段	53	於部署環境中應針對相關資通安全威脅，進行更新與修補，並關閉不必要服務及埠口。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. <input type="checkbox"/> 本系統主機為 Windows 系統，由資訊處協助更新及修補(Patch) <input type="checkbox"/> 本系統主機為 Linux 系統/其他作業系統，最近一次針對資通安全威脅或弱點執行更新或修補(Patch)的時間:____年__月__日 2. 已開啟本機防火牆，並關閉不必要服務及

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
						埠口，目前開啟 Port：_____
5.系統與服務獲得	5-5.系統發展生命週期部署與維運階段	54	資通系統相關軟體，不使用預設密碼。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統相關軟體未使用預設密碼
		55	於系統發展生命週期之維運階段，須注意版本控制與變更管理。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統使用的版本控管機制為：_____ 2. 本系統依「系統獲取開發與維護管理規範」填寫「正式作業變更管制紀錄表」進行變更管理
	5-6.系統發展生命週期委外階段	56	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求（含機密性、可用性、完整性）納入委外契約。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已填寫「防護需求等級評估表」完成資通系統分級作業，並將安全需求納入本系統需求書
	5-7.獲得程序	57	開發、測試及正式作業環境應為區隔。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統開發、測試及正式作業環境皆有區隔
	5-8.系統文件	58	應儲存與管理系統發展生命週期之相關文件。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統皆有儲存與管理系統發展生命週期之相關文件_____（如：系統設計分析文件、系統維護文件、操作手冊）
6.系統與通訊保護	6-1.傳輸之機密性與完整性	59	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已採用 Https 加密機制，並使用合法憑證中心(政府憑證管理中心 GCA 或國軍憑證管理中心 MCA)核發之伺服器憑證。
		60	使用公開、國際機構驗證且未遭破解之演算法。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已採用 Https 加密機制，並使用合法憑證中心(政府憑證管理中心 GCA 或國軍憑證管理中心 MCA)核發之伺服器憑證。
		61	支援演算法最大長度金鑰。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統已採用 Https 加密機制，並使用合法憑證中心(政府憑證管理中心 GCA 或國軍憑證管理中心 MCA)核發之伺服器憑證。

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
6.系統與通訊保護	6-1.傳輸之機密性與完整性	62	加密金鑰或憑證週期性更換。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	憑證及金鑰的有效期限：____年____月____日
		63	伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	已依本部「密碼措施管理規範」實施應有之安全防護措施
	6-2.資料儲存之安全	64	靜置資訊及相關具保護需求之機密資訊應加密儲存。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統靜置資訊(如應用系統設定之備份檔)及相關具保護需求之機密資訊已加密儲存
7.系統與資訊完整性	7-1.漏洞修復	65	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統依最近一次資訊業管單位弱點掃描結果修補並確認已無中高風險或已接受無法修補風險之時間：____年____月____日
		66	定期確認資通系統相關漏洞修復之狀態。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	
	7-2.資通系統監控	67	發現資通系統有被入侵跡象時，應通報機關特定人員。	普	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	如發現資通系統有被入侵跡象，將通知資訊部門。
		68	監控資通系統，以偵測攻擊與未授權之連線，並識別資通系統之未授權使用。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統已納入 SOC 監控偵測攻擊(由資訊業管單位統一辦理) 2. 本系統已保留嘗試錯誤(登入失敗)之稽核紀錄識別系統之未授權使用
		69	資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統自動化工具監控機制： _____

構面	措施內容	項次	防護項目	等級	是否符合	自評說明
7.系統與資訊完整性	7-3.軟體及資訊完整性	70	使用完整性驗證工具，以偵測未授權變更特定軟體及資訊。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統重要程式已採完整性驗證機制：_____(如：SVN)，偵測未授權變更特定軟體及資訊
		71	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	本系統使用者輸入資料合法性檢查應置放於應用系統伺服器端(對於使用者輸入欄位資料，僅允許特定之內容，並於伺服器端檢查)
	7-3.軟體及資訊完整性	72	發現違反完整性時，資通系統應實施機關指定之安全保護措施。	中	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	如發現違反完整性時(如：資料或程式遭竄改)，資通系統將進行回復作業
		73	應定期執行軟體與資訊完整性檢查。	高	<input type="checkbox"/> 符合 <input type="checkbox"/> 未符合 <input type="checkbox"/> 不適用	1. 本系統檢查週期為：_____(每年/季/月) 2. 最近一次執行特定軟體與資訊完整性檢查：____年____月____日

註：稽核處理失效包括：軟/硬體錯誤、稽核擷取機制失效、稽核儲存容量飽和或超過。可採取下列額外的行動，例如：關閉資訊系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等。

附表五

資通專案委外安控作業程序			
採購階段	前	中	後
採購作業	計畫編製	專案執行	驗收結案
檢核表格	委外資通系統（服務）之安全管控項目查核表	委外廠商資安自我查核項目表	資通系統防護基準確認書
適用對象	計畫申購單位	得標廠商	計畫申購單位
審查單位	資通(安)單位 採購單位	計畫申購單位 資通(安)單位	資通(安)單位
作業說明	計畫申購單位依專案需求完成查核表自檢，審查確認後納入採購相關文件，律定廠商須配合執行資安管控事項。	廠商投標前得提供甲方列入參考，不列入審查文件。得標廠商於專案啟始前，須正式完成資安自我查核並提交自評表；契約甲方得於履約期間依此表進行委外廠商（含分包商）資安查核作業。	計畫申購單位於系統建置完畢，專案採購驗收或上線啟用前，依防護基準進行自我檢核，經確認安全無虞後，納入履約驗收文件，驗收合格始上線運行。