需求說明書（含驗收規範）

壹、購案名稱

「114 年全會資安內部稽核服務」採購案

貳、履約期限與預算

一、 履約期限（如遇假日，原則順延至次一工作日，有分階段交付者亦同；惟實際是否順延仍依本會需求為準）

■決標次日起至 114 年 12 月 24 日止

二、 預算

新台幣 490,000 元整（含稅）。

參、需求說明

一、 專案目標

透過外部顧問提供之全會資安內部稽核服務，以標準化與外部專業稽核者的角色，協助財團法人資訊工業策進會（以下簡稱本會）進行資安法遵以及 ISO 27001 國際標準之稽核作業，俾利符合自身之資安維運作業與主管機關之稽核相關要求。

二、 專案範圍

全會資安內部稽核：

本專案適用本會資訊安全政策所定義之範圍。受稽核單位包含本會各部門及資安管理推動組，共計 13 個部門與 1 個組別之資安稽核作業。

稽核要項包含：

(一) 資通安全管理法及其子法(含資通安全實地稽核項目檢核表)、資通安全維護計畫

(二) 本會資通安全管理規範

(三) 本會 ISMS 管控目標與措施，包含但不限：

- 資安政策、組織、適用性聲明
- 文件與紀錄管制方法與實作
- 資通系統及資產管理、風險評鑑
- 人力資源安全、資訊安全教育訓練
- 實體與環境安全
- 通訊與作業管理
- 資訊系統取得、開發與維護
- 存取控制
- 資訊安全內部稽核
- 資安事件管理
- 矯正與預防
- 營運持續管理
- 供應商管理
- 管理階層審查
- 遵循性

三、 工作項目與說明

提供全會資安內部稽核服務，須依據前項之稽核要項，協助執行本會 13 個部門與 1 個組別之資安內部稽核作業，以符合內部維運及外部稽核之相關要求。

項目	項目名稱	內容說明
1	資安內部稽核規劃	提出內部稽核細部計畫並與相關人員溝通確認
2	資安內部稽核啟動會議	與受稽核單位說明稽核時程、流程及範圍
3	資安內部稽核實施	執行資安內部稽核作業
4	資安內部稽核報告整理與確認	提出與確認資安內部稽核報告
5	資安內部稽核發現事項改善建議	提供內部稽核發現事項改善建議
6	資安內部稽核結案會議	資安內部稽核發現事項改善措施總結說明，並提供受稽核單位改善諮詢

四、 品質管控

為確保本專案如期完成且符合應有品質，得標廠商應針對本專案之需求，指派專案經理至少 1 人專責執行本專案所需之各項作業，如人力配置、任務分配、進度控管、資料蒐集、作業協調及文件撰寫等執行事項；並於交付期限內提出內部稽核計畫，內容除包括對內部稽核之執行細項敘述，含組織、人力、分工、職掌、工作項目及交付時程。

參與工作小組成員之資格條件至少如下：

(一) 專案團隊成員

ISO27001 稽核員

(1) 具備 ISO27001:2022 Lead Auditor 課程證照及資格。

(2) 具備 ISO27001:2022 標準遵循性及成熟度查核經驗，並有實績證明。

五、 法令依據及相關規定

資通安全管理規定：得標廠商應遵守「委外廠商之資通安全責任事項」(詳附件)

六、 保固需求

■無

肆、交付說明

一、 交付項目、內容、期限如下：

項次	交付項目與內容	數量	交付型態	交付期限
1	資安文件-得標廠商簽署之「委外廠商資通安全管理措施說明表」 ※格式請向購案聯絡人索取。	1 式	電子檔	決標次日起 7 日曆天
2	工作計畫書：依需求內容提供，包含稽核時程、流程及範圍等規畫內容	1 式	電子檔	決標次日起 7 日曆天
3	工作小組成員資格證明	1 式	電子檔	決標次日起 7 日曆天

4	資安內部稽核計畫	1 份	電子檔	決標次日起 7 日曆天
5	資安內部稽核啟動會議簡報	1 份	電子檔	114/11/7
6	資安內部稽核檢核表(分資訊、業務、幕僚、全會資安業管)	4 份	電子檔	114/11/7
7	資安內部稽核報告	14 份	電子檔	114/12/12
8	資安內部稽核發現事項改善建議	1 份	電子檔	114/12/12
9	資安內部稽核結案會議簡報	1 份	電子檔	同本案履約期限
10	資安文件-資料返還、刪除、銷毀聲明書(詳附件)	1 份	電子檔	同本案履約期限

備註：得標廠商應依本會需求配合調整各階段交付期限，惟不可超過本案履約期限。

二、 交貨地點：台北市民生東路四段 133 號 14 樓　資安科技研究所。

三、 得標廠商應依上表提供履約標的，並提供履約通知文件予本會〔購案聯絡人〕確認。

四、 履約通知文件參考格式可至 http://www.iii.org.tw /綜合公告/採購資訊/檔案下載區下載，廠商亦可自訂格式（Email 亦視同履約通知文件，惟內容應足資識別本案）。

五、 履約通知文件僅為通知本會交付全部或部份履約標的，相關驗收事宜另依本會驗收程序辦理，本會驗收合格後方視為履約完成。

伍、驗收規範

一、 依本案需求說明書（若購案有服務建議書者亦併同納入）進行數量、內容點收。

二、 本會得要求得標廠商配合出席驗收會議，並做口頭簡報（須視本會需求提供會議文件）。

三、 本會得要求得標廠商依據本會驗收會議意見修訂調整交付項目內容，且應附上意見回覆對照。

陸、其他注意事項

一、 購案聯絡人：

姓　名：資安科技研究所　蘇冠萍小姐

電　話：(02) 6631-6331

Email：bearsu@iii.org.tw

二、 發票資料：

抬　頭：財團法人資訊工業策進會

統一編號：05076416

柒、審查須知

詳投標須知之「審查須知」內容；審查項目及建議書撰寫重點如下述。

項次	項目	服務建議書撰寫重點 **（請依下列章節序參考製作）**
		封面、目錄
1	**執行力與配合度** ●人力配置規劃	1. 公司簡介（如業務範圍、營運狀況) 2. 執行團隊組織與工作分配

	●執行團隊之相關經驗、學經歷及過去績效 ●計畫執行及管理能力	3. 專案負責人及專案團隊成員履歷：包含現職、學經歷、資安證照(ISO 27001:2022 Lead Auditor 課程證照及資格)等 4. 廠商履約實績：請詳述專案經驗及其成效；須具備 ISO 27001:2022 標準遵循性及成熟度查核經驗等相關實績證明。
2	**整體服務建議與規劃** ●企劃內容可行性 ●執行進度之時程規劃	5. 說明整體稽核內容、執行方式及專案品質管理流程等 6. 提供時程進度規劃，說明相關工作預定進度、完成時點
3	**經費合理性** ●相關執行費用估算與分配之合理性	7. 於服務建議書詳列報價內容（請詳列各物品／服務／人力……等之規格、數量、單價明細）

【附件】

委外廠商之資通安全責任事項

一、 辦理受託業務之相關程序及環境，應填寫「委外廠商資通安全管理措施說明表」佐證具備完善之資通安全管理措施，或通過第三方驗證(TAF 認證機構)，如受託業務涉及提供雲端服務者，應提供原廠 ISO 27001 標準認證。

二、 應配置充足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之資通安全專業人員，負責推動、協調及督導資通安全管理事項。

三、 經本會同意，委外廠商始得將受託業務分包予第三人，委外廠商須要求並監督該第三人應具備與委外廠商同等之資通安全維護措施及標準，並應約定分包廠商應遵循之事項，其至少包括廠商受稽核時，如稽核範圍涉及分包部分，分包廠商就該部分應配合受稽核。

四、 辦理客製化資通系統之開發，若涉及利用非自行開發之系統或資源者，應標示非自行開發之內容與其來源及提供授權證明。

五、 辦理受託業務，違反資通安全相關法令或知悉資通安全事件發生時，應立即通知本會承辦單位及採行必要之補救措施，並應配合本會之資通安全事件通報及相關處理作業。委外廠商未為通知或未配合本會相關處理作業者，應就本會因此所生之一切損害負賠償責任。

六、 委託關係終止或解除時，委外廠商就履行委託契約而持有之資料應返還、移交、刪除或銷毀，並填具「資料返還、刪除、銷毀聲明書」。

七、 委外廠商同意本會得定期或於知悉發生可能影響本案之資通安全事件時，以稽核或其他適當方式確認受託業務之執行情形。

八、 委外廠商受託業務涉及資通訊軟體、硬體或服務等相關事務者，執行本案之團隊成員不得為大陸籍人士，並不得提供及使用大陸廠牌資通產品或服務。

九、 受託業務涉及國家機密時，執行業務之相關人員應接受適任性查核，並受國家機密保護法規定之管制。

委外廠商應確保執行該業務之所屬人員及可能接觸該國家機密之其他人員，無下列事項：

(一) 曾犯洩密罪，或於動員戡亂時期終止後，犯內亂罪、外患罪，經判刑確定，或通緝有案尚未結案。

(二) 曾任公務員，因違反相關安全保密規定受懲戒或記過以上行政懲處。

(三) 曾受到外國政府、大陸地區、香港或澳門政府之利誘、脅迫，從事不利國家安全或重大利益情事。

(四) 招標公告、招標文件或契約所載其他與國家機密保護相關之具體項目。

十、 委外廠商執行受託業務之人員進出本會範圍應受限制。且應遵守本會「資通服務廠商派駐人員資通安全同意表」之資通安全相關規定。

十一、 委外廠商駐點人員若要更換或撤離，應填寫「資通服務廠商派駐人員撤離資料表」。

【附件二】

保　密　切　結　書

立書人：

因與　貴會進行 114 年全會資安內部稽核服務 之合作（下稱「合作案」），就　貴會機密資訊，願負保密義務如下：

一、 本切結書所稱「機密資訊」，係指　貴會交付立書人並註明為機密或其他同義文字之有形資訊，或以口頭方式揭露且於揭露時聲明其為機密，並於嗣後以書面追認其為機密之資訊。

二、 立書人對於下列資訊，不負保密責任：
（一）立書人於簽署本切結書前已為其合法持有或知悉之資訊。
（二）立書人自無保密義務之第三人合法取得或知悉之資訊。
（三）非因立書人之故意或過失而公開或為眾所周知之資訊。
（四）立書人（包括但不限於其員工、顧問或合作廠商）未使用任何機密資訊而自行研發或發現之資訊。

三、 保密義務
（一）立書人應盡善良管理人之注意義務，保管　貴會所揭露之機密資訊。未經貴會事前書面同意，不得以任何方式直接或間接交付或洩漏機密資訊予第三人，且不得為超出合作案目的範圍利用或使用機密資訊。
（二）立書人應負責使其員工遵守本切結書之保密義務。
（三）立書人因進行合作案而有揭露機密資訊予第三人之必要時，應事前取得該第三人同意依本切結書規定保守機密資訊之書面承諾並經　貴會書面同意，立書人並就該第三人承諾負連帶履行之義務。若該第三人違反保密義務，視為立書人之違反，立書人應依本切結書第五條之規定，對　貴會負損害賠償責任。
（四）立書人依法院或主管機關之命令而須揭露機密資訊時，應於收到該命令後立即通知　貴會，並配合　貴會採取合理必要之保密措施。
（五）本條保密義務之有效期間自　貴會向立書人揭露機密資訊時起算 3 年，不受本切結書有效期間屆滿之影響。

四、 機密資訊之所有權、專利權、著作權、營業秘密或技術秘竅（KNOW-HOW）係貴會或其原授權人所有，不因　貴會揭露予立書人而生任何讓與、授權或權利設定之效力，立書人不得據以自行實施或申請專利權、著作權或其他智慧財產權，或使第三人行使上述權利。

五、 立書人如有違反本切結書之任何條款，　貴會除得隨時要求立書人返還或銷毀機密資訊及其所有之重製物外，並得請求賠償新台幣 10 萬 元作為懲罰性違約金，如另受有損害，並得請求立書人賠償。

六、 立書人如發現第三人未經授權而違法使用機密資訊，應立即通知　貴會，並配合採取必要之排除或防止措施。

七、 本切結書自簽署日起生效，有效期間至合作案終止或完成時止。

八、 本切結書為不可撤銷、撤回或終止。

九、 因本切結書所生爭議，立書人同意以臺灣臺北地方法院為第一審管轄法院，並以中華民國法律為準據法。

此致
財團法人資訊工業策進會

立書人：
統一編號（或身份證字號）：
代表人：
職稱：
地址：

中　　華　　民　　國　　年　　月　　日

【附件】

資料返還、刪除、銷毀聲明書

填寫日期： 年 月 日

購案/委外資通作業名稱（下稱本案）		廠商名稱(下稱立書人)	(請加蓋廠商印鑑)
		立書人之負責人	(請加蓋負責人印鑑)

立書人因執行本案所持有之本案相關資料（包括但不限於開發需求規格書、原始碼、執行碼或程式等，詳如下表所列）及其影本、複製本或備份予以返還、刪除或銷毀，且將嚴格監督並確認立書人及其參與本案的相關人員（包括但不限於勞工、派遣人員、受任人或分包廠商等）未以任何形式為資料之私自留存、使用、竄改或洩漏，亦不得為自身或第三人的利益而使用。

立書人及其參與本案之相關人員若發生將資料私自留存、使用、竄改或洩漏等不利於 貴會的行為，立書人同意配合 貴會進行必要之查證行為及提供 貴會所需之協助，如經查證屬實，立書人願支付本案價金總額 20 %之懲罰性違約金及賠償 貴會所受之一切損害，並負一切法律責任，絕無異議。

編號	資料名稱	數量	檔案類型	執行方式
範例	需求/設計規格書	1	■電子檔案 ■實體檔案	■已返還 ■已刪除 ■已銷毀
範例	程式原始碼	1	■電子檔案 ■實體檔案	■已返還 ■已刪除 ■已銷毀
1.			□電子檔案 □實體檔案	□已返還 □已刪除 □已銷毀
2.			□電子檔案 □實體檔案	□已返還 □已刪除 □已銷毀

備註：表格不敷使用，請自行增加。

(資策會)點收人簽名：	(資策會)點收日期：