「112-113 年度資訊安全管理系統（ISMS）輔導及驗證」資訊服務採購案（2023-IT012）需求說明書

中 華 民 國 112 年 4 月

目　錄

壹、 專案概述

一、專案名稱

「112-113 年度資訊安全管理系統（ISMS）輔導及驗證」資訊服務採購案（2023-IT012）（以下簡稱本專案）

二、專案緣起

本中心為資通安全責任等級 C 級之公務機關（行政法人），為持續推動本中心資訊安全管理系統及維持其認證有效性，將於 112 至 113 年持續各項資訊安全維運作業，確保本中心資通安全及業務持續營運。本專案將秉持以制度化、文件化及系統化之理念，依循規劃、執行、檢查及行動之管理模式，持續維護、改善及落實資訊安全管理之理念。

三、專案目標

本專案期透過專業資安顧問廠商(以下簡稱廠商)之輔導，提供本中心與所屬機關必要專業服務，符合資通安全管理法及 ISO/IEC 27001：2022 國際標準之要求，提升本中心資訊安全管理之水準，並達成下列目標：

(一) 推展本中心專案範圍之 ISMS 風險管理，掌握並降低資安風險。

(二) 建立本中心 ISMS 風險管理，完成 ISO27001:2022 取證書作業。

(三) 建立本中心 ISMS，並強化管理制度之落實度及完整性，確保管理措施符合持續改善之要求。

(四) 提供導入訓練與諮詢，提昇資安意識及資訊安全管理能力。

(五) 辦理委外資通廠商資安稽核活動。

四、專案範圍

(一) 持續改進本中心資訊安全管理系統，以符合 ISO/IEC 27001 國際標準及資通安全管理法要求。

(二) 提升本中心相關人員實作資訊安全管理之認知與能力。

(三) 本中心資訊機房之系統，導入 ISMS。

(四) 以本中心共構機房（新莊本館及樹林片庫）、核心資通系統（如：本中心公文系統、中心官方網站、藏品管理系統，以三個核心系統範圍為原則）等驗證範圍，112 年通過 ISO/IEC 27001:2022 第三方驗證及 113 年辦理複評驗證作業，維持本中心 ISO/IEC 27001:2022 證書之有效性。

(五) 協助本中心導入 ISMS，以符合資通安全責任等級分級辦法之 C 級公

務機關應辦事項規定。

(六) 依資通安全管理法相關規定執行核心資通系統委外廠商稽核之實地稽核活動。

五、專案期程

本專案執行期程自決標日之次日起至 113 年 11 月 30 日（含）前完成本專案所有工作事項。

六、專案經費

本專案預算金額為新臺幣 **292 萬 5,300 元整**。

七、主辦單位及連絡方式

本專案主辦單位為本中心資訊室，專案聯繫資料如下：

- 地址：242030 新北市新莊區文藝路 2 號
- 聯絡人：資訊室石逸榛 小姐
- 電話：（02）8522-8000 轉 2304
- Email：sunnyecko@tfai.org.tw

貳、專案需求

一、建立本中心資訊安全管理系統(含內部稽核)

輔導本中心建置符合 ISO 27001：2022 標準之資訊安全管理系統。得標廠商需依 PDCA 管理循環，協助本中心分別於 112 年度及 113 年度執行下列工作事項各一次，並分年交付相關工作產出。

(一) 現況評估

1. 廠商應協助本中心了解其業務特性、組織與人員職責，協助鑑別資訊安全管理相關之內、外部議題、關注方需求。
2. 檢視資通安全組織及資通安全措施，分析業務流程及資通系統之重要性與可容忍中斷時間及業務衝擊。
3. 得標廠商得透過「書面自檢表」或「人員訪談」或「實地訪查」等方式完成本項作業。
4. 得標廠商依據 ISO/IEC 27001:2022 要求，與上述現況分析結果，建立符合本中心所屬資通安全責任等級C級機關需求之「**適用性聲明書**」。
5. 本項作業本中心視需求請得標廠商於專案會議中說明。

(二) 鑑別資訊資產與資通系統分級作業

1. 協助本中心進行資訊資產盤點、資訊資產分類、評定機密性（C）、完整性（I）、可用性（A）與資訊資產安全需求，並分別於 112 年度及 113 年度產出本中心「**資訊資產清冊**」。
2. 完成資通系統分級後，應依資通系統【高】、【中】、【普】等級，提供本中心資通系統防護基準建議，並產出「**資通系統清冊**」與「**資通系統分級防護基準報告**」。

(三) 輔導風險管理作業

1. 協助本中心辦理資通安全風險評鑑作業，檢視本中心現行風險評鑑方法，並進行風險再評鑑，分析資訊資產既存的威脅及潛在的問題，辨別威脅來源與脆弱點，計算並建議可接受風險等級，釐清風險安全控制的方向。
2. 依據風險評鑑作業結果評估適當風險控管方式，並針對不可接受之風險等級，提供因應對策，選擇適當的控制目標與控制措施。

3. 風險管理落實與作業後，產出 112 年度及 113 年度本中心「**資安風險評鑑報告**與**資安風險處理計畫**」。

(四) 建立、檢視及修正本中心資訊安全管理系統四階文件

依資通安全管理法等相關資通安全管理法規及最新版本 ISO/IEC 27001 標準，協助本中心於 112 年完成資訊安全管理系統四階文件建立，113 年進行檢視與修正。

(五) 資通安全內部稽核

得標廠商須協助本中心於 112 年及 113 年各執行一次資通安全內部稽核活動。

1. 辦理稽核活動前，須協助本中心擬訂「**內部稽核計畫**」。
2. 執行內部稽核時，須組成 2 人(含)以上之輔導稽核團隊(需具 ISO/IEC 27001 主導稽核員資格)，協同本中心稽核小組成員，協助本中心辦理資訊安全內部稽核作業(本中心視情況決定實際執行時間)。
3. 稽核活動完成後，須於 10 個工作天內交付「**內部稽核完工報告書**」。
4. 針對稽核發現之不符合事項，廠商應協助受稽核單位擬定矯正及預防措施並提供改善建議。
5. 若本中心當年度被行政院或文化部遴選為政府機關（構）資通安全稽核之受稽核機關，廠商須協助本中心進行相關稽核準備工作，並至少派 1 員陪同進行實地受稽作業，並提供相關改善建議。
6. 本專案時程內，若遇行政院資通安全處或文化部等相關機關辦理之網路攻防演練、情境演練或其他必要之演練，須至本中心協助辦理。

(六) 資安治理成熟度評估作業

協助本中心依資通安全管理法規定進行資安治理成熟度評估作業，並於 112 年及 113 年度分別產出「**資安治理成熟度建議書**」。

(七) 訂定績效衡量指標(KPI)

廠商應依本中心需求確認後協助制定資訊安全目標管理作業程序，使中心資訊安全目標（**績效衡量指標**）之管理有一明確之規範，並依所定之資訊安全目標檢視資通系統之控制成果，除確認潛在資訊安全風險已達有效管理與控制之目的外同時須確保本中心 ISMS 之品質及運作效率能持續提升 。

(八) 業務持續運作演練作業

得標廠商應於期限內提出業務持續運作演練規劃並交付演練計畫書，於期限內完成業務持續運作演練作業後應交付業務持續運作演練完工報告書，規範內容如下：

1. **業務持續運作演練計畫書**：廠商應協助修訂營運持續管理機制、規劃業務持續運作計畫及擬定演練計畫。
2. **業務持續運作演練完工報告書**:廠商應依據業務持續運作演練結果，協助完成「業務持續運作演練完工報告書」，並視業務需求，協助或輔導營運持續相關演練作業。
3. 辦理上述業務持續運作演練程序，廠商應提供本中心相關人員行前教育訓練至少 2 小時。

(九) 資通安全維護計畫

協助本中心配合資通安全管理法及其子法規定，編修資通安全維護相關作業各項計畫與推動，並依本中心年度資通安全運作及 ISMS 實施情形，提交資通安全維護計畫。

(十) 組織全景分析

依據本中心營運需要，深入瞭解本中心建置需求及既有限制，協助建立組織全景評鑑表。

(十一) 資訊安全相關會議

協助本中心召開資訊安全管理審查會議，包括會議資料整備與列席管理審查會議，協助檢視會議議程與會議資料完整性，列席會議提供必要之諮詢服務，並於會後協助追蹤決議事項之執行情形。

二、 第三方驗證作業

1. 協助本中心分別於 112 年通過 ISO 27001:2022 驗證並取得證書。驗證證書須為國際認證機構(IAF)或財團法人全國認證基金會(TAF)認可之第三方驗證機構所核發之證書。
2. 協助本中心受稽核單位人員與外部稽核人員之溝通，以利完成驗證過程，並於完成作業後提供「第三方 ISMS 證書或有效性文件」。
3. 第三方驗證所需費用(含重審或續審、人員、交通、餐飲等相關費用及雜支)均由廠商支應。
4. 協助確認續評所需之文件及紀錄等資料，於本專案時程內，依據本中心核定之驗證範圍完成驗證作業。
5. 進行 ISMS 第三方驗證評鑑前，廠商須提出「**外部資安稽核計畫書**」，

內容包含 ISO/IEC 27001 之驗證機構、驗證期程、驗證範圍、稽核前說明會辦理時間/形式、重審/複審/轉證等證書辦理規劃事項。

6. 於本中心進行 ISMS 第三方驗證評鑑時，廠商須指派顧問人員參與稽核活動，並陪同受稽核人員協助進行詢答。

7. 對於稽核時所發現之不符合事項，應協助本中心擬訂第三方驗證報告所列缺失之矯正與改善建議，有效改善不符合事項，通過第公正三方驗證公司之審查。

8. 稽核活動完成後，廠商須交付「**外部資安稽核完工報告書**」，報告須含外部稽核矯正及改善措施內容，針對正式評鑑發現之不符合事項，擬訂矯正及改善措施並協助完成。

三、 中心相關委外資通廠商進行稽核作業

得標廠商須協助本中心稽核所屬委外資通廠商之資通安全，以加強所屬廠商之資安防禦力，每年至少查核 3 家廠商（不限實地或書面稽核）。得標廠商需稽核前需提交「**委外廠商稽核計畫書**」，若為實行實地稽核時，得標廠商至少指派 1 位（含）以上具備 ISO/IEC 27001：2022 主導稽核員資格之稽核員協助執行稽核，於稽核作業結束後，提交「**委外廠商稽核報告書**」。

四、 資通安全教育訓練

(一) 導入訓練及資通安全通識教育訓練

1. 本專案導入資安教育訓練重點為培訓所屬中心人員推動資通安全之技術，導入 ISMS 以資通安全責任 C 級之資訊安全教育訓練內容為原則，強化所屬中心同仁資訊安全管理之能量，以建構自行維護、持續改善資訊安全管理系統能力。

2. 針對本中心員工、主管、資訊人員所需各項資安知識與技術，擬訂教育訓練計畫，並經本中心確認後實施，其教育訓練計畫須包括課程訓練進行方式、課程類別、課程名稱、課程大綱、課程時數、講師姓名及背景資歷等規劃。課程規劃時數至少 21 小時，其中包括：

(1) ISMS 導入培訓課程至少 9 小時。導入培訓課程內容須包含 ISMS 資安制度說明、資通系統分級與防護基準評估說明、資訊資產盤點實務、資安文件架構與製作說明、資安風險評鑑實務、資安內部稽核作業說明及資安管理審查實務說明。

(2) 組織全員資安認知宣導課程 112 年與 113 年，每年至少 3 小時，共 6 小時。

(3) 主管資安認知宣導課程 112 年與 113 年至少 3 小時，共 6 小時。

3. 前述訓練課程經本中心同意得集中共同辦理，上課之時間地點以本中心會議室或採視訊會議，訓練講師應由實際輔導 ISMS 經驗人員擔任。

4. 訓練課程所衍生之費用（講師鐘點費、教材編製費等費用）由廠商負擔。

5. 廠商應依本專案時程，於訓練課程開課前交付該課程講義等相關資料。

(二) 資通安全專業證照訓練

1. 服務內容需求：

(1) 得標廠商於本專案提供之資通安全專業證照，須公布列示於國家資通安全會報網站資安管理法專區之資通安全專業證照清單(以最新一期公告資料為準)，得為上述清單中各項管理類或技術類證照，本專案原則優先以上述清單所定，經 TAF 或國際認證機構認可之資安相關管理系統驗證機構所發證管理類課程之 ISO 27001:2022 或 ISO/IEC 27701:2019 主導稽核員課程或 CISSP 資安系統專家認證課程，惟可經本中心同意調整為技術類證照課程。

(2) 本資通安全專業證照須由合格訓練機構進行，並由上述資通安全專業證照清單所列示之合格發證機構發證。需提供本中心之資訊人員培訓 ISMS ISO 27001:2022 或 ISO/IEC 27701:2019 主導稽核員課程至少 4 名（提供 1 次考試）；CISSP 資安系統專家認證課程 2 名；SSCP 資安專業人員認證課程 1 名 (前述相關費用皆包含於專案內，重考費用則不計入)。

(3) 本專案專業認證課程得標廠商須以課程券或課程點數卡方式交付，所交付之課程券或點數卡須於本案履約期限內均可使用，該課程券或點數卡於履約期限內使用時，若因訓練機構調漲課程費用，相關差額費用由得標廠商負責。

(4) 訓練教材原則以中文教材為主，且經機關認可，並於課程後交付紙本或電子檔予機關，有關教育訓練餐食費、講師交通費、教材製作費、場地費、膳費及其他與課程有關之費用皆包含於專案內，機關不另支付。

(5) 廠商應負責提供報名作業、講師安排及教材提供等行政協處服務。

2. 履約程序與期程規範：

(1) 得標廠商應於決標翌日起 30 日內，提交「**資通安全專業證照執行計畫**」。「資通安全專業證照執行計畫」應提供本案資通安全專業證照課程之訓練機構、開班方式、課程類別、訓練對象、課程時程、驗證機構等規劃事項。

(2) 「資通安全專業證照執行計畫」經本中心核定後，由得標廠商依據證照受訓人數,提出訓練機構上課卷或相關課程開立授權證明，再由本中心受訓人員進行課程派訓、考試與證照取得。

(三) 顧問諮詢服務

1. 對於資訊安全管理現況進行診斷與評估，提供本中心資訊安全管理政策和目標之建議。
2. 每月需定期到本中心提供實作諮詢(到場次數、時程依工作會議協議)，內容包括（但不限於）參與各項機關資訊安全、資產盤點、風險評鑑及風險處理、內部稽核及缺失矯正等。
3. 就本中心實作資訊安全管理制度之需要，建立資訊安全管理制度文件。
4. 其他應協助本中心辦理之資訊安全作業諮詢。

參、專案管理

一、專案組織

(一) 成立專案小組

得標廠商應成立專案管理小組，並將成員之姓名、專長、學歷、相關工作資歷及專業證照等資料，詳細載明於「專案工作計畫書」中。為確保顧問輔導品質，重要成員資格條件至少如下：

1. 專案經理（至少配置1人）：

具有ISO/IEC 27001、ISO/IEC 27701證照，及具備輔導全機關或全組織通過ISO/IEC 27001驗證之實績，並於該專案中擔任專案經理職務。

(1) 大學畢業（含）以上，具備 **5** 年以上資訊安全規劃與專案管理之經驗。

(2) 具有 ISO 27001 與 ISO27701 主導稽核員（Lead Auditor）證照，持有 ISO 27001 主導稽核員（Lead Auditor）。

(3) 具有參與 ISMS 與 PIMS 整合專案建置及後續輔導維護並通過 ISO 27001、ISO 29151 第三方後續審查之經驗尤佳。

(4) 具備實際輔導資安責任等級至少 B 級以上機關之資訊安全管理制度實績，並於該專案中擔任專案經理職務。

(5) 具保持專案營運持續應 ISO22301 證照尤佳。

(6) 因應雲端服務(資訊安全與個人資料)與資安封包分析之觀念，具有 ISO27017/27018 與 NSPA 證照尤佳。

2. 資通安全輔導顧問與內部稽核顧問：

(1) 人員配置：

- 資通安全輔導顧問：至少 2 人。
- 資通安全內部稽核顧問：至少 2 人，且不得由資通安全輔導顧問兼任。

(2) 大學畢業(含)以上，並具 3 年以上 ISMS 資訊安全管理及 PIMS 個人資料管理教育訓練講師經驗尤佳。

(3) 同時具有 ISO 27001 與 BS 10012 主導稽核員（Lead Auditor）證照尤佳。

(4) 須具有參與 ISMS 與 PIMS 整合專案建置及後續輔導維護並通過 ISO 27001、ISO 29151 第三方後續審查之經驗尤佳。

(5) 具備實際輔導資安責任等級至少 B 級以上機關之資訊安全管理制度實績尤佳。

(6) 具保持專案營運持續應 ISO22301 證照尤佳。

(7) 具備 CISSP 國際資安專業證照尤佳。

(二) 人員管理

1. 專案小組成員於契約期間非因離職或本中心要求不得任意更換，如須異動時，應於異動前1個月將符合資格之接替人員相關資料以書面方式通知本中心，經本中心審核同意後更換。

2. 專案小組成員如有服務表現不佳或違反本中心相關規定，本中心得要求廠商撤換。廠商應於接獲本中心書面通知起10個工作天內提出符合契約規定之替代人選，經本中心審核同意後更換。

3. 上述人員更換時，接替人員應連續同步至少5個工作天，以利工作銜接。

二、專案工作計畫書

於決標翌日起10個工作天內提交專案工作計畫書，內容至少包括專案執行方法與配合事項、專案組織、時程規劃、諮詢服務及教育訓練之計畫、資通安全及保密之計畫及交付項目。

三、專案會議

本中心與廠商之專案會議，原則每月一次，會議目的在檢驗專案執行狀況，明定未確定之作業規範，解決發生之問題，討論雙方應配合及協調事項，廠商應由專案經理及專案成員參與會議；本中心可視需求調整專案溝通頻率及臨時召開專案執行會議。

四、進度管理

(一) 工作進行中如發生可能影響工作進度之事故時，得標廠商應主動回報本中心。

(二) 任一工作項目如落後預計進度超過 5 個工作天，得標廠商應主動向本

中心報告，並提出其因應對策。

肆、 執行與驗收

一、應交付項目及時程

本專案履約期限自決標日次日起，廠商並應無償提供履約文件修改、微調服務至 113 年 11 月 30 日止。本專案相關工作內容詳本文件各章節說明，廠商應安排工作時程完成，應交付之各項履約文件及交付期限要求如下表：

項次	工作項目	交付項目	交付期限
一	112 年工作項目（資訊安全管理系統導入）	● 專案工作計畫書 ● 保密切結書、保密同意書	決標日次日起 10 工作天內
		● 導入訓練及資通安全通識教育訓練計畫 ● 資通安全專業證照課程執行計畫	決標日次日起 30 日內
		● 資安現況與差異分析報告（含組織全景評鑑表） ● 資通系統清冊 ● 資訊資產清冊 ● 資通系統分級與防護基準報告 ● 資安風險評鑑報告 ● 資安風險處理計畫 ● 業務持續運作演練計畫書 ● 內部稽核計畫書	112 年 8 月 31 日（含）前
		● 資訊安全管理制度（ISMS）四階管理文件（含政策、管理程序書、作業標準書及各式表單文件） ● 資安治理成熟度建議書 ● 適用性聲明書 ● 績效衡量指標 ● 委外廠商稽核計畫書 ● 外部資安稽核計畫書	112 年 9 月 30 日（含）前
		● 內部稽核完工報告書（含改善建議） ● 委外廠商稽核報告書（含改善建議） ● 外部資安稽核完工報告書	完成稽核日起算 10 工作天內交付。
		● 業務持續運作演練完工報告書	完成演練日起算 10 工作天內交付。
		● 管理審查會議完成報告（含會議紀錄） ● 提交次年度擬執行之機關資通安全維護計畫	112 年 10 月 15 日（含）前

		● 交付第三方認證機構（TAF）認可之驗證機構所核發之 ISO 27001 新版驗證通過證明文件或中英文證書	應於驗證完成 10 工作天內交付公正第三方驗證單位核發之驗證通過證明。
		● 資安顧問到場輔導服務紀錄（含簽到表）	112 年 11 月 30 日（含）前，交付 112 年服務紀錄
二	113 年工作項目（資訊安全管理系統維護）	● 資通系統清冊 ● 資訊資產清冊 ● 資通系統分級與防護基準報告 ● 資安風險評鑑報告 ● 資安風險處理計畫 ● 修正後資訊安全管理制度（ISMS）四階管理文件 ● 資安治理成熟度建議書 ● 組織全景評鑑表 ● 資通安全通識教育訓練	113 年 5 月 30 日（含）前
		● 內部稽核計畫書 ● 委外廠商稽核計畫書 ● 業務持續運作演練計畫書 ● 外部資安稽核計畫書	113 年 8 月 31 日（含）前
		● 內部稽核完工報告書（含改善建議） ● 委外廠商稽核報告書（含改善建議） ● 外部資安稽核完工報告書	完成稽核日起算 10 工作天內交付
		● 業務持續運作演練完工報告書	完成演練日起算 10 工作天內交付
		● 管理審查會議完成報告（含會議紀錄） ● 提交次年度擬執行之機關資通安全維護計畫	113 年 10 月 15 日（含）前
		● 公正第三方複評驗證通過證明	應於複評驗證完成 10 工作天內交付證書有效性證明。
		● 資安顧問到場輔導服務紀錄（含簽到表）	113 年 11 月 30 日（含）前，交付 113 年服務紀錄
備註：各項交付文件項目除保密切結書、保密同意書須以正本紙本交付，其餘文件以**電子郵件方式交付審查**，並於本中心同意備查後再以 A4 尺寸紙張直式橫書雙面製作印刷並製成二份，結案時須交付電子檔光碟片 1 式 2 份。			

二、智慧財產權歸屬

廠商交付本中心之所有文件，其著作權及智慧財產權均屬本中心所有。廠商交付之本專案相關軟體項目、網頁製作內容及電子文件資料檔案中如包含第三者開發之產品(或無法判斷是否為第三者之產品時)，應保證(或提供授權證明文件)其軟體使用之合法性(以符合中華民國著作權法規為準)，如隱瞞事實或取用未經合法授權使用之軟體或識別標誌、圖檔、背景音樂等，致使本中心遭致任何損失或聲譽損壞時，廠商應負責一切損害賠償責任(含訴訟及律師費用)，並盡最大努力維護本中心權益

三、基本服務水準（違約處罰基準）

詳如契約書第十五條

伍、 服務建議書製作規定

一、服務建議書製作規格

廠商參與本案之投標，須提交服務建議書書面文件 1 式 9 份，封面應註明標案名稱、投標廠商名稱等項目，以供本案評選委員作為評分參考。服務建議書規範及內容說明如下：

(一) 紙張大小：以 A4 規格大小繕打。

(二) 繕打及裝訂方式：由左至右橫式繕打，加註頁碼，加裝封面，封面上註明廠商名稱、本案名稱及時間。裝釘線在左側。

(三) 頁首依評選項目標示參閱頁次，並依據所提服務建議書內容，提出本專案規劃之特色或優勢項目，俾利審查。

(四) 目錄及頁次：應製作目錄，以利索引，除封面及目錄頁上無須加註頁碼外，餘(含圖表)一律於各頁下方中央位置加註頁碼。

(五) 服務建議書應符合本專案採購需求書，須以繁體中文撰寫，專有名詞可為外文。

(六) 服務建議書中重點及要項，請以放大字體、粗體或劃線標示，以利評審。

(七) 得標廠商服務建議書於決標後，除本中心存查之 1 份外，得標廠商可於決標當日取回，未取回者建議書由本中心處理。

二、服務建議書大綱及內容

(一) 服務建議書內容大綱詳如附錄 1。

(二) 評選項目與服務建議書內容對照表（詳如附錄 2）：請置放於投標服務建議書第一頁，廠商須依評選項目列出與投標服務建議書內容之對照頁次，如有提供服務優於或不同於本案服務採購需求書部分請註記。

陸、 評選規定

詳如評選須知。

柒、 附則

本文件及廠商服務建議書於決標後納入契約附件。

捌、 附錄清單

附錄 1、服務建議書內容大綱

附錄 2、評選項目與服務建議書內容對照表

附錄 3、報價單格式

附錄 1、服務建議書內容大綱

目錄	詳列綱要、附件及頁次
第一章	概述
第一節	專案名稱
第二節	專案緣起
第三節	專案目標及預期成效
第四節	服務範圍
第五節	專案時程
第二章	投標廠商簡介
第一節	公司簡介（須包含人力規模及組織編制）
第二節	相關經驗與實績（應提出承包相關專案之契約或完工證明影本）
第三節	近三年營運狀況（財務狀況、經營能力）
第三章	專案執行規劃
第一節	對本專案需求及本中心現行狀況之瞭解程度
第二節	輔導方法說明，維護本中心 ISMS 之執行能力
第四章	專案組織與管理
第一節	專案組織人力配置與工作職掌
第二節	專案小組成員之學經歷與專業能力
第三節	人員管理
第四節	專案需求、時程及重要查核點
第五節	交付文件項目（以表列方式說明本專案各階段交付之項目及日期）
第六節	專案品質保證措施
第五章	費用分析 (以表列方式說明本專案各項專案需求、驗證及其它費用)
第六章	其他建議及優規說明 (廠商得就有助於提升本專案效益之作為，但未列為本專案需求者提出建議及提供優於本文件之差異分析)
附件	相關證明文件影本

附錄2、評選項目與服務建議書內容對照表

※請置放於投標服務建議書第一頁，廠商須依評選項目列出與投標服務建議書內容之對照頁次，如有提供服務優於或不同於服務採購需求書部分請註記。

評選項目		服務建議書內容對照			
項次	評選內容	內容摘要（針對內容提出概述，特色或優勢說明）	章節	頁次	備註
一、廠商實績	1. 廠商簡介 2. 承辦類似本專案之資訊相關流程領域與電腦稽核領域之實務經驗 3. 相關證照(如經濟部工業局之資安服務能量登錄資格….)				
二、專案規劃與執行能力	1. 專案規劃及交付項目是否完整確實可行 2. 專案執行工作項目是否明確周延 3. 時程與查核點之安排是否合理可行 4. 專案管理與品質保證措施是否確實 5. 教育訓練內容				
三、專案管理能力	1. 專案負責人及專案經理之資訊相關流程領域專業資歷 2. 參與本專案之執行人員之的執行能力（專業資歷及相關專業證照） 3. 專案組織之編組與成員分工是否完整				
四、價格之合理性	標價合理性、經費結構完整性及正確性				

附錄3、報價單格式（廠商請依照此格式報價）

說明：

- **各項費用報價須含稅（單位：新臺幣元）。**
- 契約總價如經減價而確定，則各單項報價金額應依同一減價比率調整。投標文件中報價之分項價格合計數額與總價不同者，亦同。
- **本案預算金額為新台幣292萬5,300元整(含稅)，投標廠商之總標價如超預算為不合格標，不納為評選對象。**
- 「經費分析總表」格式範例：

經費分析總表

項次	項目		單位	數量	單價(元)	總價	備註
一	112年資訊安全管理制度(ISMS)導入與驗證費用	資安現況分析作業	式	1			詳需求說明書規定
		資訊安全管理制度（ISMS）四階管理文件（含政策、管理程序書、作業標準書及各式表單文件）建置	式	1			詳需求說明書規定
		風險評鑑作業	式	1			詳需求說明書規定
		營運持續作業	式	1			詳需求說明書規定
		資訊安全內部稽核與矯正	式	1			詳需求說明書規定
		委外廠商稽核	式	1			詳需求說明書規定
		管理審查會議作業	式	1			詳需求說明書規定
		外部稽核與矯正	式	1			詳需求說明書規定
		公正第三方驗證	式	1			第一年 ISO 27001：2022 公正第三方驗證費用

		導入訓練、資安通識教育課程與資安專業證照課程	式	1			(1)導入訓練與資安通識教育課程（15 小時） (2)ISO 27001：2022 或或 ISO/IEC 27701:2019 主導稽核員課程（4 人次） (3)資安專業證照課程： a. SSCP 課程 1 人次 b. CISSP 課程 2 人次 其餘詳需求說明書規定
二	113 年資訊安全管理制度(ISMS)維護輔導與複評驗證費用	資訊安全管理制度（ISMS）四階管理文件（含政策、管理程序書、作業標準書及各式表單文件）修定	式	1			詳需求說明書規定
		風險評鑑作業	式	1			詳需求說明書規定
		營運持續作業	式	1			詳需求說明書規定
		資訊安全內部稽核與矯正	式	1			詳需求說明書規定
		委外廠商稽核	式	1			詳需求說明書規定
		管理審查會議作業	式	1			詳需求說明書規定
		外部稽核與矯正	式	1			詳需求說明書規定
		公正第三方驗證	式	1			第二年 ISO 27001：2022 公正第三方複評驗證費用
		資安通識教育課程	式	1			資安通識教育課程（6 小時） 其餘詳需求說明書規定
合計(含稅)							元整