

需求說明書

一、採購案名：ISO 27001 與 ISO 27701 標準顧問服務案

二、預算金額：新臺幣 220 萬元整(含稅)

三、採購目的

本中心現以 ISO 27001:2013 及 BS 10012:2017 標準範圍之實務運作與相關業務流程，為配合 ISO 27001:2022 標準公告，擬委託透過廠商提供相關輔導及諮詢顧問，調整本中心現有資通安全暨個資保護管理制度並導入 ISO 27001:2022 標準及 ISO 27701:2019 標準，並協助本中心通過第三方稽核與取得驗證，爰規劃「ISO 27001 與 ISO 27701 標準顧問服務案」（以下簡稱本案）。

四、顧問服務範圍

本案顧問服務範圍包含本中心全組織所有資通系統(包含中心 ISO 27001:2013 證書取證通過之涵蓋所有資通系統，如：NPAC 系統、中心官網、公文管理系統等)、人員、辦公環境及機房為範圍，其辦公場域位於新北市板橋區及高雄市路竹區，兩個場域人員數各約為 120~130 人左右。

本中心包含中心本部、稽核室、行政組、檢測暨網通技術組、資通安全組、應用服務組及研究企劃組等。

五、需求說明

(一)工作計畫

1. 工作計畫書

得標廠商應交付「工作計畫書」且內容應至少包含下列事項：

- (1) 專案概述：包含專案名稱、專案範圍、專案目標。
- (2) 專案工作時程及交付項目：包含專案工作時程規劃、專案交付項目及檢查時間點等說明。
- (3) 專案團隊：執行本案之專案成員人力配置及分工等說明。
- (4) 專案資訊安全管理及個資保護計畫：說明執行本案之資訊安全防護措施及個資保護管理措施。

2. 專案啟動會議

得標廠商須召開專案啟動會議以報告本案規劃，並應交付「專案啟動會議簡報」。

3. 保密同意書與保密切結書

得標廠商及其專案成員應簽署「保密同意書」與「保密切結書」，並應遵守保密相關規定。

(二)資通安全管理制度落差分析

得標廠商應依據 ISO 27001:2022/CNS 27001:2023 標準檢視本中心資通安全管理制度實施狀況，並辦理現況診斷與落差分析，並交付「資通安全管理制度落差分析報告」

需求說明書

以作為後續導入 ISO 27001:2022/CNS 27001:2023 標準改善建議。

(三)資通安全暨個資保護管理制度文件增修

1. 112 年資通安全暨個資保護管理制度文件增修

得標廠商應檢視本中心資通安全暨個資保護管理制度現有文件及運作情形，並且依據 ISO 27001:2022/CNS 27001:2023 標準及 ISO 27701:2019 標準協助本中心產製一階政策、二階程序書、三階作業要點及四階表單等合規於資通安全暨個資保護管理制度之草案文件。

得標廠商須配合前述草案文件與本中心進行修改討論，並依所提修改討論建議改修文件至本中心同意為止，以確保資通安全暨個資保護管理制度文件適切性。

2. 113 年資通安全暨個資保護管理制度文件增修

本中心於 112 年資通安全暨個資保護管理制度增修文件公告實施後，得標廠商應配合本中心各業務需求及建議與本中心進行修改討論，並依討論結果協助修正資通安全暨個資保護管理制度文件（包含一階政策、二階程序書、三階作業要點及四階表單）並提供修正版之草案文件，所提修正版之草案文件須經本中心同意為止，以確保資通安全暨個資保護管理制度文件適切性。

(四)資訊資產與個人資料盤點乙次

得標廠商應依本中心所公告資通安全暨個資保護管理制度規定，協助本中心辦理資訊資產及個人資料重新盤點，並交付「資訊資產清冊」及「個人資料盤點表」。

(五)資通安全暨個資保護風險評鑑及處理乙次

1. 得標廠商應依本中心所公告資通安全暨個資保護管理制度規定，協助本中心辦理資通安全風險評鑑作業及個資保護風險評鑑作業，並交付「資通安全風險評鑑報告」及「個資保護風險評鑑報告」。
2. 得標廠商應依本中心所公告資通安全暨個資保護管理制度規定，本中心辦理資通安全風險處理作業及個資保護風險處理作業，並交付「資通安全風險處理計畫」及「個資保護風險處理計畫」。

(六)資通安全暨個資保護內部稽核及建議改善乙次：

1. 得標廠商應依據本中心資通安全暨個資保護管理制度規定、ISO/IEC 27001:2022/CNS 27001:2023 標準、ISO/IEC 27701:2019 標準交付「資通安全暨個資保護內部稽核計畫」。
2. 得標廠商應辦理內部稽核啟始會議，並交付「資通安全暨個資保護稽核啟始會議簡報」及「資通安全暨個資保護稽核啟始會議會議紀錄」。
3. 得標廠商應依據本中心資通安全暨個資保護管理制度規定協助本中心辦理自行評估作業，並交付資通安全管理制度「稽核檢核項目自行評估表」與個資保護管理制度「稽核檢核項目自行評估表」。
4. 得標廠商應依據本中心資通安全暨個資保護管理制度規定、ISO/IEC 27001:2022/CNS 27001:2023 標準、ISO/IEC 27701:2019 標準執行內部稽核作業，並交付「內部稽核報告」、資通安全管理制度「稽核檢核項目表」與個資保護管

需求說明書

理制度「稽核檢核項目表」。

5. 得標廠商應辦理內部稽核結束會議，並交付「資通安全暨個資保護稽核結束會議簡報」及「資通安全暨個資保護稽核結束會議會議紀錄」。
6. 得標廠商依據內部稽核之發現事項提出改善措施建議，並交付「改善措施處理單」以協助本中心確保相關事項獲得適當處置與改善建議。

(七) 資通安全暨個資保護管理審查會議乙次

得標廠商應依據本中心資通安全暨個資保護管理制度規定、ISO/IEC 27001:2022 / CNS 27001:2023 標準、ISO/IEC 27701:2019 標準協助本中心完成管理審查會議召開，並交付「資通安全暨個資保護管理制度管理審查會議簡報」及「資通安全暨個資保護管理制度管理審查會議會議紀錄」。

(八) 資通安全暨個資保護外部稽核協助

1. 得標廠商應協助本中心全組織於民國 114 年 2 月 28 日前通過完成本專案範圍 ISO 27001:2022/CNS 27001:2023 及 ISO/IEC 27701:2019 第三方驗證作業(含前置作業)。
2. 得標廠商之輔導顧問應於第三方驗證機構於本中心進行驗證稽核(包含預先稽核及正式稽核)作業時到場陪同，並彙整各稽核員詢問之問題，以供本專案作為改善之參考。
3. 得標廠商應依據第三方驗證機構之驗證稽核(包含預先稽核及正式稽核)作業中發現之不符合事項及改善機會提出原因分析及改善建議，並交付「改善措施處理單」以協助本中心確保相關事項獲得適當處置與改善建議。

(九) 資通安全暨個資保護教育訓練

1. 112 年度教育訓練

項次	教育訓練名稱	時數
1	ISO 27701:2019 隱私資訊管理教育訓練 (課程內容包含 ISO 27701:2019 標準介紹、從 BS 10012 標準轉為 ISO 27701 標準建置重點、個資安全宣導等)	3 小時
2	資訊資產/個人資料風險評鑑與管理教育訓練 (課程內容包含資訊資產盤點說明、個人資料盤點說明、資訊資產風險評鑑方法、個人資料風險評鑑方法及風險管理觀念等)	3 小時
3	Web 應用程式安全教育訓練 (課程內容包含 Web 應用程式發展與安全、Web 應用程式常見資安風險、安全的軟體開發生命週期(SSDLC)等)	3 小時

需求說明書

2. 113 年度教育訓練

項次	教育訓練名稱	時數
1	資訊安全/個資保護文件宣導教育訓練 (課程內容包含中心管理制度因應 ISO 27001 轉標及個資轉標準文件修訂清單、資通安全管理制度文件修改說明、個資保護管理制度文件修改說明等)	3 小時
2	資通系統防護基準實務教育訓練 (課程內容包含資通安全責任等級分級辦法之表十《資通系統防護基準》所有構面要求說明、所有構面要求實例作說明等)	3 小時
3	資訊安全/個資保護外部稽核實務教育訓練 (課程內容包含外部稽核流程、外部稽核應答技巧、外部稽核缺失提醒等)	3 小時
4	系統與網站滲透教育訓練 (課程內容包含滲透測試流程介紹、滲透測試各階段說明及攻擊驗證與事件稽核等)	3 小時

3. 教育訓練課程要求說明

- (1) 得標廠商應配合本專案執行進度於可採實體課程(於本中心新北辦公室或高雄本部)或線上課程方式提供教育訓練課程，應於服務企劃書中提出課程內容規劃，並工作計劃書中提出實施期程。
- (2) 每堂教育訓練課程應包含以下文件：
 - A. 「教育訓練計畫」至少應包含教育訓練課程名稱、時間、地點、講師姓名、課程大綱、課程時數及舉辦方式。
 - B. 「教育訓練簡報」應為教育訓練課程教材電子檔。
 - C. 「教育訓練簽到表」應為參與課程人員紙本簽名或線上課程擷圖畫面文件。
 - D. 「教育訓練錄音或錄影電子檔」。

五、履約期限

自決標日起至民國 114 年 2 月 28 日前完成履約。

需求說明書

六、履約期程及交付項目表(以下簡稱表 1)

項次	履約期限	工作項目	交付項目	交付格式
1	自決標日起 30 日	工作計畫	1.1 工作計畫書	電子檔 1 式 1 份
			1.2 專案啟動會議簡報	電子檔 1 式 1 份
			1.3 保密同意書及保密切結書	專案人員 每位紙本 1 式 1 份
2	112 年 8 月 31 日	資通安全管理 制度落差分析	2.1 資通安全管理制度落差分析報告	電子檔 1 式 1 份
3	112 年 12 月 31 日	資通安全暨個 資保護管理制 度文件增修— 112 年資通安全 暨個資保護管 理制度文件增 修	3.1 資通安全暨個資保護管理制度文 件增修清單 3.2 資通安全暨個資保護管理制度文 件增修草案	電子檔 1 式 1 份
4	112 年 12 月 31 日	資通安全暨個 資保護教育訓 練—112 年度教 育訓練	4.1 ISO 27701:2019 隱私資訊管理教 育訓練 4.1.1 教育訓練計畫 4.1.2 教育訓練簡報 4.1.3 教育訓練簽到表 4.1.4 教育訓練錄音或錄影電子檔 4.2 資訊資產/個人資料風險評鑑與 管理教育訓練 4.2.1 教育訓練計畫 4.2.2 教育訓練簡報 4.2.3 教育訓練簽到表 4.2.4 教育訓練錄音或錄影電子檔 4.3 Web 應用程式安全教育訓練 4.3.1 教育訓練計畫 4.3.2 教育訓練簡報 4.3.3 教育訓練簽到表 4.3.4 教育訓練錄音或錄影電子檔	電子檔 1 式 1 份
5	113 年 3 月 31 日	資訊資產與個人 資料盤點乙次	5.1 資訊資產清冊乙式 5.2 個人資料盤點表乙式	電子檔 1 式 1 份
6	113 年 8 月 31 日	資通安全暨個 資保護風險評 鑑及處理乙次	6.1 資通安全風險評鑑報告乙份 6.2 個資保護風險評鑑報告乙份 6.3 資通安全風險處理計畫乙份 6.4 個資保護風險處理計畫乙份	電子檔 1 式 1 份

需求說明書

項次	履約期限	工作項目	交付項目	交付格式
7	113 年 10 月 31 日	資通安全暨個資保護內部稽核乙次	7.1 資通安全暨個資保護內部稽核計畫乙份 7.2 資通安全暨個資保護稽核啟始會議簡報乙份 7.3 資通安全暨個資保護稽核啟始會議會議紀錄乙份 7.4 資通安全管理制度「稽核檢核項目自行評估表」乙式 7.5 個資保護管理制度「稽核檢核項目自行評估表」 7.6 內部稽核報告乙份 7.7 資通安全管理制度「稽核檢核項目表」乙式 7.8 個資保護管理制度「稽核檢核項目表」乙式 7.9 資通安全暨個資保護稽核結束會議簡報 7.10 資通安全暨個資保護稽核結束會議會議紀錄 7.11 改善措施處理單乙式	電子檔 1 式 1 份
8	113 年 10 月 31 日	資通安全暨個資保護管理制度文件增修—113 年資通安全暨個資保護管理制度文件增修	8.1 資通安全暨個資保護管理制度文件增修清單 8.2 資通安全暨個資保護管理制度文件增修草案	電子檔 1 式 1 份
9	113 年 11 月 30 日	資通安全暨個資保護管理審查會議乙次	9.1 資通安全暨個資保護管理制度管理審查會議簡報 9.2 資通安全暨個資保護管理制度管理審查會議會議紀錄	電子檔 1 式 1 份
10	113 年 12 月 31 日	資通安全暨個資保護教育訓練—113 年度教育訓練	10.1 資訊安全/個資保護文件宣導教育訓練 10.1.1 教育訓練計畫 10.1.2 教育訓練簡報 10.1.3 教育訓練簽到表 10.1.4 教育訓練錄音或錄影電子檔 10.2 資通系統防護基準實務教育訓練 10.2.1 教育訓練計畫 10.2.2 教育訓練簡報 10.2.3 教育訓練簽到表	電子檔 1 式 1 份

需求說明書

項次	履約期限	工作項目	交付項目	交付格式
			10.2.4 教育訓練錄音或錄影電子檔 10.3 資訊安全/個資保護外部稽核實務教育訓練 10.3.1 教育訓練計畫 10.3.2 教育訓練簡報 10.3.3.教育訓練簽到表 10.3.4 教育訓練錄音或錄影電子檔 10.4 系統與網站滲透教育訓練 10.4.1 教育訓練計畫 10.4.2 教育訓練簡報 10.4.3 教育訓練簽到表 10.4.4 教育訓練錄音或錄影電子檔	
11	114 年 2 月 28 日	資通安全暨個資保護外部稽核協助	11.1 資通安全暨個資保護管理制度第三方驗證稽核簽到表 11.2 資通安全管理制度「改善措施處理單」 11.3 個資保護管理制度「改善措施處理單」	電子檔 1 式 1 份

需求說明書

七、 文件需求

得標廠商因執行本專案所產出之文件應以本中心為著作人，本中心享有著作財產權及著作人格權。本專案如因故終止，終止前完成之文件，其著作財產權悉照前述規定辦理，原始創作人並同意不行使著作人格權。

八、 資安需求

- (一) 得標廠商基於本專案需要，應簽署保密相關文件。並且就所取得之各種形式之資訊，包含文書、圖片、紀錄、照片、錄影（音）及電腦處理資料等，可供聽、讀、閱覽或藉助科技得以閱讀或理解之文書或物品，應負資訊保密及確保資訊安全責任。
- (二) 對本案以文字標示為機密資料者，非經本中心書面同意，得標廠商不得洩漏資料予第三者，致使造成之法律責任或賠償，得標廠商應負完全責任。
- (三) 得標廠商對於可能接觸與本專案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署本中心之保密相關文件。
- (四) 本案不得轉包及分包。
- (五) 得標廠商於本專案執行期間知悉發生與受託業務相關之資通安全事件時，應於知悉後一小時內通報本中心，通報內容應依資通安全事件通報及應變辦法第三條規定，後續亦應配合本中心需要，提供相關資訊。
- (六) 契約終止時，得標廠商應遵循本中心之處理程序，將有關本專案過程中本中心提供之相關資料及得標廠商處理之任何形式資訊整理歸檔後退還本中心或經本中心同意後銷毀並留存處理紀錄以供本中心查核。
- (七) 本中心對得標廠商保留實地稽核權，以確保得標廠商於本專案期間與合約終止時之資料安全、設備管理及其他安全維護事項已採取必要措施。
- (八) 履約期間因執行本專案事項，侵害他人之權利（包括智慧財產權）者，得標廠商應負賠償責任，賠償金額不以本專案契約金額為限。
- (九) 得標廠商與本中心間交換之資料應經過適當加密後始可進行傳輸，加密金鑰應與加密資料本體使用不同管道提供。
- (十) 得標廠商應遵守個人資料保護法之要求，及其相關義務及責任。履約期間因執行本專案事項而違反個人資料保護法致個資外洩所造成之損害，應負賠償責任。

需求說明書

九、專案管理需求

- (一) 本專案團隊人員至少應分為三種職務，包含專案負責人/專案經理一人、專案顧問及內部稽核人員，本專案團隊人員任一人不得於本專案擔任二個以上職務。
- (二) 本專案每種職務皆應持有 ISO 27001:2022 主導稽核員證書及 ISO 27701:2019 主導稽核員證書。
- (三) 本專案團隊人員應具中華民國國籍，並不得為人力派遣公司人員或「按時」、「按月」、「按件」計酬之臨時人員或工讀生，且實際履約人員應與提出之專案團隊人員名單相同。
- (四) 得標廠商指派執行本專案人員，應先行檢具相關資料送交本中心審查，並於本中心審查同意後方得執行服務工作。
- (五) 得標廠商應針對本專案之需求內容成立專案小組，執行本專案所需之各項作業，並指派專案經理負責督導工作項目。
- (六) 得標廠商應訂定品質管理流程與必要產出，本中心必要時得以稽查確認。
- (七) 得標廠商之專案經理於專案期間應配合本中心辦理及出席專案啟動會議、專案管理會議與相關會議，並依本中心要求定期召開及出席專案管理會議以掌控品質，會議討論內容與結果應作成會議紀錄並追蹤，會議紀錄須於會議結束後 7 日內送交本中心覆核與備查。
- (八) 專案經理除經本中心同意外，均應親自出席前款之所有會議。
- (九) 得標廠商於執行契約期間，如有專案人員之調動更換，應於 15 日前書面檢具人員資料送交本中心審查同意方得予以調動更換，替換人員之資格（學經歷、證照等）應符合本需求說明書第十三條之第(二)項之要求。
- (十) 本中心得要求得標廠商更換本案專案人員，得標廠商應於本中心通知日次日起 7 日內更換獲本中心審查同意之人選。
- (十一) 經本中心審查同意之專案人員，未經本中心同意，不得更換，如有未經本中心同意自行更換時，每更換乙次得依契約總價之千分之一計算懲罰性違約金。
- (十二) 得標廠商違反『未能於規定時間完成工作計罰』，其罰款(違約金)計算方式為每延遲 1 日(以日曆天計，不滿 1 日以 1 日計算)，本機關得按契約總價之千分之一計算懲罰性違約金。
- (十三) 本中心得不定期召開專案管理會議，惟應於會議前 48 小時以書面或電子郵件通知得標廠商。

十、履約地點

- 本中心高雄本部(高雄市路竹區路科一路 3 號)
- 本中心新北辦公室(新北市板橋區遠東路 1 號 3 樓、5 樓)

十一、驗收

- (一) 廠商應於各期履約期限前提交履約交付項目，由本中心依規定辦理驗收。
- (二) 得標廠商各期履約交付，應於履約標的預定完成履約日前或完成履約當日，將完成履約日期以書面通知本中心辦理驗收。

需求說明書

十二、付款條件

分期付款：

- 第一期：廠商於完成表 1 項次 1 至項次 4 履約交付項目，並經本中心驗收合格後，且無待解決事項後，撥付決標價金總額 30%。
- 第二期：廠商於完成表 1 項次 5 至項次 10 履約交付項目，並經本中心驗收合格後，且無待解決事項後，撥付決標價金總額 30%。
- 第三期：廠商於完成表 1 項次 11 履約交付項目，並經本中心驗收合格後，且無待解決事項後，撥付決標價金總額 40%。

十三、履約保證金

廠商於決標日起 14 日曆天內應繳納履約保證金，金額為合約金額 10%。

十四、保固保證金

無。

十五、投標廠商資格文件

- (一) 廠商登記或設立證明文件。
- (二) 廠商納稅證明。
- (三) 投標廠商應提供通過 ISO/IEC 27001:2013 標準第三方驗證之證明。

十六、聯絡方式

- (一) 需求單位：郭小姐
電子信箱: kuoliching@ttc.org.tw/連絡電話：(07)627-7063
- (二) 採購單位：廖先生
電子信箱: ChiYu.Liao@ttc.org.tw/連絡電話：(07)627-7028

十七、服務企劃書製作規定

- (一) 裝訂與數量
 - 1. 裝訂：請用 A4 規格雙面印刷，內容以中文直式橫書繕打，並併同目錄(含目次、頁次)裝訂成冊且各部分之章節號碼須前後統一，並標註頁數。
 - 2. 數量：投標廠商須於投標期限內提送服務企劃書紙本 1 式 10 份及電子檔(USB 隨身碟或光碟片以 Microsoft 系列編輯軟體製作與 PDF 軟體製作) 1 式 3 份送達本中心指定收件處所。
- (二) 一般要求
 - 1. 製作服務企劃書及契約簽訂前所費之成本，由投標廠商自行負擔。
 - 2. 投標廠商之服務企劃書及簡報資料所有權歸本中心，並視為契約應履行部份。

需求說明書

3. 服務企劃書交付後，本中心得交付評選委員審核、工作小組成員初審及承辦人員承辦。
4. 服務企劃書及所有參考資料，評選後概不退還。
5. 如有未盡事宜，以本中心解釋為準。

(三) 服務企劃書應包括章節如下表項目所示：

1. 目次
2. 專案概述
 - (1) 專案名稱。
 - (2) 專案範圍。
 - (3) 專案目標。
3. 廠商與團隊專業能力及實績
 - (1) 廠商規模及營運狀況(如組織編制、管理制度導入現況或人力規模)。
 - (2) 廠商通過 ISO/IEC 27001 之說明、認證(含資安認(驗)證)、獎項。
 - (3) 近三年營運狀況(如財務狀況或服務發展能力)。
 - (4) 相關經驗及實績，廠商於截止投標日前 5 年與本案有關且已完成之證明，並須檢附足供佐證與驗證之資料(如合約或完工證明)。
4. 專案工作規劃與執行及創新、其他優惠措施
 - (1) 整體規劃。
 - (2) 專案團隊人員(包含數量、配置規劃、學經歷、專長證照及實績)。
 - (3) 專案各其產出及執行時程規劃。(投標廠商應於服務企劃書中建議執行本專案應產生之文件與應產出之期程)
 - (4) 專案人員管理與備援。
 - (5) 專案查核規劃。
 - (6) 專案實施方式與管理方法。
 - (7) 創新與建議：含其他與本採購標的有關，且於價內之附加或創新服務 含其他與本採購標的有關，且於價內之附加或創新服務。
5. 專案價格分析

履行本案之預定支出，請詳列各工作項目之經費需求及其計算方式，製作專案費用分析表。

(四) 評選標準：

評選項目	內容	配分
一、廠商規模及經驗實績	1.1 廠商規模及營運狀況(含人力規模、資安人力) 1.2 廠商資安制度、認證(含資安認(驗)證)、獎項 1.3 近三年營運狀況 1.4 履約實績	30

需求說明書

評選項目	內容	配分
二、專案執行內容之完整性、合理性及可行性	2.1 專案組織架構與職責分工(投入本案人員學/經歷)。 2.2 專案時程規劃。 2.3 專案實施方式與管理方法。 2.4.創新增值服務及其他優惠措施。	30
三、價格合理性	價格編列之完整性及合理性。	20
四、簡報及答詢	4.1.簡報內容及答詢之專業性、完整性。 4.2.服務企劃書整體架構與內容規劃。 4.3.服務企劃書規劃內容對滿足本案需求程度。	20
總配分		100