

新北市住宅及都市更新中心
115-116 年資訊安全管理系統委外服務案
需求說明書

壹、採購目的

協助新北市住宅及都市更新中心（以下簡稱本中心）導入資通安全管理制度，並通過公正第三方稽核取得認證，以符合資通安全管理法所要求之應辦事項。

貳、專案概述

一、專案名稱

115-116 年資訊安全管理系統導入服務案（以下簡稱本專案）。

二、專案時程

本專案時程為決標日次日起至 116 年 12 月 25 日前完成所有專案需求事項並提交成果報告書，說明如下：

- （一）專案啟動：決標日次日起 20 日內成立專案小組召開啟始會議，並提交專案工作計畫書予本中心審核，經審核通過後方得據以執行。
- （二）原則於 115 年 8 月 31 日前協助本中心完成符合 ISO/IEC 27001:2022 標準要求之資訊安全管理制度建置，以及通過 ISO/IEC 27001:2022 公正第三方認證作業，並於取得證照後維持有效性至 116 年 12 月 31 日。倘因第三方緣故無法於原訂期限完成，得與本中心商議後調整。
- （三）成果報告書：廠商應分別於 115 年及 116 年 12 月 25 日前提提交成果報告書 1 式 2 份及電子檔 2 份(USB 或光碟)，成果報告書內容應包含當年度各階段執行之成果。

三、專案預算

本專案預算金額為新臺幣（以下幣值同）280 萬元；另本專案保留後續擴充之權利，擴充期間為本專案期間，且擴充之金額以 20 萬元為上限，

擴充之項目為本專案相關之工作項目，合計採購金額為 300 萬元。

四、廠商資格

本專案廠商資格應具備下列條件之一：

- (一) 技師事務所，且其執業執照所列技師科別包括資訊科者(應檢附中華民國核發之執業執照)，或；
- (二) 會計師事務所(應檢附中華民國核發之執業執照)，或；
- (三) 公司或行號(應檢附公司登記證明文件或商業登記證明文件)，或；
- (四) 前 3 款外 已立案之法人、機構或團體，依相關證明文件得提供機關資訊軟體服務、資訊軟體之規劃、設計開發、研究、分析、建置、組合、測試、維護、整合或相關業務者(應檢附由政府機關或其授權機構核發予投標廠商係合法登記或設立之證明文件)。

五、專案範圍

115 至 116 年專案主要範圍如下：

(一) 資通系統分級及防護基準評估：

1. 執行本項作業時，應針對本中心資訊系統管理者、業務承辦人、資安人員及系統廠商人員等相關人員，辦理資通系統分級及防護基準評估作業說明，並完成資通系統清冊之維護與更新，以利本項作業順利進行。
2. 依據資通安全責任等級分級辦法附表九要求，以本中心提供之最新自行或委外開發系統清單，檢視與輔導其自行或委外開發之資通系統安全等級評估結果合適性。
3. 將完成等級評估之資通系統清冊，對照資通安全責任等級分級辦法附表十要求，進行系統防護基準達成狀態評估，並針對未達標之項目提供改善建議。

(二) 資訊資產盤點與風險評鑑：

1. 執行本項作業時，應針對本中心資訊系統管理者、業務承辦人及資安人員等相關人員，辦理資訊資產盤點與風險評鑑作業說明，以利本項作業順利進行。
2. 資訊資產盤點工作如下：
 - (1)輔導本中心之資訊系統管理者、業務承辦人及資安人員等相關人員，了解資訊資產分類方式、資產盤點及價值評估等相關作業。
 - (2)協助檢視本中心資訊資產清冊內容正確性與完整性，並完成資訊資產清冊之維護與更新。
3. 風險評鑑工作如下：
 - (1)輔導本中心之資訊系統管理者、業務承辦人及資安窗口等相關人員，依本中心之風險評鑑方法辦理。
 - (2)分析本中心之內外部議題、關注方需求、資訊資產既存的威脅及潛在問題，辨別威脅來源與自身脆弱點。
 - (3)協助檢視本中心之風險擁有者評估之風險等級，確保風險評估之適切性，計算並建議風險等級，釐清現存減輕風險的安全控制方式，產出資訊安全風險評鑑報告。
 - (4)規劃風險處理計畫：依據風險評鑑之結果，針對不可接受風險等級建立風險管理機制（如降低、移轉、避免或接受），協助風險擁有者選取適當的安控目標與安控措施，並提供建議之改善活動及控制措施，識別風險擁有者、訂定已分析風險之風險處理優先序，以建立妥適之風險處理計畫。

(三) 資安管理制度文件制定與修訂：

1. 依資通安全管理法、ISO/IEC 27001:2022 資安標準及本中心資安實際運作現況需求，制定或檢視 ISMS 之政策、管理組織、程

序文件及紀錄表單等四階文件之內容合適性。

2. 協助制定或修訂績效衡量指標 (KPI)，以提升本中心之資安管理與控制目標。
3. 依據資訊資產清冊、風險評鑑結果、風險管理控制措施，審視及修訂本中心之適用性聲明書。
4. 文件修訂完成後，配合本中心資安推動需求，辦理文件修訂後之宣導，以確保本中心內部人員落實執行相關規定。
5. 得標廠商須一併將資安事件通報演練相關法定規範之管理面事項，納入本文件制定內容中，並提供對應之管理面輔導服務。

(四) 業務持續運作演練：

1. 執行本項作業時，應針對本中心資訊系統管理者、業務承辦人、資安人員及系統廠商人員等相關人員，辦理業務持續運作演練作業協處事宜，以利本項作業順利進行。
2. 協助本中心核心資通系統建立業務持續管理機制、訂定業務持續運作演練計畫及演練紀錄範本。
3. 廠商須陪同核心資通系統之業務持續運作演練作業，並依演練結果提供檢討與改善建議。

(五) 資訊安全內部稽核：

1. 執行本項作業時，應針對本中心資訊系統管理者、業務承辦人、資安人員及稽核培訓人員等相關人員，辦理內部稽核實務說明，以利培育本府內部稽核能量。
2. 針對本專案範圍協助規劃年度稽核計畫與時程，製作資訊安全管理系統（含法規遵循）之稽核查檢表，作為實地內稽查核之用。
3. 廠商須指派具備 ISO/IEC 27001:2022 主導稽核員證書之合格人員，到場執行實地內部稽核作業，並於完成稽核工作後，提交

含稽核結果及改善建議之內部稽核報告。

4. 於內部稽核後 1 個月內，協助追蹤不符合事項之改善成效確認。

(六) 資安管理審查會議：

1. 協助本中心資安承辦人員蒐集與整理會議議題，並協助檢視會議議程與會議資料完整性。
2. 廠商應派員列席資安管理審查會議，提供必要之諮詢服務，並就決議事項、待改進事項等會議待追蹤議題，協助本中心進行列管與跟進管控。

(七) 委外廠商查核：

1. 稽核規範

依據數發部資通安全署相關規範，進行本中心與委外廠商第二方稽核服務，確認所辦理程序符合法定規範。

2. 稽核方式

- (1) 非因不可抗力因素或經本中心同意，原則皆以實地稽核為主。稽核過程之稽核人力、設備、與廠商之稽核人員交通費用原則皆應含於本專案價金中，本中心不另提供。
- (2) 稽核方式原則以文件初審、承辦人員現場訪談、高階主管會談、機房勘查等方式為之，並得視實際狀況需求，適度調整稽核期程並分階段為之。

(八) 公正第三方驗證暨續審：

1. 驗證機構

- (1) 本 ISO/IEC 27001 驗證服務，須經國際認證機構(IAF)及財團法人全國認證基金會(TAF)認可之公正第三方驗證機構執行，且驗證機構之指定須經本中心確認。如因驗證機構因素致使須重審/複審/轉證等，相關衍伸費用包含於本專案價金

中，本中心不另支付價金。

(2)基於利益衝突避免原則且以第三方客觀角度進行驗證，得標廠商不得為本專案之公正第三方驗證機構。

2. 驗證期程

(1)得標廠商須參考本中心之資訊安全管理系統導入期程與各項驗證現況，合理規劃驗證期程，得標廠商需將本中心既有辦理狀況一併估量並且合理規劃各工作細項辦理時程。

(2)如因驗證期程(限)須進行相關前置作業，包含核心資通訊系統之 ISO/IEC 27001 資訊安全管理系統相關事宜、資通系統分級及防護基準評估、資訊資產盤點與風險評鑑、資安管理制度文件制定與修訂、業務持續運作演練、資訊安全內部稽核、資安管理審查會議等，概由得標廠商合理規劃辦理並包含於本專案價金中，本中心不另支付價金。

3. ISO/IEC 27001 驗證範圍

ISO/IEC 27001 驗證範圍原則為本中心核心系統「新北市青年社會住宅租賃管理系統」與實體環境，惟經實際盤點後，得與本中心商議適度調整之。

4. 驗證稽核作業

稽核前、稽核中、稽核後，得標廠商須無償配合並提供下列工作事項：

(1)稽核前：稽核時程前一個月內，應針對本專案驗證範圍內之相關人員，原則以實體會議形式為主（除有特殊情形經本中心同意後得改採線上或其他方式）辦理稽核前注意事項說明，以利協助本中心順利通過驗證。

(2)稽核中：稽核作業時，得標廠商須指派具備 ISO/IEC

27001:2022 主導稽核員證書之合格人員，全程陪同並協助本中心受稽人員進行詢答與提供相關佐證資料，以利驗證過程順利進行。

(3)稽核後：稽核結束後，得標廠商須針對發現或改善事項提供矯正改善措施建議，並協助追蹤矯正改善作業完成。

5. 其他

本專案驗證範圍之公正第三方驗證之驗證機構人力費用、證書年費與相關驗證費用均包含於本專案價金中，本中心不另行支付任何額外費用。

參、 履約程序與期程規範

得標廠商應依「履約文件及交付期限表」執行下述工作並交付相關文件：

一、 服務前置作業：

- (一)得標廠商應到本中心進行現場了解，據以進行資訊安全管理系統服務作業，並提交「資安現況與差異分析報告」。
- (二)「資安現況與差異分析報告」應就本中心之資訊安全政策、資訊安全組織、業務特性，以及對資訊安全管理現況等，依據資訊安全國際標準 ISO/IEC 27001 最新版之規定進行差異分析，並提供改善建議。

二、 資訊安全管理系統服務作業

- (一)協助規劃及執行委外廠商查核及本中心內部資訊安全稽核作業，以便執行監控程序及定期審查作業，並依據稽核結果，製作稽核報告，包括資訊安全管理制度修訂建議，以維持資訊管理系統之有效性。
 - 1. 資通系統清冊：廠商協助本中心之資通系統等級分級盤點作業，並彙整資通系統清冊。
 - 2. 資通系統分級與防護基準報告：廠商完成清冊彙整後，進行審閱

並提交資通系統分級與防護基準報告。

(二) 資訊資產盤點與風險評鑑作業：得標廠商應協助建立風險評鑑作業程序，將風險評鑑執行方法詳載於風險評鑑相關管理文件，並完成資訊資產盤點與風險評鑑作業，交付資訊資產清冊與資安風險評鑑報告，規範內容如下：

1. 資訊資產清冊：廠商應依據風險評鑑作業程序，協助建立資訊資產列表，確認資訊資產分類分級及標示原則，進行資訊資產評價，產出資訊資產清冊。
2. 資安風險評鑑報告：協助評鑑資訊資產既存的風險、風險發生可能性與潛在後果，釐清現存減輕風險控制措施，產出風險評鑑報告。

(三) 訂定與修訂資安管理制度文件：得標廠商應完成資安管理制度文件訂定與修訂事宜，並交付完整資安管理制度文件與資安風險處理計畫，規範內容如下：

1. 資安管理制度文件：得標廠商應檢視現有資訊安全政策與相關制度文件，依據 ISO/IEC 27001 條款要求及業務特性，規劃建置或調整資訊安全管理制度文件，並於期限內交付，再由管理階層核准發行。
2. 資安風險處理計畫：得標廠商應依據風險評鑑結果，與業務負責同仁討論後，協助決定可接受風險等級，建議風險管理機制（如：降低、接受、避免或轉移），選擇適當的控制措施，提出風險處理計畫。

(四) 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業務持續運作演練計畫書，於期限內完成業務持續運作演練作業並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：得標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：得標廠商應依據業務持續運作演練結果，協助完成「業務持續演練完工報告書」，並視業務需求，協助或輔導營運持續相關演練作業。

(五) 資訊安全內部稽核：得標廠商應於期限內提出資訊安全內部稽核規劃並交付資訊安全內部稽核計畫書，於期限內完成資訊安全內部稽核作業並交付資訊安全內部稽核報告，規範內容如下：

1. 資訊安全內部稽核計畫：得標廠商應負責製作內部稽核相關規範、程序書及內部稽核計畫，並協助完成內部稽核作業。
2. 資訊安全內部稽核報告：得標廠商應依據內部計畫協助完成內部稽核後，應協助完成內部稽核報告與矯正措施建議，並完成內部稽核完工報告，內容包含：內部稽核檢查表、內部稽核報告與矯正措施單。

(六) 資安管理審查會議：得標廠商應於期限內，完成資安管理審查會議工作事宜，包含管理審查會議議題蒐集及會議報告準備，並列席及協助會議進行與會議紀錄。

(七) 資訊安全管理系統服務，得標廠商須於履約期間內，無償提供文件增修、文件維護、文件保固等服務，本中心不另支付價金。

(八) 本專案履約期程，如有資通安全管理法、相關子法、行政命令暨法規微調事宜，得標廠商須就法定管理面相關事宜配合辦理，本中心不另支付價金。

三、委外廠商查核：

(一) 規劃作業：

得標廠商應於本中心通知日起 10 工作天內完成查核規劃並提出「委

外廠商查核計畫書」，內容包含查核團隊成員組成、查核期程、稽核方式、稽核範圍、受稽單位配合事項、本中心配合事項等規劃事項。

(二)稽核作業：

依據本中心核定之稽核計畫內容進行稽核作業。

(三)稽核完成：

得標廠商應於完成稽核日起算 10 工作天內交付「委外單位資安查核完工報告書」，包含查核結果、發現事項、後續改善建議內容等。

(四)後續精進：

稽核結果如有發現或改善事項須提供矯正改善措施建議，須將相關追蹤矯正改善作業與矯正改善措施建議內容，一併於本案專案會議辦理以為後續精進。

四、公正第三方驗證：

(一)規劃作業：

得標廠商應於決標日次日起 20 日內併同「專案工作計畫書」提出「公正第三方驗證暨續審計畫書」，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。

(二)前置作業：

針對本專案驗證範圍內之相關人員，原則以實體會議形式為主（除有特殊情形經本中心同意後得改採線上或其他方式），針對本中心辦理稽核前注意事項說明，以利協助機關順利通過驗證。

(三)公正第三方驗證作業：

本案完成公正第三方驗證暨續審後，於驗證完成 20 工作天內交付公正第三方驗證暨續審完工報告書，包含驗證稽核報告、驗證通過證明、驗證期程、範圍。如有發現或改善事項須提供矯正改善措施建

議，須將相關追蹤矯正改善作業完工證明與矯正改善措施建議內容，一併檢附於前述公正第三方驗證暨續審完工報告書，以為本公正第三方驗證暨續審工作事項完工佐證。

肆、 專案團隊與管理

一、 專案團隊

- (一) 本專案廠商之專案經理應具備良好之協調及資訊專業能力，以掌控本專案之執行進度及成果，並符合本中心需要。
- (二) 本專案參與人員需具資訊安全規劃及導入技能，並具相關證照（如 CISSP、CISA、ISO 27001 LA 或其他類似之文件），以確保能執行本專案相關工作，建議書應附參與本專案人員履歷表及相關佐證資料。
- (三) 專案團隊成員中應指定專案負責人、專案經理、專案聯絡人（此三者得為同一人），均應為得標廠商現職正式員工。
- (四) 專案經理應具備學士學歷且具備10年以上資訊服務或資訊安全專案管理經驗，或碩士以上學歷並具備5年以上資訊服務或資訊安全專案管理經驗，須為得標廠商之全職員工，且連續在職1年以上（以決標日期往前計算），實際負責本契約得標廠商各項履約工作及進度管理，至少具備下列任一項經驗：
 - 1. 曾任專案經理且負責專案為資安相關專案，具備 PMP 證照。
 - 2. 具有參與輔導政府機關(構)通過 ISO/IEC 27001:2022 驗證之經驗。

二、 人員管理

- (一) 廠商執行本專案所需之人員、交通、保險及相關管理措施及所衍生之相關費用等，含括於本專案經費內由得標廠商自行提供或負擔。
- (二) 參與計畫人員之更換，應具備相同資格，並於兩週前主動通知本中心，並經本中心同意後始得更換。

- (三) 本中心對不符本專案執行需要之人員，得要求得標廠商更換，得標廠商應提供適當人選更換，並於兩週內完成人員交接。

伍、 服務建議書相關事宜

一、 服務建議書格式

- (一) 建議書 1 式 (含附件) 7 份並附電子檔 USB (或光碟) 2 份，建議封面加蓋公司及負責人印章。
- (二) 用紙：建請以 A4 之紙張、直式橫寫格式製作，並以電腦繕打，但相關之圖說不在此限。
- (三) 繕打方式：除圖表、型錄外，由左至右橫式繕打。
- (四) 裝釘方式：裝訂線在左側，裝釘成冊，如有一冊以上，請於封面註明總冊數及冊次。
- (五) 服務建議書裝訂後，如有缺漏、錯誤或需補充部分，得製作勘誤表或補充說明，份數與服務建議書冊數相同，併同服務建議書送達。
- (六) 其他：
1. 建請加目錄、編頁碼、加封面(請註明本案名稱及投標廠商名稱)。
 2. 服務建議書內容中引用相關書籍、資料，建請加註所引用之出處。
 3. 服務建議書內容次序建請按評分表之評選項目次序排列。

二、 建議書內容

(一) 廠商實績及履約能力(15 分)

1. 廠商基本資料及簡介。
2. 廠商獲得之資安認證及得獎紀錄。
3. 廠商人力資源。
4. 廠商最近五年相關實績 (不含分包廠商)。
5. 最近五年營運狀況。
6. 合作廠商及專家學者。

(二) 專案團隊執行能力(25 分)

1. 專案團隊組織。
2. 專案人力配置及成員分工。
3. 專案成員能力(資歷證照)。

(三) 專案規劃與技術能力(40 分)

1. 資訊安全管理系統服務規劃。
2. 公正第三方驗證規劃。

(四) 價格組成及合理性(10 分)

(五) 創意及優規服務(5 分)

創意及優規(其他與本採購案標的有關，且含於標價內之附加或創新服務)

(六) 簡報及答詢(5 分)

1. 簡報及應詢是否完整、表達是否明確。
2. 專案負責人或專案經理有無親自出席簡報。

三、評選規定

(一) 優勝廠商評定方式：序位法

(二) 本採購案總滿分為 100 分，總滿分之合格分數為平均總評分 75 分。

(三) 標價不納入評比(依投標須知載明之固定價格(或費率)給付)，但標價組成內容納入評比。

(四) 個別評選委員於各評選項目分別評分後，如有不同廠商之加總分數相同致予相同序位者(例如第二名有二家)，其接續之其他廠商序位：以一、二、二、四、五、六方式表示。

(五) 優勝廠商為 1 家者，以議價方式辦理；優勝廠商在 2 家以上者，依優勝序位以依序議價方式辦理。如有 2 家(含)以上優勝廠商序位合計值相同者，擇配分最高之評選項目之得分合計值較高者，優先

議價；如配分最高之評選項目有兩項以上者，以該等項目得分合計值較高者，優先議價；得分仍相同者，就該等廠商再進行綜合評選一次，以序位合計值最低者，優先議價；其再次相同者，抽籤決定之。但綜合評選次數已達政府採購法第 56 條規定之 3 次限制者，逕行抽籤決定之。

(六)其餘依投標須知之規定。

附表

履約文件及交付期限表

項次	履約文件項目	工作要求及履約期限
1	專案管理	
1-1	專案工作計畫書	決標日次日起 20 日內。
1-2	保密切結書及著作人約定書	併同專案工作計畫書交付。
2	資訊安全管理系統服務	
2-1	資安現況與差異分析報告	依專案工作計畫書規劃
2-2	資通系統清冊	
2-3	資通系統分級與防護基準報告	
2-4	資訊資產清冊	
2-5	資安風險評鑑報告	
2-6	資安風險處理計畫	
2-7	資安管理制度文件	
2-8	業務持續運作演練計畫書	
2-9	業務持續運作演練完工報告書	
2-10	資訊安全內部稽核計畫書	
2-11	資訊安全內部稽核完工報告書	
2-12	資安管理審查會議完成報告	
3	第三方稽核服務	
3-1	委外廠商查核計畫書	於本中心通知日起 10 工作天內交付。
3-2	委外廠商查核完工報告書	於完成稽核日起算 10 工作天內交付。
4	公正第三方驗證	
4-1	公正第三方驗證暨續審計畫書	併同專案工作計畫書交付。
4-2	公正第三方驗證暨續審完工報告書	於驗證完成 20 工作天內交付公正第三方驗證暨續審完工報告書與公正第三方驗證單位核發之驗證通過證明。倘因第三方緣故無法於原訂期限完成，得與本中心商議後調整。
5	成果報告書	各年度 12 月 25 日前。