

**政府機關資訊安全管理系統(ISMS)
第三方驗證委外服務案
建議書徵求文件
(V1.0)**

修訂歷史紀錄

版次	發行修訂生效日期	變更說明
▪ 第 1.0 版	▪ 103 年 11 月 1 日	▪ 新版正式發行
▪	▪	▪
▪	▪	▪
▪	▪	▪
▪	▪	▪
▪	▪	▪
▪	▪	▪
▪	▪	▪
▪	▪	▪

目 次

壹、 專案概述.....	1
一、 專案名稱.....	1
二、 專案目標.....	1
三、 專案範圍.....	1
四、 專案期間.....	1
貳、 專案工作項目.....	2
一、 廠商執行標準驗證作業，所有人天數需符合相關標準規範。.....	2
二、 若通過資安驗證標準第三方稽核國際驗證，提供國外認證授權中、英文證書，依機關要求至少 N 張。.....	2
三、 提供驗證稽核報告，以及若有驗證稽核發現之不符合項 (Nonconformities) 的追蹤報告文件。.....	2
參、 管理需求.....	3
一、 廠商資格.....	3
二、 服務水準協定(SLA)與罰責.....	3
三、 品質需求與驗收標準.....	5
四、 業務保密安全責任.....	5
五、 專案經費預算金額.....	6
肆、 交付項目.....	7
一、 交付項目與時程.....	7
二、 交付文件格式.....	7
三、 交付項目說明.....	7
伍、 建議書製作規定.....	8
一、 服務建議書格式.....	8
二、 服務建議書內容.....	8

陸、建議書評選事宜.....	10
一、評選辦法.....	10
二、評選標準.....	11
三、其他評選注意事項.....	11

壹、專案概述

一、專案名稱

「資訊安全管理系統(ISMS)」第三方驗證委外服務案（以下簡稱本案）。

二、專案目標

- (一)進行驗證/重新驗證稽核(Certification Audit /Re-certification Audit) ，
驗證機關資訊安全管理系統 (ISMS, Information Security Management System)，符合 ISO27001 資安驗證標準。
- (二)進行後續兩年之追查稽核(Surveillance Audit)。
- (三)完成符合資安驗證標準 2013 年版。

三、專案範圍

- (一)以「○○○計畫」/「○○○業務」所涉及辦公環境為驗證範圍，驗證該範圍內之相關資訊安全管理系統。

四、專案期間

自簽約日起至 XXX 年 XX 月 XX 日止。

貳、專案工作項目

資訊安全管理系統(ISMS)第三方驗證專案，應涵蓋以下內容。

- 一、廠商執行標準驗證作業，所有人天數需符合相關標準規範。
- 二、若通過資安驗證標準第三方稽核國際驗證，提供國外認證授權中、英文證書，依機關要求至少 N 張。
- 三、提供驗證稽核報告，以及若有驗證稽核發現之不符合項 (Nonconformities) 的追蹤報告文件。

參、管理需求

一、廠商資格

為確保資訊安全及得標廠商所提供的服務水準，得標廠商應符合下列條件，並於服務建議書專章詳述：

- (一)凡在政府機關登記合格，無不良紀錄之廠商（檢附設立及登記證明、納稅證明及信用證明）且不得為陸資企業（包括子公司、分公司、獨資或合夥事業及其轉投資事業）。本案服務人員需具有中華民國國籍，不得為外籍勞工或大陸來台人士。
- (二)本案服務內容將涉及敏感資訊，得標廠商不得轉包或分包予其他廠商執行。
- (三)投標廠商須實施資訊安全管理制度，通過 ISO 27001 或其他類似驗證，並於專案執行期間持續有效，以保護執行本案所取得之資料。
- (四)本案團隊人力至少應包含專案負責人/專案經理與 ISMS 稽核人員。ISMS 稽核人員應具備以下所列舉之經歷及相關之專業證書，以確保服務水準，並於建議書中檢附成員姓名、專業證書及服務實績證明等影本以供審核。應具備資格說明如下：
 - 1.合格之稽核員證書證明。
 - 2.具二年（含）以上之 ISMS 稽核相關經驗。

二、服務水準協定(SLA)與罰責

(一)服務水準規範

本案服務水準協定（Service Level Agreement，SLA），以必須達成該項工作服務項目要求為依據，透過客觀的證據或指標，做為品質管制，以預防各項不符合作業的事項發生，降低委外作業的風險，詳細服務水準規範如下表：

項次	項目	服務水準
1	驗證稽核報告	<ul style="list-style-type: none"> ▪ 詳列稽核相關資訊與發現 ▪ 若有驗證稽核發現之不符合項 (Nonconformities) 的追蹤報告文件
2	驗證合格證明	<ul style="list-style-type: none"> ▪ 通過驗證時，驗證合格之證明

(二)相關說明：

- 1.承作廠商違反『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，星期日、國定假日及其他休息日均應計入，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，款項可自契約總價或履約保證金項中扣抵。
- 2.違約金上限依採購法之採購契約要項第四十五點規定，違約金以契約總價之20%為上限。如違約金逾20%時，本機關得以書面通知得標廠商終止契約或解除契約之部分或全部，且不補償得標廠商所生之損失。
- 3.得標廠商指派之專案負責人及工作成員，未經本機關同意，不得更換，如有未經本機關同意自行更換時，每更換乙次得依契約總價之千分之一計算懲罰性違約金。
- 4.得標廠商應將文件品質保證納入專案品質保證項目，嚴謹製作本專案各項文件，包含版面及內容皆須嚴格要求一致性及正確性。交付本機關之文件經本機關審閱時，所發現錯漏處達N處以上，或業經本機關要求修訂仍未修訂者，本機關得按每字新台幣XXX元計算懲罰性違約金，並自付款項中扣抵；其有不足者，得通知

廠商繳納或自履約保證金扣抵。

三、品質需求與驗收標準

(一)品質需求

- 1.為確保專案如期如質完成，廠商應針對本專案之需求，妥慎成立專案小組，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。
- 2.得標廠商訂定品質管理流程，本機關得以稽核。
- 3.得標廠商於專案期間應辦理啟始會議與結束會議，會議討論內容與結果需作成紀錄。

(二)驗收標準

得標廠商應依貳、專案工作項目之服務需求，以及符合服務水準協定(SLA)中所列事項，完成專案工作，並依本說明文件所訂之交付時程，完成相關文件之交付。

(三)驗收方式

本機關將於各項工作項目交付完成後進行審查作業，得標廠商需依本機關審查意見修正交付項目，並再送至本機關複驗。

四、業務保密安全責任

- (一)廠商基於本案需要，所取得各種形式之資訊，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，並簽定保密協議書。
- (二)廠商對特別以文字標示或口頭明示為機密資料者，非經本機關書面同意，不得洩漏資料予第三者，致使造成之法律責任或賠償，廠商應負

完全責任。

(三)廠商對於可能接觸與本案相關資料或文件之人員，須提供保密管理機制，相關人員均須簽署保密切結書(切結書形式由廠商自訂)。

(四)契約終止時，廠商應將有關本案過程中處理之任何形式資訊，整理歸檔後退還本機關或經本機關同意後銷毀。

(五)履約期間造成保密及安全事件，得歸咎於廠商之責任時，廠商應負所有法律及賠償責任。

(六)本機關對廠商保留實地稽核權，以確保廠商於委外服務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。

五、專案經費預算金額

(一)本案 YYY 年度預算金額為新台幣 N 萬元整。

(二)本採購保留未來向得標廠商增購之權利，第 2 及第 3 年後續追查稽核驗證(Surveillance Audit)相關費用(包括申請、驗證、改版轉證、證書年費…等)。擴充期間 YYY+1、YYY+2 年度費用各約 m 萬元整，總經費為新台幣 M 萬元整。

肆、交付項目

一、交付項目與時程

(一)工作計畫書：決標日起 2 週(日曆天)內交付。

(二)驗證稽核報告：依工作計畫書載明之交付時程。

(三)驗證合格證明：依工作計畫書載明之交付時程。

二、交付文件格式

各項文件應提供紙本 N 份，光碟電子檔 N 份。

三、交付項目說明

交付項目	內容說明
1. 工作計畫書	<ul style="list-style-type: none">▪ 工作計畫書應以廠商投標時之「建議書」為基礎，並依採購評選意見修改▪ 內容除包括對本專案之執行敘述，含專案管理、組織、人力、分工、職掌、細項工作規劃內容、執行方式及時程說明
2. 驗證稽核報告	<ul style="list-style-type: none">▪ 文件內容應包括：稽核相關資訊與發現、若有驗證稽核發現之不符合項(Nonconformities)的追蹤報告文件
3. 驗證合格證明	<ul style="list-style-type: none">▪ 通過驗證時，驗證合格之證明

伍、建議書製作規定

一、服務建議書格式

- (一)紙張：宜用 A4 規格。
- (二)繕打及裝訂方式：由左至右橫式繕打，加註頁碼，加裝封面及目錄，封面上註明廠商名稱、廠商地址、本案名稱及日期，裝訂線在左側。
- (三)目次：應標示各章節之出處頁碼。
- (四)廠商投標建議書之份數為 1 式 N 份。

二、服務建議書內容

(一)專案概述

- 1.專案名稱
- 2.專案目標
- 3.專案時程

(二)廠商說明

- 1.廠商簡介
- 2.公司營運狀況，包含參與人員名單、能力證明及經驗說明
- 3.稽核報告書面範例
- 4.資訊安全及個資保護(相關安全維護之規劃及執行方式)

(三)專案計畫

- 1.專案服務內容、交付項目及時程規劃
- 2.組織與人力配置
- 3.專案品質與風險管理

(四)價格分析

- 1.詳列稽核人員人/天價格（所需之差旅及交通費用請內含於稽核人員費用中）
- 2.有證書年費者請載明證書年費、證書申請費用等。
- 3.詳列第2及第3年後續追查稽核驗證費用

陸、建議書評選事宜

一、評選辦法

- (一)依據「政府採購法」第 22 條第 1 項第 9 款之規定辦理，透過書面審查及簡報答詢的方式，以合於招標文件，標價合理且在預算金額內，經評選委員評選為合格的廠商，依序議價。
- (二)由本機關邀集專家學者組成評選委員會，除對廠商之建議書進行書面審查外，並由本機關召開評選會議，由廠商提出 15 分鐘對建議書之簡報，其後並接受評選委員之詢問，答詢時間以不超過 10 分鐘為限，惟因評審委員詢問題目過多時，主席得酌以延長答詢時間。評選會議時間及地點，將於資格審查時當場宣布或另備文通知，而廠商之簡報順序，亦於資格審查時抽籤決定。
- (三)簡報及答詢結束後，各評選委員根據本徵求建議書說明文件第柒之二「評審項目」所列項目及配分評定各廠商名次及其是否為合格廠商（以總得分 XX 分(含)以上為合格）。
- (四)各評選委員評定結果不得有同名次或從缺情形。
- (五)過半數(含)評選委員評定為合格之廠商方列入排名與序分計算；另半數以上(含)評選委員評定不合格之廠商，視為不合格，若所有廠商均不合格時，主席應宣布廢標，重新辦理本案。
- (六)本案評選採序位法辦理，就各評審項目分別評定並換算為序位，再加總計算廠商序位，最低者為第 1 優先序位，次低者為第 2 序位，餘依此類推。
- (七)經評選委員會評定優勝廠商，依優勝序位，自最優勝者起，依序以議價方式辦理，但有二家以上廠商為同一優勝序位者，以建議書的標價低者優先議價，若仍相同者，則擇獲得評選委員評定序位第一較多者決標；仍相同者，抽籤決定之。

(八)評選結果簽請首長或授權人員核定後，由本機關另定時間通知廠商依序辦理議價。

二、評選標準

本案由評選委員就廠商所提出建議書之內容，針對其經驗、能力與服務水準，依下列各項目及配分，予以評分，總分 100 分，得分總計達 XX 分(含)以上者為合格。

評審項目	評審項目內容	配分
廠商業績及履約能力	1.廠商人力規模、商譽 2.資安實績與相關技術經驗	20
專案管理	1.對本案工作內容之瞭解 2.進度時程控管、資料管制與品質保證 3.本案之團隊規模與專案負責人之經驗 4.本案團隊成員之專業證照符合程度	20
專案規劃完整性	1.本案要求之各項服務項目的執行專業性 2.本案要求之各項交付項目之完整性	30
成本合理性	本案規劃、執行、專案管理及報告撰寫等各項費用估算之合理性	20
簡報及答詢	廠商簡報與答詢內容是否清楚、完整	10
總分		100
是否合格		<input type="checkbox"/> 合格 <input type="checkbox"/> 不合格
名次序位		

三、其他評選注意事項

(一)本機關得因故終止評選事宜，通知投標廠商領回建議書。

(二)本文件未盡事宜，依據「政府採購法」相關規定辦理。