財團法人中華民國證券暨期貨市場發展基金會資訊安全管理系統(ISMS)委外服務案建議書徵求文件

目　次

壹、專案概述

一、專案名稱

「資訊安全管理系統(ISMS)及資通安全維護計畫」委外服務案（以下簡稱本案）。

二、專案目標

期透過本案輔導機關建置資訊安全管理系統（ISMS，Information Security Management System）及編製資通安全維護計畫，使符合資安驗證標準與國家法規法令要求。另協助機關施行內部稽核與相應矯正預防措施，俾利機關通過第三方稽核與取得驗證目的。

三、專案範圍

(一)以「資訊安全管理系統(ISMS)及資通安全維護計畫」所涉及辦公環境為驗證範圍，並建置該範圍內之相關資訊安全管理系統。

(二)建置資訊安全管理系統，以符合法規及通過 CNS27001 最新管理標準驗證。

(三)協助機關施行內部稽核與相應矯正預防措施。

四、專案期間

自簽約日起至 109 年 1 月 31 日止。

貳、專案工作項目

資訊安全管理系統(ISMS) 專案，應涵蓋以下所列所有服務項目。

一、編製資通安全維護計畫

依據資通安全管理施行細則第六條規定資通安全維護計畫規定辦理，並參考附件範本編製。

二、建置資訊安全管理系統(Information Security Management System, ISMS)

(一)依據機關風險管理作業原則，完成驗證範圍內之脆弱與風險評估，並提出妥適之風險處理計畫。

(二)建置資訊安全管理制度，並協助修訂機關資訊安全管理系統相關四階文件並遵循機關內部控制制度 / 檢視現行資訊安全管理制度，針對四階文件提供調整建議，並協助文件調整。

三、與現有管理機制與資源之整合

(一)整合 ISMS 與個人資料保護等現有管理制度，以提升業務管理流程之效能與效率。

(二)就已導入或全新建置之管理或技術系統，分析範圍內之管理組織、制度、人員、會議、文件及紀錄表單等四階文件，以一致性之管理作業加以整合。

四、輔導通過 CNS 27001 最新管理標準之稽核與驗證

(一)依據驗證範圍，進行 ISMS 管理系統內部稽核事項。

(二)協助機關進行 CNS 27001 最新管理標準，第三方驗證審查作業，管理驗證相關制度與四階文件，協調機關內部及驗證前準備作業。

五、提供一年保固服務

協助持續維護管理系統複驗之相關事宜，並提供服務流程調整與稽核報告缺失之改善方案。

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 CNS 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 執行人員。ISMS 執行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.ISO 27001:2013 主導稽核員證書（ISO 27001:2013 Lead Auditor Course Certification）。

2.具二年（含）以上之 ISMS 輔導相關經驗。

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	風險評鑑	▪ 分析機關面臨的威脅及潛在的問題，辨別威脅來源與脆弱點，釐清降低風險的安全控制點，進行衝擊分析，計算並決定可接受風險等級 ▪ 建議風險管理機制(如降低、移轉、避免或接受)，選取適當的安控目標與控制點，完成風險處理計畫並通過機關審查 ▪ 風險評鑑執行時程依核定之工作計畫書內容
2	ISMS 系統四階文件	▪ 依計畫進度完成符合最新版本 CNS 27001資訊安全管理系統標準要求，遵循內部控制制度之相關四階文件並完全通過機關審核 ▪ 四階文件執行時程依核定之工作計畫書內容

項次	項目	服務水準
3	內部稽核	▪修訂 ISMS 系統內部稽核制度及訂定年度稽核計畫，並持續改善機關資訊安全政策之落實 ▪製作 ISMS 系統(含法規遵循)之稽核查檢表，並詳列查核項目之查核重點。依機關稽核分組要求，稽核時廠商至少派 3 人(含)以上到稽核團隊，協助執行至少 1 次內部稽核，並於完成稽核工作後5個日曆天內提交含改善建議稽核報告 ▪稽核時程依核定之工作計畫書內容 ▪稽核後1個月內完成不符合事項改善之持續追蹤與成效確認
4	第三方驗證缺失改善	▪協助持續維護管理系統複驗之相關事宜，並提供服務流程調整與稽核報告缺失之改善方案 ▪驗證審查後1個月內完成不符合事項改善之持續追蹤與成效確認

(二)相關說明：

1.專案期間違反上述任何所述者，視同違反『未能於規定時間完成工作計罰』，如須延長日期或非廠商之問題(不納入計罰)，須經機關同意。

2.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。

3.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。

4.得標廠商應於議價後所提成本分析中，詳列各項工作項目成本，如於驗收時，經審查發現有不合格之工作項目，得標廠商應依期限予以改正。如未改正，本機關有權扣除該項工作之款項。

5.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。

6.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 10 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一千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，並視情況召開專案管理會議以掌控品質，會議討論內容與結果需作成紀錄與追蹤辦理，送本機關備考。

(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，完成相關文件與紀錄之交付。

(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。

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)資通安全維護計畫：108年1月中旬前交付。

(三)風險評鑑報告：依工作計畫書載明之交付時程。

(四)ISMS 四階文件：依工作計畫書載明之交付時程。

(五)內部稽核報告：依工作計畫書載明之交付時程。

(六)服務工作報告：依工作計畫書載明之交付時程。

二、交付文件格式

(一)各項文件應提供紙本3份，電子檔3份（以光碟或本機關同意之儲存媒體及提交方式）。

(二)必要時本機關得要求派員親臨說明。

三、交付項目說明

交付項目	內容說明
1. 工作計畫書	▪ 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(包括起始會議與結束會議)
2. 資通安全維護計畫	▪ 依據資通安全管理施行細則第六條規定資通安全維護計畫應規定辦理，並參考附件範本編製
3 風險評鑑報告	▪ 文件內容應包括：風險評鑑執行內容、風險處理計畫
4. ISMS 四階文件	▪ 新增與修訂之 ISMS 四階文件
5. 內部稽核報告	▪ 文件內容應包括：內部稽核結果、改善建議
6. 服務工作報告	▪ 文件內容應包括：第三方驗證缺失改善內容、工作小組會議紀錄、結論與建議

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 10 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、能力證明及廠商經驗說明

(三)專案計畫

1.專案服務內容項目

2.組織與人力配置

3.專案時程、品質、風險管理與交付項目計畫，包含工作項目、時程規劃及查核點

4.本案帶來之預期效益

5.本案 SLA 之承諾

(四)其它