招標規範

資訊安全管理制度(ISMS)建置輔導暨 ISO27001 驗證服務採購案

需求計劃書

財團法人公共電視文化事業基金會

2020 年 4 月 20 日

目錄

壹、 專案概述

一、專案名稱

財團法人公共電視文化事業基金會(以下稱本會)「資訊安全管理制度(Information Security Management System，ISMS)建置輔導暨 ISO27001 驗證服務採購案」(以下稱本專案)

二、專案目的

為確保本會資訊資產的機密性、完整性與可用性，有效降低資安風險，並使本會符合資通安全法令規定。爰此規劃本專案，建置本會 ISMS 並通過 ISO27001 標準之驗證，落實本會資通安全及業務持續營運。

三、專案目標

委由廠商提供必要的資安顧問輔導及諮詢服務，達成下列目標：

(一) 建立本會符合 ISO27001：2013 標準之 ISMS：

1. 強化專案範圍內之資通安全作業與環境之技術防護能力。
2. 強化制度之落實度及完整性。

(二) 協助檢視本會資通安全各項防護措施，提出改善建議方案，以符合資通安全責任等級辦法 A 級之特定非公務機關之各項規範及要求。

(三) 依本會擇定之驗證範圍，協助通過 TAF 認可之第三方驗證單位查核，並取得 ISO27001：2013 國際資安證書。

(四) 協助本會同仁取得 ISO27001：2013 LA 資安專業證照 4 張。

(五) 協助提升本會同仁資安防護意識及資通安全管理與技術專業能力。

四、專案範圍

(一) ISMS 實施範圍

本專案以本會 ISMS 驗證範圍為主要之實施標的，另須包含與 ISMS 制度實施相關單位或人員。本專案主要工作項目如下：

1. 協助完成「資通安全管理法」及其子法要求之事項
2. 輔導建置 ISMS。
3. 規劃及執行「資通安全教育訓練講習」
4. 統籌「第三方 ISO27001:2013(或最新版)稽核驗證相關作業」
5. 提供資通安全領域之「顧問諮詢服務」

(二) ISMS 輔導/驗證範圍

本專案「ISO 27001:2013」之輔導/驗證範圍如下：

※輔導人員範圍：工程部，新媒體部。

※驗證人數：總計 25 人(實際驗證人數得視實際執行情形經本會同意進行調整後，廠商須配合辦理)。

※驗證實體環境：本會經主管機關核定之關鍵基礎設施(數位信號發射)、核心資通系統、資訊機房及相關應用系統之安全維運管理，驗證範圍得視實際執行情形經本會同意後進行調整，廠商須配合辦理。

五、專案時程

本專案時程自決標次日起 18 個月完成。(2021/12/31 前)

六、專案經費

實際經費以決標後簽約金額(含稅)為準，契約價金總額係包含本專案契約有效期間內執行本專案所需之一切費用，包含輔導、教育訓練與驗證費用等。

七、專案聯繫

對本專案需求規格如有疑問請洽本會承辦人：

新媒體部資訊管理組/吳中榮 電話：02-26332000#1940

貳、 專案需求

一、現況差異性分析

經由訪談及本會現有文件資料與實地討論的現況調查，依專案範圍之資訊系統運作業務與 ISO27001 標準要求的差異分析，作為公司資訊管理、委外廠商管理、資安防護等文件及流程改造之規畫依據，產製「資安現況分析報告」。

二、ISMS 文件建置

廠商應針對本會之組織分工、業務流程、計畫特性及未來之發展方向，建立本會 ISMS 文件，此涵蓋下列作業：

（一）依據 ISO27001：2013 要求，建立本會 ISMS 相關文件。

（二）建立分析資安管理目標指標。

（三）與本會既有相關文件與表單修訂與整合。並依據內部稽核結果討論，協助資訊安全文件與表單修訂。

（四）協助本會配合資通安全管理法及其子法規定，編訂資通安全維護相關作業各項計畫與推動。結合導入之 ISMS 制訂「資通安全維護計畫」文件與完成主管機關之稽查要求為首要。並依本會年度資通安全運作及 ISMS 維運情形，彙整提報「資通安全維護計畫實施情形」，協助本會提交次年度之資通安全維護計畫。

三、風險評鑑與風險管理作業

（一）依照資訊資產評鑑作業進行資訊資產清查，確認資訊資產分類法則，與資產價值評估，產製「資訊資產清冊」。

（二）進行業務衝擊分析(Business Impact Analysis)，包含本會關鍵基礎設施資安防護建議。

（三）執行風險評鑑作業：分析本會關鍵基礎設施及資通資產既存的威脅及潛在的問題，以辨別威脅來源與脆弱點，計算並建議風險管理機制(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「資安風險評鑑報告」。

（四）針對採用之風險處理措施，擬訂風險處理計畫，協助定期檢討其執行進度或成效。

四、資訊安全事件管理

（一）評估本會資訊安全管理之實際運作，提供事件之處理建議。

（二）建立業務持續運作計畫、持續運作手冊與演練計畫。

五、資訊安全內部稽核

（一）ISMS 運作過程，協助彙整管理階層審查必要之各項資料。

（二）擬定內部稽核計畫與稽核時程。

（三）組成至少 2 位(含)以上，具有 ISO27001 LA 考試合格的稽核員執行一次資訊安全內部稽核，並提出稽核結果之缺失矯正與持續改善建議。

六、資訊安全管理審查會議

（一）廠商於會議前 10 個日曆天內協助蒐集與整理會議議題，並負責準備會議簡報檔與會議資料。

（二）廠商協助會議召開並完成會議記錄，並完成會議決議事項之追蹤與執行。

七、資訊安全相關會議

（一）廠商應協助本會研訂管理審查事項，並視需要派員參與會議提供諮詢服務。

（二）本專案時程內，若遇主管機關至本會進行資通安全外部稽核時，或將本會列為情境演練對象、或辦理其他指示事項時，顧問須至本會協助辦理，並協助完成待改善事項之矯正及預防措施。

八、協助取得 ISO27001 證書

（一）正式驗證

1. 確保本專案導入之 ISMS 符合 ISO27001 最新版規範，協助本會通過 ISO27001 正式驗證作業並取得證書。驗證期間顧問應至本會參與驗證活動，並陪同受稽核人員進行詢答。
2. 驗證結束後，針對審查發現之不符合事項(包含建議事項及觀察事項)，研訂矯正及持續改善措施並協助完成，於下次驗證日期前有效改善不符合事項。

（二）費用

統籌規劃本會通過 ISO27001 驗證之相關事宜，第三方驗證機構之驗證費用及證書年費全由廠商負責，本會不另支付任何費用。

九、教育訓練

（一）廠商應提出教育訓練計畫。本專案期間依照建置需求舉辦至

少應包含 ISO27001 標準架構說明、資產盤點、風險評鑑、業務持續演練、內外部稽核注意事項與一般同仁資安概念等課程，總時數不得少於 24 小時。

（二）廠商須提供 4 名 ISO27001：2013 LA 國際認證外訓課程名額，授課與證書發證單位須 IRCA 或同等級之國際組織評鑑認可資格。

參、 管理需求

一、廠商資格

（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 27001:2013 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）專案服務團隊

為確保本專案服務品質與人員業務分工職掌明確，廠商應成立服務團隊，成員應衡酌本專案範圍、工作項目、時程，其資格至少應符合以下要求。

人員	人數	資格
專案經理(可兼資安顧問)	1	☑ 具有 PMP、ISO27001：2013 LA 證照 ☑ 具備輔導過資安責任等級 B 級(含)以上之政府機關通過 ISO 27001：2013 驗證之實績達 3 家以上 ☑ 具有 5 年(含)以上 ISO27001 輔導顧問年資，曾擔任專案經理職務。
資訊安全輔導顧問	至少 2 人	☑ 具有 ISO27001：2013 LA 證照 ☑ 具實際輔導政府機關建置 ISMS 之實績 ☑ 3 年(含)以上 ISO27001 輔導顧問年資

（五）人員管理

1. 本專案成員如有異動須事先通知並獲本會同意：一個月前函請本會同意，並檢附接替人員相關學經歷、專長、負責本專案之工作項目與內容、在職證明及相關證照，並須由本會查核通過後始得更換。
2. 專案服務團隊成員如有服務表現不佳或違反本會相關規定，本會得要求廠商撤換。廠商應於接獲本會書面通知起 15 個

日曆天內提出符合契約規定之替代人選。

3. 上述人員更換時，接替人員應至少 15 個日曆天之交接期，以利工作銜接。

（六）本規範有疑問時，以本會解釋為準。

二、專案工作計劃書

廠商須於「專案工作計畫書」中說明本專案擬執行之工作範圍、工作時程、交付項目、專案管理方式及檢查時間點、執行專案工作項目所需成立之專案組織、具體可行之專案執行策略與建議方案以及本專案進行過程中所建立之執行與管制紀錄。

三、專案會議

本專案進行期間，本會與廠商視需要召開會議，其目的在檢驗計畫執行狀況，明訂未確定之作業規範，解決發生問題，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。

四、文件之審核

廠商應依計畫書、契約及相關計畫規定之日期提出各項計畫、交付文件及報告，並經本會審核通過據以實施或使用。(並依月、季、年之週期提供工作報告書)

五、專案執行方式

本專案除 ISMS 驗證作業外，得標廠商必須自行完成其餘所有工作項目履約工作，不得另行轉包。

六、安全需求

項次	規範
1	廠商執行本專案如取用未經合法授權使用之軟體或硬體產品或識別標誌、圖檔等，致使本會遭致任何損失或聲譽損害時，廠商應負責一切損害賠償責任。
2	廠商從事本專案相關工作經手、保管或取得之個人資料、管理文件、帳號密碼及公務機密，非因公務並經本會授權，不得對外提供。
3	廠商於本專案服務期間所知悉、獲得、蒐集與本專案相關之個人資訊、其他相關規劃資訊、單位訊息資料等，其所有權歸屬本會，非經本會書面同意，廠商不得提供給任意之第三方參考或加值運用。

項次	規範
4	廠商至本會提供服務時，應遵守本會個人資料保護與資訊安全相關規定。

七、智慧財產權歸屬

廠商交付本會之所有文件，其著作權及智慧財產權均屬本會所有，並放棄著作人格權。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，致使本會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會權益。

八、服務水準協定與罰則

評估項目	評斷方式	要求基準	處罰規則
專案人員資格與到場服務	廠商若未依顧問資格人力規範，於兩周內安排符合資格之對應人力到場提供服務	每次統計	每逾 1 個日曆天計罰當期價金總額 1‰
專案品質改善要求	廠商接受本會提出專案品質改善要求，應於 15 個日曆天內提出改善方式經本會同意後執行	每次統計	每逾 1 個日曆天無法改善品質計罰款新臺幣 1500 元
專案交付項目期限	除經本會及廠商同意，廠商應於期限內完成交付項目	每次統計	每逾 1 個日曆天無法交付文件及驗收計罰款新臺幣 1500 元
罰款上限與延遲交付	罰款超過契約價金總額 20%或各項應交未交付之項目超過該項應交付時程 30 天	每 30 天	解約

肆、 交付項目時程及驗收付款

一、交付項目與時程

廠商交付項目詳如下表，結束時交付執行成果工作摘要，經本會確認驗收後始完成交付，以做為辦理驗收付款之依據，但仍待本會內部上簽程序完成。各項交付文件得以電子檔方式交付。額外提供光碟或 USB 隨身碟。(一式兩份)

項次	工作項目	交付時程	交付項目
1	合約簽訂	決標日起 4 周內	合約
2	專案規劃	決標日起 4 周內	專案工作計劃書/啟始會議記錄
3	現況與差異分析	決標日起 4 周內	資安現況分析報告
4	資訊安全範圍/政策/目標	決標日起 8 周內	資訊安全政策/組織全景分析/資訊安全制度範圍
5	資產盤點	決標日起 24 周內	資訊資產管理程序/資訊資產清冊
6	風險評鑑	決標日起 24 周內	資訊安全風險管理程序/資安風險評鑑報告
7	ISMS 文件編修與發行	決標日起 36 周內	ISMS(1~4 階)文件/發行
8	營運持續計畫與演練	決標日起 48 周內	營運持續演練計畫與演練紀錄
9	內部稽核	決標日起 60 周內	內部稽核計畫與稽核報告/矯正措施
10	管理階層審查會議	決標日起 60 周內	管理階層審查會議簡報/會議記錄
11	驗證前文件記錄審視	決標日起 64 周內	ISMS 文件一覽表
12	協助第三方驗證	決標日起 64 周內	第三方稽核報告
13	第三方驗證後矯正措施	決標日起 64 周內	矯正措施(若有缺失)/第三方推薦證明書

項次	工作項目	交付時程	交付項目
14	專案結束	2021/11/30 前	輔導總報告書
15		2021/11/30 前	ISO 27001LA 證書 4 張

二、驗收付款說明

（一）驗收審查

本專案驗收審查期間不計入履約期限，廠商於履約期限內完成所有工作並交付相關文件後，由本會安排辦理驗收工作，廠商應派員配合本會驗收。

（二）罰款處理

完成驗收合格且無待解決事項後付款，廠商如有應計罰之款項，本會得於付款時逕行扣除之。

（三）因故致損

廠商於本專案進行中因故致使本會蒙受損失或有設備系統安全受損害，無法正常運作時，概由廠商負責賠償，而本會得自應付價金中扣抵。

（四）提前驗收

廠商如提前完成本專案作業，得函文本會申請提前驗收，並經本會審核同意後提前辦理本專案驗收及付款作業。

（五）請領契約價金

本會於完成驗收紀錄書面審查合格後以電話(或傳真)通知廠商，廠商應於接獲通知後即開立統一發票請領契約價金。

伍、 建議書製作規定

一、服務建議書格式

（一）紙張：A4 規格，字體以標楷體、字型大小除各章節標題以 16 點書寫，餘以 14 點為原則。

（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、本專案名稱及日期，裝訂線在左側。

（三）目錄：應標示各章節之出處頁碼。

（四）廠商投標建議書之份數為一式三份及文件電子檔一份(PDF)。

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. 簡要敘述廠商概況，包含人力規模、組織編制，公司能力說明(專業技術)、最近營運狀況。
2. 列舉廠商之專業實績及類似專案之服務經驗，並檢附佐證與驗證之文件。

（三）專案計畫

1. 本專案服務內容項目
2. 本專案服務團隊的組織架構與工作職掌及人員學經歷專長(含專業技術服務人員)
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. 總經費估算彙總表(估算說明)

（四）優規加值服務說明廠商對本專案之建議與補充說明

（五）附錄：商業登記證、在職證明與要求資格證照等佐證影本。

陸、 建議書評選事宜

一、評選辦法

（一）透過書面審查，需同時符合建議書製作規定、符合本會需求與標價合理，即為合格廠商，再進行議價。

（二）若所有廠商均不合格時，重新辦理本專案。

二、其他評選注意事項

本會得因故終止評選事宜，通知投標廠商領回建議書。本文件未盡事宜，依據「政府採購法」相關規定辦理。