

**109 年度警政資訊安全管理系統  
認證作業輔導委外服務  
規範書**

中華民國 109 年 2 月

## 目 錄

<b>壹、 專案概述</b> .....	<b>2</b>
一、 專案名稱 .....	2
二、 專案目標 .....	2
三、 專案執行期間 .....	2
<b>貳、 需求說明</b> .....	<b>3</b>
<b>參、 專案管理及監控</b> .....	<b>8</b>
一、 專案管理 .....	8
1. 專案期程.....	8
2. 專案組織與人力 .....	8
3. 專案人員管理 .....	8
4. 聯絡窗口服務諮詢方式 .....	8
二、 監控與查核 .....	9
1. 月工作報告.....	9
2. 協調會議.....	9
<b>肆、 廠商資格與專案組織人力</b> .....	<b>10</b>
<b>伍、 應交付項目時程與查核點</b> .....	<b>11</b>
<b>陸、 其他</b> .....	<b>12</b>

## 壹、專案概述

### 一、專案名稱

109 年度警政資訊安全管理系統認證作業輔導委外服務案(以下簡稱本專案)。

### 二、專案目標

提供警政署資訊安全管理系統(ISMS)認證作業輔導及資安顧問服務相關工作。

### 三、專案執行期間:

自簽約日起至 109 年 12 月 25 日止。

## 貳、需求說明

### 一、工作內容

#### (一) 警政資訊安全管理系統認證作業輔導

##### 1. 資訊安全管理系統(ISMS)認證作業輔導及資安顧問服務相關工作範圍如下：

###### (1)因應法令法規變更或組改調整管理制度

依據警政署主管機關(行政院)要求及資通安全管理法相關法規所訂定之規範與作業程序，修正警政署資訊安全管理制度文件。例如：協助警政署依照資通安全管理法等相關法規，進行資安管理制度調整，並協助產製與修訂「資通安全維護計畫」、「資通安全事件通報及應變管理程序」、「資通安全維護計畫實施情形」，以符合法規要求。

###### (2)資通系統分級及防護基準

依據資通安全管理法及其子法「資通安全責任等級分級辦法」規定，協助重新盤點資訊系統，並重新更新、檢視及調整資訊系統安全分析結果，包含資訊類別、影響構面、業務屬性、安全等級等內容，並考量資訊系統業務屬性、安全等級之關聯性，檢視安全等級之合理性，並協助完成資通系統防護基準檢核表。提供警政署資訊系統執行安全等級評估、識別實作及防護基準控制措施執行之諮詢服務。

###### (3)資訊安全管理系統維護

依據 ISO27001 標準之要求、警政署組織全景、風險評鑑結果及資通安全管理法規定，就警政署資訊業務流程及環境等異動，審查及增修警政署資訊安全管理程序、作業規範、標準作業流程及相關表單，提供警政署 ISMS 修訂建議，使警政署 ISMS 更為健全及符合實務之需求。

###### (4)風險評鑑管理

A. 協助警政署進行組織全景分析及業務衝擊分析。

B. 資訊盤點服務

協助警政署進行資訊資產盤點作業，維護資訊資產盤點

程序與方法，重新確認資訊資產分類法則、資訊資產盤點及資訊資產評價，維護警政署資訊資產清冊。

C. 風險評鑑管控作業服務

協助警政署進行年度風險評鑑作業，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，協助檢視風險評鑑方法、風險評鑑相關表單及紀錄，並提供建議及說明。

(5)風險評鑑報告、風險處理計畫書確認

協助警政署核心資訊系統依據風險評鑑管控作業，產製風險評鑑報告，再依據評鑑結果建議風險管理機制(如降低、移轉、避免或接受)，選取適當的安控目標與控制點，以建立風險處理計畫，協助檢視風險再評鑑作業，提供相關建議，並於每次第三方稽核前須完成上述所有相關工作。

(6)營運持續演練

協助驗證範圍內各資訊系統，擬定營運持續管理計畫，提供營運持續演練規劃與實作諮詢服務。並就營運持續演練結果，提供改善建議方案。

(7)資安治理成熟度評估

依主管機關(行政院)規劃資安治理架構運作模式，針對警政署進行資安治理成熟度分析，並依據成熟度等級，提供建議改善與提升成熟度方案及協助警政署完成自我評估與文件製作。

2. 規劃及執行 ISMS 內部稽核作業

(1)依據警政署及「資訊安全管理制度(ISMS)」之作業規定，指派輔導顧問至警政署執行內部稽核作業，藉以評估警政署及「資訊安全管理制度(ISMS)」是否有效落實。

(2)稽核前應協助警政署製作「內部稽核計畫」以及與內部稽核相關之表單紀錄，提升稽核作業之績效及有效性。

(3)協助規劃及執行內部稽核作業，並組成至少 2 人以上之輔導稽核團隊，協同警政署內部稽核人員，進行內部稽核工

作，並於完成稽核工作後 5 個工作日內，協助提供稽核報告(含改善措施與建議)。

### 3. 修訂績效衡量指標(KPI)

協助檢視及視需要修訂既有之資訊安全管理目標，並檢討及分析各項管理目標之達成情況，針對未達成之目標提出修正建議，確保警政署「資訊安全管理制度(ISMS)」之品質及運作效率能持續不斷地提升。

### 4. 協助召開管理審查會議

依據警政署「資通安全維護計畫」及「資訊安全管理制度(ISMS)」之規劃期程，參與各項資通安全相關之管理審查會議，並於會議時列席備詢，工作包括但不限於：擬定會議議題、準備會議報告文件、維護有效性量測表、擬定會議紀錄及追蹤改善建議等。

### 5. ISMS 複評

(1)為持續維持驗證的有效性，應協助依照警政署已通過驗證之第三方稽核驗證公司規劃與實施 ISMS 第三方稽核複評作業及負擔所需費用，並就第三方稽核複評所需，協助警政署備妥相關稽核複評佐證文件與紀錄，以警政署提報核定之核心系統為 ISMS 驗證範圍，若有異動以警政署最新核定為依據，承商應配合辦理。

(2)執行標準驗證之複評作業時，應提供符合標準規範所需之人天數以及稽核員餐點，派員陪同實地審查。

(3)提供驗證之稽核複評報告，且若有稽核發現之不符合項目時，應提供追蹤報告文件，並協助進行相關改善作業。

### 6. 辦理警政署署屬機關(構)及委外廠商稽核作業

(1)協助警政署至署屬機關(構)進行資通安全維護計畫實施情形之稽核作業，專案執行期間至少稽核 3 個署屬機關(構)，於稽核作業前擬定稽核計畫，稽核後產生稽核結果及報告，並就稽核結果進行評估及提出改善建議，稽核對象由警政署指定。

(2)協助辦理委外廠商資訊安全稽核作業，專案執行期間至少稽核 1 家委外廠商，於稽核作業後產生稽核結果及報告，並就稽核結果進行評估及提出改善建議，稽核對象依警政署實際需求指定。

7. 陪同警政署接受外部機關稽核與諮詢服務

出席警政署合約期間內資通安全外部機關稽核，提供稽核內容諮詢及稽核結果之矯正改善建議與改善報告書。

8. 提供定期及不定期資通安全管理系統之諮詢服務

包含內部資通安全管理系統及個人資料保護管理制度維護諮詢、外部單位資通安全作業稽核諮詢、資通安全事件諮詢等，摘要說明如下：

(1)發生資訊安全事件提供諮詢服務。

(2)行政院國家資通安全會報交辦事項諮詢。

(3)資通安全責任等級 A 級之公務機關應辦事項諮詢。

(4)其他應協助辦理之資訊安全作業諮詢。

9. 撰寫及提交 ISMS 輔導成果報告

提供 ISMS 資安認證相關成果報告，包括風險評鑑成果、內部稽核及第三方驗證審查成果、相關教育訓練與顧問諮詢服務成果等，作為後續改善之參考。

10. 資通安全維護計畫實施情形報告之提出依照警政署資通安全維護計畫實施情形，協助撰寫及提供年度資通安全維護計畫實施報告，以符合資通安全管理法第 12 條規定。

11. 辦理資通安全教育訓練

(1) 為符合資通安全責任等級應辦事項，承商應依警政署需求，提供下列資訊安全訓練課程、資安專業證照及職能訓練課程，課程名稱、時數與梯次可依警政署實際需求進行調整與修正。

類別	No	課程名稱	梯次/ 人次	上課 地點
稽核 領域	1	資通安全專業課程訓練或資通安全 職能訓練(12 小時)	1 梯	警政署
資安 專業 證照 及職 能	1	ISO 27001：2013 資訊安全管理系統 主導稽核員訓練課程	1 人	訓練機構
	2	ISO/IEC 27701:2019 或 BS10012 個 人資訊管理系統-主導稽核員訓練課 程	1 人	訓練機構
	3	資通安全職能評量訓練課程	4 人	訓練機構

- (2) 完成資通安全訓練課程後應交付教育訓練課程講義及上課人員簽到紀錄，課後須進行評量測驗，以量測學習成效確保訓後能有效提升資訊安全防護能力。
- (3) 於辦理教育訓練前，須提出「教育訓練計畫書」，且經警政署核可後。
- (4) 計畫內容應包含課程名稱、課程大綱、上課時數、預定上課時間、講師姓名及背景資歷等，送交審核認可。依照教育訓練計畫提供師資及教材，並準備訓練事宜。
- (5) 講師鐘點費及其交通費與教材製作費、學員午餐費等皆包含在本專案中，警政署與本院無需支付任何額外費用，另上課時間由警政署決定，承商需配合辦理之。
- (6) 承商應充份了解通過資訊安全管理標準應執行之工作事項，並適時進行輔導及協助，不得以本規格書文件未明列為工作事項，而做為卸責之理由。
- (7) 其他臨時工作或需求，得依雙方同意後彈性調整之。

二、其他臨時工作或需求，得依雙方同意後彈性調整之。

## 參、專案管理及監控

### 一、專案管理

承商須提出「專案管理計畫書」，詳細說明本專案於簽約日至契約結束期間之專案工作項目、專案管理方式及其內容。專案管理計畫至少包含：

1. 專案期程：承商應詳述本專案預定執行項目及進度。
2. 專案組織與人力：專案組織與人力需求說明。
3. 專案人員管理
  - (1) 計畫主持人或專案經理於專案執行期間應按專案進度向警政署與本院業務相關人員提報本專案執行進度、遭遇之問題、解決事項之優先順序或建議，並須接受警政署與本院督導。
  - (2) 專案執行期間，專案成員請假須具備代理人機制，專案成員須配合警政署與本院需求加班，且專案成員更換須經警政署與本院書面同意，若未經警政署與本院同意即更換則依合約計罰規定辦理。
  - (3) 專案執行期間，若有不適任者，經警政署與本院通知承商，承商須儘快調派適當人員接替服務，交接部分須並行工作兩週始可接替。
  - (4) 計畫執行期間，必要時需配合本專案需求至各地出差，專案人員（除警政署與本院人員外）相關住宿、交通費用由本專案承商自行支付。
4. 聯絡窗口服務諮詢方式

為確保專案服務品質，需提供負責聯絡窗口與電話，其標準諮詢服務處理流程如下：

#### A. 電話詢問：

##### a、上班時間：

週一至週五，平日上午 8 時至下午 5 時應有專人接聽電話，並受理諮詢。收到詢問時，如無法即時解答，應說明何時可以回復；惟最後回復期間最長不得超過 3 天。

b、非上班時間：

應有語音錄音受理服務，並於上班時間回復。於上班後當天中午 12 時前完成。如無法即時解答，應說明何時可以回復；惟最後回復期間最長不得超過 3 天。

B. e-mail 詢問：

收到詢問 2 小時內完成。如無法即時解答，應說明何時可以回復；惟最後回復期間最長不得超過 3 天。

## 二、 監控與查核

為求專案進行過程的透明化與可追蹤性，並提升專案結果的品質，承商應確實滿足以下需求：

### 1. 月工作報告

承商應於簽約後，每月 1 日前提交上月之月工作報告予本院。月工作報告內容應包含該月工作進度、執行報告、異常狀況及因應對策、下月預定工作項目及專案所有蒐集資料(包括訪談資料、會議紀錄及其他有關專案工作所產出之文件、圖表或增補資料)，並依本院需要進行口頭報告。

### 2. 協調會議

本專案進行期間，本院與承商得視需要不定期召開會議，以檢驗專案執行狀況，明定未確定之作業規範，解決發生之問題，討論雙方應配合及協調事項。

## 肆、廠商資格與專案人力

為確保本專案不中斷與服務品質，承商需具備以下資格：

- 一、專案成員至少3人，需為投標廠商之正職員工，投標時須檢附勞保及在職證明書，且應具備以下證照。
  1. 具有 PMP 國際專案管理師證照。
  2. 具有 CISA 國際電腦稽核師認證。
  3. 具有 ISO27001 LA 與 BS10012 LA 國際資安認證考試合格證書
  4. ECSA Certified Security Analyst Course 資安分析專家認證或 CEH(Certificated Ethical Hacker)之國際駭客技術專家認證或 ECSA 資安分析專家認證。
- 二、專案經理需具備至少8年以上參與政府警政機關或民間企業管理制度導入的經驗。同時具備 ISMS 建置經驗者尤佳；專案經理以外之成員需具備3年內參與政府機關或民間企業 ISMS 專案建置並輔導通過認證之經驗。

## 伍、應交付項目時程與查核點

本專案所需交付項目、履約期限與監控查核交付日期，分別詳列如下：

項次	交付項目	履約期限	查核交付日期
一.	ISMS 輔導成果報告	109/12/25	109/12/05
二.	工作月報		每月 1 日前提交上月之月工作報告 (12月工作報告於109年12月25日前交付)

## 陸、其他

### 一、 驗收方式

承商完成本專案工作後，提交成果文件報請警政署與本院驗收，經警政署與本院以書面驗收審查符合契約規定後，始為驗收合格。

### 二、 付款方式

承商所交文件經警政署與本院審查核可後，檢齊相關資料送交本院核符後一次付清貨款。

### 三、 其他事項

1. 開標後契約之履行（工期之起算）自契約生效日起開始，承商不得要求因通貨膨脹等因素而增加成本之給付。而得標後，承商為履行本契約所做一切準備工作所生之成本均不得向本院要求給付。