**財團法人保險事業發展中心**

**強制汽車責任保險系統**

**資安攻防演練委外服務案**

**需求說明書**

**合約附件一**

ss

**中 華 民 國 114 年 10 月 30 日**

**目 錄**

壹、 專案概述 3

[貳、 專案作業項目 5](#_TOC_250003)

[參、 專案管理需求 8](#_TOC_250002)

[肆、 交付項目 12](#_TOC_250001)

[伍、 工作計畫書 14](#_TOC_250000)

**壹、專案概述**

## 一、專案名稱

「強制汽車責任保險系統資安攻防演練委外服務案」

(以下簡稱本案)

## 二、專案目標

為健全強制汽車責任保險(簡稱強制車險)之發展，並確保投保車主權益，財團法人保險事業發展中心(簡稱本中心)爰受主管機關之委託，成立強制車險資訊作業中心，透過網際網路提供保險相關資訊服務，俾利保險業遂行強制車險承保業務，並供警政機關及交通監理機關查驗投保狀況使用。

惟資訊作業中心運用網際網路提供各項資訊服務之時，必須考量資訊之安全性，保障與連線單位往來資訊之機密，防範網路遭受駭客之惡意入侵，尤其可能造成內部破壞或資料外洩，更是資訊作業中心資訊安全之重要課題。

爰此，本中心擬委外提供資訊安全攻防演練服務，針對資訊作業中心進行網站系統及應用程式之滲透評估，透過專業人員模擬駭客攻擊之手法搜尋資安漏洞，以分析潛藏的風險與危機，

並進行阻擋、記錄後，提供建議解決措施以進行修正，以期減

低資訊作業中心所遭遇資安風險，維持高資訊安全水準。

## 三、專案範圍

本案服務範圍計分二部分：

(一) 滲透測試服務執行標的，如下提供之 FQDN： 1、https://insfee.cali.org.tw

2、https://public.cali.org.tw 3、https://ws.cali.org.tw

(二) 社交工程演練服務標的：

依據每次服務執行前本中心所提供之郵件清單。

## 四、專案期間

本專案期間自 115 年 1 月 1 日起生效，至 116 年 12 月 31 日 廠商完成與本中心合約約定之履約標的。

# 貳、專案作業項目

本案之資訊安全攻防演練服務，期能達成之目標如次：

* 搜尋資訊作業中心潛在資訊安全漏洞，並加強防範機制。
* 提升本中心同仁對資訊安全之警覺性，以降低資訊外洩風險。

## 一、服務說明

### (一) 滲透測試

針對受測標的建立執行架構、規劃執行策略並進行資料蒐集，以發現潛在資安漏洞，建議參考國際資安檢測標準，並定期檢視是否有更新版本：

* OSSTMM (Open Source Security Testing Methodology Manual)

開源安全測試方法手冊

* OWASP Top 10 (Open Web Application Security Project)

網站暨其應用程式安全測試清單

* OWASP Testing Guide
* CWE/SANS Top 20 常見軟體安全弱點
* ISSAF (Information System Security Assessment Framework)

資訊系統安全評估框架

* PTES 滲透測試執行標準

### 測試內容

滲透測試服務內容包含下列類別：

* + 網路探勘(Network Surveying)
  + 鑑別系統服務(System Services Identification)
  + 檢測資訊洩露（Information Leak Digging）
  + 弱點研究與驗證（Vulnerability Research and Verification）
  + 檢測網路應用（Internet Application Testing & Routing）
  + 檢測存取權限（Access Control testing）
  + 權限提升與跳脫（Privilege Escalation and Abuse）
  + 可用度解析（Survivability Review）

### 測試方式

* + 每半年需至少執行 1 次遠端完整滲透測試檢測之服務。
  + 每個月需透過工具檢查是否有新型攻擊手法造成之漏洞。
  + 前述服務測試時間如無法依工作計畫時程進行作業，應與本中心協調執行時間。
  + 正式報告內容應提供檢測時間列表及檢測結果截圖作為佐證。
  + 檢測中發現漏洞風險應盡速通知本中心，並提供修補建議，且於本中心告知修補完成後，辦理漏洞修補確認之檢測作業，並提供佐證資料。

### 分析報告

針對測試期間狀況進行分析後，提供修正或補強建議，並視需要進行風險修正討論會議。另配合強制車險資訊作業中心舉辦之專案會議，於每年上下半年會議上各做 1 次簡報，會議確切時間依本中心排定之時間為準。

### 風險管理

在滲透測試執行期間，若需執行具侵入性質或高強度之檢測作業皆需與本中心進行確認，並於雙方議定之適當時間且具備適當應變措施與風險評估後，才進行相關檢定作業。

## (二) 社交工程演練

依據本中心所提供之電子郵件帳號進行社交工程電子郵件檢測，提醒受測同仁認識社交工程之執行方式以提高警覺性，並根據測試結果了解可能造成之內部資安漏洞，藉以實施內部資安觀念之補強。

### 測試內容

廠商須依據本中心每次演練前提供之電子郵件清單，進行測試服務，各帳號進行 10 封社交工程郵件測試，所使用的郵件得以匿名或非匿名、真實或假冒之寄件來源進行測試，內容可包含本文、附檔(office 文件檔、PDF 檔、壓縮檔等)、超連結資訊，並記錄

「開啟閱讀」、「點閱連結」及「開啟附件」等受測者統計比例。廠商應於每次演練前，與本中心研議郵件寄送方式(須含各類型不同內容之測試郵件範本)、郵件寄送排程設定，經本中心確認後據以執行。

### 測試方式

每年排定 2 次以電子郵件進行社交工程演練測試，測試時間須經本中心確認。

### 分析報告

每次演練結果之報告應包含各統計資料圖表，包含不同郵件類 型、分組、派送時間等，以及記錄「開啟郵件」、「點閱連結」及

「開啟附件」等受測者行為資料與統計比例結果。

### 風險管理

廠商應於每次演練前與本中心確認郵件範本類型，不可使用來源

不明且實際具攻擊性之範本。

# 參、專案管理需求

## 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：

(三) 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)。

(四) 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。

(五) 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，以保護滲透測試服務所取得之資料。

(六) 本案涉及資通訊軟體、硬體或服務等相關事務，不得提供及使用大陸廠牌資通訊產品。

(七) 應確保一切資料存取、備份、及備援之實體所在地，應為我國管轄權所及之境內。

(八) 本案團隊人力要求

* 1. 服務人員須年滿 18 歲以上，身體健康無法定傳染病，且具有中華民國國籍，不得為外籍勞工或大陸來台人士，於履約期間不得同時於大陸地區工作。
  2. 專案人員應包含專案負責人/專案經理與滲透測試作業人員。

其中，每位滲透測試作業人員至少應具備 1 張資訊安全專業證照，以確保服務水準，並於建議書中檢附成員姓名、員工證明 (如勞健保證明)、專業證照等影本以供審核。

每位滲透測試服務人員應具備專業要求，於下列選項擇 1 提供證明。

* + - CEH(EC-Council Certified Ethical Hacker)
    - CPENT(EC-Council Certified Penetration Tester)
    - CompTIA PenTest+
    - CPSA(The CREST Practitioner Security Analyst )
    - OSCP( Offensive Security Certified Professional)

## 二、服務水準協定(SLA)與罰則

### (一) 服務水準規範

本案各項服務水準協定（Service Level Agreement，SLA），以必須達成該項服務作業項目要求為依據，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** | 執行時程及報告交  付時間 | * 每次測試最長以兩週為限。 * 應於檢測完成後3週內提供正式檢測報告。 |
| **2** | 測試需求 | * 本案滲透測試服務須以維持系統軟硬體正常運作作為主要原則，不得造成系統效能低落甚或服務中斷 * 本案社交工程演練須確保測試郵件範本之來源且不具實質攻擊性 |

### (二) 相關說明

1. 承作廠商無法達成本案服務作業項目需求、服務水準(SLA)項目或準時依循文件交付時程，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)，本中心得按契約總價之 3 ‰ 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。

1. 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，本中心得以書面通知得標廠商終止契約或解除契約之部份或全部，且不補償得標廠商所生之損失。
2. 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，本中心有權扣除該項工作之款項。
3. 得標廠商指派之專案負責人及工作成員，未經本中心同意，不得任意更換，如有不得已之情事需於異動生效日前 1 週左右，未經本機關同意自行更換時，每次得依契約總價之 1 ‰ 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。交付本中心之文件經本中心審閱時，所發現錯漏處經本中心要求修訂仍未修訂者，本中心得按每字新台幣 5 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. 為確保本案如期如質完成，廠商應針對本案需求，審慎選擇專案人員，執行本案所需之各項作業，並指派專案經理負責督導工作項目，且於執行作業或交付文件時，先行檢視審核。
2. 於專案期間視情況召開專案管理及討論會議以掌控品質，會議討論內容與結果需作成紀錄與追蹤辦理，送本中心備考。

### (二) 驗收標準

得標廠商應依「貳、專案作業項目」之需求，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

本中心將於各階段工作項目完成並交付相關文件後，進行審查作業，得標廠商須依本中心審查意見修正交付項目，並重新交

付審核。

## 四、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，非經本中心書面同意，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，整理歸檔後退還本中心或經本中心同意後銷毀。

(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) 本中心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

契約生效日起 1 個月(日曆天)內交付，須經本中心審核確認。

### (二) 滲透測試服務報告

1. 自契約生效日起二年內完成本專案滲透測試服務，並依與本中心討論之時程，分別交付共 4 次「滲透測試評估服務報告書」。
2. 廠商應依時程之安排，於測試完成後 3 週內(日曆天)交付正式

報告結果，交付項目包含「滲透測試服務檢測報告書」紙本 2

份及光碟(包含測試內容電子檔及紙本報告電子檔)2 份 。

### (三) 社交工程演練報告

1. 自契約生效日起二年內完成本專案社交工程演練服務，並依與本中心討論之時程，分別交付共 4 次「社交工程演練服務報告書」。
2. 廠商應依時程之安排，於測試完成後 3 週內(日曆天) 交付正式報告結果，交付項目包含「社交工程演練服務報告書」紙本 2 份及光碟(包含測試內容電子檔及紙本報告電子檔)2 份。。

### (四) 整體資訊安全改善建議書

1. 廠商應交付予本中心基於本案服務之「整體資訊安全改善建議書」，內容建議如下：

(1)執行規範、作業方式與測試流程。 (2)測試執行項目、結果及改善方式。 (3)本專案之建議事項。

(4)對本專案之有關受測項目，提出未來可再強化之具體詳細建議內容與說明。

1. 廠商應於交付第 2 次及第 4 次正式報告時，一併交付「整體資訊安全改善建議書」紙本 2 份及光碟(建議書電子檔)2 份。

### (五) 教育訓練課程

為協助提升中心資安人員之資安管理、技術等觀念，以利因應日新月異之資安攻擊，廠商應提供每年 6 小時資訊安全相關教

育訓練課程，課程時數共 12 小時，課程內容需經本中心同意。

## 二、交付文件方式

(一) 本案所應交付之各項文件應於測試完畢後 3 週內提交正式文件(需於交付前先提供電子檔予本中心預審確認內容無誤)，交付項目包含紙本 2 份及光碟 2 份。

(二) 必要時本中心得要求廠商派員提供測試內容說明或修補建議。

(三) 本專案演練相關文件內容，本中心擁有永久使用權/修改權。

## 三、交付項目說明

|  |  |
| --- | --- |
| **交付項目** | **內容說明** |
| **工作計畫書** | * 內容除包括對本專案之執行敘述，含專案管理、組織、人力(含證照及經驗)、分工、職掌、工作項目、執行測試方式、時程說明、工作進度稽核點及品質管理流程。 |
| **滲透測試服務報告** | * 文件內容至少應包含：   1. 摘要說明   受測目標風險等級與數量列表/  受測目標風險漏洞名稱列表/風險漏洞分布列表、專案執行計畫 |

|  |  |
| --- | --- |
|  | (檢測期間/檢測項目/檢測範圍  /檢測工具及版本/風險定義/檢測專案成員資格)。   1. 滲透測試檢測   應說明測試項目執行過程並檢 附測試內容截圖作為佐證，若檢測出弱點，應詳細說明弱點內容及可能造成的風險 (包括檢測目標/弱點名稱/問題URL或IP/問題參數/測試語法/測試截  圖)。   1. 改善與建議   著重於弱點修補建議，以利中心快速掌握弱點成因與影響範圍，並參考改善方式進行修復。   1. 結論 |
| **社交工程演練報告** | * 文件內容至少應包括：   執行結果摘要說明、專案執行計畫(執行期間/執行項目/執行範圍/執行專案成員資格)、執行情形(整體結果統計圖表、不同郵件類型測試的排序統計圖表、郵件派送時間表、統計開啟郵件/點閱連結/開啟附件等受測者行為與細部時間紀錄)、改善與建議、結論。 |

# 伍、工作計畫書

## 一、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) 工作計畫書應提供電子檔及紙本各1份。

## 二、內容

(四) 專案概述

1. 專案名稱
2. 專案範圍及目標
3. 專案時程

(五) 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

(六) 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、文件交付預定時程及查核點)

1. 本案帶來之預期效益
2. 本案SLA 之承諾
3. 資訊安全及資料保密

(七) 其它補充說明

1. 本中心之業務單位與資訊單位應配合事項