中華民國人壽保險商業同業公會

保險科技運用共享平台資訊系統弱點掃描、滲透測試及資安健診委外服務案

採購規格書

中　華　民　國　一　百　十　四　年　二　月　七　日

目　　錄

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、　專案期程 1
貳、　專案需求 2
　一、　弱點檢測服務 2
　二、　滲透測試 4
　三、　資安健診服務 6
參、　管理需求 8
　一、　廠商資格 8
　二、　服務水準協定(SLA)與罰則 9
　三、　品質需求與驗收標準 10
　四、　業務保密安全責任 11
肆、　交付項目 12
　一、　交付項目與時程 12
　二、　交付文件格式 12
　三、　交付項目說明 12
伍、　服務建議書製作規定 15
　一、　服務建議書格式 15
　二、　服務建議書大綱 15
　陸、服務建議書評選及權重 ..... **錯誤! 尚未定義書籤。**
柒、　附件 16

壹、 專案概述

一、 專案名稱

中華民國人壽保險商業同業公會 (以下簡稱本會)「保險科技運用共享平台資訊系統弱點掃描、滲透測試及資安健診服務案」以下簡稱本案

二、 專案目標

(一)以弱點掃描服務檢測受測目標之資安防護能力與發現潛在作業系統弱點，並依據檢測結果提出改善建議，協助受測目標提升系統安全防護成效。

(二)期透過本案整合各項資訊安全項目的檢視服務，提供資安改善建議，以提升本會網路與資訊系統安全防護能力。

三、 專案範圍

本案的服務範圍設備清單詳見附件。

四、 專案期程

自簽約日起 一年 止。

貳、 專案需求

一、 弱點檢測服務

得標廠商需每年提供 **2 次(每次均含初測、複測)**弱點掃描服務，針對本會 **IP 及 URL** 進行安全弱點掃描，評估掃描標的物是否存在安全弱點，同時提供相關掃描結果，作為主機資訊安全的管理依據，並協助弱點修補方法之參考建議，待修正弱點後提供複掃，以確認弱點已經排除。

(一) 掃描內容

弱點掃描分為系統弱點掃描及網站弱點掃描。

1. 系統弱點掃描

係針對作業系統的弱點、網路服務的弱點、作業系統或網路服務的設定及帳號密碼設定等進行弱點檢測，系統弱點掃描的檢測項目須符合 Common Vulnerabilities and Exposures (CVE)發布的弱點內容，至少包含以下項目：

(1). 作業系統未修正的弱點掃描

(2). 常用應用程式弱點掃描

(3). 網路服務程式掃描

(4). 木馬、後門程式掃描

(5). 帳號密碼破解測試

(6). 系統之不安全與錯誤設定檢測

(7). 網路通訊埠掃描

2. 網站弱點掃描

係針對本會對外主機網頁安全弱點進行掃描，檢測項目須符合最新版 OWASP TOP 10 ，以下為 2021 年 TOP 10 的項目參考：

(1). A01:2021-Broken Access Control

(2). A02:2021-Cryptographic Failures

(3). A03:2021-Injection

(4). A04:2021-Insecure Design

(5). A05:2021-Security Misconfiguration

(6). A06:2021-Vulnerable and Outdated Components

(7). A07:2021-Identification and Authentication Failures

(8). A08:2021-Software and Data Integrity Failures

(9). A09:2021-Security Logging and Monitoring Failures

(10). A10:2021-Server-Side Request Forgery

(二) 檢測次數

服務項目	次數
主機系統弱點檢測	2 次檢測(初測、複測)
Web 網頁弱點檢測	2 次檢測(初測、複測)

(三) 執行方式

1. 得標廠商應於需求訪談階段先分就本會之網路架構及本項服務之標的設備進行了解，如設備廠牌、系統版本等，以利後續進行弱點分析及修補建議。
2. 掃描工具為取得授權使用的商用軟體，於每次弱點掃描前，將工具之弱點資料庫更新至最新版本，並應提供佐證資料，以確保本項服務之完整正確。
3. 得標廠商應依排定之日期執行弱點掃描，於非公務時段或與本會協調取得適當時間進行掃描作業。
4. 得標廠商應於弱點初掃後協助本會進行弱點修補，針對應修補之弱點進行追蹤管理，包括彙整本會之弱點修補情形，維護未修補清單中之未修補或排除原因等。

(四) 其他

相關要求及說明驗收交付報告所列之要求。

二、 滲透測試

(一) 測試項目

表 1 測試項目

測試類別	測試項目	測試說明
	輸入驗證(1)	至少包含XSS 弱點測試、SQL Injection測試、LDAP Injection 測試、XML Injection 測試、SSIInjection測試、XPath Injection測試及Code Injection測試等項目
	輸入驗證(2)	至少包含XSS 弱點測試、SQL Injection 測試、OS Commanding 測試及偽造HTTP協定測試等項目
網站服務	Web Service	至少包含WSDL測試、XML架構測試、XML內容測試及XML參數傳遞測試等項目
	Ajax	至少包含Ajax弱點測試等項目，如輸入驗證缺失、權限控管及套件弱點等測試項目
密碼破解	密碼強度測試	至少包含WEB、FTP、SSH、TELNET、SMTP、POP3、IMAP、SNMP、NetBIOS、RDP、VNC及Database 等常見對外服務之密碼字典檔測試。

(二) 執行方式

1. 得標廠商應組成滲透測試小組，模擬駭客利用各伺服器／主機作業系統、應用軟體、網路服務，以及防火牆、路由器、交換器等網路設備之安全弱點（例如網站設計不當，或防火牆、路由器等安全政策設定錯誤）進行滲透測試，設法取得未經授權之存取權限，並測試內部資訊是否有遭受不當揭露、竄改或竊取之可能。

2. 得標廠商應分別針對本會網際網路滲透測試。網際網路滲透測試係滲透測試小組直接由遠端進行。

3. 得標廠商應依排定之日期執行滲透測試，於非公務時段或與本會協調取得適當時間進行測試作業。

4. 得標廠商應彙整分析測試結果，提出測試報告，並視需求安排測試結果簡報。

5. 得標廠商於檢測後，對於所提建議，應協助本會進行改善，並針對應修補之弱點進行追蹤管理。

(三) 其他

相關要求及說明詳驗收交付報告所列之要求。

三、 資安健診服務

資安健診服務內容應涵蓋以下所列的所有服務項目,廠商應具備完成各項服務所需之軟、硬體設備，專案執行期間需提供上班日 5x8 小時之專案諮詢服務，並配合本會辦理說明會議。

(一) 網路架構檢視

針對本會網路架構圖進行安全性弱點檢視,檢視之項目包含設計邏輯是否合宜、主機網路位置是否適當及現有防護程度是否足夠。

(二) 有線網路惡意活動檢視

1. 封包監聽與分析

(1). 在本會有線網路(內網、外網、DMZ 區或側錄點)適當位置架設側錄設備，觀察內部電腦或設備是否有對外之異常連線或 DNS 查詢，並比對是否連線已知惡意 IP、中繼站(Command and Control，C&C)或有符合惡意網路行為的特徵

(2). 發現異常連線之電腦或設備應確認使用狀況與用途。

(3). 封包側錄至少以 6 小時為原則,以觀察是否有異常連線。

2. 資安設備紀錄檔分析

(1). 檢視網路與資安設備 (如：防火牆、入侵偵測/防護系統等)紀錄檔，分析過濾內部電腦或設備是否有對外之異常連線紀錄。

(2). 發現異常連線之電腦或設備應確認使用狀況與用途。

(3). 資安設備紀錄檔分析以 1 個月或 100M byte 內的紀錄為原則。

(三) 伺服器主機檢視

1. 伺服器主機惡意程式或檔案檢視

針對伺服器主機進行是否存在惡意程式或檔案檢視，檢視項目包含活動中與潛藏惡意程式、駭客工具程式及異常帳號與

群組。

2. 伺服器主機更新檢視

針對伺服器主機進行作業系統與伺服器主機安裝之 Microsoft 各項應用程式安全性更新作業系統、Office 應用程式、Adobe Acrobat、Adobe flash player 及 Java 應用程式更新檢視(包含檢視伺服器是否使用已經停止支援之作業系統或軟體(如 Windows XP、Windows Server2003 或 Office 2003))

針對伺服器主機防毒軟體安裝、更新及定期全系統掃描狀況進行檢視。

(四) 安全設定檢視

1. 目錄伺服器(如 MS AD) 組態設定檢視

檢視目錄伺服器中，針對 AD 伺服器組態設定，依行政院國家資通安全會報技術服務中心，官方網站「政府組態基準」專區所公布安全性檢視之內容為主，以確認本會對於組態設定之落實情形。參考網址為 http://www.nccst.nat.gov.tw/GCB。

若無 AD 伺服器，可以其他目錄伺服器(如 LDAP)或以個別使用者端電腦檢視方式完成「密碼設定原則」與「帳號鎖定原則」安全設定檢視。

2. 防火牆連線設定

檢視防火牆的連線設定規則(如外網對內網、內網對外網、內網對內網)是否有安全性弱點，確認來源與目的 IP 與通訊埠連通的適當性(包含設置「Permit All/Any」與「Deny All/Any」等 2 項防火牆檢測規則確認)。

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)，其資本額需於新臺幣3百萬(含)以上。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，如通過 ISO 27001:2013 以上版本、ISO 20000、ISO 22301…等，上述認證至少壹張；或其他類似驗證，並於專案執行期間持續有效，以保護本案服務所取得之資料。

（四） 本案團隊人力至少應包含：專案負責人、專案經理、與其他檢測服務人員，並應具備以下所列舉之技能，且各類技能至少有一名成員，以確保服務水準，並於建議書中檢附成員姓名、訓練證書或專業證照等影本以供審核。應具備必要資訊網路、系統技能說明如下：

1. 專案人員應包含專案負責人/專案經理與執行檢測服務人員。每位執行檢測服務人員應具備以下專業要求，擇 1 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。每位執行檢測服務人員應具備專業要求，擇 1 證照。
   - 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)。
   - 其他資安相關專業證照。
2. 具備網管能力，具有 CCNA(Cisco Certified Network

Associate)、或其他類似網路管理相關課程訓練。

3. 具備惡意程式檢視能力，具有 CEH(Certified Ethical Hacker)、或 ECSA(EC-Council Certified Security Analyst)或其他類似相關課程訓練。
4. 具備封包分析能力，具有 NSPA(Network Security Packet Analysis)或其他類似相關課程訓練。
5. 具備 AD(Active Directory)管理能力，具有 MCSE(Microsoft Certified Solutions Expert)、或 MCITP(Microsoft Certified IT Professional)或其他類似相關課程訓練。
6. 具備整體資訊安全技術或管理知識 CISSP(Certified Information Systems Security Professional)或 ISO/CNS 27001 Lead Auditor 或其他類似相關課程訓練。

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：

表 2 服務水準

項次	項目	服務水準
1	執行時程	初掃：每次以2週為限 複掃：每次以2週為限 檢測報告：初掃及複掃結束後2週內提供
2	設備服務中斷時間	因執行弱點掃描服務造成軟硬體設備服務中斷時，應協助本會恢復正常運作，服務中斷時間不得超過8小時。

（二） 相關說明

1. 承作廠商無法達成相關工作項目要求或交付文件，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)，本會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，本會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，本會有權扣除該項工作之款項。

4. 得標廠商指派之專案負責人及工作成員，未經本會同意，不得更換，如有未經本會同意自行更換時，每更換乙次得依契約總價之千分之一計算懲罰性違約金。

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，本會得以稽核。

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並追蹤辦理，送本會備查。

（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

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

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，非經本會書面同意，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，整理歸檔後退還本會或經本會同意後銷毀。

（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） 本會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。

（七） 本案服務執行過程中，有涉及本會 ISMS 評定系統安全等級作業或公務機關查核時，需協助有關資訊業務委外受託者自我評核及查核項目表等表單及相關服務。

肆、 交付項目

一、 交付項目與時程

（一） 弱點掃描工作計畫書：決標日起 3 週(日曆天)內交付。

（二） 弱點掃描初掃中文報告：依工作計畫書載明之交付時程。

（三） 弱點掃描複掃中文報告：依工作計畫書載明之交付時程。

（四） 滲透測試工作計劃書：決標日起 3 週(日曆天)內交付。

（五） 滲透測試初測中文報告：依工作計畫書載明之交付時程。

（六） 滲透測試複測中文報告：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（以光碟或本會同意之儲存媒體及提交方式）。

（二） 必要時本會得要求派員親臨說明。

三、 交付項目說明

表 3 交付說明

交付項目	內容說明
1. 弱點掃描工作計畫書	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(須含專業認證證明)、分工、職掌、工具(須含授權及使用最新版號、標準)、工作項目、執行掃描方式、時程(須含初掃、弱點修補、複掃、報告提交等)、工作進度稽核點及品質管理流程

2. 弱點掃描初掃中文報告	文件內容應包括：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/ 專案成員)、掃描工具說明（須含最新版號、標準)、掃描方式、弱點統計(依風險等級、弱點類別排序)、弱點清單(弱點名稱、弱點描述、設備名稱、IP/URL、Portname、風險等級、修補建議)、掃描誤判之弱點清單(說明誤判理由)、弱點排除清單(說明排除理由，如無法修補須說明原因與配套措施)。
3. 弱點掃描複掃中文報告	文件內容應包括：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/ 專案成員)、掃描工具說明（須含最新版號、標準)、掃描方式、弱點統計(依風險等級、弱點類別排序)、弱點清單(弱點名稱、弱點描述、設備名稱、IP/URL、Portname、風險等級、修補建議)、掃描誤判之弱點清單(說明誤判理由)、弱點排除清單(說明排除理由，如無法修補須說明原因與配套措施)、與初掃之差異化報表(例如未修補弱點及新發現弱點等相關描述與統計)。
4. 滲透測試工作計畫書	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、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
5. 滲透測試初測中文報告	文件內容應包括：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(執行期間/執行項目/執行範圍/專案成員)、執行結果(受測目標/漏洞名稱/問題URL或IP/ 問題參數/測試語法/測試截圖等)、改善與建議、結論。

6. 滲透測試複測中文報告	文件內容應包括：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(執行期間/執行項目/執行範圍/專案成員)、執行結果(受測目標/漏洞名稱/問題URL或IP/ 問題參數/測試語法/測試截圖等)、改善與建議、結論。

伍、 服務建議書製作規定

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）廠商服務建議書交付:

交付日期、交付份數及方式，請依招標文件相關規定辦理。服務建議書不得逾期交付，否則視為資格不符；服務建議書交付後不得修改或增訂。

二、 服務建議書大綱

以下為本案服務建議書參考大綱，如需額外說明之內容，廠商可添增章節說明之。

(一) 專案概述

1. **專案名稱**
2. **專案目標**
3. **專案範圍**
4. **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) 專案工作規劃

(四) 專案組織與管理

1. **人力配置、資格及管理**
2. **專案時程規劃**
3. **專案管理規劃**
4. **交付文件項目**
5. **本案帶來之預期效益**

6. 本案 SLA 之承諾

(五) 價格分析

(六) 其他

陸、附件

弱點掃描及滲透測試服務範圍設備清單

辦理項目	服務內容	子項目	頻率	單位	數量
資通安全健診	網路架構檢視		一次	式	1
	網路惡意活動檢視	封包監聽與分析	一次	式	20
		網路設備紀錄檔分析	一次	式	20
	伺服器主機惡意活動檢視	惡意程式、木馬檢測與更新檢視	一次	台	302
	網通設備組態設定檢視		一次	式	20
	防火牆連線設定檢視		一次	台	20
安全性檢測（遠端或到場服務）	網站弱點掃描	含初、複測	二次	URL	28
	滲透測試	含初、複測	一次	URL	28
	主機系統弱點掃描	含初、複測	二次	IP	302