宏泰人壽115年電腦系統資訊安全評估作業項目規格-保險業電腦系統第一類、第二類、IoT設備與API(SBOM)檢測

※請參照目前最新「保險業辦理資訊安全防護自律規範」辦理，如修正日期民國113年07月18日。
(網址 https://law.lia-roc.org.tw/Law/Content?lsid=FL072726)
※提供服務企劃建議書(RFP)項目如下，項目、內容說明有不足之處或建議事項請逕行調整、修訂與補充。

※需求項目規格-115年電腦系統資訊安全評估作業之保險業電腦系統第一類、第二類、IoT設備與API(SBOM)檢測，應依目前最新「保險業辦理資訊安全防護自律規範」辦理資訊安全評估作業。
※需配合主管機關等稽核與檢查要求，在需求規格項目、數量不足之處，可調整數量。

項次	內容/說明	數量單位	服務人天	備註
一、	**資訊安全評估作業項目**	一式		電腦系統第一類、第二類、IoT設備與API等項。(單一系統發生重大資訊安全事件，應於三個月內重新完成資訊安全評估作業。) 1.伺服器第一類、第二類預估74台 2.重要網路(儲存)設備預估16台 3.終端設備抽測比例每次至少應占該系統全部設備之10%或100台以上。 4.IoT設備預估56台 5.資安設備預估7台 6.對外提供服務之應用程式介面(簡稱API)預估6台 *甲方對於預估數量不足之處，可調整數量
1	(一)資訊架構檢視 1.檢視網路架構之配置、資訊設備安全管理規則之妥適性等，以評估可能之風險，採取必要因應措施。 2.檢視單點故障最大衝擊與風險承擔能力。 3.檢視對於持續營運所採取相關措施之妥適性。 4.適時參考金融資安資訊分享與分析中心（F-ISAC）所發布之資安威脅情資及資安防護建議，並採取相關措施。 5.檢視伺服器應依電腦系統分類或系統功能或服務特性進行網段區隔。 6.檢視邊界防護設備(包含閘道器、路由器、防火牆、防護裝置等設備)與外部網路連接之網點，是否設立防火牆控管內外部網路資料傳輸及資源存取，並限制非必要之連線對象與服務。	一式		說明如下： 1. WAN Load Balance：A10 Thunder 840*1 2. 外網防火牆: PA820*2 (HA) 3. SPAM:中華數位SPAM SQR*2 4. IPS: Cisco Firepower2110*1 5. WAF：iMmperva x2010*1 6. Core SW:CISCO 4503*2 7. 內網路由器：Cisco 2800*2;Cisco 2960G_DMZ*1 8. 內網防火牆:FortiGate 301E *1、PA410*1、 PA220*2(分公司、公會、IDC) 9. 網段數量:約16至25個 10.網段功能:LAN/WAN/DMZ/UAT/PRD/DEV都有
2	(二)網路活動檢視 1.檢視網路設備、伺服器及物聯網設備之存取紀錄及帳號權限，識別異常紀錄與確認警示機制。 2.檢視資安設備（如：防火牆、入侵偵測或防禦、惡意軟體防護、網路釣魚偵測、網頁防護等）之監控紀錄，識別異常紀錄與確認警示機制。 3.檢視網路是否存在異常連線或異常網域名稱解析伺服器（Domain Name System Server ,DNS Server）查詢或監控進出之通訊流量，並比對是否為已知惡意IP、中繼站或有符合網路惡意行為的特徵。 4.檢視是否訂定偵測偽冒網站之處理措施。	一式		說明如下： 1.網路設備如Core SW:CISCO 4503*2(3F)、交換器： Cisco 2960X *2;C3560E(3F、4F)*2、內網路由器： Cisco 2800*2、Cisco 2960G_DMZ*1等。 2.第一類、第二類伺服器、IoT設備等 3.資安設備如外網防火牆PA-820*2 (HA)、IPS Cisco Firepower2110*1、WAF iMmperva x2010*1 、內網防火牆:FortiGate 301E *1、PA410*1、PA220*2、防毒Symantec主機 *1 4.網路活動檢視-網路、伺服器與資安設備紀錄分析 5.網路活動檢視-封包監聽與分析 6.網段選擇2個側錄位置：DMZ、Core Switch

3	(三)網路設備、伺服器、終端設備及物聯網設備等設備檢測 1.辦理網路設備、伺服器、終端設備及物聯網設備等設備的弱點掃描與修補作業。 2.檢測終端機及伺服器是否存在惡意程式。 3.檢測系統帳號登入密碼複雜度；檢視外部連接密碼（如檔案傳輸（File Transfer Protocol, FTP）連線、資料庫連線等）之儲存保護機制與存取控制。 4.辦理物聯網設備檢測作業時，依據「保險業使用物聯網設備作業準則」第四、五、六、七條之安全控管規範進行評估。	一式		說明如下： 1.每季弱掃檢測報告。 2.電腦系統第一類、第二類、IoT設備等：如網路設備、伺服器、終端設備及物聯網設備等設備檢測 (1)伺服器預估74台 (2)重要網路設備預估16台 (3)終端設備抽測比例每次至少應占該系統全部設備之10%或100台以上。 (4)IoT設備預估56台 (5)資安設備預估7台 3.待測目標IP或網段承包後提供
4	(四)可由外部Internet直接連線之網路設備、伺服器及物聯網等設備，應辦理下列事項： 1.進行滲透測試。 2.進行伺服器應用系統之程式原始碼掃描或黑箱測試。 3.檢視伺服器目錄及網頁之存取權限建立對外網站網頁防竄改機制。 4.檢視系統是否有異常的授權連線、CPU資源異常耗用及異常之資料庫存取行為等情況。	一式		說明如下： 1.每季滲透測試報告、原始碼掃描報告。 2.可由外部Internet直接連線之網路設備、伺服器及物聯網等設備(DMZ區)：如官網*1、網投*1、業通*1、建議書*2、無障礙網*1、DNS*1、通報*1、Trustgate *1、測試*2) 3.待測目標IP承包後提供
5	(五)客戶端應用程式檢測 保險業與客戶端之應用程式應採加密連線，並針對保險業交付給客戶之應用程式進行下列檢測： 1.提供https、SFTP者應進行弱點掃描。 2.程式原始碼掃描或滲透測試。 3.敏感性資料保護檢測（如記憶體、儲存媒體）。 4.金鑰保護檢測。 5.採最小權限原則，僅允許使用者依任務及業務功能所需完成指派之授權存取控管。	X		現無交付給客戶之應用程式
6	(六)安全設定檢視 1.檢視伺服器（如網域服務Active Directory）有關「密碼設定原則」與「帳號鎖定原則」設定。 2.檢視防火牆是否開啟具有安全性風險的通訊埠或非必要通訊埠，連線設定是否有安全性弱點。 3.檢視系統存取限制（如存取控制清單Access Control List）及特權帳號管理。 4.檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新設定及更新狀態。 5.檢視金鑰之儲存保護機制與存取控制等安全措施。 6.檢視從外部網路連回內部時需確認使用者身分。	一式		說明如AD主機、防火牆、電腦系統如第一類、第二類、終端設備、IOT等

7	(七)資訊系統可靠性與安全性侵害之對策 1.公司應就提升資訊系統可靠性研擬相關對策，其內容包括： (1)提升硬體設備之可靠性：包含預防硬體設備故障與備用硬體設備設置之對策。 (2)提升軟體系統之可靠性：包含提升軟體開發品質與提升軟體維護品質對策。 (3)提升營運可靠性之對策。 (4)故障之早期發現與早期復原對策。 (5)災變對策。 (6)備份之系統備份媒體，須擬定驗證計畫，並驗證備份媒體之可靠性及資訊之完整性。 2.公司應就資訊安全性侵害，研擬相關對策，其內容包括： (1)資料保護：包含防止洩漏、防止破壞篡改與相對應檢測之對策。 (2)防止非法使用：包含存取權限確認、應用範圍限制、防止非法偽造、限制外部網路存取及偵測與因應之對策。 (3)防止非法程式：包含防禦、偵測與復原對策。 3.檢視電腦系統是否符合「保險業辦理資訊安全防護自律規範」、「保險業經營電子商務自律規範」、「保險業辦理電子保單簽發作業自律規範」、「保險業經營行動服務自律規範」及主管機關相關函文之要求。 4.如有使用SWIFT系統者，需檢視電腦系統之SWIFT系統是否符合SWIFT公布之Customer Security Programme規範及公會相關函文之要求，若與本作業原則衝突，依SWIFT公布為主。	一式		無有使用SWIFT系統
二、	第一類、第二類電腦系統應依前項評估項目全部納入資訊安全評估作業以確保評估作業之有效性。	一式		電腦系統第一類、第二類、IoT、API檢測、報告等項
三、	DDoS演練 -提供演練計劃書 -DDoS演練報告書 -非上班日執行(如周六)	一式		演練至少含以下： -流量型(快功) -連線型(慢攻)
四、	社交工程演練 每年應至少一次針對使用電腦系統人員，於安全監控範圍內，寄發演練郵件，加強資通安全教育，以期防範惡意程式透過社交方式入侵。 - 提供演練計劃書 - 含上半年、下半年	一式		說明如下： 1.員工至少500人，每人5封。 2.依合格標準開啟率16%，點閱率6%辦理： 上半年1次(至多2次)，下半年1次(至多2次)演練，
五、	評估單位資格與責任 -依「保險業辦理資訊安全防護自律規範」之柒辦理	一式		同二、廠商資格(依「保險業辦理資訊安全防護自律規範」之柒、二辦理)
六、	1.資安人員15小時(法令規定) 以上資訊安全專業課程訓練或職能訓練。-需提供上課證 2.資訊人員6小時以上資訊安全專業課程訓練或職能訓練-需簽到+課後評量(10題是非或選擇題)	一式		1.資安人員至少3員 2.如包班：資安人員(6小時+9小時=15小時)與資訊人員合計約25人(簽到+課後評量10題是非或選擇題)

七、	防火牆規則檔分析顧問服務(含軟體授權)-使用AlgoSec Firewall Analyzer (AFA)政策分析工具識別並排列規則中的風險，減少網路違規 一.規則完整性檢視 (Rule Review & Health Check) 找出那些「寫得不好」或「有安全隱患」的規則： 1.Any-to-Any 規則檢測:揪出過於寬鬆、讓任何人都能存取敏感服務的危險設定。 2.隱藏規則分析 3.過時規則清理 二.網路架構與邏輯驗證 從高處審視規則是否符合企業的資訊安全政策 (Security Policy)： 1.分段驗證 (Segmentation Check)： 確保 DMZ、內部網路與資料庫區 (DB Zone) 之間的隔離確實執行。 2.合規性對應： 檢核規則是否符合國際標準 (如 ISO 27001, PCI-DSS 或 NIST) 或國內法規要求。 3. 風險評估與弱點分析 1.服務風險評估：對開放的 Port (如Telnet 23) 評估其必要性，建議更安全的加密協議。 2.攻擊路徑模擬： 分析黑客是否能透過現有的規則漏洞進行橫向移動 (Lateral Movement)。 三.效能優化建議 (Performance Tuning) 防火牆的處理效能與規則的「順序」： 1.順序調整： 根據流量頻率，建議將最常使用的規則向上移動，以降低 CPU 負載。 2.規則整合： 將多個零散的物件 (Objects) 整合成群組，簡化設備處理邏輯。	一式		
八、	提供服務之應用程式介面(Application Programming Interface；以下簡稱 API)檢測-依公會檢送主管機關來文要求(112-08-29)有關注意強化應用程式介面API(SBOM)之安全控管與設計(不足之處請逕行補充說明)	一式		每季檢測報告。
九、	評估報告(電腦系統資訊安全評估作業) 依「保險業辦理資訊安全防護自律規範」之規辦理，如「電腦系統資訊安全評估報告」內容應至少包含評估人員資格、評估範圍、評估作業項目與標的、評估紀錄、評估時所發現之缺失項目、缺失嚴重程度、缺失類別、風險說明、具體改善建議、社交演練及資訊安全合規遵循等。	一式		電腦系統資訊安全評估作業報告(年)至少含以下附件： 伺服器暨重要網路設備弱點掃描報告、IoT設備弱點掃描報告、終端設備(PC)弱點掃描報告 、資安設備弱點掃描報告、終端機(PC)檢測結果匯整表、伺服器檢測結果匯整表、滲透測試檢測報告書、原始碼掃描報告書、上半年電子郵件警覺性檢測報告、下半年電子郵件警覺性檢測報告、網站遭受阻斷式(DDoS)服務攻擊演練報告、應用程式介面API軟體元件清單(SBOM)檢測報告、電腦病毒擴散及網路駭客入侵及資訊安全合規遵循情形之整體
十、	資訊安全評估服務報告簡報與顧問服務 -啟動、結案會議簡報 -項目每季檢測顧問服務	一式		資訊安全評估作業顧問服務
十一、	其他： 1.項目、內容說明有不足之處或建議事項請逕行調整、修訂與補充。 2.如有未盡事宜，悉依相關法令函釋、自律規範相關規定辦理。	一式		需協助補充辦理未盡事宜項目
備註	付款方式：簽約60%，結案驗收40%。			
二、	廠商資格(依「保險業辦理資訊安全防護自律規範」之柒、二辦理)			

1	辦理第一類電腦系統資訊安全評估作業之評估單位應具備下列各款資格條件；辦理第二類及第三類電腦系統資訊安全評估作業者，依評估作業項目需要，具備下列相關資格條件之一： (一) 具備資訊安全管理知識，如持有國際資訊安全經理人(Certified Information Security Manager,CISM) 證書或通過國際資安管理系統主導稽核員(Information Security Management System Lead Auditor,ISO 27001 LA)考試合格等。 (二) 具備資訊安全技術能力，如國際資訊安全系統專家(Certified InformationSystems Security Professional,CISSP)證書等。 (三) 具備模擬駭客攻擊能力，如滲透專家(Certified Ethical Hacking,.CEH)證書或事件處理專家(Certified Incident Handler,CIH)證書等。 (四) 熟悉金融領域載具應用、系統開發或稽核經驗。