保險代理人公司及兼營保險代理業務之銀行辦理電腦系統資訊安全評估作業原則

遵奉金融監督管理委員會保險局103年12月2日保局(綜)字第10302572750號書函暨
保險局103年11月19日召開資安自律規範檢視會議決議辦理修訂
104年1月22日第6屆第5次理監事聯席會議決議暨105年1月28日第6屆第9次理監事聯席會議決議修訂
遵奉金融監督管理委員會保險局112年10月31日保局(綜)字第1120434468號准予備查
112年11月2日第9屆第3次理監事聯席會議追認修訂

壹、前言

為確保保險代理人公司及兼營保險代理業務之銀行（下稱銀行）提供電腦系統具有一致性基本系統安全防護能力，擬透過各項資訊安全評估作業，發現資安威脅與弱點，藉以實施技術面與管理面相關控制措施，以改善並提升網路與資訊系統安全防護能力，訂定本作業原則。

貳、評估範圍

一、保險代理人公司及銀行應就整體電腦系統（含自建與委外維運）依據本作業原則建構一套評估計畫，基於持續營運及保障客戶權益，依資訊資產之重要性及影響程度進行分類，定期或分階段辦理資訊安全評估作業，並提交「電腦系統資訊安全評估報告」，辦理矯正預防措施，並定期追蹤檢討。

二、評估計畫應報董（理）事會或經其授權之經理部門核定，但外國保險代理人公司在台分公司，得授權由在中華民國負責人為之。評估計畫至少每三年重新審視一次。

參、電腦系統分類及評估週期

一、電腦系統依其重要性分為三類：

電腦系統類別	定義	評估週期	建議之資安管理標準
第一類	直接提供客戶自動化服務或對營運有重大影響之系統	每年至少辦理一次資訊安全評估作業	建議應取得ISO27001認證
第二類	經人工介入以直接或間接提供客戶服務之系統(如客戶服務、保單行政系統等系統)	每三年至少辦理一次資訊安全評估作業	如為已建立內部控制稽核制度之保險代理人公司（下稱內稽內控公司）應於建立制度後二年內辦理國際資安管理標準（ISMS）第三方之驗證；非內稽內控公司應要求合作之系統合作廠商其公司應取得相關資安管理標準之認證
第三類	未接觸客戶資訊或服務且對營運無影響之系統(如人資、財會、總務等系統)	每五年至少辦理一次資訊安全評估作業	應要求合作之系統合作廠商其公司應取得相關資安管理標準之認證

二、單一系統而為數眾多且財產權歸屬於公司之設備得以抽測方式辦理，抽測比例每次至少應占該系統全部設備之10%或100台以上。

三、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。

四、保險代理人公司及銀行如有第一類電腦系統應定期辦理下列項目：

(一)至少每二年辦理一次內部資通安全稽核。

(二)保險代理資訊系統中與客戶權益相關之第一類系統至少每二年辦理一次業務持續運作演練。

五、保險代理人公司及銀行如有第一、二類電腦系統，建議應要求合作之該類電腦系統廠商具有相當之資訊安全認知，如有相關資訊安全認證、至少一名持有資訊安全相關證照且持續維持證照有效性之人員，或定期辦理前項各款之內容等。

肆、資訊安全評估作業

一、資訊安全評估作業項目：

(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。

(二)網路活動檢視

1.檢視網路設備、伺服器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、防毒軟體、資料防護等）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(DomainNameSystemServer,DNSServer)查詢，並比對是否有符合網路惡意行為的特徵。

(三)網路設備、伺服器及終端機等設備檢測

1.檢視網路設備、伺服器及終端機的弱點與修補。

2.檢視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（FileTransferProtocol,FTP）連線、資料庫連線等）之儲存保護機制與存取控制。

(四)網站安全檢測

1.針對網站進行滲透測試或針對網站及客戶端軟體進行弱點掃描、程式原始碼掃描或黑箱測試。

2.檢視網站目錄及網頁之存取權限。

3.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。

(五)安全設定檢視

1.檢視伺服器(如網域服務ActiveDirectory)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AccessControlList)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。

(六)合規檢視

檢視整體電腦系統是否符合本作業原則「伍、資訊系統可靠性與安全性管理對策」之規範：

二、第一類電腦系統應依前項辦理資訊安全評估作業，第二類及第三類電腦系統辦理資訊安全評估作業則依系統特性選擇前項必要之評估作業項目。

伍、資訊系統可靠性與安全性管理對策

一、保險代理人公司及銀行應就提升資訊系統可靠性研擬相關對策，其內容包括：

（一）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。

（二）提昇軟體系統之可靠性：包含提升軟體開發品質與提升軟體維護品質對策。

（三）提升營運可靠性之對策。

（四）故障之早期發現與早期復原對策。

（五）災變對策。

二、保險代理人公司及銀行應就資訊安全性侵害研擬相關對策，其內容包括：

（一）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。

（二）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。

（三）防止非法程式：包含防禦、偵測與復原對策。

陸、資通安全防護

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。

具有郵件伺服器之公司，應備電子郵件過濾機制，並持續更新病毒碼、惡意郵件特徵等，適時進行軟、硬體之必要更新或升級。

柒、評估單位資格與責任

一、評估單位可委由外部專業機構或由保險代理人公司及銀行內部單位進行。如為外部專業機構，應與提供、維護資安評估標的之機構無利害關係，若為內部單位，應獨立於原電腦系統開發與維護等相關單位或可採用獨立電腦系統（弱點掃描工具、原碼掃描平臺、滲透測試工具、原碼掃、社交工具平臺、惡意程式或防毒軟體檢測平臺…等）輔助進行評估。

二、辦理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：

（一）參加相關資訊安全管理課程訓練達一定時數並取得教育訓練合格證明文件者或具備相關證照者；

（二）熟悉金融領域作業流程或具備稽核經驗者。

三、相關檢視文件、檢測紀錄檔、組態參數、程式原始碼、側錄封包資料等與本案相關之全部資料，評估單位應簽立保密切結書並提供適當保護措施，以防止資料外洩。

四、評估單位及人員不得隱瞞缺失、不實陳述、洩露資料及不當利用等情事。

捌、評估報告

「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、具體改善建議及社交演練結果，且應送稽核單位進行缺失改善事項之追蹤覆查。該報告應併同缺失改善等相關文件至少保存五年。