保險業電子商務參考查核項目

財政部保險司 93.5.12 台保司四字第 0930704024 號函
金融監督管理委員會 104.11.12 金管保綜字第 10400104370 號洽悉

目前保險業，可依據「保險業辦理電子商務應注意事項」規定透過開放性電腦網路（網際網路）辦理保險業務。由於網際網路無遠弗屆的發展，透過電腦網際網路提供保險業務服務，讓客戶可在全球各地經由網際網路使用保險業電子商務交易，使交易更有效率、更便利，亦有成本降低之優點，進而提昇保險業之競爭力，故未來保險業電子商務業務將可望持續發展。

本參考查核項目係為一般保險業電子商務業務之查核所編撰，供檢查保險業電子商務業務經營決策、管理、操作及內部稽核等之參考，檢查人員於實地檢查時，應衡酌受檢單位保險業電子商務業務範圍、性質及風險，依實際情況需要，決定查核範圍、重點及查核項目。

壹、 董事會與專責管理階層之監督管理

保險業辦理電子商務業務前，應當瞭解電子商務所帶來之風險，若決策未經衡量而採取不適當之措施及不符合保險業營運目標及營運範圍，將導致對目前或未來之資本或盈餘產生衝擊之風險，及易有經營上之風險，董事會應確認保險公司所辦理之各項業務是否符合其經營策略、目標及是否符合穩健經營原則，保險業新辦理網路投保業務，若依相關法令或自律規範規定應提報董事會，應擬具業務計畫，提報董事會後執行，專責管理階層應負責執行董事會核定之經營策略及政策，為瞭解董事會對業務部門之監督與管理，及專責管理階層之執行狀況，應調閱董事會會議記錄及相關計畫書與報告，以查核下列事項

一、董事會部分

（一）保險業辦理網路投保業務，是否研擬詳細計畫（如交易流程與作業要點、營運效益評估、風險評估與管理等）提報董（理）事會 （外國保險公司在台分公司為董事會授權人員）？

（二）保險業辦理網路投保業務，是否詳予分析各類風險並依業務性質訂定各種交易風險承擔限額，提報董（理）事會 （外國保險公司在台分公司為董事會授權人員）？

二、專責管理階層部分

（一）保險業辦理電子商務業務，專責管理階層是否督導業務部門研析各類風險（如信用、交易風險等），對需控管之風險，是否由專責管理階層督導業務部門建置風險控管程序？

（二）保險業專責管理階層，發現有疑似保險犯罪情事時，是否依公司相關作業程序通報及處理？

貳、風險管理

保險業辦理電子商務業務，係透過網際網路提供客戶有關保險業務之服務，除提供服

務之通路不同外，其業務性質與一般保險業務相同，亦須面臨風險控管之挑戰，對辦理保險業電子商務業務所帶來之風險，若未採取適當之管理措施，易導致風險已造成而仍渾然不知，或常發生不可預期之突發狀況對保險公司之資本或盈餘產生不利之衝擊。

依「保險業經營電子商務自律規範」規定，應承擔交易風險之責任，並建立電子交易風險內部管控機制。

為評估保險業電子商務業務之風險管理，調閱辦理保險業電子商務之計畫書及管理規範或作業規範，及保險業電子商務業務系統發展（自行或委外）之相關文件（如系統開發文件、系統流程、交易流程），以瞭解風險管理情形

一、保險業辦理電子商務業務所可能發生之風險分析及控管程序是否依「保險業風險管理實務守則」訂定及執行？

二、有關風險分析、管理或監控等項工作之分派與執行，是否符合分工牽制（制衡）原則？

三、保險業是否依所訂之風險控管程序及規範確實執行？

四、保險業於辦理電子商務業務過程中，如有業務推展需要或遇環境之變化（如保險環境改變、網路技術提昇重購軟硬體系統，或網路入侵等情況之發生）是否能依業務需要檢討修正其風險管理相關程序與規範？

五、保險業是否依業務性質及風險大小，訂定相關交易限額，以控管交易風險？

六、對透過網際網路之交易，保險業是否依「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」（有辦理簽發電子保單公司適用）及產（壽）險業辦理電腦系統資訊安全評估作業原則，參酌相關之安控標準適時更新所使用之安全及憑證技術，以保持或提升交易安全等級？

參、相關法律、規章之遵守

保險業若未依「保險業辦理電子商務應注意事項」向主管機關申請或未經核准即辦理網路投保業務，不僅會受主管機關之核罰，保險業辦理電子商務業務，若未遵守保險法、公平交易法、消費者保護法、金融消費者保護法、個人資料保護法、電子簽章法、洗錢防制法、保險業招攬及核保理賠辦法等相關法令之規定，即可能因違反相關法令受罰而致信譽受損及損失客戶之權益，保險業辦理電子商務業務，除其業務之交易面及管理面之安全需求及安全設計應遵守「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」（有辦理簽發電子保單公司適用），及與客戶所訂契約應符合「網路保險服務定型化契約範本」之規範外，其他保險業務相關法規亦應一併遵守，主要查核項目如下：

一、調閱保險業辦理電子商務交易種類、作業流程資料及與客戶之契約文件，以查核

(一)保險業辦理網路投保業務，是否已依「保險業辦理電子商務應注意事項」規定向主管機關提出申請，並經主管機關核准後辦理？

(二)保險業辦理各項電子商務，是否依「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」（有辦理簽發電子保單公司適用），及主管機關「網路保險服務定型化契約範本」之規範辦理。

(三)保險業辦理電子商務業務，是否符合保險法、公平交易法、消費者保護法、金融

消費者保護法、個人資料保護法、電子簽章法、洗錢防制法、保險業招攬及核保理賠辦法等相關法令之規定？若有涉及違反規定之情事，應依「保險業內部控制及稽核制度實施辦法」相關規定處理。

二、若有發生舞弊等重大偶發事件，是否依金融機構發生重大偶發事件通報規定辦理？

肆、作業安全控管設計

保險業電子商務為透過各種電子設備及通訊設備（如網際網路設備）與電腦軟體系統，提供客戶各項金融服務及進行交易之業務，保險業必須設計符合業務需要之安全控管機制，以確保交易與系統之安全。

一、資訊架構檢視

（一）是否已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？

（二）是否已檢視單點故障最大衝擊與風險承擔能力？

（三）是否已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

（一）是否已檢視網路設備、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？

（二）是否已檢視資安設備（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？

（三）是否已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，並比對是否有符合網路惡意行為的特徵。

三、網路設備、伺服器等設備檢測

（一）是否已辦理網路設備及伺服器的弱點掃描與修補作業？

（二）是否已檢測終端設備及伺服器是否存在惡意程式？

（三）是否已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？

四、外部網站安全檢測

（一）是否已針對網站進行滲透測試及弱點掃描？

（二）是否已檢視網站目錄及網頁之存取權限？

（三）是否已檢視網站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

（一）是否已檢視伺服器（如網域服務 Active Directory）有關「密碼設定原則」與「帳號鎖定原則」設定？

（二）是否已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？

（三）是否已檢視系統存取限制（如存取控制清單 Access Control List）及特權帳

號管理？

（四）是否已檢視作業系統、防毒軟體、辦公軟體及應用軟體等之更新設定及更新狀態？

（五）是否已檢視金鑰之儲存保護機制與存取控制？

六、資訊系統可靠性與安全性侵害之對策

（一）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。

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。

（二）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。

（三）檢視整體電腦系統是否符合上開相關對策之規範？

七、社交工程演練

是否已針對使用電腦系統人員，於安全監控範圍內，每年至少一次寄發演練郵件，加強資通安全教育，以期防範惡意程式透過社交方式入侵？

八、數位簽章、認證及交易安全管理（採用數位憑證進行交易者適用）

（一）保險業對電子商務有關交易面之安全需求 （如訊息隱密性、訊息完整性、訊息來源辨識、不可重複性、無法否認傳送及接收訊息等）是否有依「網路保險服務定型化契約範本」有關規定辦理？

（二）保險業電子商務客戶執行風險交易如有使用數位簽章，其使用之金鑰是否由客戶自行產生？若保險業自發憑證之金鑰軟體由保險業或其他第三人提供，有關對軟體之提供、啟用、維護及更新作業，是否有安全控管措施？

（三）調閱數位簽章申請書及認證作業規範文件，以評估認證(CA)機制，是否妥適？認證作業及金鑰之管理與控制程序是否妥適？

1.有關憑證之申請、核發及各項相關之作業（如憑證之註銷、中止等作業），是否皆訂有規範及作業程序？

2.對如何確認申請人身分，是否有明訂確認之程序，以防止冒名申請？

3.有關金鑰之長度是否符合「保險業辦理電子保單簽發作業自律規範」（有辦理簽發電子保單公司適用）之規定？

4.對金鑰及認證資料與檔案目錄，是否有安全保護措施：

（1）金鑰之產生，是否有確保其隱密性措施？

（2）是否有限制可存取之人員？

（3）人員存取資料，系統是否有留下稽核軌跡？

（4）對金鑰及認證資料之存取之妥適性，是否有列入稽核單位之稽核程序或項目？

（四）認證系統是否建置於獨立之主機或伺服器上？若否，認證系統與其他系統間，是否有規範加以區隔，及其區隔方式（如軟硬體系統之區隔、人員之區隔）？相關人員之權限是否符合內部牽制原則？

伍、作業控制

操作及管理規範訂定不完整，業務或作業處理上易產生疏失或遺漏，為能確認保險業對辦理電子商務業務從客戶之申請至中止作業，及保險業所提供各項之服務作業，能正確執行及有效運作，應調閱相關作業規章及規章研定會議記錄與各項管理報表，以瞭解保險電子商務作業控制狀況，

一、保險業辦理電子商務業務，就業務管理面之安全設計，是否符合「保險業經營電子商務自律規範」之規定？

二、保險業各項電子商務業務之作業是否符合內部牽制？作業及管理規範訂定之過程，必要時應有法令遵循、內部稽核及風險管理單位等相關單位之參與。

三、保險業對電子商務業務各連接點間，是否有訂定控管措施？

陸、與客戶、委外廠商或其他第三者之關係

保險業與客戶、委外廠商或其他第三者之合約內容不明確或不完備，可能造成雙方權責有爭議，或造成保險業權益上的損失，合約內容應明確或完備，以有效保護保險業權益。

一、是否明訂與客戶、委外廠商或其他第三者，如憑證機構、結算機構、清算機構、商家、供應廠商等之權利義務關係契約？

二、對外訂定之契約內容，是否視情況需要，涵蓋訂約雙方在業務與資訊、通訊技術等層面有關安全及資訊隱密性維護等方面之權責，包括發生問題時，責任之認定，及造成損失時，賠償責任之歸屬等？

三、辦理保險業電子商務業務，對與憑證機構、客戶及其他第三者所訂契約中，相互關聯部分，是否綜合考量，俾求內容周延且相互一致？

四、對保險業將系統之開發、維護或操作委外處理，調閱保險業內部稽核報告，查核內部稽核作業是否切實依照「保險業經營電子商務自律規範」等相關規定辦理，並留存完整內部稽核紀錄？

五、是否由有關單位，如法務、資訊、業務等有關單位人員參與契約內容之訂定或檢討，俾確保內容之周延及妥適性？

柒、業務之復原及災變應變計畫

保險業須建立提高系統可靠性之措施，以避免或減輕因電腦系統之故障或不可預測之災變而中斷電子商務業務，所造成對營運之衝擊，為瞭解保險業建置情形，調閱故障復原

程序及災變應變計劃書及演練記錄等文件，以查核

一、保險業之災變應變計劃書，是否已針對電子商務業務無法運作時，對保險業營運之衝擊影響進行評估並研擬因應措施？

二、保險業是否定期舉行業務之復原及災害緊急應變之測試演練？並是否檢討修定故障復原與災變應變計畫書？

三、保險業對系統故障或災害引起電子商務業務無法運作，所引發之法律責任，是否列為因應措施之一環？

捌、客戶端之服務

網際網路無遠弗屆，網路空間詭譎多變，未明確告知客戶相關之權利義務，及配合事項，可能會造成客戶之不便，或與客戶產生爭議者，若無法得知保險業電子商務之服務範圍或操作方式，可能會造成操作上的不便，或因操作上的錯誤而造成損失，保險業應提供客戶網路安全空間，以進行保險電子商務交易，為了解保險業辦理情形，調閱各項宣傳廣告資料或客戶契約並上網瀏覽以查核

一、是否提供客戶端操作說明，此操作說明是否正確、清楚？

二、保險業對有關電子商務業務客戶之權益或義務（如隱密性、資訊安全性及客戶對密碼之設定及管理等應注意與配合事項），是否有以書面（如於客戶契約中明示）或其他適當之方式（如於網站顯示）告知？

三、保險業是否有提供（告知）電子商務客戶，如何判斷及正確連上保險公司網站之資料訊息？

玖、內部稽核辦理情形

內部稽核之目的，主要為查核、評估保險業之內部控制制度之運作及衡量營運效率，及能適時提出改善意見，確保保險業之內部控制制度能持續有效實施，為瞭解內部稽核執行情形，調閱稽核手冊、檢查計劃及內部稽核報告，主要查核項目有：

一、保險業是否已將電子商務業務納入內部稽核及自行查核作業規範，以供辦理內部稽核及自行查核遵循？

二、保險業對前開規範內容是否配合業務推展需要定期檢討修正？

三、保險業是否確依內部稽核作業規範辦理內部稽核？其範圍是否妥適（如保險業電子商務各項業務、廠商管理及各項安控規範之遵循等）？

四、保險業辦理電子商務內部稽核所發現缺失事項，是否均送請相關單位辦理改善？並追蹤其改善情形？