金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

107 年度下半年主要檢查缺失

-人壽保險公司

目　　次

業務項目：核保及保全作業

缺失態樣

對法人為員工投保案件，未評估法人以員工為被保險人投保之合理性及指定或變更受益人是否符合投保目的。

缺失情節

- 對機構法人以員工福利為由為員工投保人身保險商品，惟滿期/祝壽保險金或生存還本保險金均指定受益人為該法人本身，非被保險人或其家屬，保險公司之核保作業未就所指定受益人是否與投保目的相符審慎評估。
- 機構法人以員工退休規劃為由為員工投保人身保險商品，且指定被保險人為受益人，惟嗣後進行契約變更受益人為該機構法人，保險公司辦理契約變更作業未審查受益人變更後是否符合原投保目的，不利確保受益人變更之合理性及妥適性。

改善作法

- 對於機構法人為員工投保人身保險商品，應注意依本會107.10.4 金管保壽字第 10704281220 號函規範辦理，應評估機構法人以員工為被保險人投保之合理性，及確保嗣後變更受益人時，不致有無法符合原投保目的之情形發生，避免機構法人假員工福利或員工退休規劃之名，行機構法人資金運用之實。

業務項目：核保及保全作業

缺失態樣

保全作業之處理程序規範欠完備。

缺失情節

- 辦理非要保人及被保險人親赴公司變更要保人案件，於完成保全作業審核時僅通知新要保人，未通知原要保人，不利原要保人知悉其保單狀況。
- 就保單借款業務進行之保全電訪，僅就單張保單借款達一定金額者為之，未將保戶短期間就多張保單辦理保單借款累積達一定金額者納入電訪範圍，電訪作業有欠周延。
- 未建立保戶地址建檔規則(如字型為大寫字體或阿拉伯數字等之一致性)或未完整將招攬通路之營業處所或業務員地址建檔，致未能精確檢核保險相關文件所載地址是否為招攬通路之營業處所或業務員地址，不利落實遵循本會 103.10.6 金管保壽字第 10302549351 號令第 4 點規定。

改善作法

- 應就保單借款、要保人變更等保全作業，建立確認要、被保險人申請真意之風險控管機制，並留存相關檢核紀錄，落實遵循本會 103.10.6 金管保壽字第 10302549351 號令規定。

業務項目：利害關係人交易

缺失態樣

利害關係人資料未確實建檔控管；召開董事會對涉及董事自身利害關係之討論案，有未迴避之情事。

缺失情節

- 未於董事異動時即時取得董事擔任企業董事資訊，致未更新利害關係人資料。
- 董事會討論案內容與董事自身有利害關係者，有未於董事會中說明利害關係，並予以迴避。

改善作法

- 利害關係人資料應於人員異動時配合隨時更新，並定期洽請保險業負責人確實填列或檢核所申報利害關係人資料之正確性。
- 應建立及落實審議利害關係人交易程序及控管機制，並注意依「保險業與利害關係人從事放款以外之其他交易管理辦法」第 4 條第 2 項「出席董事對與本人或與本人有利害關係者之案件應行迴避，並不得代理其他董事出席行使表決權」及「公開發行公司董事會議事辦法」第 17 條第 1 項第 7 款「…議事錄應詳實記載…利害關係重要內容之說明、其應迴避或不迴避理由」等規定辦理。

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

辦理姓名及名稱檢核範圍欠完整；客戶風險評估因子之風險分級欠合理。

缺失情節

- 對要、被保險人為未成年保件之法定代理人，未辦理姓名及名稱檢核，不利 AML/CFT 作業之落實。
- 辦理客戶風險評級作業，所設定之客戶風險評分因子未參考「國家洗錢及資恐風險評估報告」，將律師及會計師等職業定義為「高洗錢風險」職業，或未將未遵循或未充分遵循國際防制洗錢組織建議之國家或地區列為高風險國家，致影響客戶風險評估之正確性。

改善作法

- 應檢討姓名及名稱檢核作業之完整性，檢討客戶風險評級因子之合理性，加強客戶風險評估，以充分反映並控管風險，落實防制洗錢及打擊資恐作業。

業務項目：資通安全

缺失態樣

系統主機之特殊權限帳號控管機制及系統安全檢測相關作業規範未完備。

缺失情節

- 系統主機之特殊權限帳號已建置系統管理，可設定特殊權限帳號使用期間，惟資訊人員可經常性不間斷申請使用，致使用期間連續未間斷，管理機制形同虛設；另系統每日產出之監控報表，未對非上班時間登入系統作業之情形產製報表，未能監控是否有員工之帳號遭盜用之情事，不利及時發現並查明是否有異常入侵事件。
- 對源碼檢測、弱點掃描及滲透測試等發現之漏洞修補及追蹤處理，未訂定明確作業規範，且僅就「高」以上風險等級系統弱點評估是否有修補必要，對其他風險等級弱點則未有相關控管機制。

改善作法

- 應檢討系統主機特殊權限帳號之使用管控機制，據以研擬改善方案，以維系統安全。
- 資訊系統安全評估之相關作業規範應力求完整，對掃描結果應依風險等級評估影響性，安全漏洞須及時研擬補強措施並建立後續追蹤控管機制。

業務項目：個人資料保護

缺失態樣

對個資傳遞及使用之控管機制欠嚴謹。

缺失情節

- 已建置電子郵件稽核系統管理對外寄送含一定筆數個資之電子郵件資料偵測作業，惟對未達所設定之數量或無法判讀之加密檔、圖檔等，則未加以檢核或採取其他補強措施，逕予以寄送。
- 將正式作業主機之個資檔案及資料庫複製至開發測試主機作業，未將個資資料予以去識別化。

改善作法

- 應對含有個人資料之外寄電子郵件，設定妥適過濾原則及安全控管政策，建立定期檢視機制，確實將個人資料完整納入系統設定之過濾原則，針對附件為加密檔、圖形檔等無法辨識過濾之電子郵件，建立事前審核檔案傳輸之管控機制。
- 應重新檢視複製正式主機檔案及資料庫至測試主機去識別化作業程序之妥適性，避免將客戶真實資料複製至測試環境作業，如確有須將未去識別化個資複製至測試環境之業務需求，除應建立申請、刪除、留存完整稽核軌跡之控管機制外，並應嚴格管理該等資料檔案之存取權限。