金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

112 年度下半年主要檢查缺失

－人壽保險公司

目　　次

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

未參考防制洗錢金融行動工作組織(FATF)公布之高風險國家或地區，即時更新所建置之高風險國家名單。

缺失情節

- 雖已建置高風險國家名單，惟對法務部調查局公告 FATF 公布之高風險國家或地區相關訊息，未即時更新高風險國家名單，並調整相關因子之風險給分，致低估客戶風險評級。

改善作法

- 應參考防制洗錢金融行動工作組織(FATF)公布之高風險國家或地區等外部管道資訊，即時更新高風險國家或地區名單，以落實評估客戶風險評級。

業務項目：消費者保護

缺失態樣

對不同保戶之通訊資料有相同或集中情形，未落實檢核控管機制。

缺失情節

- 辦理寄發保單資訊之通知，對不同要保人有寄發至同一地址情形，未主動瞭解及聯繫保戶處理。

改善作法

- 應依「保險業保險經紀人公司及保險代理人公司防範保險業務員挪用侵占保戶款項相關內控作業規定」及本會 108 年 11 月 8 日金管保壽字第 10804358671 號函等規定，建立機制檢核保戶留存之通訊資料不得為招攬之保險業務員之通訊資料，且應比對上述通訊資料是否有相同或集中之異常情形，並應就該等情形主動瞭解及聯繫保戶處理。

業務項目：保險商品管理作業

缺失態樣

利率變動型保險商品宣告利率之訂定程序有欠周延。

缺失情節

- 利率變動型保險商品宣告利率之訂定，以區隔資產帳戶固定收益債券利息收益率為主要依據，並扣除必要利潤率、費用率及平穩結餘調節項等參數後決定，惟就平穩結餘調節項為負值者，未提報宣告利率會議說明理由並分析其合理性。

改善作法

- 應依「人身保險業辦理利率變動型保險商品業務應注意事項」第 3 點及第 5 點規定，訂定宣告利率之平穩結餘調節項為負值時，須於每月召開之宣告利率會議中說明理由並分析其合理性。

業務項目：國外投資

缺失態樣

辦理國外金融債之投資前風險評估欠周延，且未訂定差異化風險管理措施。

缺失情節

- 辦理具資本性質及吸收損失能力國外金融債之投資前評估報告，未分析債券之吸收損失條款、本金轉換或資本減記條件暨相關風險。
- 未完整盤點具資本性質及吸收損失能力金融債之暴險，並對吸收損失順序與觸發條件進行風險分類，訂定差異化管理機制。

改善作法

- 應依本會112年8月1日金管保財字第11204312022號函規定，投資外國銀行因資本要求發行之具資本性質及吸收損失能力債券，應先辨識各類型資本工具之風險、條款內容及差異、清償順序、觸發條件、及停止支付條件等，再據以訂定差異化風險管理限額與相關風險控管措施。

業務項目：國外投資

缺失態樣

投資限額之控管及檢核範圍欠完整。

缺失情節

- 辦理國外金融債之法令限額控管作業，僅控管投資於每一銀行發行之債券部位，未依「保險業辦理國外投資管理辦法」第6條第4項第2款第3目規定，將每一銀行保證之債券部位列入控管。
- 對「保險業辦理國外投資管理辦法」第3條第5項及第6條第4項第2款第3目等有關債券及股票等合計數之限額規定，未納入法令限額檢核範圍。

改善作法

- 應確實依「保險業辦理國外投資管理辦法」等規定建立法令限額控管機制，並加強法令限額檢核作業之覆核機制。

業務項目：資訊安全

缺失態樣

防火牆規則設定或管理作業欠妥。

缺失情節

- 未依最小授權原則設定防火牆規則，如：允許委外廠商或開發人員不經跳版機直接遠端連線至上線前確認環境(UAT)、允許可連線網際網路之個人電腦遠端連線至正式主機。
- 防火牆規則所設定主機有不存在或存有無業務需求之防火牆規則，如：對已下線之系統主機未同步調整防火牆規則、允許無上網需求之主機連線至網際網路。
- 辦理防火牆規則檢視作業，未將無流量防火牆規則納入檢視，或對採用高風險通訊協定之防火牆規則，未評估其必要性。

改善作法

- 應依最小授權原則設定防火牆規則，刪除非必要之網路連線，並妥適訂定防火牆規則定期檢視之重點項目，落實辦理檢視作業。

業務項目：資訊安全

缺失態樣

對使用外部網路連線至內部電腦之安全控管作業欠嚴謹。

缺失情節

- VPN 及 VDI 等供異地辦公或遠端工作所使用設備之相關規範，未納入資料傳輸及加密機制、異常行為監控等安全管控作業規定，不利落實「保險業辦理資訊安全防護自律規範」第 12 條第 2 款規定。
- 對使用 VPN 自外部遠端登入存取之行為，僅以帳號密碼登入驗證，未採多因子驗證，與「保險業辦理資訊安全防護自律規範」第 19 條第 3 款規定不符。
- 對員工申請以 VPN 遠端連線至內部電腦系統，其後未有使用紀錄者，未評估所需權限之必要性及合理性。

改善作法

- 應依「保險業辦理資訊安全防護自律規範」訂定 VPN 及 VDI 等設備相關使用規範，對自外部連線至內部電腦系統之行為，採用多因子方式驗證，並定期評估開放遠端登入權限之妥適性。