金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

103 年度下半年主要檢查缺失

-人壽保險公司

目　　次

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；利害關係人提報董事會及審計委員會資料不完整或重度決議程序欠周延情事。

缺失情節

- 利害關係人資料有未建檔情形，如：未將公司董事或監察人之配偶、二親等以內之血親，以及董監事本人或配偶擔任董事、監察人或總經理之企業等列入利害關係人建檔資料。
- 向利害關係人購買不動產，提報審計委員會及董事會之投資效益分析資料，未包含關係人取得價格及交易對象、現金收支預測表及評估資金運用之合理性等資料，核與「公開發行公司取得或處分資產處理準則」第 14 條規定不符。
- 董事會對利害關係人交易案，有重要事項未經討論，即予重度決議通過。

改善作法

- 利害關係人資料應確實建檔，並配合人員異動適時更新。
- 定期洽請保險業負責人確實填列及檢核利害關係人資料表之正確性。
- 定期透過外部資訊蒐集利害關係人資料，檢核保險業負責人提供之利害關係人資料，以確保建檔資訊之即時性與正確性。
- 提案單位對提報董事會決議之利害關係人交易議案，應提供充分書面資料敘明交易對象與公司或董事之利害關係，並檢附與同類對象交易之價格條件資料，以供董事審議交易條件是否未優於其他同類交易對象；董事會對相關內容並應充分討論。

業務項目：資產減損評估程序

缺失態樣

資產減損作業未由獨立於資產交易單位以外之其他單位負責辦理，有違內部牽制原則。

缺失情節

- 辦理不動產減損作業係由不動產暨放款部評估，經總經理核定後，送交會計室入帳，未由獨立之其他單位負責辦理評價作業，有失內部牽制原則。
- 內部控制作業程序未明確規範辦理金融資產評價及減損作業之權責單位，實際作業由原投資部門辦理，未符合內部牽制原則。

改善作法

應建置符合內部牽制原則之資產減損檢核及控管程序，由獨立於資產交易單位以外之其他單位負責辦理評價作業並落實執行。

業務項目：招攬、核保之作業流程與控管機制

缺失態樣

辦理招攬及核保作業有未落實辦理財務核保及電話訪問情事。

缺失情節

- 承保同一被保險人累計其他同業之人壽保險及傷害保險投保金額超過被保險人家庭年收入二十倍之案件，有未辦理財務核保作業者，核與「保險業招攬及核保作業控管自律規範」第 3 條第 3 項規範不符。
- 對業務員停止招攬處分期間屆滿或撤銷登錄後重新登錄之日起一年內之招攬件，有未執行財務核保者。
- 對銀行通路銷售投資型人身保險及以外幣收付之非投資型人身保險保單符合一定條件者，有未以電話訪問向要保人確認招攬人員是否已確實說明商品相關資訊及瞭解其適合度，核與「銀行、保險公司、保險代理人或保險經紀人辦理銀行保險業務應注意事項」第 11 點之 2 規定不符。

改善作法

應依相關規定及公司核保處理制度及程序，落實執行財務核保程序，確實評估客戶之實際經濟需求以及風險承受能力，並應加強落實電訪作業，向要保人以電話訪問說明商品相關資訊及瞭解其適合度，以保障消費者權益及避免消費爭議。

業務項目：資訊作業

缺失態樣

資訊系統作業權限未明確劃分；使用者權限授予及控管有欠妥適。

缺失情節

- 應用系統程式設計人員擁有變更保單資料庫及查詢、變更客戶資料之權限，程式撰寫及資料檔案變更作業未分工擔任，且未就變更情形留存稽核軌跡以供覆核。
- 資訊系統作業權限之授予，有未依職權賦予適當權限之情形，如：保全人員有核保權限、主管擁有經辦權限，不符內部牽制原則。
- 未就公司資訊系統最高權限帳號之申請及核准訂定管理程序，且使用情形未留存覆核紀錄，不利追蹤控管使用之妥適性。

改善作法

- 電腦系統使用者帳號應基於內部牽制原則依職能分工賦予適當作業權限。
- 電腦系統最高權限或特殊權限帳號應訂定密碼設定原則及控管機制，並對使用情形建立稽核報表覆核機制，以維系統運作安全。

業務項目：電子化個資檔案安全維護

缺失態樣

對存放含有客戶個資之公用檔案伺服器及個人電腦資料檔案之權限管理有不利個資安全防護情事。

缺失情節

- 存放含有客戶個資明碼資料之公用檔案伺服器及個人電腦檔案夾相關存取權限及檔案分享功能有授予非職務所需之人員。
- 對存放含有客戶個資檔案之伺服器及個人電腦，有開啟「網路芳鄰分享資料夾」功能，且未建立定期檢視分享資料夾權限及留存存取紀錄等管理機制，不利個資安全維護。

改善作法

涉及個資檔案之存取，應嚴格控管該等資料夾之存取權限，依職務需要覈實授權，相關存取應留存完整稽核軌跡、建立主管覆核及定期清查等管控機制，並落實執行。

業務項目：電子化個資檔案安全維護

缺失態樣

對外傳送電子郵件未建立控管機制。

缺失情節

經由電子郵件系統或連接外部網頁對外傳送含有個資或機敏資料，未建立過濾機制及控管措施。

改善作法

- 建置電子郵件內文過濾系統，並就對外傳送含有個資或機敏資料之電子郵件建立審核及追蹤控管機制。
- 建置資料外洩防護(DLP)系統，以監控、管理並預防個資或機敏資料外洩。

業務項目：電子化個資檔案安全維護

缺失態樣

未留存稽核軌跡或稽核軌跡留存欠完整，或對稽核軌跡未建立覆核機制。

缺失情節

- 未留存稽核軌跡或稽核軌跡留存欠完整：
  - 電子商務服務系統未留存執行查詢及變更密碼交易之稽核紀錄。
  - 伺服器僅留存開啟傳檔連線之紀錄，未啟用檔案傳輸稽核功能，留存檔案存取之稽核紀錄。
  - 僅對資料庫特殊權限帳號管理作業啟用稽核功能，其他使用帳號則未予以稽核，且對資料選取（select）、更新（update）及刪除（delete）等存取作業，亦未留存稽核軌跡。
- 資料庫帳號管理、系統參數設定及執行查詢、變更等作業，雖已留存稽核紀錄，惟未建立覆核機制。

改善作法

- 清查應用系統是否已設計留存查詢個人資料之稽核紀錄、傳檔系統是否已建立檔案傳輸稽核軌跡，確實留存完整之稽核軌跡。
- 檢討資料庫稽核軌跡之完整性，除調整資料庫系統之稽核功能或建置資料庫稽核系統外，並留存完整之資料存取稽核軌跡。
- 建立稽核軌跡覆核作業機制，並落實執行。

業務項目：電子化個資檔案安全維護

缺失態樣

對業務員疑似個資外洩事故之通報及後續改善措施欠完善。

缺失情節

- 對業務員疑似個資外洩事件，未納入個資事故通報範圍，且未明定事故通報相關部門主管及核定層級。
- 對疑似個資事故通報案件之改善措施，僅對業務員加強宣導保護個資，未對業務員個人行動裝置所儲存之客戶個資研議加強保護措施。

改善作法

- 對個資外洩事件建立妥適之通報及善後處理標準作業程序，以利個資外洩事件作業風險控管及處置。
- 對業務員個人行動裝置應訂定使用規範，並對所儲存之客戶個資建立適當保護措施，俾防範個資外洩。

業務項目：網路安全

缺失態樣

對行動裝置應用軟體(APP)委外開發維護作業之管理有欠妥適。

缺失情節

- 行動裝置應用軟體(APP)委外開發上架前，未辦理原始碼檢測。
- 逕以受託廠商編譯之應用軟體(APP)，發布於行動平臺供下載使用。

改善作法

- 對提供網際網路服務之電子商務系統，應建立原始碼檢測機制，確保應用軟體(APP)已包含攻擊防禦設計。
- 應比照自行開發程式變更之作業流程，對委外廠商交付之應用軟體(APP)原始程式碼，進行程式比對及編譯後再上架，以確保程式異動均屬合法及正確。