金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

114 年度上半年主要檢查缺失

-信用合作社

目　　次

防制洗錢、打擊資恐及反武擴作業 1

授信業務 2

內部管理 3

資訊安全 4

金管會檢查局

業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

未落實對實質受益人之辨識作業。

缺失情節

- 對未完成實質受益人辨識之客戶臨櫃辦理交易時，端末系統交易畫面雖有提醒櫃員辦理實質受益人辨識作業，惟尚未建立後續管控措施，致漏未對客戶補辦實質受益人辨識作業並進行建檔。

改善作法

- 應依照「金融機構防制洗錢辦法」第3條第4款規定辦理客戶實質受益人之辨識，並以合理措施驗證其身分。

業務項目：授信業務

缺失態樣

未確實辦理購地貸款業務。

缺失情節

- 辦理購地貸款，對借款人未依興建計畫之預定日期動工興建，未瞭解原因，且於展期時亦未重新徵提興建計畫憑核。
- 借款人購置之土地未動工興建，未依規保留1成俟借款人動工興建後撥貸。

改善作法

- 應參照「中央銀行對金融機構辦理不動產抵押貸款業務規定問與答」二、購地貸款Q1及Q2相關規定辦理，並瞭解未依興建計畫動工原因、確實徵提及審核興建計畫。
- 應參照「中央銀行對金融機構辦理不動產抵押貸款業務規定」第5點第2款，金融機構承作購地貸款，貸款額度最高不得超過購買土地取得成本與金融機構鑑價金額較低者之五成，其中一成應俟借款人動工興建後始得撥貸。

業務項目：內部管理

缺失態樣

對員工櫃員卡管理欠妥適。

缺失情節

- 營業單位主管同時持有主管卡及保管櫃員卡，有失內部牽制原則。

改善作法

- 應檢討主管保管櫃員卡之妥適性，並落實職務分工原則，以維交易安全。

業務項目：資訊安全

缺失態樣

資訊系統帳號密碼及最高權限帳號控管作業有待強化。

缺失情節

- 未設定妥適之密碼檢核邏輯(含最小長度、密碼複雜度、密碼歷程紀錄等)及密碼定期變更週期，且帳號有共用情形。
- 最高權限帳號係由管理人員自行持有及變更密碼，未建立最高權限帳號收回封存、使用前取得權責主管同意、使用後儘速變更密碼、保留稽核軌跡及定期抽查使用結果等機制。

改善作法

- 應確實依「信用合作社資通安全防護基準」第4條及第8條規定，避免共用帳號、納管主機最高權限帳號並定期抽查使用結果。

業務項目：資訊安全

缺失態樣

系統及應用程式變更上版作業有欠妥適。

缺失情節

- 上版作業尚未明定作業流程，明確定義各作業人員權責及留存作業軌跡、建立應用程式提領申請審核程序、應用程式上版所應交付之必要文件(如：上版程式清單、程式變更內容、程式異動前後差異比對表、測試報告及原始碼掃描文件等)及上架前安全檢測等規範。
- ATM 系統更版作業，對於廠商所修正之可執行程式未辦理惡意程式掃描及進行完整性(如：MD5)與來源辨識性(如：ZIP 加密)驗證，且未建立換版需求單及版本控管作業，並交付派版必要文件，於風險評估後再進行上版。
- App Store 及 Google Play 商店管理帳號交由開發廠商使用並辦理上版作業，未要求廠商採行 2 人或 2 項以上技術進行發布程序管控。

改善作法

- 應明定應用程式變更上版作業流程，並依「金融機構提供自動櫃員機系統安全作業規範」第3條及第4條規定及「金融機構提供行動裝置應用程式作業規範」第3條規定建立上版前之安控機制。