金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

113 年度下半年主要檢查缺失

-信用合作社

目　　次

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

對客戶風險定期審查作業未落實。

缺失情節

- 未依自身業務情形，妥適訂定符合「一定條件」之低風險客戶、「事件觸發」之門檻條件及其相應之「適當管控措施」。
- 未訂定低風險客戶定期審查時點，致開戶逾5年之低風險客戶未辦理定期審查作業。

改善作法

- 應參照本會108年4月16日金管銀法字第10801049290號函復銀行公會所訂「銀行辦理客戶定期審查或風險評估資料之取得或更新作業參考簡化措施」規定辦理。
- 應參照「金融機構防制洗錢辦法」規定，依據客戶之重要性及風險程度所訂之定期審查時點辦理確認客戶身分。

業務項目：授信業務

缺失態樣

辦理利害關係人授信之控管作業欠確實。

缺失情節

- 未訂定相關標準作業程序，如：利害關係人資料之填報、建檔、更新及確認之時間及流程、定期確認利害關係人資料之正確性、辦理授信及交易前再次檢視及確認之控管程序等。
- 辦理授信條件變更，未辦理是否未優於其他同類對象之檢核作業。

改善作法

- 辦理利害關係人授信及交易，應參照「信用合作社辦理與利害關係人授信及交易應行注意事項」規定，訂定法令遵循標準作業程序。
- 應參照「信用合作社辦理與利害關係人授信及交易應行注意事項」規定，對授信利害關係人辦理授信(含續約或變更條件)時，其條件不得優於其他同類授信對象，並留存相關資料佐證，以利查核。

業務項目：內部管理

缺失態樣

對電腦作業權限管理欠妥適。

缺失情節

- 未依員工擔任之職務核予適當電腦權限。

改善作法

- 應檢討電腦權限授權之妥適性，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

辦理網路安全管理作業欠妥。

缺失情節

- 辦理防火牆規則定期檢視作業，對未限縮之連線範圍(ANY 或網段)、高風險服務(ANY、FTP、SSH、HTTP、TELNET、RDP、SMB 及 MS-SQL 等)及實際流量為零等規則，未敘明留用之必要性。
- 測試主機與正式主機置於同一網段，未依主機重要性與業務性質，以防火牆或其他網路存取管控，限制主機間之連線行為。
- 未訂定弱點掃描、滲透測試及程式碼掃描等管理規範，包含弱點修補期限、弱點不予修補者之補償性措施及追蹤管理程序等。

改善作法

- 應確實依「信用合作社辦理電腦系統資訊安全評估辦法」規定，落實防火牆規則檢核作業、妥適配置網段區隔，並建立弱點掃描修補機制。

業務項目：資訊安全

缺失態樣

辦理主機系統管理作業欠妥。

缺失情節

- 對開放系統、資料庫及網路設備等最高權限或特殊功能帳號，未定期抽查使用結果。
- 未訂定作業系統安全強化標準，並定期檢視系統安全設定。
- 資訊系統經原廠公告停止提供更新及漏洞修補服務(EOS)，未訂定汰換計畫，並建立汰換前之風險補償措施。

改善作法

- 應建立特權帳號申請及控管措施，定期抽查使用結果、訂定重要系統安全強化標準，並定期檢視及對原廠已停止支援系統之資安風險，積極研擬具體改善措施。