



金融監督管理委員會檢查局

Financial Examination Bureau, Financial Supervisory Commission, ROC

111 年度下半年主要檢查缺失

-本國銀行

目 次

防制洗錢、打擊資恐及反武擴作業	1
法令遵循	3
消費者保護	5
數位金融	7
授信業務	9
內部管理	12
資訊安全	13



✓ 業務項目：防制洗錢、打擊資恐及反武擴作業

缺失
態樣

對交易監控資訊系統或監控程序之設計欠完善。

缺失
情節

對符合稅務犯罪及租稅規避之可疑交易，未予檢核產出警示，不利稅務洗錢風險之防制，如：

- 客戶運用網路平台銷售貨物，並利用其存款帳戶收取貨款，且來自該平台頻繁存入達一定金額，惟該等營業人客戶均尚未申請稅籍登記。
- 應支付予公司之票款有存入負責人或第三人帳戶者，疑有公司銷貨收入或營利所得存放個人帳戶之情形。
- 註冊於境外之法人客戶，有透過行內帳戶匯款至負責人或其他受益人情形。

改善
作法

- 應適當納入本會 107.6.8 銀局(法)字第 10702114350 號函轉財政部提供之稽徵實務常見「租稅規避及逃漏稅態樣」之可疑交易情境，建立辨識逃漏稅相關之疑似交易態樣或警示指標，優化監控機制以察覺高稅務洗錢風險之交易。



業務項目：防制洗錢、打擊資恐及反武擴作業

缺失態樣

對虛擬通貨交易平台業者之客戶審查、使用者實名制及平台使用者交易監控，未依本會規定確實辦理。

缺失情節

- 未確實辦理客戶審查，致未辨識出客戶係實際經營虛擬通貨交易平台業務，並納入高風險客戶控管。
- 未對虛擬通貨交易平台業者徵提佐證資料，以確認其對使用者已採取實名制。
- 虛擬通貨交易平台業者有將部分帳戶同時供自用及平台使用者使用之混用情形，影響對相關帳戶之交易監控。

改善作法

- 應確實辦理客戶審查，並依本會 107.7.27 金管銀法字第 10702729040 號函及「銀行與虛擬通貨交易平台業者建立業務關係審查實務參考做法」規定第三點，確認虛擬通貨交易平台業者已對平台使用者採取實名制，並訂定明確之審查及驗證標準。
- 應依「金融機構防制洗錢辦法」第 3 條第 4 款規定，所訂確認客戶身分措施，應包括瞭解業務關係之目的與性質。



業務項目：法令遵循

缺失
態樣

未確實辦理法令遵循自評作業。

缺失
情節

- 法令遵循單位未將新開辦業務納入自評項目，致營業單位未辦理相關業務自評作業。

改善
作法

- 應強化法令遵循自評機制，確保自評單位及評估項目完整性。



業務項目：法令遵循

缺失
態樣

未依規定投資及管理不動產。

缺失
情節

- 帳列自用不動產之自用面積有低於 50% 情事。
- 以訓練中心名義向本會申請核准供作非營業用辦公場所並列為自用不動產，惟無相關訓練紀錄。
- 對因概括承受其他金融機構而持有超逾自用所需之不動產，未訂定儘速處分時程及計畫，致有長期持有情事。

改善
作法

- 應確實依「商業銀行投資不動產辦法」第 3 條規定之自用面積比率區分自用與非自用不動產。
- 應依實際用途向本會申請設置非營業用辦公場所，並落實銀行法第 75 條第 2 項規定。
- 應依「商業銀行投資不動產辦法」第 4 條第 1 項規定，儘速處分因概括承受其他金融機構而持有超逾自用所需之不動產。



✪ 業務項目：消費者保護

缺失
態樣

信用卡催收作業有欠妥適。

缺失
情節

- 催收人員可取得並利用信用卡申請書所載持卡人以外之第三人資料進行不當催收，或對與債務無關之第三人進行干擾，內部控管機制有欠完善。
- 時隔多年始向債務人催收信用卡費用及以法定最高利率累積之循環利息，期間均未妥善告知債務明細及還款方案，且循環利率未考量實質利率水準變化。

改善
作法

- 應強化保障客戶個人資料，確實依「信用卡業務機構管理辦法」第 42 條第 4 項及第 51 條規定辦理催收作業。
- 應確實告知債務人債務明細及提供還款方案，並依本會 110 年 11 月 8 日金管銀控字第 11002273521 號函規定，於執行債務協商機制時，考量實質利率水準變化、本金收回情形及違約金收回有無過高等因素，與債務人協商還款，以充分落實訂約公平誠信原則。



✱ 業務項目：消費者保護

缺失態樣

銷售金融商品予高齡客戶，未落實本會「金融服務業公平待客原則」。

缺失情節

- 銷售投資型保險商品予高齡客戶，未清楚說明投資標的轉換費用及高齡客戶需支付高額危險保費。
- 受理高齡客戶投資金融商品，未確認客戶是否具溝通、閱讀及判斷金融商品風險等行為能力，並留存相關紀錄。

改善作法

- 應督導業務人員向高齡客戶明確說明投資型保險商品轉換費用及危險保費之計收方式，以落實本會「金融服務業公平待客原則-告知與揭露原則」。
- 應建立確認高齡客戶具溝通、閱讀及判斷等行為能力相關規範及管控機制，以落實本會「公平待客原則-注意與忠實義務原則」。



✓業務項目：數位金融

缺失態樣

辦理電子銀行業務，交易面之安全設計有待加強及未確實控管轉帳交易限額。

缺失情節

- 對客戶採用固定帳號密碼登入網路銀行，採電子郵件通知客戶登入訊息，惟對客戶未留存或留存無效電子信箱者，未建立其他替代通知之控管機制。
- 對第三類數位存款帳戶轉帳限額之控管，未將客戶透過 ATM 及行動銀行之轉帳交易納入控管，致有超逾限額。

改善作法

- 應依「金融機構辦理電子銀行業務安全控管作業基準」第 10 條第 1 款規定，就採用固定密碼進行網路銀行身分確認者，加強相關安全機制。
- 應確實遵循銀行公會「銀行受理客戶以網路方式開立數位存款帳戶作業範本」第 4 條所訂轉帳限額。



✓業務項目：數位金融

缺失
態樣

受理客戶將數位存款帳戶轉換為一般帳戶有未確實審查。

缺失
情節

- 受理客戶臨櫃申請將數位存款帳戶轉換為一般帳戶，未採用開戶檢核表進行審核。
- 未確實審查客戶資料即同意轉換為一般帳戶，且有轉換不久即遭通報為警示帳戶情事。

改善
作法

- 應依銀行公會「銀行受理客戶以網路方式開立數位存款帳戶作業範本」第5條第5款規定辦理。
- 應加強教育訓練及覆核機制，督導行員確實執行客戶身分審查作業程序。



✪ 業務項目：授信業務

缺失
態樣

海外授信案暴險控管欠妥適。

缺失
情節

- 未就海外總體經濟環境（包含政治風險）之變化，滾動式檢討海外暴險限額之妥適性。
- 辦理海外授信業務貸後管理，對國家主權評等轉劣、政經情勢不明或惡化、有貿易紛爭，或對受疫情衝擊致產業面已有重大改變者，未評估借戶重大營運風險，並納入預警範圍。

改善
作法

- 應依本會 104 年 3 月 30 日金管銀控字第 10400051850 號函說明四(二)2 規定，因應總體經濟、政治發展情勢及金融環境變化，妥適訂定內部控管調整機制及限額預警門檻。
- 應依本會 109 年 12 月 10 日金管銀國字第 1090273912 號函說明三及四規定，就各海外經營環境之差異、適時因應當地經濟情勢變化，積極採取相對應之風險管理措施，於 COVID-19 疫情期間，仍應確實執行相關貸後管理及債權確保作業。



✓業務項目：授信業務

缺失
態樣

不動產抵押貸款徵審及貸後管理流於形式。

缺失
情節

- 辦理購地貸款(含續貸或轉貸)，對借戶購地後久未開發興建，除未徵提具體之興建開發計畫，批覆條件亦未加註未依約動工將提高利率或逐步收回貸款等條款。
- 對借戶購置土地未依約興建開發，雖有調升利率，惟旋即又依借戶申請調降利率，或未審慎評估即同意借戶延後興建開發，並免除其興建動工切結承諾。

改善
作法

- 應依 109 年 11 月 20 日金管銀法字第 1090273985 號函說明一(八)2 規定，分析借戶所提供興建計畫之可行性，並加強核貸條件之審核。
- 應切實辦理貸後覆審工作，建立並落實執行對借戶之督促興建機制。



✓ 業務項目：授信業務

缺失
態樣

辦理購屋貸款相關防杜炒房管理機制未臻完善。

缺失
情節

- 對進件來源或申貸戶涉及媒體報導炒房集團成員、職員及代書者，未納入觀察名單加強控管。
- 對不同客戶由同一炒房集團相關人員代理提領大額現金之異常情事，未確實瞭解雙方關係、交易目的及資金流向。
- 借戶購屋資金部分由炒房集團相關人員提供，或貸款本息由炒房集團相關人員代為繳納。

改善
作法

- 應依銀行公會「投資客炒房及人頭戶申請不動產貸款可能模式與態樣及防範機制」，強化招攬作業管控機制、確實審查購屋自備款來源及貸款資金流向、研擬有效還款來源監控措施，並注意買賣交易真實性。



✓ 業務項目：內部管理

缺失
態樣

未確實瞭解理財專員信用及財務狀況。

缺失
情節

- 對理財專員信用狀況符合所設之風險態樣者，僅洽其自行說明原因，未徵取相關資料評核；或理財專員個人存款帳戶往來明細備註欄註記有與期貨公司資金往來情形者，未進一步查明原由或調整列入高風險理財專員名單。
- 檢視理財專員信用及財務狀況，有未將金融機構大額無擔保授信列為審查條件。

改善
作法

- 應加強對理財專員信用及財務狀況之檢視作業。
- 應確實遵循「銀行防範理財專員挪用客戶款項相關內控作業原則」第4條規定，對於現職理財專員，應定期或不定期瞭解其信用及財務狀況，預防弊端之發生。



☑ 業務項目：資訊安全

缺失
態樣

電子銀行業務以簡訊 OTP 辦理身分驗證，作業有欠妥適。

缺失
情節

- 執行非約定轉帳交易時，僅須輸入固定密碼及系統即時發送之簡訊 OTP 即可完成轉帳，惟未考量裝置遭植入惡意程式導致 OTP 被竊之風險，增加其他有效防範機制，不利帳戶安全。
- 簡訊 OTP 係委由某科技公司發送並提供簡訊系統平台供銀行查詢發送情形，惟查 OTP 以明文於簡訊系統平台顯示，且多達上百個帳號可登入該系統即時查詢其內容，不利確保 OTP 密碼之隱密性。

改善
作法

- 應依「金融機構辦理電子銀行業務安全控管作業基準」第9條第3款第2目第3子目之2規定，對應用簡訊傳送OTP於非約定轉入帳戶轉帳交易時，採取加強防護機制。
- 應確認簡訊OTP之隱密性，確保傳遞過程無第三人可即時查詢其內容。



業務項目：資訊安全

缺失
態樣

對外服務網站安全防护作業有欠妥善。

缺失
情節

- 對外服務網站對用戶端瀏覽器之設定，未採用安全標頭(Headers)設計，如：未採用強化網頁瀏覽機制 (Strict-Transport-Security)、防禦跨網站指令攻擊(Content-Security-Policy)、防禦內嵌惡意網頁攻擊(X-Frame-Options)、避免瀏覽器誤判文件格式(X-Content-Type-Options)、保護資訊洩漏(Referrer-Policy)及管控特定應用程式介面(API)或瀏覽器功能(Permissions-Policy)等安全標頭，不利防範網路攻擊。
- 網站仍接受 TLS1.0 及 1.1 等不安全加密方式風險弱點，可能導致攻擊者進行中間人攻擊，解密網站伺服器與使用者間通訊。

改善
作法

- 應建立定期檢視對外服務網站安全機制，以確保網頁安全及降低駭客攻擊之風險。



 業務項目：資訊安全

缺失
態樣

連線正式營運環境之管控措施有欠妥適。

缺失
情節

- 雖已有建置跳板機，惟仍允許資訊室系統管理人員之個人電腦直接連線正式主機，進行資料庫存取服務(MS-SQL)、遠端登入服務(VNC、RDP)等高風險性網路通訊服務，未評估其安全性及必要性者。
- 資料處理科同仁逕以可對外連線網際網路及收發電子郵件之個人電腦直接連線正式營運伺服器辦理日常維運作業，易致帳號密碼外洩，影響系統安全。

改善
作法

- 應覈實檢視連線正式營運環境之管控措施，並評估其安全性及必要性。