財團法人中華民國證券櫃檯買賣中心

112 年第 3 季查核證券商及槓桿交易商財務業務內部稽核作業常見缺失彙總表

缺　　失　　內　　容
一、證券商辦理防制洗錢及打擊資恐作業，有未確實依審查評估項目辨識客戶風險之情事。
二、證券商未確實執行客戶出借股票扣帳作業，致接受客戶委託賣出時誤認客戶委託數量未逾其集保帳戶餘額，發生客戶超賣情事。
三、證券商業務人員於 LINE 聊天室向客戶轉貼未經公司核准之業務相資訊，且向客戶推介買賣有價證券前，未與客戶簽訂推介契約。
四、證券商辦理採購付款及交際費支出作業，未依核決權限規定辦理簽核。
五、證券商自營部之投資決策報告未經權責主管簽准，且未依據買賣決策決定之投資組合買賣有價證券。
六、證券商於營業處所買賣僅限銷售予專業投資人之國際債券，於賣出時未明確告知買方再行賣出之交易對象以專業投資人為限。
七、證券商業務人員受託買賣處置股票及變更交易股票，有於完成預收款券前即辦理買賣申報之情事。
八、證券商董事有於其他證券商開戶之情事。
九、證券商於評估營業員帳戶交易情形與其所得財力是否相當時，未對營業員業績過度集中於自身交易帳戶者訂定量化標準並進行評估。
十、證券商辦理不限用途款項借貸業務，對於客戶於簽訂契約後始具內部人身分者之情形，未依規訂定內部控制制度。
十一、 資通安全部分：
(一)重要系統之稽核紀錄未依規留存三年。
(二)未對弱點掃描所辨識出之潛在系統弱點，評估其風險或安裝修補程式、執行複測，並留存紀錄。
(三)電腦系統或網路未適當區分使用者權限。
(四)未訂定資訊分級與處理之相關規範。
(五)未確實對異常及不明來源 IP 連線進行監控分析及留存紀錄。
(六)客戶帳號發生異常態樣登入時，未留存通知客戶紀錄。

缺　　失　　內　　容
(七)防火牆進出紀錄及其備份未依規定至少保存三年。
(八)未定期或適時修補網路運作環境之安全漏洞（例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等）並留存相關文件。
(九)個人端（含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦未安裝防毒軟體並及時更新程式及病毒碼。
(十)未定期評估自身網路系統安全。
(十一)網際網路下單服務品質標準未包含系統可用性或未評估網路下單品質之可用性並留存相關評估紀錄。
(十二)辦理網路下單業務，未依規每半年執行網路系統外部弱點掃描作業一次。
(十三)透過網際網路使用管理帳號登入重要系統時，尚未採用多因子認證機制。
(十四)未定期審查並檢討久未使用之使用者權限。
(十五)未全面使用優質密碼設定，或未定期每三個月更新使用者密碼。
(十六)違反證券商內部控制制度標準規範 CC-19000 有關程式原始碼安全規範。
(十七)內部稽核人員未依內部控制制度之電腦作業與資訊提供循環所規定之週期，就資訊軟、硬體設備及作業管理之委外管理執行相關稽核作業。
(十八)未建立相關資訊安全機制或未擬定緊急應變計畫及備援措施。
(十九)未於委外契約（至少應含委外管理範圍、委外管理期間、委外管理費用、委外管理責任、智慧財產權協議、保密義務、查核條款等）中明確訂定雙方電腦資訊作業管理之安全性規範、業務（含內部稽核）之責任區分及雙方之資訊人員管理規範。