財團法人中華民國證券櫃檯買賣中心

111 年第 3 季查核證券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時，未運用適當之風險管理機制辨識實質受益人。
二、證券商自營部門交易員從事可轉換公司債策略交易時，有低賣高買予自己所使用之他人經紀帳戶之情事。
三、證券商辦理衍生性金融商品交易業務客戶屬性年度評估作業，有未由銷售衍生性金融商品以外之人員辦理，且未經適當之單位或人員進行覆核之情事。
四、證券經紀商有接受未經經濟部投資審議會核准之華僑及外國人客戶委託賣出有價證券之情事。
五、證券商之交際費支出未確實依公司訂定之控管措施執行。
六、證券商未於規定時限內申報投資人違約資訊。
七、投資人於 T+2 日委託賣出 T 日買進之處置股票，因證券商業務人員延遲辦理股票圈存作業，造成投資人可委託賣出時，標的股票股價已達跌停，致投資人無法賣出而有權益受損之情事。
八、證券商以普通戶違約專戶處分違約投資人證券業務借貸款項擔保品，有未依規定於借貸款項違約處理專戶處分擔保品之情事。
九、資通安全部分：
（一）證券商未安裝網路伺服器端電腦之防毒軟體。
（二）證券商未定期審查並檢討久未使用之使用者權限。
（三）證券商未依「個人資料保護法」，妥善處理客戶及公司內部人個人資料。
（四）證券商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。
（五）證券商未建置「網路下單網頁與程式異動偵測系統」。
（六）證券商之資訊處理部門與業務單位在組織功能上之權責未明確劃分，在執行資訊系統相關業務時，未明確劃分業務範圍、責任及權限。
（七）證券商之個人電腦、伺服器及網路通訊設備之系統參數採用系統預設值，尚未建立並落實安全性組態基準設定。
（八）證券商未依「證券商內部控制制度標準規範」之規定，落實網際網路下單服務品質維護之相關標準。

缺　　失　　內　　容
（九）證券商有違反程式原始碼安全規範之情事。
（十）證券商辦理網路下單業務，未確實執行網路系統弱點掃瞄作業。
（十一）證券商系統開發及維護之委外作業，與委外廠商簽訂契約內容未包含資訊安全協定與對委外廠商資安稽核權等條款。
（十二）證券商之網路未有適當區隔機制。
（十三）證券商未建立防火牆。
（十四）證券商存放個人資料及機敏資料之主機未放置於安全的網路區域。
（十五）證券商透過網際網路以管理帳號登入重要系統時，未採用多因子認證機制。
（十六）證券商未依規定使用最高權限管理帳號並留存紀錄。
（十七）證券商未全面使用優質密碼設定，或未定期每 3 個月更新使用者密碼。
（十八）證券商未於啟動 APP 時偵測行動應用裝置是否遭破解，並提示使用者風險相關訊息。