資安查核缺失案例分享

臺灣證券交易所
券商輔導部

TAIWAN
STOCK EXCHANGE

報告大綱

竭誠為您服務

壹、查核常見缺失
貳、案例介紹
參、近期法規宣導

常見查核缺失

一. 防火牆進出紀錄及其備份未依規定至少保存三年。

二. 未建立防火牆。

三. 已完成之程式因故須維護時，未依據經過正式核准之程序辦理。

四. 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。

常見查核缺失

五. 辦理網路下單業務，未依規每半年至少應執行資訊系統弱點掃描乙次，針對所辨識出之潛在系統弱點，應評估其相關風險或安裝修補程式，並留存紀錄。

六. 未訂定資訊分級並作標示處理之相關規範。

七. 風險評鑑管理未確定公司各作業可接受之資訊安全風險等級。

八. 系統開發及維護委外作業，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。

常見查核缺失

九. 重要系統之稽核紀錄未依規留存三年。

十. 對重要系統(如主機連線系統、網路下單系統等)之稽核日誌紀錄未完整(內容應包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項)。

十一. 於官方網站提供連結供使用者連至公司外之社群媒體時，未出現提示視窗告知使用者該連結非公司本身之網站。

常見查核缺失

十二. 系統復原計畫未定期辦理模擬演練。

十三. 檢查公司現有系統軟硬體設備，使用預設或簡易之帳號密碼，未能使用優質密碼設定或未能定期3個月內更新相關使用者密碼。

十四. 電腦系統容量評估及壓力測試範圍欠完整。

十五. 對於程式、檔案、網路及資訊系統之存取使用，應按權限區分，公司應定期審查資訊機房門禁管制權限、久未使用的使用者帳號權限。

常見查核缺失

十六. 未訂定委外人員帳號權限申請程序及權限使用未經適當控管。

十七. 行動應用程式每年與初次上架應委由合格第三方檢測實驗室進行並完成通過資安檢測，如通過實驗室檢測後一年內有更新上架之需要，應於每次上架前就重大更新項目進行委外或自行檢測，檢測範圍以 OWASP MOBILE TOP 10之標準為依據，並留存檢測紀錄。

十八. 未依個人資料保護法妥善處理客戶及公司內部個人資料。

常見查核缺失

十九. 公司提供網路下單服務，應於網路下單登入時採多因子認證方式（例如：下單憑證、綁定裝置、OTP、生物辨識等機制），以確保為客戶本人登入。

二十. 公司應訂定資訊安全訊息通報機制，針對與資訊系統有關之資訊安全或服務異常事件應依「證券期貨市場資通安全事件通報應變作業注意事項」辦理，並採取適當矯正程序，留存紀錄。

案例介紹

案例一~案情摘要

陳情人申訴證券商接受投資人買進上櫃股票，疑有未對投資人檢核買賣額度，未於下單前進行風控檢核等情事。

經櫃買中心查核發現該證券商為使用主機共置機房之證券商，有辦理主機共置服務未公平對待投資人、將主機共置機櫃空間提供第三人使用、未完整留存投資人委託資料紀錄與交易主機等系統登出入紀錄及其他

案例一~案情摘要

資安上缺失。故本公司於109年11月對使用主機共置機房之所有證券商進行資安專案查核作業。

案例一~違規及處置

缺失事項

1. 辦理主機共置服務未能公平對待投資人。
2. 有實質上將機櫃空間提供第三人使用。
3. 未完整留存客戶交易委託紀錄檔。
4. 主機共置服務網路連接證交所之設備未裝置防火牆或未落實定期檢視防火牆存取控管設定。
5. 未制定主機共置服務書面使用規則或未依其制定之主機共置使用規則辦理。
6. 將最高權限相當之帳號提供維運廠商使用。
7. 未定其變更交易主機帳號之密碼、未定期執行弱點掃描作業、未依規範寫程式更新紀錄表、未依規定完整保存主機共置機房主機系統之稽核日誌紀錄內容、未依規保

案例一~違規及處置

缺失事項

存防火牆進出紀錄及其備份、未能控管上線程式內容等情事。

案例一~違規及處置

違反規定

1. 證券商內部控制制度標準規範CA-11210、(一)、23。
2. 證券商內部控制制度標準規範CC-18000存取控制。
3. 證券商內部控制制度標準規範CC-17010網路安全管理。
4. 證券商內部控制制度標準規範CC-19000系統開發及維護。
5. 本公司主機共置服務管理辦法第11條、14條。
6. 本公司營業細則第75條第8款。
7. 本公司107年8月2日臺證作字第1070701866號函。

案例一~違規及處置

處置

公司部分：

1. 函請該公司注意改善，併課違約金新臺幣5~30萬元，並責成其落實內部控制制度之執行。
2. 函請該公司注意改善，並責成其落實內部控制制度之執行。
3. 暫停該公司主機共置服務，於改善完成後再向本公司申請恢復。

案例二~案情摘要

投資人檢舉證券商官網資安漏洞。

110年1至2月底陸續接獲主管機關轉民眾陳情，有四家證券商官網涉有資安漏洞應強化資訊安全等來函與資料影本。

案例二~案情摘要

檢舉人自行以偵測軟體從外部掃描證券商官網，發現並檢舉證券商有不同風險等級(高、中、低與LOG等級之修補建議事項)之弱點。

主管機關來函請證交所納入證券商資訊安全防護作業參考，並持續督導其落實執行資訊安全防護措施。

案例二~違規及處置

缺失事項：

1. 公司應定期(至少每半年一次)辦理資訊系統弱點掃描作業針對所辨識出之潛在系統弱點，應評估其相關風險或安裝修補程式， 並留存紀錄。
2. 應定期評估自身網路系統安全，並留存相關紀錄。
3. 定期或適時修補網路運作環境及作業系統之安全漏洞。

違反規定：

1. 證券商內部控制制度標準規範CC-17010網路安全管理。
2. 證券商內部控制制度標準規範CC-19000系統開發及維護。

處置：

1. 公司部分：請該公司注意改善。

近期法規宣導

一、設置副總層級資安長

二、落實資安通報機制

近期法規宣導

一、設置副總經理層級以上資訊安全長

1. 緣起:

- ✓ 配合行政院推動金融資安行動方案，強化資安監理。主管機關於110年9月30日金管證審字第1100363789號令修正發布第36條之2條文，各服務事業符合一定條件者，應指定副總經理層級以上或職責相當之人兼任資訊安全長，綜理資訊安全政策推動及資源調度事務；其一定條件，由主管機關定之。

近期法規宣導（續）

2. 設置條件:

- ✓ 第一級及第二級證券商:實收資本額達新台幣100億元以上。
- ✓ 電子下單達一定比率之證券商（包括：網際網路下單加計電子式專屬線路下單成交金額達公司成交金額60%、經紀業務成交金額市占率達全市場2%，且自然人客戶數達公司客戶數50%者），目前有國泰、新光、台新、華南永昌等4家證券商符合條件。

近期法規宣導（續）

- 3.證交所每年1月底前公告符合適用條件之證券商(名單 將公告於本公司「國內業務宣導網站」-「券商輔導」 - 「文件下載」 https://dsp.twse.com.tw/)

- 4.證券商獲悉符合適用條件後，應於每年3月底前設置完畢。

二、落實資安通報機制

- ✓ 106年4月26日主管機關證期(資)字第1060009117號函。
- ✓ 重申證券商針對與資訊系統相關之資訊安全或服務異常事件應依證券期貨市場資通安全事件通報應變作業注意事項，並採取適當矯正程序，留存紀錄。

感謝您的聆聽！

業務查核缺失案例分享

臺灣證券交易所
券商輔導部

報告大綱

壹、查核常見缺失

貳、案例介紹

常見查核缺失

一. 證券經紀商接受未經經濟部投資審議會核准賣出有價證券之華僑及外國人，開戶委託賣出有價證券

二. 業務人員利用客戶名義或帳戶，買賣有價證券

三. 內部人員原已開立之普通交易帳戶未予註銷

四. 未依「公布或通知注意交易資訊暨處置作業要點」之規定預收款券

五. 業務人員與客戶間有借貸款項、有價證券或為借貸款項、有價證券之媒介情事

六. 證券商受僱人代客戶保管款項、印鑑及存摺

七. 受託買賣業務員向客戶推介股票未依本公司「證券商推介客戶買賣有價證券管理辦法」規定辦理

常見查核缺失

八. 證券商電子交易系統發生故障而無法立即修復時，未立即依規向本公司通報

九. 辦理電子交易型態之受託買賣業務時，未就特殊身分客戶交易進行控管

十. 調閱客戶之開戶、徵信、交易、集保等相關資料，未依「證券商受僱人員查詢客戶資料管理作業要點」規定辦理

十一. 違反該券商自訂之「客戶申訴或檢舉案件處理作業流程表」規定

十二. 證券商未依其內部控制制度辦法辦理

案例介紹

案例一~案情摘要1

1. 投資人主張營業員與客戶有款項借貸、代操虧空及資金來源不明之情事，該分公司及主管應屬知情。
2. 經查與營業員有資金往來者計有33名投資人或民眾，所提供與營業員銀行往來資料之金額約1600萬元，其中13名客戶有提供多筆與營業員私人之銀行及郵局款項往來資料。

案例一~案情摘要2

3. 核有申購ETF基金及營業員表示賣出該基金虧損由其負擔之LINE截圖影像。
4. 16名客戶均表示，與營業員款項往來之原因為請其代操期貨或選擇權，且有2名客戶出具於其證券帳戶操作買進與賣出策略(期貨)之委任約定書影本

案例一~違規及處置

缺失事項：

1. 業務人員對客戶作贏利之保證。
2. 業務人員辦理承銷、自行或受託買賣有價證券時，有隱瞞、詐騙或其他足以致人誤信之行為。
3. 證券商負責人有未善盡督導管理之責情事。

違反規定：

1. 證券商負責人與業務人員管理規則第18條第2項第4款。
2. 證券商負責人與業務人員管理規則第18條第2項第10款。

處置結果：

1. 公司部分：函請公司注意改善，併科違約金10萬元整。
2. 受託買賣業務人員暫停執行業務6個月處置，惟因已往生，故不予處置。
3. 經理人暫停執行業務1個月處置。

案例二~案情摘要

A君陳情

於某證券商開立買賣之證券帳戶交易內容外流

案例二~違規及處置

缺失事項：

作業中心經理人接受高層以為聲請假執行所需為由，交辦部門業務人員查詢其某分公司A客戶之交易資料。

違反規定：

1. 證券商負責人與業務人員管理規則第18條第2項第2款。
2. 證券商受僱人員查詢客戶資料管理作業要點第7、8點。
3. 內部控制制度標準規範CA-11210受託買賣作業要點(四十一)。

處置：

1. 證券商注意改善，併課罰金暨責成其落實內部控制制度及加強員工對個資保護之教育訓練。
2. 違規之經理人及作業人員予以警告處置。

案例三~案情摘要

A上市司內部人電話告知營業員，其配偶帳戶下午要進行交易，擬盤後轉讓A公司股票500千股予特定人B，該筆交易已依規向主管機關申報。

嗣營業員準備鉅額交易檢核及錄音致電內部人詢問實際下單人及價格，併兩次強調以「鉅額交易」作為下單方式，內部人未異議，事後內部人主張申報轉讓方式為「盤後定價交易」 。

案例三~違規及處置

缺失事項：

受理上市A公司內部人以巨額配對方式賣出股票時，有未確認其轉讓對象須符合證交法第22條之2第1項第3款所定之特定人規定之情事。

違反規定：

1. 本公司營業細則第18條第2項。
2. 本公司97年10月28日臺證交字第0970205887號公告 。

處置：

1. 證券商注意改善。
2. 業務人員予以警告處置。

案例四~案情摘要1

內部稽核執行查核業務時發現：
營業員子女帳戶與客戶帳戶，買賣IP位置相同，
且買賣標的、數量雷同
惟一方為買方，另一方為賣方

案例四~案情摘要2

營業員A保管客戶甲之銀行及集保存摺、圖章，且利用客戶甲名義買賣有價證券，因客戶甲往生，請營業員B，使用手機採電子式交易賣出客戶甲帳戶內之股票，並使用營業員B未成年子名帳戶買進相同股票

案例四~缺失事項

缺失事項

營業員A

- 利用客戶名義或帳戶買賣有價證券
- 代客戶保管證券及銀行之存摺及圖章
- 為規避查核，將客戶地址填寫其本人地址(不同樓層)買賣代理人及緊急聯絡人填寫其本人家屬，有使人誤信行為

營業員B

- 知悉有利用他人名義買賣時，未拒絕接受委託買賣
- 將內部人98帳戶借予他人使用
- 證券商內部人代理或利用他人帳戶，進行網際網路委託買賣

案例四~違規及處置

違反規定：

- 證券商負責人與業務人員管理規則第18條第2項第7款、第10款、第11款。
- 內部控制制度標準規範CA-11210受託買賣作業要點(四十一)。
- 證券商內部人員在所屬證券商開戶委託買賣有價證券管理辦法第3條第1項。
- 證券商負責人與業務人員管理規則第18條第2項第17款。

處置：

1. 函請該公司注改善，併課違約金6萬元。
2. 營業員A及營業員B分別暫停執行業務6個月及1個月。

案例五及六~案情摘要

〈案例五〉

單一投資人連續2日申報違約金額達9.5億元

〈案例六〉

110年上半年申報客戶違約人次占集中市場36%

案例五及六~違規及處置

缺失事項：

證券商內部控制制度標準規範CA-11120客戶徵授信作業

違反規定：

本公司營業細則第135條第2項、第144條

處置：

<案例五>

函請該公司注意改善，併課違約金5萬；業務人員予以警告處置

<案例六>

函請該公司注意改善，併課違約金5萬

感謝您的聆聽！