

證券商經營自行買賣具證券性質之虛擬通貨業務之稽核

目錄

一、證券商經營自行買賣具證券性質之虛擬通貨業務之稽核(每日隨案處理).....	1
二、證券商經營自行買賣具證券性質之虛擬通貨業務之稽核(每週至少查核乙次)	3
三、證券商經營自行買賣具證券性質之虛擬通貨業務之稽核(每月至少查核乙次)	6
四、證券商經營自行買賣具證券性質之虛擬通貨業務之稽核(每季至少查核乙次)	11
五、證券商經營自行買賣具證券性質之虛擬通貨業務之稽核(每半年至少查核乙次)	12
六、證券商經營自行買賣具證券性質之虛擬通貨業務之稽核(每年至少查核乙次)	14

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	定期(每日隨案處理)	<p>一、交易及給付結算方式：</p> <p>(一)公司之報價是否符合下列規範：</p> <ol style="list-style-type: none"> 1.報價為參考報價，提供買進及賣出之雙邊報價，成交价格由公司與客戶自行議定。 2.本於專業判斷提供合理之報價，並視市場情況有效調節市場之供求關係，不得提供偏離合理價格之報價，損及公正價格之形成。 <p>(二)公司是否每日將虛擬通貨之異動及餘額明細等資料傳送至證券集中保管事業指定之資訊申報系統；發現不符時，是否與證券集中保管事業共同查明原因更正之。</p> <p>二、公司於交易平台自行發行虛擬通貨：</p> <p>(一)公司進行報價及議價買賣時，是否特別注意價格之合理性，並符合公司所訂定之報價決定依據及議價成交原則。</p> <p>三、資通安全作業：</p> <p>(一)發生重大影響客戶權益或正常營運之資訊服務異常事件或資通安全事件，公司是否於知悉事件三十分鐘內，於「證券期貨市場資通安全通報系統」，辦理事件初步通報，並分別於查明事件及事件處理完成後，辦理正式通報及事件</p>	

編 號	作業項目及目的	作業週期	作 業 程 序 (方 法) 及 稽 核 重 點	依 據 資 料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	定 期 (每 日 隨 案 處 理)	解除通報。 (二)公司發生資安事件時，是否依資訊安全事件管理程序辦理。 四、營業糾紛及訴訟之處理作業： (一)公司與客戶發生交易糾紛時，是否由業務單位會同內部稽核人員依規定處理程序辦理，並於事後留存完整之處理報告紀錄。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	不定期(每週至少查核乙次)	<p>一、財務、業務管理及資訊申報：</p> <p>(一)公司是否未投資非於公司交易平台辦理發行之虛擬通貨。</p> <p>(二)公司持有任一發行人虛擬通貨之成本總額，是否未超過證券商管理規則第十九條規定之限額。</p> <p>二、發行程序及管理：</p> <p>(一)公司是否督促發行人，或是否於公司自行發行時確實依虛擬通貨管理辦法第三十七條及第三十八條規定辦理資訊揭露，並持續提供及維護資訊揭露專區供其揭露。</p> <p>(二)發行人有虛擬通貨管理辦法第四十條第一項所訂情事之一者，公司是否即公告其自公告日之次五營業日起停止虛擬通貨於公司交易平台買賣。</p> <p>(三)發行人有虛擬通貨管理辦法第四十條第四項所訂情事之一者，公司是否即公告其自公告日之次四十日起終止虛擬通貨於交易平台買賣。</p> <p>三、交易及給付結算方式：</p> <p>(一)公司與專業投資人之自然人進行議價買賣時，是否先檢核其持有單一虛擬通貨之庫存餘額成本加計當筆交易擬議定之成交金額合計數未逾新臺幣三十萬元。</p>	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	不定期(每週至少查核乙次)	<p>(二)公司與客戶議價買賣虛擬通貨，同一營業日買進及賣出單一虛擬通貨之成交數量合計是否未逾該虛擬通貨流通在外數量之百分之五十。</p> <p>(三)公司是否執行虛擬通貨管理辦法第四十九條規定之價格穩定機制與強化資訊揭露機制。</p> <p>(四)公司與客戶議價買賣虛擬通貨，是否對客戶預先收足買進之款項或賣出之虛擬通貨，是否經公司評估客戶信用狀況後始免預收。</p> <p>(五)公司於與客戶議價買賣虛擬通貨成交者，是否採即時逐筆給付結算方式與客戶完成款項與虛擬通貨之收付，並製發買賣成交紀錄予客戶。</p> <p>四、公司於交易平台自行發行虛擬通貨：</p> <p>(一)公司議價買賣需要在交易平台議價買賣自行發行之虛擬通貨，每日庫存餘額是否未超過流通在外數量之百分之三，如有超額情事是否於三個營業日內改善完成。</p> <p>五、資通安全作業：</p> <p>(一)公司是否建立病毒偵測機制並更新病毒碼。</p> <p>(二)公司是否 <u>就提供外部連線使用之系統</u> 偵測網頁與程式異動並留存異動紀錄，非預期性異動是否即時通知相關人員處</p>	

編 號	作業項目及目的	作業週期	作 業 程 序 (方 法) 及 稽 核 重 點	依 據 資 料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	不 定 期 (每週至少查核乙次)	理。 六、防制洗錢作業： (一) 疑似洗錢或資恐交易之申報 1.公司對於經檢視屬疑似洗錢或資恐交易者，及依資恐防制法對經指定制裁對象之財物或財產上利益及所在地之通報，是否於知悉後即依法務部調查局所定之通報格式及方式，簽報專責主管核定，並向法務部調查局通報，核定後之通報期限不得逾二個營業日。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
		不定期(每月至少查核乙次)	<p>一、財務、業務管理及資訊申報：</p> <p>(一)公司之財務比率、資金運用及投資是否符合下列規定： (證券商僅經營虛擬通貨業務者適用)</p> <ol style="list-style-type: none"> 1. 對外負債總額不得超過其淨值。 2. 資金不得貸與他人或移作他項用途，資金之運用，以下列為限： <ol style="list-style-type: none"> (1) 新臺幣銀行存款。 (2) 購買政府債券或金融債券。 (3) 購買國庫券、可轉讓之銀行定期存單或商業票據。 (4) 其他經櫃檯買賣中心核准之用途。 3. 不得轉投資證券、期貨、金融及其他事業。 <p>二、客戶註冊程序、契約簽訂及身分驗證：</p> <p>(一)公司於接受客戶認購及議價買賣虛擬通貨，是否完成下列程序：</p> <ol style="list-style-type: none"> 1. 盡合理調查之責任，並向投資人取得合理可信之佐證依據，審核客戶符合專業投資人之條件。 2. 要求客戶於交易平台完成註冊。 	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
		不定期(每月至少查核乙次)	<p>3. 確認客戶已簽訂開戶契約及風險預告書。</p> <p>(二) 客戶首次參與認購及議價買賣虛擬通貨，公司是否先確認客戶以本人名義於金融機構開立款項收付之帳戶，並透過該帳戶以新臺幣匯出、入款方式交付或收受款項。</p> <p>(三) <u>客戶於網路下單登入時是否採多因子認證方式，以確保為本人登入。</u></p> <p>三、發行程序及管理：</p> <p>(一) 發行人發行之虛擬通貨種類，是否以不具有股東權益之分潤型及債務型虛擬通貨為限，募集之資金及發行後分配之利潤或利息是否以新臺幣為限，同次發行之虛擬通貨，其發行條件是否相同，且價格是否歸一律。</p> <p>(二) 公司受理發行人辦理發行虛擬通貨前，是否先確認該發行人僅透過公司交易平台辦理發行虛擬通貨，其累計募資金額是否未逾新臺幣三千萬元。</p> <p>(三) 公司是否履行盡職調查程序確認發行人符合虛擬通貨管理辦法第二十九條之規定，內部稽核人員是否覆核該盡職調查程序依規定執行及落實後，始將相關資訊揭示於公司交易平台。(請隨案查核)</p> <p>(四) 發行人買回其發行之虛擬通貨，公司是否確認其符合下列</p>	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
		不定期(每月至少查核乙次)	<p>規定：</p> <ol style="list-style-type: none"> 1. 已於公開說明書揭露虛擬通貨買回機制。 2. 該虛擬通貨已在公司交易平台交易滿一年。 3. 經其董事會三分之二以上董事出席及出席董事超過二分之一同意，並於公司交易平台買回。 4. 應於依虛擬通貨管理辦法第三十七條輸入公司資訊揭露專區之即日起算二個月內執行完畢。 5. 買回後立即辦理註銷。 6. 買回虛擬通貨後，如流通在外數量低於原發行數量之百分之十者，公司公告終止該虛擬通貨之買賣。 <p>(五)專業投資人之自然人每一虛擬通貨募資案認購金額是否未逾新臺幣三十萬元。</p> <p>(六)發行人辦理發行虛擬通貨募資期間，發生足以影響其繼續營運之重大情事，或其他櫃檯買賣中心認為有必要之原因者，公司是否立即停止其透過交易平台之募資。</p> <p>四、交易及給付結算方式：</p> <p>(一)公司是否依客戶別分別設置虛擬通貨之登載、移轉及保管機制，憑以辦理客戶虛擬通貨之收付、異動及庫存保管等事宜。</p>	

編 號	作業項目及目的	作業週期	作 業 程 序 (方 法) 及 稽 核 重 點	依 據 資 料
		不 定 期 (每 月 至 少 查 核 乙 次)	<p>五、公司於交易平台自行發行虛擬通貨：</p> <p>(一) 公司非因議價買賣需要，買回其自行發行之虛擬通貨，是否符合下列規範：</p> <ol style="list-style-type: none"> 1. 已於公開說明書揭露虛擬通貨買回機制。 2. 該虛擬通貨已在公司交易平台交易滿一年。 3. 經公司董事會三分之二以上董事出席及出席董事超過二分之一同意，並於公司交易平台買回。 4. 應於依虛擬通貨管理辦法第三十七條輸入公司資訊揭露專區之即日起算二個月內執行完畢。 5. 買回後立即辦理註銷。 6. 買回虛擬通貨後，如流通在外數量低於原發行數量之百分之十者，公告終止該虛擬通貨之買賣。 <p>(二) 專業投資人之自然人每一虛擬通貨募資案認購金額是否未逾新臺幣三十萬元。</p> <p>(三) 募資期間，發生足以影響公司繼續營運之重大情事，或櫃檯買賣中心認為有必要之原因者，公司是否立即停止其透過交易平台之募資。</p> <p>六、資通安全作業：</p> <p>(一) 公司是否建立私密金鑰管理程序，明訂並落實私密金鑰</p>	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
		不定期(每月至少查核乙次)	<p>遺失、重新核發、停用、銷毀、備份等處理機制。</p> <p>(二) 公司是否將營運設備置放於機房內，並建立門禁管制、環境監控機制。</p> <p>(三) 公司是否審查機房進出登記紀錄，如有異常時是否適當處置。</p> <p>(四) 公司是否建立系統開發暨變更管理作業程序並遵循變更控制程序，由二人以上進行變更(如:執行、覆核)且依據正式核准之程序辦理。</p> <p>(五) 公司是否於交易平台程式上線前，針對異動程式進行程式碼掃描或黑箱測試。</p> <p>(六) 公司是否對系統軟體與應用軟體進行相關安全更新與修補。</p> <p>(七) 公司對於虛擬通貨作業環境與其他網路間之連線是否透過防火牆或路由器進行控管。</p> <p>(八) 網路設備之設定是否經權責主管之核准。</p> <p>(九) <u>公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣是否即通知客戶，並留存紀錄，避免非客戶本人登入情事：(1) 密碼輸入錯誤或帳戶被鎖定；(2)申請或更新憑證；(3)變更基本資料；(4)異常來源或行為嘗試登入等；(5)密碼申請異動或補發時。</u></p>	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
			<p>(十) <u>公司是否依其所屬資安分級對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，並定期檢視以確認機制有效運作：(1) 同一來源 IP 登入不同帳號達一定次數以上；(2) 同一帳號在一定時間內由不同國家登入；(3) 異常來源 (如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單或國外 IP)嘗試登入。</u></p> <p>七、防制洗錢作業：</p> <p>(一)公司是否按所訂防制洗錢及打擊資恐計畫，辦理確認客戶身分、客戶及交易有關對象之姓名及名稱檢核、帳戶及交易之持續監控及紀錄保存。</p>	

編 號	作業項目及目的	作業週期	作 業 程 序 (方 法) 及 稽 核 重 點	依 據 資 料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	不 定 期 (每季至少查核乙次)	一、資通安全作業 (一)公司是否辦理資訊安全查核作業，並針對前開之資訊安全查核報告辦理追蹤改善情形。 (二)公司是否分析異常稽核軌跡紀錄，設定合適告警指標並檢討修訂。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	不定期(每半年至少查核乙次)	<p>一、資通安全作業：</p> <p>(一)公司是否建立開源軟體使用規範，並重新評估其安全性。</p> <p>(二)公司是否對交易平台進程式碼掃描或黑箱測試。</p> <p>(三)公司是否進行弱點掃描，並針對其掃描或測試結果進行風險評估，針對不同風險訂定適當措施及完成時間，填寫評估結果與處理情形，採取適當措施並確保作業系統及軟體安裝經測試且無弱點顧慮之安全修補程式。</p> <p>(四)公司是否審查帳號與權限之合理性，人員離職或調職時是否及時更新權限，以符合職務分工與牽制原則。</p> <p>(五)<u>公司是否建立系統最高權限帳號管理辦法，使用最高權限帳號時是否取得權責主管同意，並留存相關紀錄。</u></p> <p>(六)公司是否建立回存測試機制，以驗證備份之完整性及儲存環境之適當性。</p> <p>(七)公司是否定期檢視防火牆存取控管設定。</p> <p>(八)公司對於防火牆進出紀錄及備份是否至少保存三年。</p> <p>(九)公司是否保留必要交易相關紀錄、操作紀錄(包含應用系統及作業系統等)之軌跡資料至少十年以上，並確保其真實性及完整性。</p>	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	不定期(每半年至少查核乙次)	二、防制洗錢作業： (一)洗錢及打擊資恐內部控制制度 1. 公司是否依洗錢與資恐風險及業務規模，並參酌證券商業同業公會「證券商防制洗錢及打擊資恐注意事項範本」訂定相關注意事項及建立防制洗錢及打擊資恐之內部控制與稽核制度，經董事會通過，並定期檢討是否有修正之必要。 2. 公司相關內部控制制度內容是否包括依據「證券商評估洗錢及資恐風險及訂定相關防制計畫指引」，訂定對洗錢及資恐風險進行辨識、評估、管理之相關政策及程序，及依該指引與風險評估結果暨業務規模訂定防制洗錢及打擊資恐計畫，以管理及降低已辨識出之風險，並對其中之較高風險，採取強化控管措施。 3. 有關洗錢及資恐風險之辨識、評估與管理，是否至少涵蓋客戶、地域、產品及服務、交易或支付管道等面向，並製作風險評估報告，送主管機關備查。 4. 有關防制洗錢及打擊資恐計畫，是否包括確認客戶身分、客戶及交易有關對象之姓名及名稱檢核、帳戶及交易之持續監控、紀錄保存、疑似洗錢或資恐交易申報	

編 號	作業項目及目的	作業週期	作 業 程 序 (方 法) 及 稽 核 重 點	依 據 資 料
			等之政策、程序及控管機制。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	不定期(每年至少查核乙次)	一、資通安全作業： (一) <u>公司是否對自行或委外開發之資訊系統完成資訊系統分級，資訊系統等級是否至少區分核心與非核心系統，每年是否至少檢視一次資訊系統分級妥適性。</u> (二) 公司是否評估電腦系統容量及安全措施之機制與程序，並對系統容量進行壓力測試。 (三) 公司是否每年對 <u>提供網際網路服務之</u> 交易平台執行滲透測試。 (四) <u>公司是否建立入侵偵測及防禦機制並定期更新惡意程式行為特徵。</u> (五) <u>公司是否建立應用程式防火牆。</u> (六) 公司是否訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序及導入流量清洗機制並每年定期演練。 (七) 公司是否對資訊人員(系統管理及程式開發人員)進行系統安全管理及安全程式開發之教育訓練。 (八) 公司是否對所有具證券性質之虛擬通貨相關從業人員定期執行資安認知、電子郵件社交工程演練、洗錢防制及反詐騙相關教育訓練。 (九) 資通安全專責人員是否持有二張以上資通安全專業證照，並持續維持證書之有效性。	

編號	作業項目及目的	作業週期	作業程序(方法)及稽核重點	依據資料
AA-19F10	證券商經營自行買賣具證券性質之虛擬通貨業務之稽核 目的： 確定上述作業是否符合規定辦理	不定期(每年至少查核乙次)	<p>(十) 公司 <u>作業委託他人處理</u> 是否 <u>簽訂書面契約，並依「證券商作業委託他人處理應注意事項」辦理。</u></p> <p>(十一) 公司是否每年驗證及演練其營運持續性控制措施，並保留相關演練紀錄及召開檢討會議。</p> <p>(十二) 公司是否依「個人資料保護法」稽核個人資料管理情形。</p> <p>(十三) 公司使用雲端服務處理之客戶資料及其儲存地，是否以位於我國境內為限並依內部控制制度標準規範要求使用雲端服務。</p> <p>二、防制洗錢作業：</p> <p>(一) 公司是否依證券暨期貨市場各服務事業建立內部控制制度處理準則規定辦理下列事項之查核，並提具查核意見。</p> <ol style="list-style-type: none"> 1. 洗錢及資恐風險評估與防制洗錢及打擊資恐計畫是否符合法規要求並落實執行。 2. 防制洗錢及打擊資恐計畫之有效性。 <p>(二) 查核報告有缺失者，是否要求作業單位出具改善計畫並追蹤至改善完畢止。</p> <p>(三) 疑似洗錢或資恐交易之申報：是否於會計年度終了後 15</p>	

編 號	作業項目及目的	作業週期	作 業 程 序 (方 法) 及 稽 核 重 點	依 據 資 料
			日內將上一年度所申報之態樣項目及其件數，函報目的事業主管機關備查，並副知證交所、櫃檯買賣中心及證券商公會。	