會計師出具資訊系統及安全控管作業評估報告原則性規範

前言

為配合財團法人中華民國證券櫃檯買賣中心（以下簡稱本中心）「證券商經營自行買賣具證券性質之虛擬通貨業務管理辦法」第二十二條規定，證券商向本中心申請設置或遷移營業處所時及每會計年度終了後三個月內，應由會計師出具資訊系統及安全控管作業評估報告，本中心爰訂定「會計師出具資訊系統及安全控管作業評估報告原則性規範」，以利各會計師執行查核作業。

本規範旨在提供會計師對經營自行買賣具證券性質之虛擬通貨業務證券商出具資訊系統及安全控管作業評估之基本查核，各會計師依本規範辦理查核時，仍應考量受查證券商之規模、業務範圍及其風險，蒐集充分及適切之證據，俾憑提出具體結論意見。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
一、 組織與人員管理	(一) 公司應指派一人為主管，負責資訊安全之協調督導事宜，並設置至少一名經營自行買賣虛擬通貨業務之資訊安全專責人員，專門負責資訊安全相關工作或職務。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務管理辦法第 9 條 2. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範二、(三)、5	1. 取得公司組織圖、資訊部門之組織圖及工作職掌說明文件，檢查資訊部門作業分工規劃並確認資訊安全主管及人員編制是否合規。 2. 檢查資訊安全專責人員工作職務內容，確認有無兼任資訊相關或利益衝突之工作。
	(二) 資訊安全專責人員應取得二張以上資通安全專業證照並持續維持證照之有效。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務管理辦法第 9 條 2. 參酌資通安全責任等級分級辦法-B 級之特定非公務機關	1. 取得資訊安全專責人員持有之資通安全專業證照。 2. 檢查資訊安全專責人員持有之專業證照是否符合行政院國家資通安全會報網站所公告之「資通安全專業證照」列表，並確認是否具有效性。
二、 客戶註冊程序、契約簽訂及身分驗證	(一) 公司應訂定受理客戶身分驗證機制，至少包含下列措施： 1. 受理客戶註冊時，所採行之身分確認程序設計安全管控措施： (1). 確認行動電話號碼：確認客戶可操作並接收訊息通知。 (2). 確認於金融機構開立款項收付帳戶之持有人與註冊之客戶相符：應向金融機構查詢或確認該帳戶持有人之資料與註冊客戶之資料相符。 (3). 確認證明文件影本：得採上傳或拍照方式取	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範四、(五)、1 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第 4 條	1. 取得公司訂定客戶身分驗證機制文件，確認客戶註冊時，所採行之身分確認程序設計安全管控措施。 2. 檢查公司確認客戶註冊之行動電話號碼係可操作並接收訊息通知、確認客戶於金融機構開立款項收付帳戶之持有人與註冊之客戶相符及確認證明文件影本為完整清晰可辨識之影像檔。 3. 檢查證明文件電子影像檔處理及

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	得完整清晰可辨識之影像檔，並足資識別為本人申請。		儲存機制，抽核已儲存之影像檔並確認儲存方式、存取權限管制、儲存地點是否合宜。
	2. 公司應提供客戶以帳號加上固定密碼、或簡訊傳送一次性密碼、或雙因子認證(Two Factors Authentication)含以上等安全登入方式，並依客戶操作場景進行風險評估，針對登入所採行之身分確認程序設計安全管控措施。帳號及採用固定密碼之安全設計如下： (1).帳號如使用顯性資料(如商業統一編號、身分證統一編號、行動電話、電子郵件帳號等)作為唯一之識別，應另行增設使用者代號以資識別。使用者代號亦不得為上述顯性資料。 (2).密碼不應少於六位，且不應與帳號相同，亦不得與使用者代號相同。 (3).密碼不應訂為相同之英數字、連續英文字或連號數字。 (4).密碼建議應採英數字混合使用，且宜包含大小寫英文字母或符號。 (5).密碼連續錯誤達五次時應限制使用，須重新	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範四、(五)、2 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第5條	1. 取得公司提供客戶所採行之身分確認程序設計安全管控措施。 2. 檢查公司固定密碼之安全設計： (1).檢查若帳號設計為顯性資料(如商業統一編號、身分證統一編號、行動電話號碼、電子郵件帳號等)，客戶是否需另行設定使用者代號。 (2).若須設定使用者代號，檢查使用者代號是否可為顯性資料。 (3).檢查公司密碼設定規則： A. 密碼不應少於六位，且不應與帳號相同，亦不得與使用者代號相同； B. 密碼不應訂為相同之英數字、連續英文字或

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	申請密碼。 (6).變更後之密碼不得與變更前一次密碼相同。 (7).密碼超過一年未變更，公司應做妥善處理。 (8).安全登入方式，應符合下列要求： A. 應設計防止惡意程式假冒機器人交易，以確保交易安全。 B. 公司若提供以客戶所擁有之設備(如行動裝置、硬體式虛擬通貨錢包等)作為登入交易平台之方式時，公司應確認該設備為該客戶已於公司約定登錄之設備。		連號數字； C. 密碼複雜度(是否採英數字混合使用，且宜包含大小寫英文字母或符號)； D. 密碼連續錯誤五次時，是否限制使用，並確認重新申請密碼的機制。 E. 密碼變更歷程次數。 (4).檢查使用者密碼超過一年未變更，是否主動通知或於下次使用者登入時通知或強迫變更密碼。 3. 檢查公司簡訊傳送一次性密碼(One Time Password, OTP)機制： (1).簡訊傳送OTP的傳送機制。 (2).簡訊傳送OTP的有效時間。 (3).密碼之保護機制。(如：防止簡訊遭竊取或轉發的情況發生。) 4. 檢查公司雙因子認證(Two Factors Authentication)含以上使用之技術及其登入流程。 5. 如提供客戶擁有之設備作為登入交易平台，檢查公司是否確認該設備為該客戶於公司約定登錄之設備。
	(二) 公司對於客戶帳戶相關電子資料應設置存取	1. 證券商經營自行	1. 取得客戶帳戶相關電子資料存

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	權限，並定期更新，且應建立定期監控機制，對於異常存取活動應查明原因，即時檢討改善，防止不當洩露客戶資訊。	買賣具證券性質之虛擬通貨業務內部控制制度標準規範四、(六) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第13條	取權限設定與監控機制。 2. 檢查客戶帳戶與電子錢包之間的對應關係，並抽核交易紀錄，確認交易紀錄內所記載的帳戶與電子錢包的對應是否與公司提供資訊一致。 3. 檢查公司監控異常條件設定是否適當，及發生異常狀況時，是否查明原因，並進行檢討改善。
三、 資通安全作業	(一) 公司應盤點與資訊安全相關法規規定，並將相關資訊安全要求與內部控制制度結合。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(一) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第23條	1. 取得資訊安全相關法規規定清單。 2. 檢查公司是否適時盤點資訊安全相關規定並更新內部控制制度。
	(二) 公司應依據法令規定、內部控制制度及業務需求，訂定資訊安全政策，據以評估風險並建立各項資訊安全管理機制，以確保虛擬通貨發行及交易之安全措施有效性。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務管理辦法第23條 2. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(二)	1. 取得公司訂定之資訊安全政策。 2. 檢查公司資通安全政策是否包含相關資安法令規定、內部控制制度及業務需求。
	(三) 公司應訂定定期（每年至少一次）由內部或	1. 證券商經營自行	1. 取得公司訂定之電腦系統容量

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	委託外部專業機構評估電腦系統容量及安全措施之機制與程序，定期對系統容量進行壓力測試，並留存紀錄。	買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(三) 2. 參酌「建立證券商資通安全檢查機制」7	及安全措施之機制與程序。 2. 檢查公司是否定期對系統容量進行壓力測試並留存紀錄。
	(四) 公司應訂定定期（每季至少一次）由內部或委託外部專業機構辦理資訊安全查核作業，並應留存查核紀錄，並針對前開之資訊安全查核報告辦理追蹤改善情形（包括查核摘要、查核範圍、缺失說明及改進建議等）。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(四) 2. 參酌「建立證券商資通安全檢查機制」11	檢查公司資訊安全年度查核計畫、查核報告及追蹤改善情形。
	(五) 營運設備應置放於機房內，機房應建立門禁管制、環境監控機制；進出登記紀錄應定期審查，如有異常應適當處置。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(五) 2. 參酌「建立證券商資通安全檢查機制」6 3. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第15條	1. 取得營運設備或機房門禁管理程序。 2. 實地觀察主要營運系統之機房，確認機房實體環境安全防護設備（如：防火、防水、空調、不斷電系統、環控系統等）及營運設備配置情況。 3. 檢查公司有關營運設備異動申請與機房進出登記紀錄是否依程序辦理。 4. 檢查公司機房進出登記紀錄，異常時是否依程序辦理。 5. 如非自建機房者，取得並檢查託管機房之合約、託管機房最近一

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
			期相關之專業第三方實體安全或資訊安全查核報告。
	(六) 金鑰管理 1. 公司應妥善管理客戶的私密金鑰，並保存每一筆認購及交易紀錄以備日後查詢。(公司受託管理客戶私密金鑰時適用) 2. 公司應評估私密金鑰儲存地點之安全性，並僅允許必要之管理人員存取私密金鑰，確實管理並降低私密金鑰外洩的可能性。(公司受託管理客戶私密金鑰時適用) 3. 公司應明確告知客戶私密金鑰相關之權益、管理方式及可能風險。 4. 公司應建立私密金鑰管理程序，明訂並落實私密金鑰遺失、重新核發、停用、銷毀、備份等處理機制。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(六) 2. 參酌現行實務及「電子支付機構資訊系統標準及安全控管作業基準辦法」第 14 條	1. 取得該公司訂定之私密金鑰管理程序，檢查是否明定並落實私密金鑰遺失、重新核發、停用、銷毀、備份等處理機制。 2. 檢查公司金鑰的產生方式、金鑰的長度、金鑰加解密方式是否妥適。 3. 檢查公司對於認購及交易紀錄是否妥善管理並抽核確認其正確性。 4. 檢查客戶私密金鑰儲存地點(公司受託管理客戶私密金鑰時適用)。 5. 檢查公司是否告知並確認客戶知悉私密金鑰相關之權益、管理方式及可能風險，告知紀錄是否留存。
	(七) 系統開發生命週期管理 1. 公司應建立系統開發暨變更管理作業程序，於開發階段起至營運階段，遵循變更控制程序處理並留存相關紀錄；營運環境變更（如執行、覆核）應由二人以上進行，以相互牽制並依據經過正式核准之程序辦理變更。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、1 2. 參酌「建立證券商資通安全檢查機制」9 3. 參酌「電子支付	1. 取得公司系統開發暨變更管理作業程序。 2. 詢問相關人員確認正式環境之參數、程式原始碼、執行碼及網頁變更是否由兩人以上執行(如執行、覆核）後，始得變更，覆核時是否有考量職務分工與牽制原則。 3. 抽核變更紀錄(含「虛擬通貨利用程式碼自動執行之內容」)是

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		機構資訊系統標準及安全控管作業基準辦法」第17、19條	否符合變更管理作業程序，並確認變更程序之合理性，包含是否填寫變更申請書，取得正式核准後進行變更作業。 4. 檢查公司程式變更是否經過需求單位測試（留存測試紀錄）並經正式核准。
	2.系統軟體變更應先進行技術審查並測試；套裝軟體不應自行異動，並應先進行風險評估；程式不應由開發人員自行換版或產製比對報表，應建立程式原始碼管理機制，以符合職務分工與牽制原則。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、2 2. 參酌參酌「建立證券商資通安全檢查機制」9 3. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17、19條	1. 檢查公司系統軟體變更紀錄是否有於變更前執行技術審查並進行測試，確認其變更(含技術審查、測試紀錄)紀錄是否妥適。 2. 檢查公司套裝軟體管理機制。 3. 檢查公司程式原始碼管理機制。 4. 檢查公司程式或參數之變更，是否由非開發人員異動程式或產製比對報表，並抽核程式異動或參數異動紀錄，以確認是否符合職務分工與牽制原則。
	3.應建立開源軟體使用規範，引用開源軟體時應注意是否有相關安全漏洞，並應定期重新評估其安全性。	證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、3	1. 取得公司訂定的開源軟體使用規範。 2. 檢查公司對於開源軟體使用的情況，並檢查是否定期評估其安全性。
	4.虛擬通貨交易平台之設計原則，應符合下列要求： (1).網際網路應用系統設計要求：	1. 證券商經營自行買賣具證券性質之虛擬通貨業務	檢查網路傳輸封包，確認機敏資料於網際網路傳輸時是否全程加密。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	A.機敏資料於網際網路傳輸時應全程加密；	內部控制制度標準規範八、(七)、4、(1) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第10條	
	B.應設計連線控制及網頁逾時中斷之機制，逾時未使用時應中斷連線；	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、4、(1) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第10條	1. 取得公司設計連線控制及逾時中斷機制之說明文件。 2. 檢查公司虛擬通貨交易平台，如未操作網頁逾公司設定的時間時，是否確實中斷連線。
	C.應進行客戶身分確認，執行交易時須採用一次性亂數或時間戳記，以防止重送攻擊。前述所指之一次性亂數，如需使用亂數函數進行運算時，須採用安全亂數函數產生所需之亂數；	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、4、(1) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第	1. 檢查公司網頁(WEB)或行動應用程式(APP)軟體開發過程中之相關文件(如：系統需求規格、系統分析及設計規格、測試報告等)，於客戶身分確認與交易機制時是否增加一次性亂數或時間戳記等安全設計。 2. 如有使用亂數函數作為安全設計，檢查其是否使用隨機、不可預測等安全亂數的方式產生所

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		10 條	需亂數。
	D. 客戶密碼應於加密後儲存，不得以明碼方式儲存於資料庫；	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、4、(1) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第10 條	1. 取得公司密碼儲存機制,瞭解密碼是否以加密方式儲存。 2. 檢查客戶密碼儲存是否確實非以明碼方式儲存於資料庫。
	E. 應設計客戶修改個人資料、約定或變更所設定之金融帳戶資訊時，須先進行身分確認後，始可受理變更；	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、4、(1) 2. 參酌「電子支付機構資訊系統標準及安全控管作	1. 檢查公司是否設計客戶修改個人資料、約定或變更所設定之金融帳戶資訊時,須先進行身分確認後，始可受理變更之規定。 2. 抽查客戶變更身分基本資料(如：姓名、國籍、身分證明文件編號、出生年月日)時，是否重新進行身分確認程序。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		業基準辦法」第10條	
	F.應設計客戶個人資料顯示之隱碼機制；	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、4、(1) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第10條	1. 取得個人資料檔案及資料庫之管理規範，並檢查公司是否訂定個人資料隱碼規則。 2. 檢查並比對正式系統畫面設計，確認已依規則進行隱碼。
	G.應設計客戶個人資料檔案及資料庫之存取控制與保護監控措施。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、4、(1) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第10條	1. 取得公司訂定個人資料檔案及資料庫之存取控制與保護監控措施。 2. 檢查具證券性質之虛擬通貨業務作業環境，確認是否符合前項控制措施要求。
	(2).行動裝置應用程式設計要求： A.於發布前檢視行動裝置應用程式所需權限應與提供服務相當；首次發布或權限變動，應經相關部門同意，以利綜合評估是否符合個人資料保護法之告知義務。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、	公司如提供行動裝置應用程式供客戶使用時： 1. 檢查公司行動裝置應用程式係自行開發或委外開發。如為委外，取得委外開發契約。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	B.應於官網上提供行動裝置應用程式之名稱、版本與下載位置。 C.啟動行動裝置應用程式時，如偵測行動裝置疑似遭破解，應提示使用者注意風險。 D.行動裝置應用程式設計要求應符合中華民國證券商業同業公會所訂定之「中華民國證券商業同業公會新興科技資訊安全自律規範」及「證券期貨市場相關公會新興科技資訊安全管控指引」。	(七)、4、(2) 2. 參酌「中華民國證券商業同業公會新興科技資訊安全自律規範」 3. 參酌「證券期貨市場相關公會新興科技資訊安全管控指引」 4. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第10條 5. 中華民國證券商業同業公會新興科技資訊安全自律規範 6. 證券期貨市場相關公會新興科技資訊安全管控指引	2. 檢查公司委外開發是否取得行動應用程式原始碼，如無取得原始碼，是否要求委外廠商提供安全要求佐證文件(如：確保程式未含惡意程式碼、程式碼未含敏感性資料、行動應用程式是否定義特殊符號篩選機制)。 3. 檢查安裝行動應用程式時，實際授權項目與告知客戶內容是否一致。 4. 檢查公司行動應用程式發布與權限變動時，是否符合個人資料保護法之告知義務，並抽核行動應用程式發布時相關文件，確認是否確實評估。 5. 檢查公司官網是否有提供行動裝置應用程式之名稱、版本與下載位置等資訊。 6. 檢查公司偵測行動裝置疑似遭破解時，是否提示使用者注意風險。 7. 取得公司行動應用程式之發佈、控管規範與管理辦法。 8. 檢查公司行動應用程式安全控管要求： (1).行動應用程式對交易或帳務等敏感性資料之存取驗證機制。 (2).行動應用程式發送簡訊或

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
			其他訊息通知方式告知使用者敏感性資料時，去識別化機制。 (3).檢查透過行動應用程式傳送帳號、密碼及其他敏感性資料時，是否以憑證驗證或加密機制確保傳送安全。 (4).檢查透過行動應用程式儲存密碼、憑證、交易或帳務等敏感性資料時，是否對儲存之資料進行雜湊（Hash）或加密控管保護。 (5).檢查透過行動應用程式處理交易或金流作業時，是否有留存存取日誌並限制未經授權存取。 9. 檢查公司行動應用程式之發佈至 Apple Store 及 Google Store 權限是否妥適。 10. 檢查公司行動裝置應用程式資安檢測報告內容，是否符合上述行動應用程式安全控管要求之規定。
	(3).如採用 QR Code 或其他以掃描方式取代人工輸入虛擬通貨錢包地址時，應用程式應以彈出式視窗或其他方式提供使用者檢視資料內容。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、4、(3)	公司如採用 QR Code 或其他以掃描方式取代人工輸入虛擬通貨錢包地址時，檢查應用程式是否以彈出式視窗或其他方式提供使用者檢視資料內容。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		2. 參酌「金融機構提供 QR Code 掃描支付應用安全控管規範」第 4 條	
	(4).採用 QR Code 或其他取代人工輸入方式所解析與生成之終端裝置，對所產生之網站連結，應採包括但不限於白名單或伺服器認證等機制進行網站合法性檢查，以預防連結惡意網站或執行惡意程式風險。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、4、(4) 2. 參酌「金融機構提供 QR Code 掃描支付應用安全控管規範」第 9 條	公司如採用 QR Code 或其他取代人工輸入方式所解析與生成之終端裝置，檢查其對所產生之網站連結，所採行預防連結惡意網站或執行惡意程式的機制，是否包括但不限於白名單或伺服器認證等機制進行網站合法性檢查。(預防中間人攻擊)
	(5).交易平台上線前應針對異動程式及每半年進行程式碼掃描或黑箱測試，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，記錄矯正處理情形並追蹤改善。	證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(七)、5	1. 取得公司訂定程式上線管理作業程序、程式碼掃描或黑箱測試管理規範。 2. 檢查公司交易平台程式碼掃描或黑箱測試之機制，確認是否於程式異動前及每半年執行程式碼掃描或黑箱測試。 3. 檢查公司是否針對程式碼掃描或黑箱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，記錄矯正處理情形並追蹤改善。
	(八) 系統平台維運之安全管理(包含對外提供服	1. 證券商經營自行	1. 檢查公司是否未採用已停止弱

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	務及內部公司使用之系統) 1.軟體安全更新 (1). 應避免採用已停止弱點修補或更新之系統軟體與應用軟體,如有必要應採用必要防護措施。 (2). 應定期對系統軟體與應用軟體進行相關安全更新與修補。	買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(八)、1 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17條 3. 參酌「建立證券商資通安全檢查機制」7	點修補或更新之系統軟體與應用軟體。 2. 檢查公司是否定期對系統軟體與應用軟體有關安全更新與修補。
	2.每半年應進行弱點掃描,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。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(八)、2 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17條 3. 參酌「建立證券商資通安全檢查機制」9	1. 取得公司訂定弱點掃描作業程序。 2. 檢查公司弱點掃描之執行範圍、標的、頻率與方式,確認是否已涵蓋具證券性質之虛擬通貨業務作業環境相關設備(包含對外提供服務及內部公司使用之系統)。 3. 檢查公司是否每半年進行弱點掃描,確認弱點掃描紀錄與掃描風險事項改善後續追蹤,是否針對不同風險訂定適當措施及完成時間。
	3.公司每年應對交易平台執行滲透測試,以加強資訊安全。	1. 證券商經營自行買賣具證券性質	1. 取得公司訂定滲透測試作業程序。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		之虛擬通貨業務內部控制制度標準規範八、(八)、3 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17條	2. 檢查公司滲透測試報告，確認是否每年定期執行交易平台之滲透測試。 3. 檢查公司滲透測試報告及執行範圍，對於不同風險是否訂定適當措施及完成時間，並確實執行追蹤與改善。
	4.監控管理 (1). 應建立系統平台異常監控機制。 (2). 應建立病毒偵測機制並定期更新病毒碼。 (3). 應偵測網頁與程式異動並留存異動紀錄，非預期性異動應即時通知相關人員處理。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(八)、4 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17條 3. 參酌「建立證券商資通安全檢查機制」7	1. 檢查公司是否建立系統平台異常監控機制。 2. 檢查公司病毒偵測機制，是否涵蓋所有設備。 3. 檢查公司病毒碼更新機制與頻率，並檢核更新紀錄，確認是否有設備長時間未執行更新或設備失聯的情況。 4. 抽核個人電腦、公用電腦、主機伺服器及獨立設備（未納AD中控）等，是否皆已安裝防毒軟體、並且定期更新病毒碼。 5. 檢查公司網頁與程式異動之管理機制，確認監控異動的範圍是否完整。 6. 抽核監控異動紀錄、異常通知及處理紀錄。
	5.存取管制(白名單、權限審查等) (1). 應建立員工之註冊、異動及撤銷註冊程序，用以配置適當之存取權限。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務	1. 檢查公司是否建立員工註冊、異動及撤銷註冊程序。 2. 檢查公司是否至少每半年定期

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	(2). 應至少每半年定期審查帳號與權限之合理性，人員離職或調職時應及時更新權限，以符合職務分工與牽制原則。 (3). 硬體設備、應用軟體、系統軟體之最高權限帳號或具程式異動、參數變更權限之帳號應列冊保管；最高權限帳號使用時須先取得權責主管同意，並保留稽核軌跡。 (4). 應確認人員之身分與存取權限，必要時得限定其使用之機器與網路位置(IP)。 (5). 於登入作業系統進行系統異動或資料庫存取時，應留存人為操作紀錄。如採用列冊保管之帳號進行前述異動或存取時，應於使用後儘速變更密碼；但因故無法變更密碼者，應建立監控機制，避免未授權變更，並於使用後覆核其操作紀錄。 (6). 帳號應避免多人共用同一個帳號為原則，如有共用需求，申請與使用須有其他補強管控方式，並留存操作紀錄且應能區分人員身分。 (7). 採用固定密碼者，應符合優質碼為原則並定期變更密碼或其他補強管控方式（如限制人工登入）。 (8). 加解密程式或具變更權限之公用程式（如資料庫存取程式）應列冊管理並限制使用，該程式應設定存取權限，防止未授權存取，並保留稽核軌跡。	內部控制制度標準規範八、(八)、5 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第12條 3. 參酌「建立證券商資通安全檢查機制」8	審查帳號與權限之合理性，並取得現職人員名冊、部門資訊並檢視系統相關權限，檢查其權限設定與職務權責是否妥適。 3. 取得當年度離、調職人員清冊，並檢查其帳號與權限是否及時更新調整。 4. 檢查公司當年度帳號與權限定期審查紀錄(包含硬體設備、網路設備、應用系統、作業系統及資料庫等) 5. 檢查公司最高權限之帳號管理方式，是否列冊保管。 6. 抽核公司系統稽核軌跡（網路設備、應用系統、作業系統及資料庫等），最高權限帳號申請紀錄，是否取得權責主管同意。 7. 檢查公司最高權限帳號使用、防火牆規則變更、程式異動、重要系統參數變更、帳務調整、資料異動等特殊作業，是否有限定其使用之設備與網路位置（IP）。 8. 抽核前項特殊作業之操作稽核軌跡，確認是否為授權之合法連線來源。 9. 檢查公司登入交易平台之作業系統進行系統異動或資料庫存取，是否有留存人為操作紀錄（如：登入紀錄、系統異動紀

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
			錄、資料庫操作紀錄、資料異動紀錄、應用系統操作紀錄、透過應用系統進行異動紀錄等)。 10. 檢查公司前項異動之申請程序,透過系統所留存的人為操作紀錄,確認是否有相對應的變更申請及覆核紀錄。 11. 檢查公司是否有共用帳號的情況,若有,則須確認共用帳號之管理方式,是否有其他補償性控管措施(如:保留可區分人員身分的操作軌跡或申請紀錄) 12. 檢查公司系統畫面,確認使用者帳號之密碼原則設定。 (優質碼得參考「建立證券商資通安全檢查機制」:公司應使用優質密碼設定(長度6個字元(含)以上,且具有文數字或符號),並加強宣導客戶定期更新使用者密碼以不超過三個月為宜。除客戶外,公司其他使用者之密碼應至少每三個月變更一次。) 13. 檢查公司是否有無法定期變更密碼的情況,是否有其他補強管控方式。 14. 檢查公司具加解密功能或變更權限功能之公用程式是否有限制存取人員,並留有稽核軌跡。
	6. 應訂定系統安全強化標準,建立並落實虛擬通貨作業環境安全設定辦法。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務	1. 檢查公司是否訂定系統軟體及硬體設備安全強化標準。 2. 檢查具證券性質之虛擬通貨業

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		內部控制制度標準規範八、(八)、6 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第16條	務作業環境(含網路設備、交易平台系統主機、交易平台系統資料庫、資訊安全設備及高權限帳號使用之人員電腦)之系統安全強化執行紀錄，並確認系統是否依據基準執行強化。
	(九)備份管理 1.應建立定期備份機制及備份清冊，備份媒體或檔案應妥善防護，確保資訊之可用性及防止未授權存取。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(九)、1 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第16條 3. 參酌「建立證券商資通安全檢查機制」7	1. 取得備份作業管理辦法及備份清冊。 2. 檢查公司備份管理機制、備份媒體保管方式及備份媒體調閱方式。 3. 檢查公司備份排程並確認備份媒體清冊之正確性。(各類媒體隨機抽樣一筆) 4. 檢查備份環境系統主機權限及資料存取權限是否合宜，如採用磁帶、外接硬碟等備份媒體，檢視備份媒體保存環境是否妥適。
	2.應建立回存測試機制，以驗證備份之完整性及儲存環境之適當性。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(九)、1 2. 參酌「電子支付	1. 檢查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。 2. 檢查備份回存測試執行紀錄。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		機構資訊系統標準及安全控管作業基準辦法」第16條 3. 參酌「建立證券商資通安全檢查機制」7	
	(十)網路安全管理 1.應偵測惡意網站連結並定期更新惡意網站清單。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十)、1 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17條	1. 檢查公司是否建立惡意網站清單之來源與更新機制,並確認是否定期更新。 2. 檢查公司內部連線至惡意網站清單內之網址時,是否確實進行適當之處置（如：中斷連線)。
	2.應建立入侵偵測或入侵防禦機制並定期更新惡意程式行為特徵。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十)、2 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17條	1. 取得網路架構圖及入侵偵測或入侵防禦機制(包含來源與頻率)，並確認惡意程式行為特徵更新紀錄。 2. 檢查公司異常紀錄及其處理方式。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	3.應建立上網管制措施，限制連結非業務相關網站，以避免下載惡意程式。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十)、3 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17條	1. 檢查公司內部上網管制措施，確認是否限制網站瀏覽之內容，限制下載檔案來源及檔案類型。 2. 檢查公司內部是否確實不得連結非業務相關不明網站及下載惡意程式。
	4.虛擬通貨作業環境與其他網路間之連線必須透過防火牆或路由器進行控管，前揭網路設備之設定應經權責主管之核准。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十)、4 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第18條	1. 取得公司訂定之網路管理辦法。 2. 檢查公司網路架構圖，確認虛擬通貨作業環境網路區隔方式是否妥適。 3. 檢查公司網路安全防護機制（如：網路防火牆、應用系統防火牆、入侵防護IPS/IDS、APT、防毒系統等)於網路架構之位置是否妥適，及是否已限制跨網域的存取行為。 4. 檢查公司網路安全防護設備設定是否經核准後變更。
	5.系統僅得開啟必要之服務及程式，人員僅能存取已被授權使用之網路及網路服務。內部網址及網路架構等資訊，未經授權不得對外揭露。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十)、5	1. 取得公司訂定之網路管理辦法、系統管理辦法。 2. 檢查公司系統是否僅開啟必要之服務及程式。 3. 檢查公司已開啟之網路服務，是否皆經過授權及是否異常開放

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第18條	的網路服務。 4. 檢查公司可得知內部網址及網路架構等敏感資訊之人員，是否與其職務是否相符。
	6. 應建立防火牆安全管理規則並定期檢視存取控管設定，防火牆進出紀錄及備份應至少保存三年。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十)、6 2. 參酌「建立證券商資通安全檢查機制」7	1. 取得公司防火牆之存取控管設定，並檢查是否為業務必要使用及是否存在高風險設定（如：Internet IP可存取內部Server網段、any IP、any Port、any Service)。若存在高風險設定，則確認申請目的為何，有無其他補償性控制措施（如：搭配OTP或限制來源IP等）。 2. 取得公司存取控管設定變更之申請方式，並抽核確認規則之設定是否經授權。 3. 檢查公司防火牆定期檢視頻率，對於不提供服務(下線)的設備、無業務使用需求或已長期無網路流量的防火牆規則是否確實停用或刪除。 4. 檢查公司防火牆進出紀錄及備份年限，是否至少保存三年。
	7. 經由網際網路連至內部網路進行遠距之系統管理工作時，應建立相關管控規定，以控管其連線目的、授權機制、身分認證及留存操作紀錄。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、	1. 取得公司訂定之網路管理辦法，確認公司是否允許由網際網路連至內部網路進行遠距之系統管理工作，若允許，則檢查公司是否建立管控規定及授權機制。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		(十)、7 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第18條	2. 取得現行可由網際網路連至內部網路進行遠距之系統管理工作的人員清單,並檢查其申請目的、期間、時段、網段、使用設備、目的設備或服務是否合宜。人員異動時有無及時進行更新及是否定期審查權限。 3. 檢查公司由網際網路連至內部網路進行遠距之系統管理工作的人員,是否僅限於其所申請遠端使用的設備,所申請遠端使用的設備是否安裝必要資訊安全防護軟體及如何確認遠端設備安全性。 4. 檢查公司除登入之帳號、通行碼外,是否有設置其他加強身分認證的登入方式。如:OTP。 5. 檢查公司由網際網路連至內部網路進行遠距之系統管理工作,是否建立監控機制,留存操作紀錄,並定期覆核。
	8. 公司應明確訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序,應包含事前準備、事件應變及事後處理機制。另應導入流量清洗機制,並且每年至少演練一次。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十)、8 2. 參酌「建立證券商資通安全檢查	1. 檢查公司是否訂定的分散式阻斷服務攻擊(DDoS)防禦與應變作業程序,確認公司對分散式阻斷服務攻擊(DDoS)防禦機制。 2. 檢查公司是否有導入流量清洗機制。 3. 檢查公司分散式阻斷服務攻擊(DDoS)演練紀錄,是否依程序辦理。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		機制」10	
	(十一)每年應依人員職務內容及層級訂定相關教育訓練計劃 1.應針對資訊人員(系統管理及程式開發人員)定期進行系統安全管理及安全程式開發之教育訓練，至少每年一次。 2.應對所有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，至少每年一次。 3.資通安全專責人員每年應參加十五小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十一) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第17條 3. 參酌「建立證券商資通安全檢查機制」3	1. 取得資訊安全教育訓練計劃。 2. 檢查資訊人員接受年度教育訓練之紀錄，確認資訊部門人員是否依工作職責需求持續接受資訊安全相關教育訓練。 3. 檢查所有虛擬通貨相關從業人員及資通安全專責人員年度教育訓練計畫、上課紀錄及上課時數是否符合規定。 4. 檢查電子郵件社交工程演練執行紀錄、演練範圍及未達目標之改善，是否至少每年辦理一次。
	(十二)資訊安全事件通報、應變管理 1.公司應訂定資訊安全事件管理程序(至少包含事件分級原則、事件確認及排除機制、事件通報機制、緊急應變機制、停止交易時機及處理程序、投資人權益補償措施、恢復交易處理、事件檢討及改善措施程序等)，並注意軌跡紀錄與證據留存之有效性，建立營運持續管理機制。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十二)、1 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第21條	1. 取得公司訂定的資訊安全事件管理程序，並檢查是否至少包含事件確認、排除機制、緊急應變機制、停止交易時機及處理程序、投資人權益補償措施、恢復交易處理、事件檢討及改善措施程序等。 2. 檢查具證券性質之虛擬通貨業務作業環境是否曾經發生資訊安全事件。若有，則調閱資訊安全事件通報暨處理作業紀錄(如：資訊安全事件通報單、資訊安全事件處理紀錄單等)，確認事件應變暨檢討改善等程序

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
			是否符合程序要求。 3. 檢查公司資訊安全事件通報暨處理作業紀錄，其軌跡紀錄與證據留存是否足夠且有效。
	2. 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，公司應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解除通報。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十二)、2 2. 參酌「證券期貨市場資通安全事件通報應變作業注意事項」	1. 確認資通安全事件通報程序。 2. 檢查公司最近一年是否有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，是否依規定在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、正式通報及解除通報。
	3. 公司遇資訊安全事件停止交易，應俟事件排除、採行預防及改善措施後，始能恢復交易。但半年內停止交易達兩次以上，應由會計師出具事件評估及改善報告，確認所採行之預防及改善措施能有效防止相同事件並向櫃檯買賣中心申報後，始能恢復交易。	證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十二)、3	檢查公司半年內是否有發生停止交易達兩次以上的事件，若有，檢查公司是否洽請會計師出具事件評估及改善報告，確認所採行之預防及改善措施能有效防止相同事件並向櫃檯買賣中心申報後，始能恢復交易。
	4. 應隨時掌握資訊安全事件，針對高風險或重要項目立即進行清查與應變。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十二)、4 2. 參酌「電子支付機構資訊系統標準及安全控管作	1. 取得資訊安全事件處理程序。 2. 檢查具證券性質之虛擬通貨業務作業環境之事件紀錄，確認事件處理狀態與相關紀錄，是否評估事件對公司之影響，並針對高風險或重要項目立即進行清查與應變。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		業基準辦法」第17條	
	5.應將各作業系統、網路設備及資安設備之日誌及稽核軌跡集中管理，進行異常紀錄分析，設定合適告警指標並定期檢討修訂。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十二)、5 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第21條	1. 取得日誌及稽核軌跡管理辦法或相關作業程序。 2. 檢查具證券性質之虛擬通貨業務作業環境之應用系統、資料庫管理系統、作業系統、網路設備及資訊安全設備，是否留存必要之日誌及稽核軌跡，並集中管理。 3. 檢查公司日誌管理系統之系統管理者帳號，是否僅被授權人員可以存取，是否定期盤點帳號與權限(應至少每半年定期審查帳號與權限之合理性)。 4. 檢查公司日誌及稽核軌跡是否進行異常紀錄分析或監控(應含作業系統、網路設備及資安設備)，針對異常警訊是否已設定合適告警指標，告警指標是否定期進行檢討修訂。 5. 檢查公司系統發出的異常警訊，是否有進行異常確認及改善，如為誤判，是否進行誤判確認並修訂告警條件。
	6.如有資訊安全事件發生時，其系統交易紀錄、系統日誌、安全事件日誌應妥善保管，並應注意處理過程中軌跡紀錄與證據留存之有效性。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標	1. 取得公司日誌管理、證據保全與事件鑑識相關作業程序。 2. 檢查公司現行留存的系統交易紀錄、系統日誌、安全事件日誌

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		準規範八、(十二)、6 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」第21條	是否有助於查明事件，且確認其內容完整性、機密性，且妥善保管。 3. 檢查公司資訊安全事件相關之系統交易紀錄(application log、transaction log)、系統日誌(system log)、安全事件日誌(security log)等證據留存是否遵循其上述程序執行，且保全紀錄與證據，並維持各項證據之證據監管鏈 (chain of custody)。
	7. 如有重大資訊安全事件時，公司應委由第三方專業機構執行數位鑑識作業。	證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十二)、7	取得公司委由外部第三方專業機構執行數位鑑識作業之資格證明文件、委外合約、執行過程紀錄及鑑識報告。
	(十三)紀錄留存與管理 1. 公司應保留交易相關紀錄、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，並應確保其真實性及完整性，以供帳務查核與勾稽。 2. 應確保數位證據之蒐集、留存與保護措施，並建立適當管理程序，數位證據相關紀錄應至少留存三年。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十三) 2. 參酌「建立證券商資通安全檢查機制」8	1. 檢查具證券性質之虛擬通貨業務交易相關紀錄、操作紀錄是否完整、安全、適當保存，並依保存期限保存。 2. 檢查公司是否建立數位證據管理程序，以確保其蒐集、留存與保護控管措施，並依保存期限保存。
	(十四)公司作業委託他人處理(以下簡稱委外)之安全管理 1. 公司於作業委外應就客戶權益保障訂定內部作	1. 證券商經營自行買賣具證券性質之虛擬通貨業務	1. 檢查公司於作業委外時，是否就客戶權益保障訂定內部作業及程序。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	業及程序，其內容應包括： (1)作業委外如涉及客戶資訊者，應於契約簽訂時訂定告知客戶之條款；其未訂有告知條款者，公司應書面通知客戶委外事項，並應依個人資料保護法之規定辦理。 (2)客戶資訊提供之條件範圍及其移轉之程序方法。 (3)對受委託機構使用、處理、控管前款客戶資訊之監督方法。 (4)公司於作業委外時應訂定客戶糾紛處理程序及時限，並設置協調處理單位，受理客戶之申訴。 (5)其他客戶權益保障之必要措施。	內部控制制度標準規範八、(十四)、3 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第7條 3. 個人資料保護法	2. 檢查公司將客戶資訊委外時，與客戶簽訂的契約內容是否訂有告知條款並以書面通知客戶委外事項。 3. 檢查公司提供客戶資訊之條件範圍及其移轉之程序方法。 4. 檢查公司對受委託機構使用、處理、控管客戶資訊之監督方法。 5. 檢查公司是否訂有客戶糾紛處理程序及時限，並設置協調處理單位，以受理客戶之申訴。 6. 檢查公司處理客戶糾紛之紀錄，是否依程序及規定的時限內處理。
	2.公司應訂定委外內部作業規範有關風險管理原則及作業程序，其內容應包括： (1)建立作業委外風險與效益分析之制度，並對受託機構進行適當之安全評估，依據最小權限及資訊最小揭露原則進行安全管控設計。 (2)建立足以辨識、衡量、監督及控制委外相關風險之程序或管理措施。 (3)訂定緊急應變計畫。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十四)、4 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第8條	1. 檢查公司是否訂定委外內部作業規範有關風險管理原則及作業程序。 2. 檢查公司訂定之風險管理原則及作業程序是否包含 (1) 建立作業委外風險與效益分析之制度。 (2) 建立足以辨識、衡量、監督及控制委外相關風險之程序或管理措施。 (3) 訂定緊急應變計畫。 3. 抽核作業委外案，是否依委外風險管理原則及作業程序辦理。
	3.公司應於委外契約載明下列事項： (1)委外事項範圍及受委託機構之權責。	1. 證券商經營自行買賣具證券性質	檢查公司委外契約是否載明下列事項：

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	(2)客戶權益保障，包括客戶資料保密及安全措施。 (3)與受委託機構終止委外契約之重大事由，包括主管機關通知依契約終止或解約之條款。 (4)受委託機構就受託事項範圍，同意主管機關及本中心得取得相關資料或報告，及進行檢查，或得命令其於限期內提供相關資料或報告。 (5)受委託機構對委外事項若有重大異常或缺失應立即通知公司。 (6)應明定非經公司書面同意，不得將作業複委託。委外契約中應對複委託情形，訂明複委託之範圍、限制、條件及要求受託機構於複委託契約中，訂定受複委託機構應依公司所訂之內部控制制度辦理。 (7)其他約定事項。	之虛擬通貨業務內部控制制度標準規範八、(十四)、5 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第10條	(1)委外事項範圍及受委託機構之權責。 (2)客戶權益保障，包括客戶資料保密及安全措施。 (3)與受委託機構終止委外契約之重大事由，包括主管機關通知依契約終止或解約之條款。 (4)受委託機構就受託事項範圍，同意主管機關及本中心得取得相關資料或報告，及進行檢查，或得命令其於限期內提供相關資料或報告。 (5)受委託機構對委外事項若有重大異常或缺失應立即通知公司。 (6)應明定非經公司書面同意，不得將作業複委託。委外契約中應對複委託情形，訂明複委託之範圍、限制、條件及要求受託機構於複委託契約中，訂定受複委託機構應依公司所訂之內部控制制度辦理。 (7) 其他約定事項。
	4.委外處理前應先對受託機構進行適當之安全評估，並依據最小權限及資訊最小揭露原則進行安全管控設計。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十四)、1 2. 參酌「電子支付	1. 取得公司訂定之資訊作業委外管理辦法或相關作業程序。 2. 檢查公司管理辦法或作業程序內容是否包含委外處理前對受託機構進行適當之安全評估要求。 3. 檢查公司於資訊作業委外前安

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		機構資訊系統標準及安全控管作業基準辦法」—第 20 條	全評估紀錄。 4. 檢查公司資訊作業委外之類型為何。委託機構是否須申請存取公司網路、系統及資料。(如：門禁、內部網路連線、系統帳號或資訊設備等)，是否經過申請程序核准並留存紀錄。 5. 檢查公司提供受託機構之帳號權限是否符合最小權限及資訊最小揭露原則，有無提供權限過大(如：管理者帳號)的帳號供受託機構使用。 6. 檢查委託機構申請公司帳號權限是否設有期間限制，如允許遠端連入公司，是否控管委託機構使用時間及目的。 7. 檢查公司是否定期盤點委外人員帳號權限機制，並調閱盤點紀錄。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	5.委託契約或相關文件中，應明確約定受託機構應遵循之規範、委外業務安全遭到破壞時應即時通知委託人、交付之系統或程式應確保無惡意程式及後門程式，其放置於網際網路之程式應通過程式碼掃描或黑箱測試。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十四)、2 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」－第 20 條	1. 取得委託契約或相關文件。 2. 檢查委託契約或相關文件，是否包含資訊安全條款、保密條款、驗收條件或其他與安全相關之要求，對於違反前揭要求時是否有訂定罰責。 3. 檢查受託機構專案成員是否有簽署保密協議書或保密相關文件。 4. 確認受託機構是否曾經發生委外業務安全遭到破壞之事件（如：資料系統遭駭客入侵、因人員處理造成資料外洩、人員作業疏失或委外開發之程式 bug 導致交易或資料錯誤），並檢查受託機構若發生前述事件時，是否主動、即時通知公司。 5. 檢查受託機構交付之系統或程式，如何確保無惡意程式及後門程式。(如：經滲透測試或弱點掃描測試) 6. 檢查受託機構交付放置於網際網路之程式時，是否對程式進行程式碼掃描或黑箱測試作業，並留存相關檢測報告。 7. 檢查滲透測試、弱點掃描、程式碼檢測或黑箱測試報告之結果，確認公司對風險處理的條件，是否針對不同風險訂定適當

內部控制制度	控制重點	相關規定/參酌來源	執行程序
			措施及完成時間。
	6.應對受託機構進行適當監督。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十四)、6 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」—第 20 條	檢查公司是否對受託機構進行適當監督(如：定期提供管理性報表、執行查核作業等)。
	(十五)營運持續管理	1. 證券商經營自行	1. 取得公司訂定之營運持續計

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	1.公司宜擬訂營運持續計畫及其必要之維護，並擬訂關鍵性業務及其衝擊影響分析(如定義最大可接受系統中斷時間，設定系統復原時間與資料復原時點等)。 2.應建立對於重大資訊系統事件或天然災害之應變程序，並確認相對應之資源，以確保重大災害對於重要營運業務之影響在其合理範圍內。 3.應每年驗證及演練其營運持續性控制措施，以確保其有效性，並應保留相關演練紀錄及召開檢討會議。	買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十五) 2. 參酌「電子支付機構資訊系統標準及安全控管作業基準辦法」－第 22 條	畫，確認內容是否辨識關鍵性業務、支援關鍵性業務所需之人員、場地、設備、資訊系統、資料、文件等資源。 2. 檢查公司是否已鑑別關鍵資訊系統最大可容忍中斷時間(MTPD)、復原時間目標(RTO)及資料復原時點(RPO)等。 3. 檢查公司是否依可能發生之威脅情境已建立相對應的緊急應變程序(包含重大資安事件、天然災害類、人為因素類或重大資訊系統類等)，程序中是否有包含關鍵所需之資源(如：人員、場地、設備、資訊系統、資料、文件等)。 4. 取得年度演練計畫及演練相關紀錄(包含演練行前說明、演練腳本、演練檢討等)，並檢查演練結果是否符合預期目標，若未符合，是否召開檢討會議進行改善。
	(十六)公司對於投資人個人資料之蒐集、處理、利用或提供主管機關及櫃檯買賣中心使用，應符合「個人資料保護法」之規定，並定期或不定期稽核依個人資料保護法定義之「個人資料保護法」管理情形。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十六) 2. 參酌「建立證券	1. 取得公司訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。 2. 抽核公司向客戶蒐集個人資料時，是否有依個人資料保護法規定，向客戶進行告知，告知事項是否完整。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		商資通安全檢查機制」8 3. 個人資料保護法	3. 檢查公司是否定期或不定期稽核「個人資料保護法」管理情形。
	(十七)公司應偵測冒名釣魚網站，提醒客戶防範網路釣魚。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十七) 2. 參酌「中華民國證券商業同業公會新興科技資訊安全自律規範」第 8 條	1. 檢查公司是否偵測冒名釣魚網站。 2. 檢查公司如何提醒客戶防範網路釣魚，以何種方式提醒。
	(十八)雲端運算安全管理 1.公司將作業委託他人處理涉及使用雲端服務，應依下列規定辦理： (1).公司應確保作業風險控管，充分評估受託機構處理之風險，採取適當風險管控措施，確保作業委外處理之品質，並應注意作業委託雲端服務業者之適度分散。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十八)、1、(1) 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第 19-1 條	1. 檢查公司是否有使用雲端服務。若有，檢查公司是否訂定雲端運算服務遴選機制及查核措施。 2. 取得公司與雲端服務業者間的契約或服務申請文件及使用雲端服務之資訊系統架構圖。契約內容是否包含委外契約應載明事項。(如：議定服務水準協議、資訊安全事件通報規定等) 3. 檢查公司決定使用雲端服務前，是否進行風險評估分析。若有，是否有針對高風險的項目，研擬因應方案。 4. 檢查公司將作業委託雲端服務

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
			業者時，是否有進行適度分散，避免因雲端服務部分設備異常，導致全面中斷服務之風險。
	(2).公司對雲端服務業者負有最終監督義務，並應具有專業技術及資源監督雲端服務業者執行受託作業，並得視需要委託專業第三人以輔助其監督作業。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十八)、1、(2) 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第19-1 條	1. 檢查雲端服務業者是否提供監控方式或工具,讓公司能監控雲端服務。 2. 檢查公司對雲端服務業者進行之監控作業。(如：雲端系統效能、網路流量異常監控、資料庫及敏感資料存取監控、網頁程式遭攻擊監控等)，並確認是否具有專業技術及資源監督雲端服務業者執行受託作業。
	(3).公司應確保其本身、主管機關及本中心，或其指定之人能取得雲端服務業者執行受託作業之相關資訊,包括客戶資訊及相關系統之查核報告，及實地查核權力。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十八)、1、(3) 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第19-1 條	1. 確認雲端服務業者是否同意公司得進行實地查核。如不同意，則取得雲端服務業者提供之國際資安相關認證(如：ISO27001,CSA Star,BS10012等)之查核報告。 2. 檢查查核報告的查核範圍是否包括客戶資訊及相關系統。
	(4).公司得自行委託，或與委託同一雲端服務業者之其他經營自行買賣具證券性質之虛擬通貨業務之證券商聯合委託具資訊專業之獨立第三人查核，並應符合下列規定：	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標	1. 取得獨立第三人所出具的查核報告。 2. 確認查核報告範圍是否包含雲端服務業者受託處理作業相關

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	A.確認其查核範圍涵蓋雲端服務業者受託處理作業相關之重要系統及控制環節。 B.應評估第三人之適格性，以及其所出具查核報告內容之妥適性並符合相關國際資訊安全標準。 C.應針對公司所委託作業範圍進行查核並出具報告。	準規範八、(十八)、1、(4) 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第19-1 條	之重要系統、控制環節與公司委託的作業範圍。 3. 檢查獨立第三人資格妥適性。
	(5).公司傳輸及儲存客戶資料至雲端服務業者，應採行客戶資料加密或代碼化等有效保護措施，並應訂定妥適之加密金鑰管理機制。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十八)、1、(5) 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第19-1 條	1. 檢查傳輸及儲存客戶資料至雲端服務業者時，所使用的資料保護機制為何。(如：採用金鑰加密、代碼化等) 2. 取得公司訂定之金鑰管理辦法或作業程序。 3. 檢查公司金鑰管理機制，是否採分持方式管理，確認其取用方式。 4. 檢查公司金鑰替換機制。(如：定期更換、有洩漏疑慮時) 5. 確認客戶資料傳輸至雲端服務業者時，傳輸過程已採行有效保護措施(如：使用超文字傳輸安全協定(HTTPS)、安全檔案傳輸協定(SFTP)等加密之網路協定或代碼化等有效保護措施)。 6. 檢查公司資料儲存於雲端服務業者所提供之儲存空間，是否確實有進行有效保護措施。
	(6).公司對委託雲端服務業者處理之資料應保有完整所有權，除執行受託作業外，公司應確保	1. 證券商經營自行買賣具證券性質	1. 檢查公司如何確保雲端服務業者不得有存取客戶資料之權

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	雲端服務業者不得有存取客戶資料之權限，並不得為委託範圍以外之利用。	之虛擬通貨業務內部控制制度標準規範八、(十八)、1、(6) 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第19-1條 3. 中華民國證券商業同業公會新興科技資訊安全自律規範 4. 證券期貨市場相關公會新興科技資訊安全管控指引	限。如無法避免，則是否有補償性控制措施。(如：設有資料存取監控機制、提供稽核軌跡紀錄、透過雙因子認證存取資料或系統) 2. 檢查公司與雲端服務業者的合約，是否有主張資料所有權為公司所有，並規範雲端服務業者不得存取客戶資料。
	(7).公司使用雲端服務處理之客戶資料及其儲存地以位於我國境內為限，不得使用境外之雲端服務。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十八)、1、(7) 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第19-1條	1. 確認公司使用雲端服務處理之客戶資料及其儲存地，是否位於我國境內為限。 2. 檢查雲端服務業者所提供之備份機制，確認備份資料儲存地，是否位於我國境內為限。

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
	(8).公司應訂定妥適之緊急應變計畫，降低因作業委託而可能有服務中斷之風險。公司終止或結束作業委託，應確保能順利移轉至另一雲端服務業者或移回自行處理，並確保原受託雲端服務業者留存資料全數刪除或銷毀，並留存刪除或銷毀之紀錄。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十八)、1、(8) 2. 參酌「金融機構作業委託他人處理內部作業制度及程序辦法」-第19-1 條 3. 中華民國證券商業同業公會新興科技資訊安全自律規範 4. 證券期貨市場相關公會新興科技資訊安全管控指引	1. 檢查雲端服務應用之業務範圍，是否涉及關鍵核心業務、資料或服務。是否包含客戶個資儲存及處理、交易資料儲存。 2. 檢查公司是否訂定妥適之緊急應變計畫，降低因作業委託而可能有服務中斷之風險。 3. 檢查公司如須移轉至另一家雲端服務業者或移回自行處理(即不使用雲端服務)，資料處理程序及如何確保雲端服務業者全數刪除或銷毀受託留存之資料。 4. 檢查雲端服務業者對應用程式、資料處理、系統平台及檔案格式是否具互通性與可移植性。
	(十九)公司運用雲端運算服務、社群媒體、行動裝置及物聯網設備等新興科技時，應依「中華民國證券商業同業公會新興科技資訊安全自律規範」及「證券期貨市場相關公會新興科技資訊安全管控指引」訂定作業管理程序。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(十九) 2. 中華民國證券商業同業公會新興科技資訊安全自律規範 3. 證券期貨市場相關	1. 確認公司是否有使用社群媒體、行動裝置及物聯網設備等新興科技。 2. 檢查公司社群媒體安全管控機制： (1) 取得公司社群媒體使用規範。確認是否界定可於公務用社群媒體上分享之業務資料及是否界定私人與公務用社群媒體之區別與應

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
		公會新興科技資訊安全管控指引 4. 中華民國證券商業同業公會會員從事廣告、業務招攬及營業促銷活動管理辦法	注意事項。 (2) 檢查開放公司網路或設備予員工使用社群媒體時，是否評估其風險及採行對應的安全管制。 (3) 檢查公司是否成立官方社群媒體。如有，是否依規揭露公司基本資訊並定期檢視隱私政策。 (4) 檢查公司是否有訂定官方社群媒體帳號權限管理機制，並對發布內容進行控管。 (5) 檢查公司是否訂定官方社群媒體異常通報及申訴處理機制。 (6) 檢查公司對非屬官方社群媒體有以公司名義從事廣告、業務招攬及營業促銷活動是否採行監管措施。 3. 取得公司訂定行動裝置相關規範。確認行動裝置運用的範圍係由公司配發公務用之行動裝置設備亦或允許員工自攜行動裝置。 4. 檢查公司是否有透過行動裝置存取公司內部網路。若允許，確認採行的安全機制為何。(如：身分識別機制、行動裝置遺失時

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
			資料清除方式等) 5. 檢查公司是否具網路連線功能且有連接外部或內部網路之自動化辦公設備(如：數位錄影機、電話交換機、傳真機、錄音機、影印機及監視器等)。 6. 取得公司物聯網設備管理清冊及採購合約。 7. 檢查公司物聯網設備是否建立安全性更新機制並定期更新,檢視安全更新紀錄。如無法更新，須提供汰換計畫或補償性控制措施執行紀錄。 8. 檢查公司物聯網設備初始密碼是否確實進行變更。 9. 檢查公司與物聯網設備相關的防火牆規則,確認是否直接對外部網路(Internet)公開。
	(二十)公司選擇區塊鏈平台底層時，應於區塊鏈上可控管資料讀寫權限、可控管發行之虛擬通貨利用程式碼自動執行之內容其佈署權及佈署方式、可控管資料揭露的原則、可控管節點參與機制等,以確保公司可對區塊鏈平台底層技術實踐有一定程度之掌控。	1. 證券商經營自行買賣具證券性質之虛擬通貨業務內部控制制度標準規範八、(二十)	1. 檢查公司區塊鏈平台規格是否符合內控要求。 2. 檢查公司區塊鏈類型(如：聯盟鏈或私有鏈)，是否可控管節點參與機制(申請程序),其節點佈署機制為何。 3. 檢查交易寫入公司區塊鏈的時機(如：交易寫入分散式帳本時機及寫入規則)，並抽核分散式帳本一致性。 4. 檢查公司資料存取權限控管機

會計師出具資訊系統及安全控管作業評估報告原則性規範

內部控制制度	控制重點	相關規定/參酌來源	執行程序
			制。 5. 檢查公司選用程式碼自動執行內容協議(如：ERC-20）之評估與審核程序。 6. 檢查公司程式碼自動執行之內容發佈機制與程序，並確認使用的協議。(如：ERC-20) 7. 檢查公司區塊鏈分散式帳本資料是否有過度揭露的情況。(除交易日期、電子錢包轉出位址、電子錢包轉入位址、交易數量等資訊外，是否有過度揭露客戶個人敏感資訊的情況)