「提供虛擬資產服務之事業或人員資產分離保管作業：內部控制制度、會計師協議程序及報告範例」

指導單位：金融監督管理委員會 Financial Supervisory Commission R.O.C

委託單位：證券櫃檯買賣中心 Taipei Exchange

執行單位：財團法人會計研究發展基金會 ACCOUNTING RESEARCH AND DEVELOPMENT FOUNDATION

中華民國 114 年 12 月 30 日

目錄

前言

1. 為配合金融監督管理委員會頒布之「提供虛擬資產服務之事業或人員（以下簡稱 VASP）洗錢防制登記辦法」第十條第一項之規定：「虛擬資產服務商業務之經營，應依法令、章程、內部控制制度及同業公會自律規範為之。」，以及同辦法第二十七條第三項之規定：「虛擬資產保管商就所保管之客戶資產，應設置定期性與經常性之對帳措施，且至少每年委任會計師出具報告並公告。」，財團法人中華民國會計研究發展基金會組成專案小組，負責研擬「提供虛擬資產服務之事業或人員資產分離保管作業：內部控制制度、會計師協議程序及報告範例」，協助 VASP 制定資產分離保管內部控制制度，以及供會計師對分離保管內部控制制度執行協議程序時參考。

2. VASP 參考本範例制定內部控制制度時，因各 VASP 之規模、營運流程、人員組織、系統與設備不盡相同，因此 VASP 應視其實際之營運狀況作調整，並遵循 VASP 洗錢防制登記辦法、VASP 防制洗錢及打擊資恐辦法與中華民國虛擬通貨商業同業公會所發布之自律規範，設計健全之內部控制制度。會計師亦應依 VASP 之實際作業及風險，運用其專業判斷，擬訂執行程序並出具合宜之協議程序執行報告。

第1章　資產分離保管內部控制制度

1.1 法定貨幣/虛擬資產餘額驗證

目的：為確保虛擬資產服務商保管客戶法定貨幣與虛擬資產之安全性，與虛擬資產服務商與客戶法定貨幣與虛擬資產餘額之正確性，特訂定法定貨幣/虛 擬資產餘額驗證之作業程序與控制重點，以達成資產分離保管內部控制制度目標。

作業	作業程序及控制重點
1.1.1 法定貨幣入金	一、作業程序 (一) 虛擬資產服務商（以下簡稱「VASP」）收受客戶之法定貨幣程序－委託第三方信託分離保管法定貨幣**【控制重點(四)】** 1 法定貨幣入金（以下簡稱「法幣入金」）之客戶，VASP 須先依照「提供虛擬資產服務之事業或人員防制洗錢及打擊資恐辦法」要求客戶完成實名制身分驗證、綁定銀行帳號後，始可取得 VASP 提供之入金帳號。**【控制重點(一)】** 2 客戶綁定前項所述之銀行帳號前，須通過 VASP 反洗錢、反詐欺與反資恐檢核（以下簡稱 AML 檢核），經 AML 檢核通過後，始完成綁定銀行帳號。僅有完成銀行帳號綁定之客戶始可進行與法幣有關之交易。 3 客戶透過網路銀行或行動銀行，將法定貨幣款項匯入「入金帳號」（此行為即「法幣入金」）。 4 客戶法幣入金時，第三方信託銀行將推播通知訊息予 VASP 系統，VASP 接收推播通知訊息後，VASP 應針對入金之客戶進行風險控管檢核措施（例如 AML 檢核、客戶資格權限比對及入金限額等）；如未通過前項風險控管檢核措施，VASP 應進行對應處理流程，例如：入金款項退款（見 1.1.1.2(二) 客戶之法定貨幣退款程序）、交易取消等。**【控制重點(三)】** 5 入金之客戶於通過風險控管檢核措施後，VASP 系統將客戶之入金自動記錄於客戶之系統帳戶。**【控制重點(二)】** (二) VASP 收受客戶之法定貨幣程序－取得銀行十足之履約保證**【控制重點(四)】【控制重點(六)】** 1 法定貨幣入金（以下簡稱「法幣入金」）之客戶，VASP 須先依照「提供虛擬資產服務之事業或人員防制洗錢及打擊資恐辦法」要求客戶完成實名制身分驗證、VASP 進行 AML 檢核並綁定銀行帳號後，始可取得 VASP 提供之入金帳號。**【控制重點(一)】** 2 客戶申請法幣入金，於交付現金前或進行匯款後，VASP 將進行風險控管檢核措施（例如 AML 檢核、客戶資格權限比對及入金限額等）；如未通過前項風險控管檢核措施，VASP 應進行對應處理流程，例如：入金款項退款、交易取消、暫停客戶交易等，以及通知銀行進行退款。**【控制重點(三)】** 3 入金之客戶於通過 AML 檢核與風險控管檢核措施後，VASP 系統將客戶之入金自動記錄於客

	戶之系統帳戶。**【控制重點(五)】** 二、控制重點 (一) 權責人員應針對入金之客戶進行風險控管檢核措施（如 AML 檢核、客戶資格權限比對及入金限額等），確認客戶確實具備法定貨幣交易之資格。 (二) 出納人員應每日透過比對網銀明細或其他銀行傳輸之資訊 ，確認系統帳戶入金之金額與銀行入金之金額一致。 (三) 若當日發生退款時，出納人員應製作當日法定貨幣退款明細，並透過當日網銀退款明細或其他銀行傳輸之資訊，以確認已將相關款項正確地退還給應退款之客戶。 (四) VASP 就虛擬資產交易及其款項代收付業務收受客戶之法定貨幣，應與其自有之法定貨幣分離保管，並應交付信託或取得銀行十足之履約保證，且除為其客戶辦理前述業務外，不得動用前款客戶之法定貨幣。 (五) VASP 就所保管之客戶法定貨幣，應留存紀錄（應至少包括姓名及法定貨幣餘額等）。 (六) 取得銀行十足之履約保證之 VASP，其收受客戶之法定貨幣應與其自身之法定貨幣分離保管，不得存放於相同之銀行帳戶。
1.1.2 法定貨幣出金/退款	一、作業程序 (一) 客戶之法定貨幣出金程序 1 完成實名制驗證、綁定銀行帳號並由銀行完成銀行帳號驗證之客戶，始可自 VASP 平台透過 VASP 之信託帳號提領法定貨幣至已完成綁定驗證之銀行帳號。 2 客戶提出法幣出金申請時，該客戶須通過 VASP 須對該客戶進行風險控管檢核措施（如客戶資格權限比對等）及 VASP 合作之第三方信託銀行之 AML 檢核，檢核通過後，系統須記錄該筆出金資訊。**【控制重點(一)】** 3 如未通過前項風險控管檢核措施或 VASP 合作之第三方信託銀行之 AML 檢核，VASP 應聯繫客戶進行對應處理流程，包括取消交易及取消該客戶進行法定貨幣交易之資格等。**【控制重點(二)】** 4 法幣出納人員應彙整當日出金明細表及信託指示書或同等效力文件，並經覆核人員簽章或依其他方式覆核後，將該明細表及信託指示書或同等效力文件交給第三方信託銀行，指示第三方信託銀行將客戶提領款項撥付至客戶已完成綁定驗證的銀行帳號。**【控制重點(三)】** 5 第三方信託銀行完成出金至客戶已完成綁定驗證的銀行帳號後，法幣出納人員應核對當日網銀或銀行以其他方式傳輸出金紀錄，確認當日網銀出金紀錄或其他銀行傳輸之資訊與出金明

	細表之金額一致，並經覆核人員簽核或依其他方式核准。**【控制重點(四)】** (二) 客戶之法定貨幣退款程序 1 進行入金或虛擬貨幣買賣交易之客戶，如未通過 AML 檢核或風險控管檢核措施，或以非綁定帳戶入金，VASP 將通知客戶進行退款，法幣出納人員應彙整當日退款明細表及信託指示書或同等效力文件，並經覆核人員簽章覆核或依其他方式覆核核准後，將該明細表及信託指示書或同等效力文件交給第三方信託銀行，指示第三方信託銀行將客戶退款款項撥付至客戶已完成綁定驗證的銀行帳號或原匯入之非綁定帳戶。**【控制重點(五)】** 2 第三方信託銀行完成出金至客戶已完成綁定驗證的銀行帳號後，法幣出納人員應核對當日網銀出金紀錄或其他銀行傳輸之資訊，確認當日網銀出金紀錄或其他銀行傳輸之資訊與退款明細表之金額一致，並經覆核人員簽核。**【控制重點(六)】** 二、控制重點 (一) VASP 權責人員應針對出金之客戶進行 AML 檢核與風險控管檢核措施（如客戶資格權限比對等），確認客戶確實具備法定貨幣交易之資格。 (二) VASP 系統人員應確認未通過作業程序第 2 項所述之風險控管檢核措施或 VASP 合作之第三方信託銀行之 AML 檢核之客戶，VASP 已對該客戶進行對應之處理流程。 (三) 當日出金明細表及信託指示書或同等效力文件應確實經覆核人員簽核或依其他方式覆核核准。 (四) 法幣出納人員應確認網銀或其他銀行傳輸之資訊出金紀錄與當日出金明細表金額一致，並經覆核人員簽核或依其他方式覆核核准。 (五) 當日退款明細表及信託指示書或同等效力文件應確實經覆核人員簽核或依其他方式覆核核准。 (六) 法幣出納人員應確認網銀或其他銀行傳輸之資訊退款紀錄與當日退款明細表金額一致及確認已退款至客戶綁定之銀行帳號或原匯入之非綁定帳戶，並經覆核人員簽核或依其他方式覆核核准。
1.1.3 虛擬資產入金與接收	一、作業程序 (一) 虛擬資產入金與接收交易流程－從 VASP 外部地址[1]發送虛擬資產至熱錢包中客戶錢包接收地址[2]

[1] VASP 外部地址包含 VASP 客戶之外部錢包地址以及非 VASP 客戶之外部錢包地址。

[2] 客戶錢包接收地址係指 VASP 提供給客戶專門用來接收來自 VASP 平台外部虛幣之地址。

	1　虛擬資產入金（以下稱「虛幣入金」）之客戶，VASP 須先依照「提供虛擬資產服務之事業或人員防制洗錢及打擊資恐辦法」要求客戶完成實名制身分驗證，客戶始可取得 VASP 提供之客戶錢包接收地址。 2　VASP 收到外部錢包發送虛擬資產至客戶錢包接收地址時，透過區塊鏈自動將虛擬資產移轉記錄於區塊鏈公鏈上。VASP 系統於接收到該等虛擬資產時，於對應之錢包接收地址帳上予以記錄。 3　VASP 進行虛擬資產買賣、接收、發送、移轉服務時應確實記錄與保存，該保存之交易紀錄應足以重建個別交易，以備作為認定不法活動之證據。**【控制重點(一)】【控制重點(二)】** (二) 虛擬資產入金與接收交易流程－從 VASP 外部地址發送虛擬資產至熱錢包中屬 VASP 之熱錢包地址 1　VASP 收到外部錢包發送虛擬資產至熱錢包時，透過區塊鏈自動將虛擬資產移轉記錄於區塊鏈公鏈上。VASP 應進行記錄並確認發送方資訊。 2　VASP 收到未完成實名制身分驗證者之虛擬資產後（包含無主入金），應予以記錄列管，並於發現異常時通報司法警察機關。**【控制重點(三)】** 3　VASP 如收到黑名單或詐騙嫌疑等高風險客戶[3]及地址所發送的虛擬資產時，應依法向法務部調查局申報可疑交易。**【控制重點(四)】** 二、控制重點 (一) VASP 進行虛擬資產買賣、接收、發送、移轉服務時應確實記錄與保存，該保存之交易紀錄應足以重建個別交易。 (二)VASP 就所保管之客戶虛擬資產，應留存紀錄（應至少包括客戶錢包地址、姓名、虛擬資產種類、及數量等）。 (三) VASP 收到未完成實名制身分驗證者之虛擬資產後（包含無主入金），應予以記錄列管，並於發現異常時通報司法警察機關。 (四) VASP 如收到黑名單或詐騙嫌疑等高風險客戶及地址所發送的虛擬資產時，應依法向法務部調查局申報可疑交易。
1.1.4 虛擬資產發送與提	一、作業程序

[3] 高風險客戶係指外國政府之重要政治性職務人士與受經濟制裁、外國政府或國際洗錢防制組織認定或追查之恐怖分子或團體，及依資恐防制法指定制裁之個人、法人或團體、以及依 VASP 依自身交易型態所辨認之高風險客戶類型。

領	(一) 虛擬資產發送交易流程－從 VASP 發送虛擬資產至外部錢包接收地址 1 客戶發起將虛擬資產發送至外部錢包接收地址之申請時（下稱「虛擬資產提領」），VASP 系統應確實記錄相關申請資訊，包括客戶發送至外部之錢包接收地址、交易幣種、交易數量、交易時間、交易序碼（TxID）等。**【控制重點(一)】** 2 VASP 系統收到客戶虛擬資產提領申請時，系統應比對該客戶及該外部錢包接收地址是否為 VASP 標註為黑名單或詐騙嫌疑等高風險客戶，若是，則 VASP 系統應限制該筆提領交易。**【控制重點(二)】** 3 VASP 系統確認客戶之提領申請時應確認熱錢包內餘額是否足夠。若熱錢包餘額不足時（水位過低），系統將推播通知錢包管理人員進行錢包移轉。**【控制重點(三)】** 4 VASP 系統將虛擬資產發送予外部錢包接收地址後，應自動通知客戶。**【控制重點(四)】** 二、控制重點 (一) VASP 系統應確實記錄相關申請資訊，包括客戶發送至外部之錢包接收地址、交易幣種、交易數量、交易時間、交易序碼（TxID）等。 (二) 若提領之客戶及該外部錢包接收地址係 VASP 標註為黑名單或詐騙嫌疑等高風險客戶，VASP 系統應限制該筆提領交易。 (三) 確認客戶提領申請後，VASP 系統應確認熱錢包內餘額是否足夠。如遇熱錢包餘額不足時（水位過低），系統應推播通知錢包管理人員進行錢包移轉。 (四) 系統應確實將虛擬資產移轉至客戶指定之錢包地址。
1.1.5 法定貨幣餘額驗證	一、作業程序 1 法幣出納人員取得合作之第三方信託銀行法定貨幣出入金變動明細及當日網銀餘額或其他銀行傳輸之資訊。 2 法幣出納人員將合作之第三方信託銀行法定貨幣出入金變動明細或其他銀行傳輸之資訊與 VASP 帳上法定貨幣出入金金額相互核對，核對完成後法幣出納人員應簽名或以其他方式記錄，並交由覆核人員進行簽核或依其他方式覆核核准。**【控制重點(一)】** 3 法幣出納人員將合作之第三方信託銀行法定貨幣當日網銀餘額或其他銀行傳輸之資訊與 VASP 法定貨幣帳簿餘額相互核對，核對完成後法幣出納人員應簽名或以其他方式記錄，並交由覆核人員進行簽核或依其他方式覆核核准。**【控制重點(二)】** 4 若法幣出納人員發現金額不一致，法幣出納人員應及時查明原因並編製調節表說明並交由覆核人員進行簽核或依其他方式覆核核准，若屬系統或人為疏失產生之錯誤，應作適當之修正，

	若無法查明原因或作適當之修正，應及時向內部稽核部門報告，差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。**【控制重點(三)】【控制重點(四)】** 二、控制重點 (一) 法幣出納人員應核對合作之第三方信託銀行法定貨幣出入金變動明細與 VASP 帳上法定貨幣出入金金額相符，並經覆核人員簽核或依其他方式覆核核准。 (二) 法幣出納人員應核對合作之第三方信託銀行法定貨幣當日網銀或其他銀行傳輸資訊餘額與 VASP 法定貨幣帳簿餘額相符，並經覆核人員簽核或依其他方式覆核核准。 (三) 法幣出納人員發現金額不一致，應及時查明原因並編製調節表並交由覆核人員進行簽核或依其他方式覆核核准，若屬系統或人為疏失產生之錯誤，應作適當之修正，並由適當權責人員覆核調節表。 (四) 法幣出納人員發現金額不一致時，若無法查明原因或作適當之修正，應及時向內部稽核部門報告，差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。
1.1.6 虛擬資產餘額驗證	一、作業程序 1 錢包管理人員自 VASP 系統產生各幣種錢包（包括冷、溫及熱錢包）之虛擬資產餘額表，虛擬資產餘額表應明確區分客戶與 VASP 各自餘額，錢包管理人員與 VASP 系統核對確認無誤後，應簽名並轉交錢包記帳人員。錢包記帳人員核對各錢包之虛擬資產餘額表與錢包帳上之餘額，核對完成後錢包記帳人員應簽名記錄，並交由覆核人員進行簽核。**【控制重點(一)】** 2 錢包管理人員自 VASP 系統產生各幣種錢包（包括冷、溫及熱錢包）之虛擬資產變動表，虛擬資產變動表除了應明確區分客戶與 VASP 各自變動之總量外，亦應載明錢包入金、錢包出金與錢包移轉之總量，錢包管理人員與 VASP 系統核對確認無誤後，應簽名並轉交錢包記帳人員。錢包記帳人員核對各錢包之虛擬資產變動表與錢包帳上之變動數，核對完成後錢包記帳人員應簽名記錄，並交由覆核人員進行簽核。**【控制重點(二)】** 3 錢包管理人員或錢包記帳人員發現數量不一致時，應及時查明原因並編製調節表說明，若屬系統或人為疏失產生之錯誤，應作適當處置並及時向內部稽核部門報告，如係差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。**【控制重點(三)】** 二、控制重點 (一) 錢包記帳人員應核對屬於客戶及屬於 VASP 之各幣種錢包（包括冷、溫及熱錢包）之虛擬資產餘額表與錢包帳上之餘額是否相符。 (二) 錢包記帳人員應核對各幣種錢包（包括冷、溫及熱錢包）之虛擬資產變動表與錢包帳上之變動數

	是否相符。 (三) 錢包管理人員或錢包記帳人員發現數量不一致時應及時查明原因並編製調節表說明，若屬系統或人為疏失產生之錯誤，應作適當處置並及時向內部稽核部門報告，如係差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。

1.2 錢包管理

目的：為避免客戶虛擬資產被不當挪用或竊取，特訂定錢包移轉及錢包與私鑰管理之作業程序與控制重點，以達成資產分離保管內部控制制度目標。

作業	作業程序及控制重點
1.2.1 將虛擬資產由熱錢包移轉至溫錢包	一、作業程序 (一) 虛擬資產由熱錢包移轉至溫錢包之移轉程序 1 為防止水位過高時產生外部資安攻擊或是內部道德風險，當熱錢包儲存水位達公司設定之門檻時，應即時通知錢包管理人員。**【控制重點(一)】【控制重點(二)】** 2 錢包管理人員接獲通知，應檢視錢包水位並立即進行錢包虛擬資產移轉。 3 進行錢包移轉時，須由錢包管理人員發起，並完整記錄以下資訊：(1)發起日期與時間(2)轉出及轉入之白名單錢包地址(3)移轉之數量、幣種與幣別(4)移轉之理由(5)發起人簽章(6) 交易序碼（TxID）(7)簽核人員（如私鑰或私鑰分片保管人）簽章(8)移轉結果或狀態。 4 錢包管理人員發起錢包移轉後，應即時通知簽核人員。**【控制重點(一)】** 5 簽核人員接收到通知後，應覆核第 3 項(1)~(5)所述資訊是否確實填寫，覆核完成後進行核准。**【控制重點(三)】【控制重點(四)】【控制重點(五)】** 6 當簽核人員之核准人數達到啟動私鑰所需之數量時，將啟動錢包移轉程序。 7 VASP 進行錢包間虛擬資產移轉時，相關人員應確保錢包移轉程序正常運行，並確認虛擬資產已移轉至指定之錢包。**【控制重點(六)】【控制重點(七)】** 二、控制重點 (一) 錢包管理相關職能人員具有清晰的權責分工，以確保其所擔任的職能滿足內部控制控制環境的要求。 (二) 即時通知之水位設定應依照公司錢包水位之規定，以及應確實於達到門檻水位時即時通知。 (三) 虛擬資產於錢包間移轉的過程，應具備機制協助相關簽核人員確保簽核移轉的地址為指定之白名

	單錢包地址。 (四) 錢包移轉應確實簽核並註明簽核之日期與時間。 (五) 保管私鑰或私鑰分片的簽核人員應具有清晰的職能分配以及對其責任的理解，以利於使用私鑰的時機與情境能夠遂行其獨立判斷。 (六) 錢包移轉完成後，相關人員應確認虛擬資產已移轉至指定之白名單錢包地址。 (七) 應具備內控措施確保資產移轉依要求於合理期間內完成。
1.2.2 將虛擬資產由溫錢包移轉至冷錢包	一、作業程序 (一) 虛擬資產由溫錢包移轉至冷錢包之移轉程序 1 為防止水位過高時產生外部資安攻擊或是內部道德風險，當溫錢包儲存水位達公司設定之門檻時，應即時通知錢包管理人員。**【控制重點(一)】【控制重點(二)】** 2 錢包管理人員接獲通知，應檢視錢包水位並立即進行錢包虛擬資產移轉。 3 進行錢包移轉時，須由錢包管理人員發起，並完整記錄包含以下資訊：(1)發起日期與時間(2)轉出及轉入之白名單錢包地址(3)移轉之數量、幣種與幣別(4)移轉之理由(5)發起人簽章(6)交易序碼（TxID）(7)簽核人員（如私鑰或私鑰分片保管人）簽章(8)移轉結果或狀態。 4 錢包管理人員發起錢包移轉後，應即時推播通知簽核人員。**【控制重點(一)】** 5 簽核人員接收到通知後，應覆核第 3 項(1)~(5)所述資訊是否確實填寫，覆核完成後進行核准。**【控制重點(三)】【控制重點(四)】【控制重點(五)】** 6 當簽核人員之核准人數達到啟動私鑰所需之數量時，將啟動錢包移轉程序。 7 VASP 進行錢包間虛擬資產移轉時，相關人員應確保錢包移轉程序正常運行，並確認虛擬資產已移轉至指定之錢包。**【控制重點(六)】【控制重點(七)】** 二、控制重點 (一) 錢包管理相關職能人員具有清晰的權責分工，以確保其所擔任的職能滿足內部控制控制環境的要求。 (二) 即使通知之水位設定應依照公司錢包水位之規定，以及應確實於達到門檻水位時即時通知。 (三) 虛擬資產於錢包間移轉的過程，應具備機制協助相關簽核人員確保簽核移轉的地址為指定之白名單錢包地址。 (四) 錢包移轉應確實簽核並註明簽核之日期與時間。 (五) 保管私鑰或私鑰分片的簽核人員應具有清晰的職能分配以及對其責任的理解，以利於使用私鑰的時機與情境能夠遂行其獨立判斷。

	(六) 錢包移轉完成後，相關人員應確認虛擬資產已移轉至指定之白名單錢包地址。 (七) 應具備內控措施確保資產移轉依要求於合理期間內完成。
1.2.3 將虛擬資產由溫錢包移轉至熱錢包	一、作業程序 (一) 虛擬資產由溫錢包移轉至熱錢包之移轉程序 1 錢包管理人員每日應確認熱錢包水位，當熱錢包儲存水位不足時，錢包管理人員應將虛擬資產由溫錢包移轉至熱錢包以補足水位。**【控制重點(一)】** 2 進行錢包移轉時，須由錢包管理人員發起，並完整記錄包含以下資訊：(1)發起日期與時間(2)轉出及轉入之白名單錢包地址(3)移轉之數量、幣種與幣別(4)移轉之理由(5)發起人簽章(6)交易序碼（TxID）(7)簽核人員（如私鑰或私鑰分片保管人）簽章(8)移轉結果或狀態。 3 錢包管理人員發起錢包移轉後，應即時通知簽核人員。**【控制重點(一)】** 4 簽核人員接收到通知後，應覆核第 2 項(1)~(5)所述資訊是否確實填寫，覆核完成後進行核准。**【控制重點(二)】【控制重點(三)】【控制重點(四)】** 5 當簽核人員之核准人數達到啟動私鑰所需之數量時，將啟動錢包移轉程序。 6 VASP 進行錢包間虛擬資產移轉時，相關人員應確保錢包移轉程序正常運行，並確認虛擬資產已移轉至指定之錢包。**【控制重點(五)】【控制重點(六)】** 二、控制重點 (一) 錢包管理相關職能人員具有清晰的權責分工，以確保其所擔任的職能滿足內部控制控制環境的要求。 (二) 虛擬資產於錢包間移轉的過程，應具備機制協助相關簽核人員確保簽核移轉的地址為指定之白名單錢包地址。 (三) 錢包移轉應確實簽核並註明簽核之日期與時間。 (四) 保管私鑰或私鑰分片的簽核人員應具有清晰的職能分配以及對其責任的理解，以利於使用私鑰的時機與情境能夠遂行其獨立判斷。 (五) 錢包移轉完成後，相關人員應確認虛擬資產已移轉至指定之白名單錢包地址。 (六) 應具備內控措施確保資產移轉依要求於合理期間內完成。
1.2.4 將虛擬資產由冷錢包移轉至溫錢包	一、作業程序 (一) 虛擬資產由冷錢包移轉至溫錢包之移轉程序 1 錢包管理人員每日應確認熱錢包水位，當熱錢包水位不足需自溫錢包移轉，而溫錢包儲存水位不足以補足熱錢包水位時，錢包管理人員應將虛擬資產由冷錢包移轉至溫錢包。**【控制重點**

	(一)】 2 進行錢包移轉時，須由錢包管理人員發起，並完整記錄以下資訊：(1)發起日期與時間(2)轉出及轉入之白名單錢包地址(3)移轉之數量、幣種與幣別(4)移轉之理由(5)發起人簽章(6) 交易序碼（TxID）(7)簽核人員（如私鑰或私鑰分片保管人）簽章(8)移轉結果或狀態。 3 錢包管理人員發起錢包移轉後，應即時通知簽核人員。**【控制重點(一)】** 4 簽核人員接收到通知後，應覆核第 2 項(1)~(5)所述資訊是否確實填寫，覆核完成後進行核准。**【控制重點(二)】【控制重點(三)】【控制重點(四)】** 5 當簽核人員之核准人數達到啟動私鑰所需之數量時，將啟動錢包移轉程序。 6 VASP 進行錢包間虛擬資產移轉時，相關人員應確保錢包移轉程序正常運行，並確認虛擬資產已移轉至指定之錢包。**【控制重點(五)】【控制重點(六)】** 二、控制重點 (一) 錢包管理相關職能人員具有清晰的權責分工，以確保其所擔任的職能滿足內部控制控制環境的要求。 (二) 虛擬資產於錢包間移轉的過程，應具備機制協助相關簽核人員確保簽核移轉的地址為指定之白名單錢包地址。 (三) 錢包移轉應確實簽核並註明簽核之日期與時間。 (四) 保管私鑰或私鑰分片的簽核人員應具有清晰的職能分配以及對其責任的理解，以利於使用私鑰的時機與情境能夠遂行其獨立判斷。 (五) 錢包移轉完成後，相關人員應確認虛擬資產已移轉至指定之白名單錢包地址。 (六) 應具備內控措施確保資產移轉依要求於合理期間內完成。
1.2.5 錢包與私鑰管理	一、作業程序 錢包與私鑰之管理，應遵循以下原則： 1 VASP 應訂定錢包水位設定，並應通過董事會或適當之治理單位，且通過後應發布予相關員工遵循。**【控制重點(一)】【控制重點(二)】** 2 VASP 應訂定將客戶之虛擬資產存放於冷錢包之比例，並應通過董事會或適當之治理單位，且通過後應發布予相關員工遵循。**【控制重點(二)】** 3 錢包地址生成時，應由錢包管理人員應提出申請，填寫錢包地址生成申請表或同等性質的系統記錄，錢包地址生成申請表須順序編號且應明確填寫以下資訊：(1)申請日期(2)申請錢包之幣種 (4)生成之理由(5)申請人簽章(6)覆核人簽章(8)IT 人員與監督人員簽章(9)申請人驗收簽

	章。**【控制重點(三)】** 4 IT 人員應依經覆核人員簽核之申請表操作錢包軟硬體設定，此步驟應設置監督人員負責監控操作過程。IT 人員於系統創建地址後，應由錢包管理人員負責確認並核准，錢包地址始能生效。**【控制重點(四)】** 5 錢包管理人員應定期更新冷錢包地址。此外，應訂有最低更新頻率與須立即更新之情況。**【控制重點(五)】** 6 硬體錢包應由錢包管理人員妥善保管，錢包移轉作業完成時，應立即從電腦中拔除，避免相關駭入風險。 7 冷錢包私鑰或私鑰分片生成時，應由 IT 人員負責透過系統創建私鑰或私鑰分片並生成密碼，私鑰或私鑰分片創建完成後，私鑰或私鑰分片管理人員應將私鑰或私鑰分片密碼文件作適當保管（例如銀行保管箱），此步驟應設置監督人員負責監控操作過程。**【控制重點(六)】【控制重點(八)】** 8 移轉虛擬資產時，相關申請人員、覆核人員、監督人員、錢包地址與時間應確實紀錄以備供查詢，上述移轉紀錄應至少保留 5 年。**【控制重點(七)】** 9 VASP 將客戶虛擬資產存放至冷錢包之比例應達客戶虛擬資產總額之 80%[4]以上，且客戶之虛擬資產存放至熱錢包之比例不得超過客戶虛擬資產總額之 20%。**【控制重點(九)】【控制重點(十)】** 10 VASP 除依法令所訂之事由外，不得動用熱錢包內之客戶虛擬資產或將熱錢包內之客戶虛擬資產移放至保管其自有資產之錢包。**【控制重點(十一)】** 二、控制重點 (一) 錢包水位設定應經董事會或適當之治理單位通過。 (二) 客戶之虛擬資產存放於冷錢包之比例應經董事會或適當之治理單位通過。該比例如有變動亦應經董事會或適當之治理單位通過。 (三) 具備清晰的錢包設立規定(包含白名單錢包)，並應依 VASP 的規模與營運複雜度對錢包設定進行調整(如冷錢包設立的數量以及其使用特性)。 (四) IT 人員生成錢包地址時監督人員應負責監控操作過程，並具備清晰的操作指引。 (五) 錢包管理人員應適時更新冷錢包地址，並訂有須立即更新之情況。 (六) IT 人員生成冷錢包私鑰時，監督人員應負責監控操作過程，並具備清晰的操作指引。 (七) 移轉虛擬資產時，相關申請人員、覆核人員、監督人員、錢包地址與時間應確實紀錄以備供查詢，

[4] VASP 將客戶虛擬資產存放至冷錢包之比例，應遵循相關法令規範或中華民國虛擬通貨商業同業公會所發布之自律規範。

	上述移轉紀錄應至少保留 5 年。 (八) 錢包與私鑰管理，應考量其權責人員執掌與相關系統存取權限是否有職能衝突之風險。 (九) VASP 應將 80%以上之客戶虛擬資產存放於冷錢包。 (十) VASP 將客戶虛擬資產存放於熱錢包之比例不得超過客戶虛擬資產總額之 20%。 (十一) VASP 除依法令所訂之事由外，不得動用客戶之虛擬資產。
1.2.6 客戶虛擬資產與 VASP 虛擬資產於相同錢包下之混合管理	一、作業程序 VASP 就虛擬資產交易及其款項代收付業務收受客戶之虛擬資產，應與其自有之虛擬資產分離保管。除為其客戶辦理前述業務外，不得動用前款客戶之虛擬資產。VASP 因營運目的而需將客戶之虛擬資產與其自有之虛擬資產於客戶錢包混合存放時，VASP 之自有虛擬資產占客戶熱錢包內客戶虛擬資產之比例不得超過 20%[5]。前述營運目的如下：**【控制重點(一)】** 1 配合買賣、提領服務等用以支付區塊鏈公鏈發送或移轉、跨鏈轉換等各項手續費用。 2 為客戶辦理交易撮合、買賣服務及各項業務所收取並暫存之費用、利息、對價、給付或擔保等。 3 用以發放系統平台上各項服務、功能之收益或獎勵等而預先存放者。 4 為及時完成客戶交易及履行客戶支付需求之預先墊付及週轉使用。 客戶冷錢包中除支付鏈上瓦斯費（上鏈費）外，應與 VASP 自有之虛擬資產分離保管，且 VASP 之自有虛擬資產占客戶冷錢包內客戶虛擬資產之比例不得超過 20%[6]。**【控制重點(三)】** 錢包管理人員應負責控管 VASP 之自有虛擬資產占錢包內客戶虛擬資產之比例，若比例超過 20%系統將發出通知，錢包管理人員接獲通知後，應進行錢包移轉，將存放至客戶錢包之 VASP 虛擬資產移轉至 VASP 之錢包。錢包管理人員應依 1.1.2.1「將虛擬資產由熱錢包移轉至溫錢包」第 3 項至第 7 項或 1.1.2.4「將虛擬資產由冷錢包移轉至溫錢包」第 3 項至第 6 項作業流程進行錢包移轉。**【控制重點(二)】** 二、控制重點 (一) VASP 虛擬資產僅於符合作業流程第一項營運目的所需時，始得將其虛擬資產存放於客戶之熱錢包。VASP 須具備機制可以正確區分與管理混同資產的比例。 (二) 錢包管理人員應負責控管 VASP 存放至客戶錢包（包含熱及冷錢包）之虛擬資產餘額不得超過客戶之虛擬資產餘額之 20%。

[5] 混合管理下，VASP 之自有虛擬資產占客戶熱錢包內客戶虛擬資產之比例，應遵循相關法令規範或中華民國虛擬通貨商業同業公會所發布之自律規範。

[6] 混合管理下，VASP 之自有虛擬資產占客戶冷錢包內客戶虛擬資產之比例，應遵循相關法令規範或中華民國虛擬通貨商業同業公會所發布之自律規範。

	(三) VASP 僅於為支付鏈上瓦斯費，始得將其虛擬資產存放於客戶之冷錢包，且 VASP 之自有虛擬資產占客戶冷錢包內客戶虛擬資產之比例不得超過 20%。

1.3 虛擬資產託管管理

目的：當 VASP 將客戶之虛擬資產託管予第三方信託機構時，為確保第三方信託機構能符合 VASP 資產分離保管內部控制制度之標準，特訂定虛擬資產託管管理之作業程序與控制重點，以保護客戶虛擬資產之安全。

作業	作業程序及控制重點
1.3.1 虛擬資產託管管理	一、作業程序 (一) 虛擬資產託管管理 1 VASP 應對第三方信託機構之資格及能力作充分之了解與評估，以確保第三方信託機構保管虛擬資產之安全性，並將相關評估結果作成書面紀錄。例如確認第三方信託機構信用狀況、是否進行外部審計以及第三方信託機構對虛擬資產分離保管之內部控制。**【控制重點一】【控制重點二】【控制重點三】【控制重點五】** 2 VASP 將冷錢包與私鑰轉交予第三方信託機構。 3 錢包記帳人員應定期將委託第三方信託機構託管之虛擬資產之帳上數量與公鏈數量相互核對，發現數量不一致時，應及時查明原因並編製調節表，若屬系統或人為疏失產生之錯誤，應作適當之修正，若無法查明原因或作適當之修正，應及時向內部稽核部門報告，差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。**【控制重點四】** 二、控制重點 (一) VASP 應對第三方信託機構之資格及能力作充分之了解與評估，並將相關評估結果作成書面紀錄。 (二) VASP 於委託第三方信託機構前，應確認該第三方信託機構在管理 VASP 託管之虛擬資產時，係與第三方信託機構之其他虛擬資產分離保管，不得存放於相同之錢包。 (三) 第三方信託機構保管 VASP 之客戶虛擬資產之錢包中，不得包含 VASP 本身之虛擬資產。 (四) 錢包記帳人員應定期將委託第三方信託機構託管之虛擬資產之帳上數量與區塊鏈瀏覽器顯示之錢包餘額相互核對，若發現數量不一致時，若無法查明原因或作適當之修正，應及時向內部稽核部門報告，差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。 (五) VASP 應定期確認第三方信託機構將 VASP 託管之虛擬資產與第三方信託之其他虛擬資產分離保管。

1.4 虛擬資產資訊安全管理

目的：為防止資訊系統受未經授權之存取、使用、控制、洩漏、破壞、竄改、銷毀或其他外部惡意侵害，並確保客戶資料與虛擬資產之機密性與安全性，特訂定虛擬資產資訊安全管理之作業程序與控制重點，以達成資產分離保管內部控制制度目標。

作業	作業程序及控制重點
1.4.1 風險評鑑與管理	一、作業程序 (一) 資訊資產風險鑑別 1 於定義各資訊資產群組時，依該資產可能遭受之侵害發生時，其喪失機密性、完整性、可用性所造成之衝擊，以及該等侵害導致違法/違約之可能性，據以判斷該資產之風險潛在後果並進行區分。 2 依 VASP 對資訊安全事件所設有的相關控制措施判斷風險發生之可能性並進行區分。 3 綜合風險潛在後果與風險發生之可能性等因素，透過 VASP 風險評鑑工具，計算風險權值，作為選擇控管措施之依據。 4 風險評鑑執行人員每年至少執行一次風險評鑑，評鑑時應考量 VASP 內外部議題、識別、分析及評估相關威脅、弱點和潛在影響、利害關係人之要求。【控制重點(一)】 5 風險評鑑執行人員依風險權值將資訊資產進行分級，資訊資產清冊中之資產進行分級後，建立「風險評鑑清冊」送風險評鑑單位主管或擁有資訊資產之單位主管簽核，該分級視實際情況予以調整及修正。**【控制重點(二)】** (二) 資訊資產風險管理 1 管理階層與資訊安全管理組織依據組織政策、業務需求及目標決定可接受風險值。可接受風險值須每年進行評估並視情況調整。 2 針對超過可接受風險值之資訊系統資產制定風險處理計畫,於計畫中說明相關風險控制措施,該措施採取(1)降低、(2)避免、(3)轉移及(4)接受之執行方法應對，各項風險處理方式應由資訊資產權責單位確認並核准。**【控制重點(三)】** 3 風險處理計畫訂定完成後，由相關權責單位執行風險處理計畫，並於改善期間內定期回報。建立相對應之指標用以反映控制措施實施之狀況及成效，並做成書面報告。 4 確認控制措施結果與期望間之差異，持續對控制措施進行改善，重新評估風險權值直至其降至可接受風險值。**【控制重點(四)】**

	二、控制重點 (一) 風險評鑑執行人員應每年對虛擬資產資訊系統中之各項資產進行風險評鑑，並留存相關紀錄。 (二) 風險應經適當評鑑並經風險評鑑單位主管或擁有資訊資產之單位主管核准。 (三) VASP 應依其本身可能面臨之風險訂定控制措施。 (四) 風險評鑑執行人員應定期評估該控制措施之適當性、合理性及有效性並進行改善。
1.4.2 資訊安全政策	一、作業程序 1 資訊安全管理組織應依據相關法令規定及 VASP 業務需求，訂定資訊安全政策、資訊安全作業程序。**【控制重點(一)】** 2 訂定 VASP 資訊安全目標： (1) 確保 VASP 資訊資產之機密性，防止資訊資產遭非授權存取 (2) 確保 VASP 資訊資產之完整性，防止資訊資產未經授權異動或內容不正確 (3) 確保 VASP 資訊資產之可用性，並維持依賴資訊系統之業務持續運作 (4) 確保 VASP 資訊作業均符合相關法令規定與合約要求 3 訂定 VASP 之資訊安全控制措施： (1) 成立資訊安全管理組織，督導資訊安全管理制度之運作，鑑別資訊安全管理制度之內、外部議題及利害相關團體對 VASP 資訊安全管理之要求與期望 (2) 管理階層應承諾維護資訊安全，持續改善資訊安全品質，減少資訊安全事件之發生，以及制定並定期更新資訊安全事件應變計畫。 (3) 資訊安全管理制度文件應適時更新，紀錄保護應有明確管理機制 (4) 定期進行資訊資產分類、盤點與風險評鑑 (5) VASP 全體人員皆有責任及義務保護公司及其個人接觸、擁有、保管或使用之資訊資產 (6) 工作分派應考量職能分工，職務責任範圍應予區分，以避免資訊或服務未經授權修改或誤用 (7) 人員安全管理、資訊安全宣導與資訊安全教育 (8) 對於與 VASP 有業務往來之廠商及其員工、訪客等外部人員，如有存取 VASP 資訊資產之需求時，應進行必要之文件化審核並傳達、溝通本公司有關資訊安全管理之要求。該等人員並負有保護其所接觸、擁有、保管或使用之 VASP 資訊資產之責任，並簽署保密協議。 (9) 依業務需求訂定資訊作業持續營運計畫，並定期測試演練

	(10) 落實通訊安全管理 (11) 確保工作區域場所之安全，以防範資訊資產遭竊取或毀損 (12) 定期量測資訊安全指標，以維持資訊安全管理制度及管控程序實施之有效性 (13) 應用系統或軟體開發、修改及建置，皆須符合並遵循資訊安全目標之規定 (14) 本政策適用對象應隨時注意是否有發生資訊安全事件、安全弱點及違反安全政策與規範之虞之情事，並依程序進行通報 (15) 遵循內、外部相關法令規定，建立應有管控程序，定期執行資訊安全查核作業 4 所訂定之資訊安全政策，提交管理階層核准後，正式發布要求所有員工共同遵守。**【控制重點(二)】、【控制重點(三)】** 5 違反任何資訊安全政策之人員可能會面臨與其違規成比例之紀律處分後果，管理階層將確定員工的違法行為的嚴重程度，並採取適當的行動。 6 訂定之資訊安全政策，應至少每年審查一次，以反映法令規章、技術及業務等最新發展現況，確保資訊安全實務作業之有效性，定期做必要之調整。於發生重大資訊安全事件或重大業務變更時，應立即進行審查並更新政策。**【控制重點(四)】** 7 資訊安全政策之評估，應以獨立及客觀之方式進行，並由內部或委託外部專業機構辦理。 8 發生資安事件時，應即刻通報內部資安部門。如涉及客戶個人資料外洩，應向主管機關通報**【控制重點(五)】** 9 VASP 應辦理核心系統導入資訊安全管理系統，並通過公正第三方之驗證，且持續維持驗證有效性。**【控制重點(六)】** 二、控制重點 (一) 資訊安全管理組織應依據相關法令規定及 VASP 業務需求，訂定資訊安全政策、資訊安全作業程序。 (二) 資訊安全政策應經管理階層核准。 (三) VASP 應將資訊安全政策發布予所有員工。 (四) 權責單位應每年至少一次對資訊安全政策進行審查。 (五) 發生資安事件應依照資安事件程度進行通報。 (六) 資訊安全管理系統應定期通過公正第三方之驗證。
1.4.3 安全組織設立	一、作業程序 1 VASP 配置適當人力資源及設備負責資訊安全制度之規劃、監控及執行資訊安全管理作業，

	且專門負責資訊安全相關工作或職務，不得兼辦資訊或其他與職務有利益衝突之業務。 2 VASP 指定副總經理或高層主管人員，綜理資訊安全政策推動及資源調度事務，成立跨部門之「資訊安全管理組織」；如 VASP 符合主管機關所訂一定條件者，指定副總經理以上或職責相當之人兼任資訊安全長辦理上開業務。 3 資訊安全管理組織可再依工作職掌細分為：資訊安全推動小組、資訊安全執行小組、資訊安全緊急處理小組、資訊安全查核小組。 4 訂定各小組人員之工作職掌： (1) 資訊安全推動小組：召開資訊安全管理審查會議，討論資訊安全相關問題、審查及訂定資訊安全管理相關政策及措施、與其他部門（如 IT、人力資源、法務等）建立合作與溝通機制 (2) 資訊安全執行分組：執行並報告資訊安全風險評鑑方法及風險評鑑結果、協助執行資訊安全管理制度之控制措施 (3) 資訊安全緊急處理小組：建立資訊安全事件分級、通報及應變機制，明確規定通告流程及應變時限。災害發生時，負責災後協調、災區指揮及原作業現場修復 (4) 資訊安全查核小組：對 VASP 之資訊安全管理制度進行內部查核。 5 資訊安全管理組織成員應建冊列管，以釐清資訊安全責任，並填寫於「資訊安全組織成員表」，遇人員異動時應加以更新。**【控制重點(一)】** 資訊安全管理審查會議由資訊安全推動小組召開，每年應至少召開會議一次。會議內容包含對 VASP 現行之資訊安全管理制度之評估、資訊安全事件之報告、資訊安全人員權責之指派及其他依據國際資訊安全管理制度標準須進行審查之議題。前開國際資訊安全管理制度標準，例如： (1) ISO27001/27701/27017/27018 國際標準 (2)歐盟雲端服務星級驗證制度（EuroCloud Star Audit, ECSA） (3)美國雲端安全聯盟（Cloud Security Alliance, CSA）STAR (4)SOC2 Type 2 認證要求**【控制重點(二)】** 6 資訊安全人員及主管每年定期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，每年至少接受一小時以上資訊安全宣導課程。重要資訊處理人員應簽署保密協議並定期(至少一年一次)審查保密協議內容，以確認是否重新簽署保

	密協議。**【控制重點(三)】、【控制重點(四)】** 7 VASP 資訊安全人力、能力及經驗，如有不足之處，得委請外界的學者專家或民間專業組織及團體，提供資訊安全顧問諮詢服務。 8 VASP 應依其所屬資安分級[7]（若尚無適用之資安分級，則依其所營事業規模與性質）要求資訊安全人員取得並維持適當之資通安全專業證照。**【控制重點(五)】** 二、控制重點 (一) VASP 應訂定相關人員之工作職掌與兼辦業務情形之規定，並應依規定配置適當人力資源及設備執行資訊安全管理作業，且資訊安全管理組織成員名單應建冊並適時更新。 (二) 資訊安全推動小組應每年召開資訊安全管理審查會議對現有資訊安全管理依實際狀況調整。 (三) 資訊安全人員及使用資訊系統之從業人員應定期參加資訊安全課程訓練。 (四) 重要資訊處理人員應簽署保密協議並定期（至少一年一次）審查保密協議內容以確認是否重新簽署保密協議。 (五) 資訊安全人員應依 VASP 所屬資安分級（若尚無適用之資安分級，則依其所營事業規模與性質）取得並維持適當之資通安全專業證照。
1.4.4 資產分類與控制	一、作業程序 1 資訊資產權責單位鑑別所管轄之資訊資產，依資訊資產之類型、用途與重要性對資訊資產予以適當群組化，資訊資產分為以下類別：(1)硬體、(2)軟體、(3)資料、(4)文件、(5)人員，並將資產類型分組後彙整建立「資訊資產清冊」，呈報資訊安全推動小組進行確認。每年至少進行一次資訊資產盤點。**【控制重點(一)】** 2 資訊資產應明確標示其類別，妥善規劃各類資訊資產之保護方式、交換方式及存取對象等。 3 各類資訊資產之異動，須由資訊資產保管者向資訊資產權責單位主管申請核准，資訊資產清冊管理人員須依經核准之申請單進行資訊資產清冊維護。資訊資產清冊管理人員應將該等異動呈報資訊安全組織。**【控制重點(二)、(三)】** 4 有關資料類型之資訊資產，再依據敏感程度區分標示為：公開資料、內部資料、客戶機密及公司機密。並依其敏感程度訂定資料保護措施，包括資料之收集、加密、備份、存取及授權等。**【控制重點(四)】** 5 規範資料及文件類型之資訊資產之保存期限，並於保存期限到期後進行刪除與銷毀，除為確

7 依數位發展部發布之「資通安全責任等級分級辦法」之規定。

	立權利或合約之證明而須儲存之資料。**【控制重點(五)】** 二、控制重點 (一) 資訊資產清冊應呈報資訊安全推動小組進行確認，且每年至少進行一次資訊資產盤點。 (二) 各類資訊資產之異動，應由資訊資產保管者向資訊資產權責單位主管申請核准。 (三) 資訊資產清冊管理人員須依經核准之申請單進行資訊資產清冊維護。 (四) 資訊資產權責單位應對資料類型之資訊資產明確標示其敏感程度，並依其敏感程度訂定資料保護措施並執行。 (五)資料類型資訊資產保管者應於資訊資產之保存期限到期後刪除與銷毀該資產。
1.4.5 人員安全	一、作業程序 1 對員工之背景進行調查，若其背景係偽造、錯誤或具誤導性，VASP 不應予以錄用，涉及財務、虛擬資產管理、資訊安全職位之人員，應進行信用紀錄與犯罪紀錄審查。**【控制重點(一)】** 2 與員工之合約應說明其於 VASP 對資訊安全方面之責任並記錄在案，當雇傭條件發生變化或終止時，應重申及記錄資訊安全之責任。另依相關法令課予機密維護責任，並填具保密切結書。**【控制重點(二)】** 3 針對人員之調動、離職或退休，應立即取消或調整其識別碼、存取權限，並收繳其通行證、卡及相關證件。**【控制重點(三)】** 4 定期（每年至少一次）對全 VASP 員工辦理資訊安全宣導講習（例如：資訊安全政策、資訊安全法令規定、資訊安全作業程序以及如何正確使用資訊科技設施等），並留存紀錄。 5 員工每年應依職務層級進行適當之資訊安全與個資保護教育訓練，並達內部所定之訓練時數。提供開發角色人員每年進行安全開發教育訓練，包括如何避免常見的程式漏洞。**【控制重點(四)】** 二、控制重點 (一) VASP 應對員工進行背景調查才得以錄用。 (二) VASP 應於合約明定員工應盡之資訊安全責任。 (三) VASP 應對異動之人員調整其資產存取及使用權限。 (四) 全 VASP 員工每年應依職務層級接受適當之資訊安全與個資保護教育訓練。
1.4.6 實體與環境安全	一、作業程序 (一) VASP 營業處所管制區域管理 1 界定電腦機房為重要管制區域，為確保相關設施之安全，非權責單位授權之人員不得擅自進

	入電腦機房或使用相關資訊設備。 2 電腦機房設有適當之門禁管制(例如：刷卡)，並應保持上鎖，若門未關閉則應發出警報。並每年定期審查電腦機房門禁權限。**【控制重點(一)】** 3 電腦機房指派專員管理，其作業項目如下： (1)機房門口應揭示值班操作人員姓名及值班期間。 (2)機房應設出入登記簿，記錄除系統管理人員及值班操作人員外之出入狀況，並配備監控錄影設備進行 24 小時監控，錄影資料至少保存 30 天，並限制存取權限。**【控制重點(二)】** (3)電腦機房監控錄影設備的拍攝應避免死角，拍攝範圍至少應包含處理虛擬資產之相關設備，且監控錄影設備與門禁應定期進行校時，以確保時間紀錄之正確性。 (4)使用機房內機具應經機房值班人員或系統管理人員同意。 (5)機房內各項作業情形，應設置環境監控機制，以管理電信、空調、消防、門禁、監視及機房溫溼度等，並設置工作日誌記錄，且記錄應保留至少六個月。**【控制重點(三)】** 4 電腦機房內設置防火設施及緊急照明設備。另應將地震、水災等天然災害因素列入考量。VASP 應委託廠商定期檢查各項安全設備 (至少一年一次)，員工應施予適當之安全設備使用訓練。**【控制重點(四)】** 5 設置獨立之空調系統及電源供應系統供電腦設備使用，定期或不定期測試其堪用性，並應規畫適當之備援對策。 6 電腦機房管理專員應隨時注意環境監控系統，掌握電腦機房內濕度及溫度維持正常。 7 為確保電腦系統正常運作，資訊資產權責單位應委託廠商定期保養、維修，並由具合格資格及經授權之廠商人員進行保養與修理設備。廠商人員於保養或維修設備時，應有相關人員會同檢修。 8 電腦機房之設備保養與修理完成後，經電腦機房操作人員檢查驗收後，紀錄於工作日誌，並交付權責主管確認。 9 未具電腦機房進出權限之人員，因執行業務需求進入機房時，須填寫「人員進出機房申請表」，向資訊資產權責單位或保管單位申請核准，由該資訊資產權責單位或保管單位指派人員隨行，將經核准之申請表交予電腦機房管理專員後方可進出電腦機房，並遵守相關設備管理之規定。**【控制重點(五)】** 10 「人員進出機房申請表」應定期經權責單位審閱，由電腦機房管理人員留存，以供備查。 (二) 一般設備安全管理

	1 員工及所租用建築物之工作人員，利用具有存取權限之識別證，控制對 VASP 辦公室之進出，並配備監控錄影設備，進行 24 小時監控，錄影資料至少保存 30 天，並限制存取權限。**【控制重點(六)】** 2 員工於下班時，須將標示為機敏性資料之文件適當存放並予以上鎖。 3 人員長時間離開座位時，伺服器或個人電腦應啟動螢幕保護與密碼保護機制，並將機敏性資料予以妥善收存。**【控制重點(七)】** 4 可攜式設備（如筆記型電腦、平板電腦等）之使用分配應受權責主管核准後始得配發，並記錄其各項設備之保管人。**【控制重點(八)】** 5 可攜式設備僅限於公務使用，禁止安裝使用非法與未經核准之軟體、非業務需用之套裝軟體或應用軟體，並定期檢視(每年至少乙次)使用軟體情形，經察覺有使用非法或未經核准之軟體一律刪除，並呈報權責單位主管。**【控制重點(九)】** 6 可攜式設備若有遺失之情事發生，應立即通報權責主管及 IT 人員，並評估資料遺失是否具有機敏性，依情節之重大程度決定是否向上呈報。 7 訂定設備報廢作業程序，報廢前應填寫報廢申請單，將機密性、敏感性資料及授權軟體予以移除、實施安全性覆寫或實體破壞，應確保報廢之電腦硬碟及儲存媒體儲存之資料不可還原，經資訊資產權責單位主管檢查並於報廢申請單簽核後，方可報廢該設備，並留存報廢紀錄以供查驗。若委託第三者銷毀時，應簽訂保密合約。**【控制重點(十)】** (三) 訪客管制 1 所有訪客進入公司前需進行登記，並由內部員工陪同進入公司。**【控制重點(十一)】** 2 所有訪客需配戴臨時識別證，並不得以未經授權之設備存取內部網路。 二、控制重點 (一) VASP 應每年定期審查電腦機房之門禁權限。 (二) 機房應配備監控錄影設備進行 24 小時間監控，錄影資料至少保存 30 天，並限制存取權限。 (三) 電腦機房管理專員應每日於工作日誌紀錄管理狀況，該紀錄應包括電腦機房內濕度及溫度，且應保留至少六個月。 (四) VASP 應委託廠商定期檢查電腦機房內之各項安全設備（至少一年一次）。 (五) 非授權之人員須經申請核准方能進入電腦機房，進出紀錄須紀錄留存。 (六) 辦公室應有管制措施（如門禁系統）並配備監控錄影設備，不具權限之人員不得進出。 (七) 伺服器或個人電腦應啟動螢幕保護與密碼保護機制。

	(八) 可攜式設備之使用分配應受權責主管核准後始得配發，並記錄其各項設備之保管人，並建立相關遺失通報程序。 (九) 定期檢視(每年至少乙次)使用軟體情形，經察覺有使用非法或未經核准之軟體一律刪除，並呈報權責單位主管。 (十) 資訊資產權責單位應確實依設備報廢作業程序移除機敏性資料後，方可報廢該設備。 (十一) 訪客進入須登記並經由內部人員陪同進入公司。
1.4.7 通訊與作業管理	一、作業程序 (一) 網路系統安全 1 定期評估公司網路系統安全(例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等)，將相關評估結果留存紀錄。**【控制重點(一)】** 2 定期檢視網路運作環境及作業系統之安全漏洞並修補（含伺服器、攜帶型、個人端及營業處所內供投資人共用之電腦等），並確保安全防護工具為最新，並留存相關文件。**【控制重點(二)】** 3 網路應考量業務需求、系統效能及網路安全等因素區分為外部網段、DMZ 網段、內部網段、公有雲端服務、私有雲端服務及混合雲端服務等，並有適當區隔機制(如防火牆、虛擬區域網路、實體隔離等)。**【控制重點(三)】** 4 因業務或營運需要新增之設備或元件，須遵照各網段使用之用途設計及安全管理政策，不可任意交叉混用或串接。 5 若為租用之公有雲端服務時應評估服務供應商對多重租戶間網路區隔管理是否符合 VASP 日常作業以及為提供服務之需求，並檢視該公有雲端服務就服務內容、範圍及性質是否通過適用之國際資訊安全標準，例如： (1) ISO27001/27701/27017/27018 國際標準 (2)歐盟雲端服務星級驗證制度（EuroCloud Star Audit, ECSA） (3)美國雲端安全聯盟（Cloud Security Alliance, CSA）STAR (4)SOC2 Type 2 認證要求 6 有關電腦網路安全（如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等）之事項應隨時對內部公告，機敏資料應適當存放。**【控制重點(四)】** (二) 網路連線管理 1 應於網路控制措施設定存取控制列表（ACL），以過濾並控制各網段之間以及 VASP 對網際網

	路提供服務之封包流向、通訊協定或網路頻寬流量，以避免未經授權之存取或不預期之過度資源耗用影響服務水準。 2 因應新增服務及通訊協定需調整前述於存取控制列表（ACL）時應經可能影響之資產擁有者授權。 3 VASP 訂定遠端連線管理辦法，對使用外部網路遠端連線至 VASP 內部作業進行控管，並應至少辦理下列防護措施： (1)遠端連線申請。 (2)設定網路防火牆，管控連線來源。 (3)透過 VPN 或 SSH 等加密連線機制進行連線，並採用高強度密碼或多因子進行身分驗證。**【控制重點(五)】** 4 留存相關申請及維護紀錄並由權責主管定期覆核。 (三) 網路設備之安全管理 1 重要網站及伺服器系統（如網路下單系統等）應建立防火牆與外網路隔離，以控管外部與內部間資料之傳輸與存取之安全性，防火牆應由權責管理人員執行控管。系統之防火牆進出紀錄及其備份應至少保存三年。**【控制重點(六)】** 2 如欲對防火牆設定進行異動時，應進行申請並經權責單位主管核准後，交由權責管理人員設定。**【控制重點(七)】** 3 VASP 每年定期檢視並維護防火牆存取控管設定，每半年檢視 DMZ 區之防火牆規則，並留存相關檢視紀錄。 4 與核心系統相關之網路設備應至少每年檢視一次存取控制列表（ACL）及網路服務，並更新。**【控制重點(八)】** (四) 網路傳輸管理 1 VASP 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，以確保為客戶本人登入。多因子認證方式應具下列至少任兩項技術： (a)VASP 所約定之資訊，且無第三人知悉（如固定密碼、圖形鎖或手勢等） (b)客戶所持有之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等），VASP 應確認該設備為客戶與 VASP 所約定持有之設備 (c)客戶提供給 VASP 其所擁有之生物特徵（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），VASP 應直接或間接驗證該生物特徵**【控制重點(九)】**

	2　利用公眾網路、行動網路或無線網路傳送機密等級資訊，應將資料加密保護，以保護資料在公眾網路傳輸的完整性及機密性，並保護連線作業系統之安全性，以避免其被未經授權之存取。 二、控制重點 (一) 應定期評估網路系統安全(例如：網站伺服器、瀏覽器、防火牆及防毒版本等)，將相關評估結果留存紀錄。 (二) 應定期檢視網路運作環境與作業系統之安全漏洞並修補，並將相關執行結果予以紀錄。 (三) VASP 應有適當網路之區隔機制。 (四) VASP 應將有關網路安全（如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等）相關事項公告予內部人員加以宣導，機敏資料應適當存放。 (五) VASP 應訂定遠端連線管理辦法並進行適當防護措施。 (六) VASP 應建立防火牆，並應由權責管理人員執行控管且定期檢視防火牆規則是否允當。 (七) 防火牆規則欲進行異動應經適當權責單位主管核准，權責管理人員應依經核准之防火牆異動申請單設定防火牆。 (八) 權責管理人員應設定存取控制列表（ACL）並每年至少檢視一次，並更新，以避免有未經授權之存取。 (九) 網路下單系統登入應採用多因子驗證。
1.4.8 存取控制	一、作業程序 (一) 權限管理 1　權限之申請及異動 1.1　應訂定資訊系統存取控制相關規定。**【控制重點(一)】** 1.2　欲使用資訊資產之員工依據其職務所需，針對作業系統、應用系統、資料庫系統、網路設備申請相對應之權限，應透過足以文件化、記錄申請/核准跡證之平台提出申請、異動或停用。 1.3　外部單位人員因業務需要申請或停用帳號與權限時，由對該外部單位人員之協助有需求之員工代為申請。 1.4　經該資訊資產權責單位主管依據申請人員負責之職務與申請內容進行必要之評估後核准。**【控制重點(二)】**

	1.5 各作業系統、應用系統、資料庫系統、網路設備資產保管人員依據申請之業務需求與內容及該資訊資產權責單位主管之核准，設定申請人員的存取權限。**【控制重點(三)】** 1.6 有關職務調動及離職時存取權限之停用，除有業務需求外，應於異動生效日即停用其存取權限，如因各式不可抗力無法由職務調動及離職提出申請，應由其代理人/職務交接人/權責主管逕行提出申請。交由資產保管人員依核定結果執行申請人之權限更動，並將該變動紀錄留存。**【控制重點(四)】** 2 進駐於 VASP 內之委外作業人員應納入公司安全管理，如欲使用內部網路資源測試時，應有安全管制措施。資訊安全人員檢查委外人員所使用之電腦紀錄，確認未授予委外人員過高之電腦通行使用權限或不當之使用權限，且於委外期間結束後，立即取消該項權限，以免被盜用、竄改資料。**【控制重點(五)】**、**【控制重點(六)】** 3 各資訊資產之存取及授權應依據職務性質進行區分（如系統開發、系統測試、系統上線、系統維護、設備管理）。不同職務性質不可出現兼任之情形。**【控制重點(七)】** 4 權責主管應定期（至少每半年一次）審查資通系統帳號及權限之適切性，並視審查結果停用資通系統閒置帳號（為客戶帳號除外）。**【控制重點(八)】** (二) 特權帳號管理 1 資通系統之特權帳號應經正式申請並經適當管理階層或治理單位核准方能使用，特權帳號授權前應妥善審查其必要性，其授權及審查記錄應留存。**【控制重點(九)】** 2 資通系統之特權帳號不得共用。 3 對於特權帳號，宜指派與該使用者日常公務使用之不同使用者 ID。 4 特權帳號之使用應保留稽核軌跡，並由資訊安全人員定期覆核使用結果，以防範未經授權之使用。如為核心資通系統，應於該等帳號被使用時，定期（至少每季一次）覆核使用結果。**【控制重點(十)】** (三) 密碼管理 1 完成帳號與權限設定後，應以安全方式交遞密碼，如：專函、使用 Email 加密傳遞或電話口頭告知等安全方式，並要求於第一次使用時應變更密碼，系統預設之初始密碼應被停用或刪除。妥善保管帳號與維持密碼之機密性，保存帳號密碼之檔案應以加密方式處理。如無交遞密碼之流程，則不適用。**【控制重點(十一)】**、**【控制重點(十二)】** 2 固定密碼之設定應訂定密碼原則機制（如最小密碼長度、複雜度、密碼歷史、帳戶鎖定閾值、帳戶鎖定時間等）。**【控制重點(十三)】**

	3　不應共用使用者帳號密碼，若有工作上代理之需要，應於代理結束後，立即更新密碼。 4　重要系統如因業務需求需使用共用帳號者，應以適當方式留存共用帳號之稽核軌跡。 5　對於使用者忘記密碼之處理，VASP 應有嚴格的身分確認程序，方可變更密碼以再次使用系統。**【控制重點(十四)】** 6　每日針對帳號登入失敗紀錄、嘗試登入嘗試紀錄等進行監控及分析，發現有帳號登入異常情事，系統於有此等情事時通知相關權責單位，相關權責單位應即時了解異常原因，並留存相關紀錄。**【控制重點(十五)】** 7　VASP 應訂定並執行金鑰之安全管理規定，包含有關用以產生、儲存、封存、檢索、分發、汰除及銷毀金鑰之規定。**【控制重點(十六)】** 二、控制重點 (一) VASP 應訂定資訊系統存取控制相關規定。 (二) 欲使用資訊資產之員工對存取權限之申請須經該資訊資產權責單位主管核准。 (三) 資產保管人員應依經核准之申請設定存取權限，並對設定情形進行記錄。 (四) 職務調動及離職時存取權限，已於異動生效日即停用。 (五) 資訊安全人員應檢查委外人員所使用之電腦紀錄。 (六) 資產保管人員應於委外人員之委外期間結束後立即將其權限取消。 (七) 各資訊資產之存取權限及授權應依職務性質進行區分(如系統開發、系統測試、系統上線系統維護、設備管理)，不同職務性質不可出現兼任之情形。 (八) 權責主管應定期（至少每半年一次）審查資通系統帳號及權限之適切性，並視審查結果停用資通系統閒置帳號（為客戶帳號除外）。 (九) 資通系統之特權帳號應進行申請並經適當管理階層或治理單位核准。 (十) 資訊安全人員應定期覆核特權帳號之使用紀錄。 (十一)　使用者密碼於首次使用後應進行更改，使用者更改之密碼應符合密碼原則，系統預設之初始密碼應被停用或刪除。 (十二)　帳號與密碼資訊應以加密方式保存。 (十三)　固定密碼之設定應訂定密碼原則機制。 (十四)　每次密碼變更時，系統應對該使用者之身分進行驗證。 (十五)　系統於有帳號登入異常情事時應通知相關權責單位，相關權責單位應即時了解異常原因，並

	留存處理紀錄。 (十六)　VASP 應訂定並執行金鑰之安全管理規定。
1.4.9 系統開發及維護	一、作業程序 (一) 資訊系統開發 1　系統之新增及修改應根據部門之技術能量、開發進度、預算及需要，來評估是開發還是購買外部製造商開發之系統。 2　若有開發新系統或更改現有系統功能之需求，根據使用者之需求提交開發需求請求文件，並載明具體系統開發需求事由，經申請單位主管覆核後送交申請至系統開發單位。**【控制重點(一)】** 3　系統開發單位收到需求申請後，依 VASP 業務及系統狀況進行可行性評估並制定開發計畫，並與使用單位進行討論和確認，以滿足使用單位之需求。**【控制重點(二)】** 4　開發計畫應將資訊安全納入考量，如涉及重要資料之存取及傳輸，須使用加密技術進行保護，亦可以邀請資訊安全或個人管理權責相關人員參與討論。 5　系統開發人員進行開發所進行之開發測試環境須與正式環境分離。**【控制重點(三)】** 6　系統開發及測試不應使用正式資料進行，如必須使用生產資料進行測試操作，則應考慮相關控制措施以保護資料的機密性 7　系統開發人員將系統開發完成後記錄開發結果，送交測試或申請單位進行測試驗收確認符合申請單位需求後，視需求之內容由資訊安全單位及系統相關權責單位或申請單位相關權責管理人員覆核後進行上線。其中，程式不應由系統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並由權責管理人員依程式原始碼管理機制完成，以確保職責明確分隔。**【控制重點(四)】** 8　系統開發時，應定期進行安全測試，以確保系統沒有潛在安全隱憂。 (二) 資訊系統維護 1　權責管理人員應對虛擬資產系統定期辦理弱點掃描、滲透測試及程式原始碼覆核或安全檢測等資安檢測作業，對發現之系統弱點進行修補。 2　若欲對系統弱點進行維護，權責管理人員提出系統維護申請送交權責單位主管進行覆核，並通知相關影響單位維護實施時間，以利維護作業之執行。 3　系統維護作業完成後，權責管理人員應對維護結果進行測試並記錄，且通知權責單位主管進行覆核。如有更新之系統資訊，則通知相關單位確認完成維護作業。**【控制重點(五)】** 二、控制重點

	(一) 系統開發需求申請應經申請單位主管核准。 (二) 系統開發人員應對經核准之系統開發需求申請進行可行性評估，並將資訊安全納入考量，以確認符合 VASP 資訊安全制度。 (三) 開發測試環境需與正式環境分離，且不應使用正式資料進行，如必須使用生產資料進行測試操作，則應考慮相關控制措施以保護資料的機密性。 (四) 開發完成之系統應經申請單位測試驗收以符合申請單位需求，其中系統程式換版或產製比對報表不應由系統開發人員執行，並經資訊安全單位主管及系統相關權責單位或申請單位相關權責人員覆核。 (五) 權責管理人員應對所檢測出來之系統弱點（包含弱點掃描、滲透測試及程式原碼覆核或安全檢測等資安檢測作業）進行維護並記錄，送交權責單位主管進行覆核。
1.4.10 營運持續管理	一、作業程序 1 資訊安全管理單位訂定系統故障復原程序，其內容至少包含下列項目之說明： (1)資料庫、檔案及程式之備援回復、(2)電腦作業系統備援及回復、(3)電腦設備備援及設備故障回復、(4)通訊設備及線路之備援及回復及(5)電力系統備援及回復。 2 系統故障復原程序經資訊安全管理單位進行週期性測試，測試後應召開檢討會議，針對測試缺失謀求改進，並留存紀錄。**【控制重點(一)】** 3 資訊安全管理單位與業務單位研討重大異常狀況發生時，根據狀況發生時點、考慮系統發生之作業需求型態、影響之業務層面及相關人員應採取之應變措施，訂定人工配合之備援計畫，以及需包含電腦系統等故障復原標準作業程序。 4 資訊安全管理單位應擬訂營運持續計畫（含起動條件、參與人員、緊急程序、備援程序、維護時間表、教育訓練、職責說明、往來外單位之應變規劃及合約適當性等）及其必要之維護，並擬訂關鍵性業務及其衝擊影響分析，評估核心系統中斷造成之衝擊程度。並依系統之復原時間目標（RTO）、資料復原點目標（RPO），作為恢復系統、備份備援規劃及執行復原作業之依據，並明訂分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。**【控制重點(二)】** 5 資訊安全管理單位擬定之營運持續計畫依其所營事業規模與性質定期（至少一年一次）辦理業務持續運作演練，VASP 應視營運持續計畫之參與人員是否涉及第三方，邀請相關廠商參與演練，並記錄演練結果進行檢視修正。**【控制重點(三)】** 6 資訊安全管理單位定期評估營運系統及設備之事故應變措施，對評估結果採取適當措施，並

	提報董事會；於永續報告書、年報、財務報告或公司網站，揭露年度內 VASP 持續營運系統及設備營運之資安政策或教育訓練計畫等項目。**【控制重點(四)】** 二、控制重點 (一) 資訊安全管理單位應訂定系統故障復原程序並定期進行測試。 (二) 資訊安全管理單位應訂定營運持續計畫。 (三) 營運持續計畫應定期（至少一年一次）完整演練並針對演練結果對營運持續計畫予以修正。 (四) 資訊安全管理單位應定期評估營運系統及設備之事故應變措施。
1.4.11 資通系統或資通服務(錢包託管技術)委外辦理	一、作業程序 (一) 委外作業計畫及廠商選用 1 業務單位承辦人員將擬進行委外業務之工作範圍、目標與需求，應對委外業務之可行性及成本效益進行評估，由業務單位主管核准評估之結果。**【控制重點(一)】** 2 業務單位承辦人員申請成立專案，將該業務資訊安全需求項目，包括基礎環境需求、系統功能需求、安全需求等進行規畫，並提交規劃書由業務單位主管核准。 3 業務單位承辦人員依據其規畫書之要求對委外廠商資格進行審核，應考量委外廠商之專業能力與經驗，並評估委外廠商提供之資訊安全需求服務之風險等級是否於 VASP 之可接受風險範圍內。所有供應商每年皆須重新評估一次。**【控制重點(二)】** 4 業務單位承辦人員擬定委外廠商服務契約，並載明「服務水準協議(SLA)」、資通安全責任及保密規定、資安要求及對委外廠商資安稽核權，經權責主管或人員核准後向委外廠商進行招標採購。**【控制重點(三)】** (二) 委外作業監督管理 1 決定選用之委外廠商應視服務模式提供完整之系統架構說明文件，送交資訊安全人員進行確認方得以測試實施。 2 委外作業人員提出作業所需內容及權限申請需求，經資訊安全人員核准後於有效期間內開放授權方得以存取資料進行使用，資訊安全人員應定期檢視系統操作紀錄。**【控制重點(四)】** 3 如有交付軟體或程式之廠商，委外廠商服務正式上線前與正式資料分隔開發、測試及運作，委外作業人員完成服務並出具報告後，送交業務單位承辦人員及資訊安全人員確認驗收。 4 資訊安全人員於開發、測試及運作中辨別可能產生之資安事故，針對該等事故設計應採取之控制措施。

	5　如有交付軟體或程式之廠商，資訊安全人員對委外廠商交付之服務系統檢查其未有植入後門程式等惡意程式，確認符合 VASP 委外規畫之需求並遵循相關法令後進行上線。**【控制重點(五)】** 6　委外作業人員須定期交付進行上線後之服務結果報告予資訊安全人員，資訊安全人員亦須定期對委外作業系統進行安全維護檢查。**【控制重點(六)】** 7　委外廠商應定期提出第三方獨立機構對其資通安全之審查報告。**【控制重點(七)】** 8　合約中應訂定與委外廠商資訊委外關係終止、解除或結束後之相關作業。對於委外廠商於委外關係所涉及之 VASP 資訊資產，應於委外關係終止、解除或結束時完整歸還、確保銷毀或轉交予其他資訊服務委外廠商，並要求資訊服務委外廠商持續遵守保密承諾。**【控制重點(八)】** 二、控制重點 (一) 業務單位承辦人員對擬委外業務之可行性及成本效益進行評估，該評估結果應由業務單位主管核准。 (二) 業務單位承辦人員應依其規畫書之要求條件評估委外廠商，並將相關評估結果作成書面紀錄。 (三) 業務單位承辦人應訂定與委外廠商之契約，該契約條款應至少包含「服務水準協議(SLA)」、資通安全責任及保密規定、資安要求及對委外廠商資安稽核權，並經業務單位主管評估後核准。 (四) 委外作業人員之資料存取權限應經適當核准。 (五) 資訊安全人員應對委外廠商交付之服務系統檢查其未有植入後門程式等惡意程式，確保系統符合需求後始正式上線運作。 (六) 資訊安全人員應定期檢查委外作業系統之安全性。 (七) 委外廠商應定期提出第三方獨立機構對其資通安全之審查報告。 (八) 合約中應訂定委外關係於終止、解除或結束後之相關作業。
1.4.12 新興科技應用	一、作業程序 (一) 雲端服務 1　雲端服務申請者應於使用雲端服務或新增既有雲端服務應用樣態、範圍（例如原本已採用某雲端服務提供者 IaaS 服務，但須另行購置資料分析 SaaS 服務）前，進行下列雲端服務評估程序： 1.1　雲端服務申請者釐清自身業務需求以及導入新雲端服務、變更既有雲端服務之適切性，並透過開放性之討論/徵詢作為，瞭解可能涉及之資訊系統維運、資通安全、機敏資訊保護等管理議題。**【控制重點(一)】**

	1.2 與資訊安全管理單位討論現有資訊系統是否足以涵蓋相關業務要求，探討所進行之作業確實有使用雲端服務的必要性；若導入相關雲端服務可能涉及之資安控管需求，包含但不限於存取控制、網路資料流內容控制與過濾、加密技術等。 2 雲端服務申請者應評估可能適格之雲端服務提供廠商（包含評估廠商機房之實體安全，檢視其機房是否已符合國際安全標準，審查其機房監控政策以確保有 24 小時監控攝影機且監控設備的拍攝範圍涵蓋所有處理虛擬資產的相關設備），基於該雲端服務提供廠商所提供服務之導入對既有資訊環境營運作業可能產生之需求與影響，評估該雲端服務之導入可行性。適當管理階層或治理單位應確認該可行性評估結果，方可核准購置。**【控制重點(二)】** 3 核准雲端服務之購置後，應考量其是否影響核心業務執行，如有則須與雲端服務提供者簽訂服務協定，明確定義其服務水準，服務等級協議與訂定服務水準不良時之相關罰則。 4 合約中應敘明雲端服務提供廠商應提出第三方獨立機構對其雲端機房物理安全措施之審查報告；雲端服務提供廠商應建立資安事件防護機制、設置工作日誌及流量監控；雲端服務提供廠商應提供門禁及監控錄影設備的定期校時紀錄；雲端服務提供廠商應監控並建立資通安全事件通報程序及處理程序，應於雲端服務運作發生資訊安全事件時，立即通知 VASP 相關人員，依程序辦理並定期更新事件處理的相關訊息；雲端服務提供廠商應提供備援及應變計畫，確保在安全事件發生時，能夠快速回復並提供足夠軌跡紀錄，查找原因並究責；如使用雲端服務期間，服務提供者頻發無法滿足服務水準，或針對支援需求處理時效、成效不佳之情事，且依契約處罰仍未見改善者，得考量終止租用相關服務。**【控制重點(三)】** 5 VASP 應對傳輸及儲存至雲端服務提供廠商之客戶資料或敏感資料，採行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。**【控制重點(四)】** 6 雲端服務申請者應於終止雲端服務使用時，確認雲端服務提供廠商在一定期限內，以無法復原之方式，刪除於使用服務期間之所有用戶資訊。**【控制重點(五)】** (二) 行動裝置 1 公務用之行動裝置 1.1 VASP 應對於行動裝置之申請、使用、更新、繳回與審核應訂有相關規範。**【控制重點(六)】** 1.2 人員異動時，行動裝置應進行重新配置或清除配置程序，以確保行動裝置環境安全性。 1.3 風險評鑑執行人員對行動裝置與行動裝置可存取之資源應進行風險評估作業，並依據風險評估結果採取適當之安全控管措施，如：螢幕鎖定、限制存取敏感資料、安裝防毒軟

	體、安裝行動裝置管理軟體等。**【控制重點(七)】** 1.4 組織針對存有敏感性資料之行動裝置宜採行以下安全控管措施： (1)行動裝置宜建立身分識別機制。 (2)行動裝置之作業系統環境設定宜由被授權者進行變更。 (3)行動裝置之作業系統與防毒軟體宜定期檢查，避免持有者私自異動設定，如：越獄（Jailbreaking）或提權（Rooting）。 (4)行動裝置宜考量遺失時資料清除方式，如：以遠端方式刪除資料或透過身分認證錯誤超過規定次數後自動刪除機制。 (5)行動裝置宜限制或關閉不需要之無線連線功能，如：NFC 、紅外線、Wifi 或藍芽等。 (6)行動裝置傳輸敏感性資料時，宜採加密或資料遮蔽方式進行保護。 (7)行動裝置宜限制敏感性資料儲存於行動裝置上或將敏感性資料進行加密保護。 1.5 行動裝置應避免安裝非官方發佈之行動應用程式，或僅安裝由 VASP 列出通過檢測可安裝之行動應用程式。行動裝置應對未通過檢測之行動應用程式之安裝設定阻擋程式。**【控制重點(八)】** 2 員工自攜行動裝置 2.1 VASP 應訂定員工自攜行動裝置之資訊安全規範與管理辦法，須包含以下項目： (1)員工自攜行動裝置之預定用途。 (2) (3)員工自攜行動裝置使用限制(如限制內部資訊設備透過員工自攜行動裝置私接存取網際網路（Internet))。 (4)行動裝置儲存機密資料之限制與管理方式。**【控制重點(九)】** (三) 物聯網 1 VASP 應建立物聯網設備管理清冊(可納入資訊資產清冊中)並至少每年更新一次，以識別設備用途、網路設定、存放位置與管理人員，評估適當之實體環境控管措施及存取權限管制。**【控制重點(十)】** 2 物聯網設備應具備安全性更新機制且定期（每年一次）更新，如存在已知弱點無法更新時，應建立補償性管控機制。**【控制重點(十二)】** 3 物聯網設備應具備身份驗證機制或配對綁定機制，並應變更該等設備之初始密碼，且以最小權限原則針對不同的使用者身分進行授權，確保僅能由經授權之使用者進行資料存取、設備

	管理及安全性更新等操作。**【控制重點(十三)】** 4 應關閉物聯網設備不必要之網路連線及服務，避免使用對外公開的網際網路位置。 5 VASP 採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。 6 如與物聯網設備供應商簽定採購合約時，其內容應包含資訊安全相關協議，明確約定相關責任（如：服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案），確保設備不存在已知安全性漏洞。**【控制重點(十二)】** 7 VASP 應定期辦理物聯網設備使用及管理人員資安教育訓練。 (四) 深度偽造（Deepfake） 1 使用影像視訊方式進行身分驗證時應強化驗證並搭配其他驗證因子（如上傳身分證件、手機簡訊 OTP），VASP 應留存影像或照片，以利後續查證。**【控制重點(十四)】** 2 VASP 如提供電話交易服務，應訂定身分驗證程序（如語音密碼）避免非本人之假冒。委託人以語音委託時，應配合電信機構開放顯示發話端號碼之功能，記錄其來電號碼。**【控制重點(十五)】** 3 VASP 應定期辦理涵蓋深度偽造認知及防範議題之資訊安全教育訓練。 二、控制重點 (一) 雲端服務申請者應對雲端服務之需求、適切性及可能涉及之資訊安全進行評估，該評估應包括與資訊安全單位討論。 (二) 雲端服務申請者對雲端服務提供廠商所提供雲端服務之購置申請，應檢附經確認之可行性評估結果，並經適當管理階層或治理單位核准。 (三) 合約中應訂定雲端服務提供廠商於雲端服務運作發生資訊安全事件時之資通安全事件通報程序及處理程序。 (四) 應對傳輸及儲存至雲端服務提供廠商之客戶資料或敏感資料，採行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。 (五) 於終止雲端服務使用時，雲端服務申請者應確認雲端服務提供廠商應於一定期限內刪除其服務期間之所有用戶資訊。 (六) VASP 應訂定公務用行動裝置之申請、使用、更新、繳回與審核等相關資訊安全規範與管理辦法。 (七) 風險評鑑執行人員應對行動裝置可存取之資源進行風險評估作業，並依據風險評估結果採取適當之安全控管措施。 (八) 行動裝置應對未通過檢測之行動應用程式之安裝設定阻擋程式。

	(九) VASP 應訂定員工自攜行動裝置之資訊安全規範與管理辦法，包括裝置使用用途、限制裝置私接存取網際網路及行動裝置儲存機密資料之限制與管理方式等。 (十) VASP 應建立物聯網設備管理清冊並至少每年更新一次。 (十一) 物聯網設備應具備安全性更新機制且定期（每年一次）更新，如存在已知弱點無法更新時，VASP 應建立補償性控管機制。 (十二) 物聯網設備應具備身份驗證機制或配對綁定機制，並應變更該等設備之初始密碼。 (十三) VASP 與物聯網設備供應商簽訂採購合約時，其內容應包含資訊安全相關協議（如：服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案）。 (十四) VASP 應對使用影像視訊方式進行身分驗證之客戶使用強化驗證並搭配其他驗證因子，並留存影像或照片。 (十五) VASP 應對使用電話交易服務之客戶，訂定身分驗證程序（如語音密碼）避免非本人之假冒。
1.4.13 符合性	一、作業程序 (一) 應定期(每年至少乙次)辦理虛擬資產資訊安全管理查核作業(內部辦理或委託外部專業機構)，並應留存查核紀錄。**【控制重點(一)】** (二) 公司是否針對前開之查核報告辦理追蹤改善情形(包括查核摘要、查核範圍、缺失說明及改善建議等)。**【控制重點(二)】** 二、控制重點 (一) VASP 是否定期(每年至少乙次)辦理虛擬資產資訊安全管理查核作業(內部辦理或委託外部專業機構)。 (二) 針對前項查核作業所發現之缺失項目是否進行追蹤及改善。

第2章 會計師對保管客戶資產執行協議程序之指引

2.1 會計師對保管客戶資產執行協議程序之指引

2.1.1法定貨幣/虛擬資產餘額驗證之協議程序

VASP 每一項作業之控制重點	會計師執行之協議程序
2.1.1.1 法定貨幣入金作業	
（一）權責人員應針對入金之客戶進行風險控管檢核措施（如 AML 檢核、客戶資格權限比對及入金限額等），確認客戶確實具備法定貨幣交易之資格。	1. 抽查權責人員針對入金之客戶進行風險控管檢核措施（如 AML 檢核、客戶資格權限比對及入金限額等）之紀錄，以確認已由權責人員進行檢核。 2. 抽查入金之客戶明細，比對至具備法定貨幣交易資格之客戶明細，以確認通過入金申請之客戶是否於具備法定貨幣交易資格之清單中。
（二）出納人員應每日透過比對網銀明細或其他銀行傳輸之資訊 ，確認系統帳戶入金之金額與銀行入金之金額一致。	3. 抽查出納人員之確認紀錄，以確認出納人員是否確實確認系統帳戶入金之金額與網銀明細或其他銀行傳輸之資料入金金額一致。 4. 抽查網銀明細或其他銀行傳輸之資料入金金額，比對至系統帳戶之入金紀錄，以確認網銀明細或其他銀行傳輸之資料入金金額與系統帳戶入金之金額是否一致。
（三）若當日發生退款時，出納人員應製作當日法定貨幣退款明細，並透過當日網銀退款明細或其他銀行傳輸之資訊，以確認已將相關款項正確地退還給應退款	5. 抽查出納人員確認當日法定貨幣退款明細與當日網銀或其他銀行傳輸之資料退款明細之紀錄，並確認該紀錄中是否包含出納人員之簽名及確認日期。

之客戶。	6. 抽查網銀或其他銀行傳輸之資料退款明細，比對至法定貨幣退款明細，以確認出納人員是否將相關款項正確地退還給應退款之客戶。
（四）VASP 就虛擬資產交易及其款項代收付業務收受客戶之法定貨幣，應與其自有之法定貨幣分離保管，並應交付信託或取得銀行十足之履約保證，且除為其客戶辦理前述業務外，不得動用前款客戶之法定貨幣。	7. 檢查 VASP 內部控制制度文件，確認其內部控制制度中是否明確規定就虛擬資產交易及其款項代收付業務收受客戶之法定貨幣，應與其自有之法定貨幣分離保管。 8. 檢查信託合約或十足履約保證契約以確認 VASP 是否已將客戶之法定貨幣交付信託或取得銀行十足之履約保證。核對第三方信託合約銀行對帳單金額與 VASP 之客戶法定貨幣帳簿餘額，確認該帳簿餘額是否與對帳單金額一致以確定 VASP 是否確實將其客戶法定貨幣皆交付信託；或核對銀行對帳單與履約保證契約，確認 VASP 之客戶法定貨幣餘額皆未超過履約保證契約之額度。 9. 抽查 VASP 系統中之客戶法定貨幣變動紀錄，比對至客戶之虛擬資產交易相關法定貨幣變動申請及出金明細，確認對交付信託之法定貨幣之動用中無非屬客戶之虛擬資產交易相關法定貨幣及出金之動用，以確認明細餘額之正確性。
（五）VASP 就所保管之客戶法定貨幣，應留存紀錄（應至少包括姓名及法定貨幣餘額等）。	10. 抽查 VASP 系統中之客戶法定貨幣變動明細表中是否包含姓名及法定貨幣餘額。
（六）取得銀行十足之履約保證之 VASP，其收受客戶之法	11. 抽查客戶入金之銀行帳戶是否與 VASP 自身之銀行帳戶不同。

定貨幣應與其自身之法定貨幣分離保管，不得存放於相同之銀行帳戶。	
2.1.1.2 法定貨幣出金/退款作業	
（一）VASP 權責人員應針對出金之客戶進行 AML 檢核與風險控管檢核措施(如客戶資格權限比對等)確認客戶確實具備法定貨幣交易之資格。	1. 抽查申請出金客戶之 AML 檢核與風險控管檢核紀錄，並確認該紀錄中是否包含檢核人員簽名及檢核日期，以確認 VASP 權責人員是否確認客戶確實具備法定貨幣交易之資格。 2. 抽查出金成功之客戶清單，比對至其 AML 檢核與風險控管檢核之紀錄，以確認該等客戶皆經 AML 檢核與風險控管檢核。
（二）VASP 系統人員應確認未通過作業程序第 2 項所述之風險控管檢核措施或 VASP 合作之第三方信託銀行之 AML 檢核之客戶，VASP 已對該客戶進行對應之處理流程。	3. 抽查未通過 AML 檢核之客戶明細，比對至系統，以確認 VASP 是否已對該客戶進行對應之處理流程。
（三）當日出金明細表及信託指示書或同等效力文件應確實經覆核人員簽核或依其他方式覆核核准。	4. 抽查當日出金明細表之個別客戶出金明細，與客戶線上操作之出金指示核對，確認個別客戶出金金額正確。抽查當日出金明細表及信託指示書或同等效力文件之覆核紀錄，以確認該等文件是否經覆核人員確實簽核。
（四）法幣出納人員應確認網銀或其他銀行傳輸之資訊出金紀錄與當日出金明細表金額一致，並經覆核人員簽核或依其他方式覆核核准。	5. 抽查法幣出納人員確認網銀或其他銀行傳輸之資訊出金紀錄與當日出金明細表之紀錄，以確認法幣出納人員是否確認相關明細餘額之正確性並經覆核人員簽核。

（五）當日退款明細表及信託指示書或同等效力文件應確實經覆核人員簽核或依其他方式覆核核准或依其他方式覆核核准。	6. 抽查當日退款明細表及信託指示書或同等效力文件之覆核紀錄，以確認該等文件是否經覆核人員確實簽核。
（六）法幣出納人員應確認網銀或其他銀行傳輸之資訊退款紀錄與當日退款明細表金額一致及確認已退款至客戶綁定之銀行帳號或原匯入之非綁定帳戶，並經覆核人員簽核或依其他方式覆核核准。	7. 抽查法幣出納人員確認網銀或其他銀行傳輸之資訊退款紀錄與當日退款明細表金額一致，以及已退款至客戶綁定之銀行帳號或原匯入之非綁定帳戶之紀錄，以確認法幣出納人員是否確認相關明細餘額之正確性並經覆核人員簽核。
2.1.1.3 虛擬資產入金與接收作業	
（一）VASP 進行虛擬資產買賣、接收、發送、移轉服務時應確實記錄與保存，該保存之交易紀錄應足以重建個別交易。	1. 檢查 VASP 是否於虛擬資產買賣、接收、發送、移轉確實保存交易記錄。 2. 抽查 VASP 系統中保存之交易紀錄是否足以重建個別交易。
（二）VASP 就所保管之客戶虛擬資產，應留存紀錄（應至少包括客戶錢包地址、姓名、虛擬資產種類、及數量等）。	3. 抽查 VASP 是否紀錄所保管之客戶虛擬資產（應至少包括客戶錢包地址、姓名、虛擬資產種類、及數量等）。
（三）VASP 收到未完成實名制身分驗證者之虛擬資產後（包含無主入金），應予以記錄列管，並於發現異常時通報司法警察機關。	4. 檢查 VASP 是否紀錄列管未完成實名制身分驗證者之虛擬資產後（包含無主入金），如發現異常時通報司法警察機關。
（四）VASP 如收到黑名單或詐騙嫌疑等高風險客戶及地址所發送的虛擬資產時，應依法向法務部調查局	5. 抽查 VASP 收到黑名單或詐騙嫌疑等高風險客戶及地址所發送的虛擬資產時，是否依法向法務部調查局申報可疑交易。

申報可疑交易。	
2.1.1.4 虛擬資產發送與提領作業	
（一）VASP 系統應確實記錄相關申請資訊，包括客戶發送至外部之錢包接收地址、交易幣種、交易數量、交易時間、交易序碼（TxID）等。	1. 抽查 VASP 系統是否正確與完整紀錄虛擬資產發送與提領申請紀錄，包含客戶發送至外部之錢包接收地址、交易幣種、交易數量、交易時間、交易序碼（TxID）。
（二）若提領之客戶及該外部錢包接收地址係 VASP 標註為黑名單或詐騙嫌疑等高風險客戶，VASP 系統應限制該筆提領交易。	2. 抽查虛擬資產提領申請紀錄是否有 VASP 標註為黑名單或詐騙嫌疑等高風險客戶或外部錢包地址之申請。若有，檢查系統拒絕該等申請之紀錄。
（三）確認客戶提領申請後，VASP 系統應確認熱錢包內餘額是否足夠。如遇熱錢包餘額不足時(水位過低)，系統應推播通知錢包管理人員進行錢包移轉。	3. 檢查 VASP 系統是否確認客戶提領申請後熱錢包內餘額是否足夠。 4. 檢查 VASP 系統是否於熱錢包餘額不足時（水位過低），推播通知錢包管理人員進行錢包移轉。
（四）系統應確實將虛擬資產移轉至客戶指定之錢包地址。	5. 抽查系統完成提領之紀錄，比對至客戶申請紀錄，以確認系統是否確實將虛擬資產移轉至客戶指定之錢包地址。
2.1.1.5 法定貨幣餘額驗證作業	
（一）法幣出納人員應核對合作之第三方信託銀行法定貨幣出入金變動明細與 VASP 帳上法定貨幣出入金金額相符，並經覆核人員簽核或依其他方式覆核核准。	1. 抽查合作之第三方信託銀行法定貨幣出入金變動明細與 VASP 帳上法定貨幣出入金金額之核對紀錄，以確認是否係由法幣出納人員核對且皆經覆核人員簽核。 2. 抽查合作之第三方信託銀行法定貨幣出入金變動明細，比對至

	VASP 帳上法定貨幣出入金金額，以確認合作之第三方信託銀行法定貨幣出入金變動明細是否與 VASP 帳上法定貨幣出入金金額相符。
（二）法幣出納人員應核對合作之第三方信託銀行法定貨幣當日網銀或其他銀行傳輸資訊餘額與 VASP 法定貨幣帳簿餘額相符，並經覆核人員簽核或依其他方式覆核核准。	3. 抽查第三方信託銀行法定貨幣當日網銀或其他銀行傳輸資訊餘額與 VASP 法定貨幣帳簿餘額之核對紀錄，以確認是否係由法幣出納人員核對且皆經覆核人員簽核。 4. 抽查第三方信託銀行法定貨幣當日網銀或其他銀行傳輸資訊餘額，比對至 VASP 法定貨幣帳簿餘額，以確認第三方信託銀行法定貨幣當日網銀或其他銀行傳輸資訊餘額是否與 VASP 法定貨幣帳簿餘額相符。
（三）法幣出納人員發現金額不一致，應及時查明原因並編製調節表並交由覆核人員進行簽核或依其他方式覆核核准，若屬系統或人為疏失產生之錯誤，應作適當之修正，並由適當權責人員覆核調節表。	5. 檢查調節表，以確認法幣出納人員是否編製調節表，並檢查各項調整項目是否有相應之支持文件，並經適當權責人員覆核調節表。 6. 檢查屬系統或人為疏失產生之錯誤之金額不一致紀錄，檢查其相對應之修正紀錄，以確認該等錯誤皆已被修正。
（四）法幣出納人員發現金額不一致時，若無法查明原因或作適當之修正，應及時向內部稽核部門報告，差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。	7. 檢查當期是否有無法查明原因或作適當修正之紀錄。若有，檢查對內部稽核部門之報告紀錄，以確認該等不一致已向內部稽核部門報告。對於該等報告紀錄中被標示為差異重大且無法查明原因者，檢查董事會會議紀錄，以確認該等差異重大且無法查明原因

	之不一致已向董事會報告。
2.1.1.6 虛擬資產餘額驗證作業	
（一）錢包記帳人員應核對屬於客戶及屬於 VASP 之各幣種錢包（包括冷、溫及熱錢包）之虛擬資產餘額表與錢包帳上之餘額是否相符。	1. 由 VASP 提供各錢包地址，案件執行人員隨機指定錢包移轉之特定金額及特定時點，觀察錢包移轉是否符合案件執行人員之預期，以確認錢包是否係 VASP 所有。 2. 透過區塊鏈瀏覽器抽查確認錢包餘額。 3. 抽查屬於客戶及屬於 VASP 之各幣種錢包（包括冷、溫及熱錢包）之虛擬資產餘額表與錢包帳上餘額之核對紀錄，以確認是否係由錢包記帳人員核對且皆經覆核人員簽核。 4. 抽查屬於客戶及屬於 VASP 之各幣種錢包（包括冷、溫及熱錢包）之虛擬資產餘額表，比對至錢包帳上之餘額，以確認該等錢包之虛擬資產餘額表與錢包帳上之餘額是否相符。
（二）錢包記帳人員應核對各幣種錢包（包括冷、溫及熱錢包)之虛擬資產變動表與錢包帳上之變動數是否相符。	5. 抽查各幣種錢包（包括冷、溫及熱錢包）之虛擬資產變動表與錢包帳上變動數之核對紀錄，以確認是否係由錢包記帳人員核對且皆經覆核人員覆核。 6. 抽查各幣種錢包（包括冷、溫及熱錢包）之虛擬資產變動表，比對至錢包帳上之變動數，以確認錢包之虛擬資產變動表與錢包帳上之變動數是否相符。
（三）錢包管理人員或錢包記帳人員發現數量不一致	7. 檢查調節表，以確認錢包管理人員或錢包記帳人員是否編製調節

時應及時查明原因並編製調節表說明，若屬系統或人為疏失產生之錯誤，應作適當處置並及時向內部稽核部門報告，如係差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。	表，並檢查各項調整項目是否有相應之支持文件。 8. 檢查屬系統或人為疏失產生之錯誤之金額不一致紀錄及相對應之修正紀錄，以確認該等錯誤皆已被修正。 9. 檢查當期是否有無法查明原因或作適當修正之紀錄。若有，檢查對內部稽核部門之報告紀錄，以確認該等不一致已向內部稽核部門報告。對於該等報告紀錄中被標示為差異重大且無法查明原因者，檢查董事會會議紀錄，以確認該等差異重大且無法查明原因之不一致已向董事會報告。

2.1.2錢包管理之協議程序

VASP 每一項作業之控制重點	會計師執行之協議程序
2.1.2.1 將虛擬資產由熱錢包移轉至溫錢包作業	
（一）錢包管理相關職能人員具有清晰的權責分工，以確保其所擔任的職能滿足內部控制控制環境的要求。	1. 檢查錢包管理相關職能與分工是否經公司之制度政策或文件予以定義，並確認該等職能已據此劃分予不同人員。
（二）即時通知之水位設定應依照公司錢包水位之規定，以及應確實於達到門檻水位時即時通知。	2. 檢查即時通知之水位設定是否係依照公司錢包水位之規定。 3. 檢查即時通知紀錄，以確認系統是否確實於達到門檻水位時發出通知。

（三）虛擬資產於錢包間移轉的過程，應具備機制協助相關簽核人員確保簽核移轉的地址為指定之白名單錢包地址。	4. 檢查公司是否建立錢包白名單，並定義白名單新增、修改、刪除之流程與授權規則。
（四）錢包移轉應確實簽核並註明簽核之日期與時間。	5. 抽查系統之錢包移轉紀錄，以確認錢包移轉係經所有權責人員簽核。
（五）保管私鑰或私鑰分片的簽核人員應具有清晰的職能分配以及對其責任的理解，以利於使用私鑰的時機與情境能夠遂行其獨立判斷。	6. 取得並檢視相關職能說明文件，以確認是否對保管私鑰或分片之人員有明確職能分配與權責敘述。
（六）錢包移轉完成後，相關人員應確認虛擬資產已移轉至指定之白名單錢包地址。	7. 抽查系統之錢包移轉紀錄，以確認所移轉之錢包地址是否皆是白名單錢包地址。
（七）應具備內控措施確保資產移轉依要求於合理期間內完成。	8. 檢查是否對移轉期限建立規定，並抽查交易以確認是否於期限內完成資產移轉。
2.1.2.2 將虛擬資產由溫錢包移轉至冷錢包作業	
（一）錢包管理相關職能人員具有清晰的權責分工，以確保其所擔任的職能滿足內部控制控制環境的要求。	1. 檢查錢包管理相關職能與分工是否經公司之制度政策或文件予以定義，並確認該等職能已據此劃分予不同人員。

（二）即使通知之水位設定應依照公司錢包水位之規定，以及應確實於達到門檻水位時即時通知。	2. 檢查即時通知之水位設定是否係依照公司錢包水位之規定。 3. 檢查即時通知紀錄，以確認系統是否確實於達到門檻水位時發出通知。
（三）虛擬資產於錢包間移轉的過程，應具備機制協助相關簽核人員確保簽核移轉的地址為指定之白名單錢包地址。	4. 檢查公司是否建立錢包白名單，並定義白名單新增、修改、刪除之流程與授權規則。
（四）錢包移轉應確實簽核並註明簽核之日期與時間。	5. 抽查系統之錢包移轉紀錄，以確認錢包移轉係經所有權責人員簽核。
（五）保管私鑰或私鑰分片的簽核人員應具有清晰的職能分配以及對其責任的理解，以利於使用私鑰的時機與情境能夠遂行其獨立判斷。	6. 取得並檢視相關職能說明文件，以確認是否對保管私鑰或分片之人員有明確職能分配與權責敘述。
（六）錢包移轉完成後，相關人員應確認虛擬資產已移轉至指定之白名單錢包地址。	7. 抽查系統人員確認虛擬資產已移轉至指定之白名單錢包地址之紀錄。 8. 抽查系統之錢包移轉紀錄，以確認所移轉之錢包地址是否皆是白名單錢包地址。
（七）應具備內控措施確保資產移轉依要求於合理期間內完成。	9. 檢查是否對移轉期限建立規定，並抽查交易以確認是否於期限內完成資產移轉。
2.1.2.3 將虛擬資產由溫錢包移轉至熱錢包作業	

（一）錢包管理相關職能人員具有清晰的權責分工，以確保其所擔任的職能滿足內部控制控制環境的要求。	1. 檢查錢包管理相關職能與分工是否經公司之制度政策或文件予以定義，並確認該等職能已據此劃分予不同人員。
（二）虛擬資產於錢包間移轉的過程，應具備機制協助相關簽核人員確保簽核移轉的地址為指定之白名單錢包地址。	2. 檢查公司是否建立錢包白名單，並定義白名單新增、修改、刪除之流程與授權規則。
（三）錢包移轉應確實簽核並註明簽核之日期與時間。	3. 抽查系統之錢包移轉紀錄，以確認錢包移轉係經所有權責人員簽核。
（四）保管私鑰或私鑰分片的簽核人員應具有清晰的職能分配以及對其責任的理解，以利於使用私鑰的時機與情境能夠遂行其獨立判斷。	4. 取得並檢視相關職能說明文件，以確認是否對保管私鑰或分片之人員有明確職能分配與權責敘述。
（五）錢包移轉完成後，相關人員應確認虛擬資產已移轉至指定之白名單錢包地址。	5. 抽查系統之移轉紀錄，以確認所移轉之錢包地址是否皆是白名單錢包地址。
（六）應具備內控措施確保資產移轉依要求於合理期間內完成。	6. 檢查是否對移轉期限建立規定，並抽查交易以確認是否於期限內完成資產移轉。
2.1.2.4 將虛擬資產由冷錢包移轉至溫錢包作業	
（一）錢包管理相關職能人員具有清晰的權責分工，以確保其所擔任的職能滿足內部控制控制環境的要求。	1. 檢查錢包管理相關職能與分工是否經公司之制度政策或文件予以定義，並確認該等職能已據此劃分予不同人員。
（二）虛擬資產於錢包間移轉的過程，應具備機制協助相關簽核人員確保簽核移轉的地址為指定之白名單錢包	2. 檢查公司是否建立錢包白名單，並定義白名單新增、修改、刪除之流程與授權規則。

地址。	
（三）錢包移轉應確實簽核並註明簽核之日期與時間。	3. 抽查系統之錢包移轉紀錄，以確認錢包移轉係經所有權責人員簽核。
（四）保管私鑰或私鑰分片的簽核人員應具有清晰的職能分配以及對其責任的理解，以利於使用私鑰的時機與情境能夠遂行其獨立判斷。	4. 取得並檢視相關職能說明文件，以確認是否對保管私鑰或分片之人員有明確職能分配與權責敘述。
（五）錢包移轉完成後，相關人員應確認虛擬資產已移轉至指定之白名單錢包地址。	5. 抽查系統之移轉紀錄，以確認所移轉之錢包地址是否皆是白名單錢包地址。
（六）應具備內控措施確保資產移轉依要求於合理期間內完成。	6. 檢查是否對移轉期限建立規定，並抽查交易以確認是否於期限內完成資產移轉。
2.1.2.5 錢包與私鑰管理作業	
（一）錢包水位設定應經董事會或適當之治理單位通過。	1. 檢查董事會會議紀錄，以確認錢包水位設定是否經董事會或適當之治理單位通過。
（二）客戶之虛擬資產存放於冷錢包之比例應經董事會或適當之治理單位通過。該比例如有變動亦應經董事會或適當之治理單位通過。	2. 檢查董事會會議紀錄，以確認客戶之虛擬資產存放於冷錢包之比例或其變動是否經董事會或適當之治理單位通過。 3. 檢查 VASP 內部控制制度文件，確認內部控制制度中是否明確規定客戶之虛擬資產存放於冷錢包之比例。
（三）具備清晰的錢包設立規定(包含白名單錢包)，並應依VASP的規模與營運複雜度對錢包設定進行調整(如	4. 檢查 VASP 內部控制制度文件，確認內部控制制度中是否明確規定錢包之設立與調整規定。

冷錢包設立的數量以及其使用特性)。	
（四）IT 人員生成錢包地址時監督人員應負責監控操作過程，並具備清晰的操作指引。	5. 抽查錢包地址生成申請表之簽章紀錄，以確認監督人員是否監控操作過程。
（五）錢包管理人員應適時更新冷錢包地址，並訂有須立即更新之情況。	6. 檢查冷錢包地址之更新紀錄，以確認錢包管理人員是否適時更新冷錢包地址。
（六）IT人員生成冷錢包私鑰時，監督人員應負責監控操作過程，並具備清晰的操作指引。	7. 抽查冷錢包私鑰生成紀錄，以確認監督人員是否有監控操作過程。
（七）移轉虛擬資產時，相關申請人員、覆核人員、監督人員、錢包地址與時間應確實紀錄以備供查詢，上述移轉紀錄應至少保留 5 年。	8. 抽查移轉虛擬資產之相關紀錄是否妥善保存至少五年。
（八）錢包與私鑰管理，應考量其權責人員執掌與相關系統存取權限是否有職能衝突之風險。	9. 取得對系統權限管理人員、私鑰管理人員及錢包管理人員之職能配置相關文件（例如職掌表、人員清冊或系統權限列表等），檢查系統權限管理人員、私鑰管理人員及錢包管理人員的權責是否在考量職能衝突風險下明確定義，且經管理階層核決。
（九）VASP應將80%以上之客戶虛擬資產存放於冷錢包。	10. 取得客戶冷錢包虛擬資產餘額表及客戶虛擬資產總額，計算客戶冷錢包之虛擬資產餘額是否達客戶虛擬資產總額80%以上。
（十）VASP將客戶虛擬資產存放於熱錢包之比例不得超過客戶虛擬資產總額之 20%。	11. 取得客戶熱錢包虛擬資產餘額表及客戶虛擬資產總額，計算客戶熱錢包虛擬資產餘額是否未超過客戶虛擬資產總額 20%。
（十一）VASP 除依法令所訂之事由外，不得動用客戶之虛	12. 抽查客戶錢包（包含冷、溫及熱錢包）虛擬資產變動表，確認該

擬資產。	等變動是否皆來自客戶發起之虛擬資產交易、系統因錢包儲存水位達門檻而發出之警示通知、因 2.1.2.6 作業流程第一項所述之營運目的所需或法令所訂之事由。
2.1.2.6 客戶虛擬資產與 VASP 虛擬資產於相同錢包下之混合管理	
（一）VASP 虛擬資產僅於符合作業流程第一項營運目的所需時，始得將其虛擬資產存放於客戶之熱錢包。VASP須具備機制可以正確區分與管理混同資產的比例。	1. 抽查自 VASP 錢包移轉至客戶熱錢包之紀錄，以確認該紀錄中之移轉理由是否皆符合作業流程第一項之營運目的。 2. 檢查VASP是否建立辨認混同資產比例之管理機制。
（二）錢包管理人員應負責控管 VASP 存放至客戶錢包（包含熱及冷錢包）之虛擬資產餘額不得超過客戶之虛擬資產餘額之 20%。	3. 檢查 VASP 自有虛擬資產占客戶錢包（包含熱及冷錢包）內客戶虛擬資產之比例超過 20%之系統警示通知紀錄及相關錢包移轉紀錄，以確認每一系統警示通知是否皆有相關移轉紀錄（移轉理由應為依系統警示通知移轉）以及移轉紀錄是否依程序簽核。 4. 取得客戶錢包（包含熱及冷錢包）之虛擬資產餘額表，計算 VASP 存放至客戶錢包之虛擬資產餘額未超過客戶之虛擬資產餘額之 20%。
（三）VASP 僅於為支付鏈上瓦斯費，始得將其虛擬資產存放於客戶之冷錢包，且VASP之自有虛擬資產占客戶冷錢包內客戶虛擬資產之比例不得超過20%。	5. 檢查客戶冷錢包中之 VASP 虛擬資產之移轉紀錄，以確認該紀錄中之移轉理由是否僅為支付鏈上瓦斯費或因所存放之鏈上瓦斯費超過客戶之虛擬資產餘額之 20%。

2.1.3虛擬資產託管管理之協議程序

VASP 每一項作業之控制重點	會計師執行之協議程序
2.1.3.1 虛擬資產託管管理作業	
（一）VASP 應對第三方信託機構之資格及能力作充分之了解與評估，並將相關評估結果作成書面紀錄。	1. 檢查對第三方信託機構之評估紀錄，以確認 VASP 是否對第三方信託之資格及能力進行評估並記錄評估結果。
（二）VASP 於委託第三方信託機構前，應確認該第三方信託機構在管理 VASP 託管之虛擬資產時，係與第三方信託機構之其他虛擬資產分離保管，不得存放於相同之錢包。	2. 檢查 VASP 對第三方信託機構之評估紀錄是否包含第三方信託機構對虛擬資產分離保管之政策，以確認該第三方信託機構在管理 VASP 託管之虛擬資產時，是否係與第三方信託機構之其他虛擬資產分離保管。
（三）第三方信託機構保管 VASP 之客戶虛擬資產之錢包中，不得包含 VASP 本身之虛擬資產。	3. 檢查第三方信託機構之客戶虛擬資產保管紀錄，以確認第三方信託機構保管 VASP 之客戶虛擬資產之錢包中，是否包含 VASP 本身之虛擬資產。
（四）錢包記帳人員應定期將委託第三方信託機構託管之虛擬資產之帳上數量與區塊鏈瀏覽器顯示之錢包餘額相互核對，若發現數量不一致時，若無法查明原因或作適當之修正，應及時向內部稽核部門報告，差異重大且無法查明原因者，內部稽核部門應立即向董事會報告。	4. 抽查錢包記帳人員核對委託第三方信託機構託管之虛擬資產之帳上數量與區塊鏈瀏覽器顯示之錢包餘額之紀錄，以確認錢包記帳人員是否定期核對。 5. 檢查當期是否有無法查明原因或作適當修正之紀錄。若有，檢查對內部稽核部門之報告紀錄，以確認該等不一致已向內部稽核部門報告。若該等報告紀錄中有差異重大且無法查明原因者，檢查董事會會議紀錄，以確認該等差異重大且無法查明原因之不一致已向董事會報告。
（五）VASP 應定期確認第三方信託機構將 VASP 託管之虛	6. 檢查 VASP 之確認紀錄，以確認 VASP 託管之虛擬資產是否與

擬資產與第三方信託之其他虛擬資產分離保管。	第三方信託之其他虛擬資產分離保管。

2.1.4虛擬資產資訊安全管理之協議程序

VASP 每一項作業之控制重點	會計師執行之協議程序
2.1.4.1 風險評鑑與管理作業	
（一）風險評鑑執行人員應每年對虛擬資產資訊系統中之各項資產進行風險評鑑，並留存相關紀錄。	1. 抽查風險評鑑之紀錄，以確認風險評鑑執行人員是否每年對虛擬資產資訊系統中之各項資產進行風險評鑑。
（二）風險應經適當評鑑並經風險評鑑單位主管或擁有資訊資產之單位主管核准。	2. 抽查風險評鑑之紀錄，以確認資訊資產是否依風險權值進行分級，並確認風險評鑑是否經風險評鑑單位主管或擁有資訊資產之單位主管核准。
（三）VASP 應依其本身可能面臨之風險訂定控制措施。	3. 檢查 VASP 之風險評鑑清冊及風險處理計畫，以確認其是否依風險評鑑結果訂定控制措施。
（四）風險評鑑執行人員應定期評估該控制措施之適當性、合理性及有效性並進行改善。	4. 抽查 VASP 之控制措施評估紀錄，以確認風險評鑑執行人員是否定期評估該控制措施並依評估結果進行改善。
2.1.4.2 資訊安全政策作業	
（一）資訊安全管理組織應依據相關法令規定及 VASP 業務需求，訂定資訊安全政策、資訊安全作業程序。	1. 檢查資訊安全管理組織是否訂定資訊安全政策、資訊安全作業程序。
（二）資訊安全政策應經管理階層核准。	2. 檢查資訊安全政策核准紀錄，以確認資訊安全政策是否經管理階層核准。

（三）VASP 應將資訊安全政策發布予所有員工。	3. 檢查資訊安全政策發布紀錄，以確認資訊安全政策已發布。
（四）權責單位應每年至少一次對資訊安全政策進行審查。	4. 檢查 VASP 對資訊安全政策之審查紀錄，以確認權責單位是否每年至少一次對資訊安全政策進行審查。
（五）發生資安事件應依照資安事件程度進行通報。	5. 抽查 VASP 資安事件紀錄，以確認是否通報內部資安部門，如涉及客戶個人資料外洩，是否通報主管機關。
（六）資訊安全管理系統應定期通過公正第三方之驗證。	6. 檢查 VASP 之資訊安全管理系統驗證紀錄，以確認資訊安全管理系統是否定期通過公正第三方之驗證。
2.1.4.3 安全組織設立作業	
（一）VASP 應訂定相關人員之工作職掌與兼辦業務情形之規定，並應依規定配置適當人力資源及設備執行資訊安全管理作業，且資訊安全管理組織成員名單應建冊並適時更新。	1. 檢查 VASP 是否訂定相關人員之工作職掌與兼辦業務情形之規定。 2. 觀察 VASP 為執行資訊安全管理作業所配置之人力資源及設備，以確認 VASP 是否係依規定配置。 3. 檢查 VASP 之資訊安全管理組織成員名單是否建冊並適時更新。
（二）資訊安全推動小組應每年召開資訊安全管理審查會議對現有資訊安全管理依實際狀況調整。	4. 檢查 VASP 之資訊安全管理審查會議紀錄，以確認資訊安全推動小組是否每年召開資訊安全管理審查會議對現有資訊安全管理依實際狀況調整。
（三）資訊安全人員及使用資訊系統之從業人員應定期參加資訊安全課程訓練。	5. 檢查 VASP 之資訊安全課程訓練紀錄，以確認資訊安全人員主管是否接受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，及使用資訊系統之從業人員是否定期參加一小時以

	上資訊安全課程訓練。
（四）重要資訊處理人員應簽署保密協議並定期（至少一年一次）審查保密協議內容以確認是否重新簽署保密協議。	6. 檢查 VASP 審查重要資訊處理人員保密協議之紀錄，以確認 VASP 是否定期（至少一年一次）審查並適時要求重要資訊處理人員簽署保密協議。
（五）資訊安全人員應依 VASP 所屬資安分級（若尚無適用之資安分級，則依其所營事業規模與性質）取得並維持適當之資通安全專業證照。	7. 檢查 VASP 內部控制制度文件，確認其內部控制制度是否依所屬資安分級（若尚無適用之資安分級，則依其所營事業規模與性質）規定應取得並維持之資通安全專業證照。 8. 檢查取得資通安全專業證照之資訊安全人員名單，以確認其是否依其內部控制制度取得並維持資通安全專業證照。
2.1.4.4 資產分類與控制作業	
（一）資訊資產清冊應呈報資訊安全推動小組進行確認，且每年至少進行一次資訊資產盤點。	1. 檢查資訊安全推動小組確認資訊資產清冊之紀錄，並確認 VASP 是否每年至少進行一次資訊資產盤點。
（二）各類資訊資產之異動，應由資訊資產保管者向資訊資產權責單位主管申請核准。	2. 抽查資訊資產異動申請單，以確認資訊資產之異動是否經資訊資產權責單位主管核准。
（三）資訊資產清冊管理人員須依經核准之申請單進行資訊資產清冊維護。	3. 抽查資訊資產清冊維護紀錄，比對至資訊資產異動申請單，以確認各類資訊資產之異動是否已納入資訊資產清冊。 4. 抽查資訊資產異動申請單，比對至資訊資產清冊維護紀錄，以確認各類資訊資產之異動是否已納入資訊資產清冊。
（四）資訊資產權責單位應對資料類型之資訊資產明確標	5. 抽查資訊資產，以確認每一資訊資產之機密等級已明確標示。

示其敏感程度，並依其敏感程度訂定資料保護措施並執行。	6. 觀察資訊資產權責單位是否依其敏感程度確實執行資料保護措施。
（五）資料類型資訊資產保管者應於資訊資產之保存期限到期後刪除與銷毀該資產。	7. 抽查資料類型資訊資產刪除與銷毀紀錄，以確認資訊資產保管者是否於資訊資產之保存期限到期後刪除與銷毀該資產。
2.1.4.5 人員安全作業	
（一）VASP 應對員工進行背景調查才得以錄用。	1. 抽查對員工之背景調查記錄，以確認 VASP 是否對員工進行背景調查。 2. 對涉及財務、虛擬資產管理、資訊安全...等職位之重要人員，於錄用或任職時應進行信用紀錄與犯罪紀錄審查。
（二）VASP 應於合約明定員工應盡之資訊安全責任。	3. 檢查合約，以確認員工是否知悉其應負擔之資訊安全責任，若具有機密維護責任，須另填具保密切結書。
（三）VASP 應對異動之人員調整其資產存取及使用權限。	4. 抽查人員異動紀錄，比對至系統之權限設定，以確認異動人員之資產存取及使用權限依 VASP 規定進行調整。
（四）全 VASP 員工每年應依職務層級接受適當之資訊安全與個資保護教育訓練。	5. 檢查資訊安全與個資保護教育訓練紀錄，以確認全 VASP 員工是否每年依職務層級接受資訊安全與個資保護教育訓練。
2.1.4.6 實體與環境安全作業	
（一）VASP 應每年定期審查電腦機房之門禁權限。	1. 抽查電腦機房之門禁權限審查紀錄，以確認 VASP 是否每年定期審查電腦機房之門禁權限。
（二）機房應配備監控錄影設備進行 24 小時間監控，錄影	2. 觀察機房監控錄影設備是否正常運作，並確認監控是否 24 小時

資料至少保存 30 天，並限制存取權限。	監控，且紀錄是否至少保存 30 天，監控僅特定人員可進行存取。
（三）電腦機房管理專員應每日於工作日誌紀錄管理狀況，該紀錄應包括電腦機房內濕度及溫度，且應保留至少六個月。	3. 抽查工作日誌，以確認電腦機房管理專員是否每日紀錄管理狀況、是否紀錄電腦機房內濕度及溫度等及該等紀錄是否保留至少六個月。
（四）VASP 應委託廠商定期檢查電腦機房內之各項安全設備（至少一年一次）。	4. 抽查電腦機房內之安全設備之檢查紀錄，以確認 VASP 是否委託廠商定期檢查各項安全設備（至少一年一次）。
（五）非授權之人員須經申請核准方能進入電腦機房，進出紀錄須紀錄留存。	5. 抽查出入登記簿，比對至人員進出機房申請表，以確認未具電腦機房進出權限之人員於進入機房時是否皆經核准。
（六）辦公室應有管制措施（如門禁系統）並配備監控錄影設備，不具權限之人員不得進出。	6. 檢查門禁系統中之權限設定，比對至具權限員工名單，以確認系統設定有權限之員工是否皆為 VASP 有開放權限之員工。 7. 觀察辦公室監控錄影設備是否正常運作，並確認監控紀錄是否至少保存 30 天，並且僅特定人員可進行存取。 8. 觀察不具權限之人員是否可進出辦公室。
（七）伺服器或個人電腦應啟動螢幕保護與密碼保護機制。	9. 抽查伺服器或個人電腦，以確認是否已設定螢幕保護與密碼保護機制。
（八）可攜式設備之使用分配應受權責主管核准後始得配發，並記錄其各項設備之保管人，並建立相關遺失通報程序。	10. 抽查權責主管核准可攜式設備之使用分配及各項設備之保管人之紀錄。 11. 檢查 VASP 是否建立相關遺失通報程序。

（九）定期檢視(每年至少乙次)使用軟體情形，經察覺有使用非法或未經核准之軟體一律刪除，並呈報權責單位主管。	12. 抽查可攜式設備使用軟體情形，並比對定期檢視紀錄，以確認未使用非法或未經核准之軟體。
（十）資訊資產權責單位應確實依設備報廢作業程序移除機敏性資料後，方可報廢該設備。	13. 抽查報廢紀錄，比對至經簽核之報廢申請單，以確認將報廢之設備係依據設備報廢程序執行。
（十一）訪客進入須登記並經由內部人員陪同進入公司。	14. 抽查訪客進入登記表，並觀察訪客登記情形，以確認訪客進入皆有進行登記。
2.1.4.7 通訊與作業管理作業	
（一）應定期評估網路系統安全(例如：網站伺服器、瀏覽器、防火牆及防毒版本等)，將相關評估結果留存紀錄。	1. 檢查網路系統安全之評估紀錄，以確認網路管理人員是否定期評估網路系統安全。
（二）應定期檢視網路運作環境與作業系統之安全漏洞並修補，並將相關執行結果予以紀錄。	2. 檢查網路運作環境與作業系統之安全漏洞檢視紀錄，比對至該等安全漏洞修補紀錄，以確認網路管理人員是否將發現之安全漏洞皆予以修補，並確保安全防護工具為最新。
（三）VASP 應有適當網路之區隔機制。	3. 觀察 VASP 網路是否有區隔機制。
（四）VASP 應將有關網路安全（如資訊安全政策宣導、防範網路駭客入侵事件、電腦防毒等）相關事項公告予內部人員加以宣導，機敏資料應適當存放。	4. 檢查公告紀錄，以確認網路安全相關事項已確實公告，並檢視機敏資料是否適當存放。
（五）VASP 應訂定遠端連線管理辦法並進行適當防護措	5. 檢查 VASP 之遠端連線管理辦法文件及進行相關安全防護之紀

施。	錄，以確認是否具有遠端連線管理辦法，以及是否依該辦法進行控管。
（六）VASP 應建立防火牆，並應由權責管理人員執行控管且定期檢視防火牆規則是否允當。	6. 觀察 VASP 是否建立防火牆。 7. 檢查防火牆之控管紀錄及防火牆規則覆核之紀錄，以確認網路管理人員是否有定期控管防火牆及是否定期檢視防火牆規則。
（七）防火牆規則欲進行異動應經適當權責單位主管核准，權責管理人員應依經核准之防火牆異動申請單設定防火牆。	8. 檢查防火牆規則異動申請單，以確認對防火牆之異動皆經權責單位主管核准。 9. 檢查防火牆規則之異動紀錄，比對至經核准之防火牆異動申請單，以確認網路管理人員是否依經核准之防火牆異動申請單設定防火牆。
（八）權責管理人員應設定存取控制列表（ACL）並每年至少檢視一次，並更新，以避免有未經授權之存取。	10. 檢查存取控制列表之檢視紀錄，比對至網路連線授權清單，以確認是否有未經授權之存取。
（九）網路下單系統登入應採用多因子驗證。	11. 觀察網路下單系統登入是否採用多因子驗證。
2.1.4.8 存取控制作業	
（一）VASP 應訂定資訊系統存取控制相關規定。	1. 檢查 VASP 是否訂定資訊系統存取控制相關規定。
（二）欲使用資訊資產之員工對存取權限之申請須經該資訊資產權責單位主管核准。	2. 抽查對存取權限之申請紀錄，以確認該申請是否經該資訊資產權責單位主管核准。
（三）資產保管人員應依經核准之申請設定存取權限，並	3. 抽查系統之權限設定紀錄，比對存取權限之申請紀錄，以確認資

對設定情形進行記錄。	產保管人員是否依經核准之存取權限申請執行權限變更。
（四）職務調動及離職時存取權限，已於異動生效日即停用。	4. 抽查職務調動紀錄或離職申請紀錄，並比對系統權限設定紀錄，以確認於異動生效日即對存取權限進行停用。
（五）資訊安全人員應檢查委外人員所使用之電腦紀錄。	5. 抽查委外作業人員之權限授予紀錄，以確認資訊安全人員是否核准授予委外作業人員之權限。
（六）資產保管人員應於委外人員之委外期間結束後立即將其權限取消。	6. 抽查委外期間結束之委外人員清單，比對至系統中對該等人員之權限設定，以確認資產保管人員是否於委外人員之委外期間結束後確實取消委外作業人員之權限。
（七）各資訊資產之存取權限及授權應依職務性質進行區分(如系統開發、系統測試、系統上線系統維護、設備管理），不同職務性質不可出現兼任之情形。	7. 抽查系統上線紀錄並比對人員存取及授權，以確認人員已依據職務性質進行區分。
（八）權責主管應定期（至少每半年一次）審查資通系統帳號及權限之適切性，並視審查結果停用資通系統閒置帳號（為客戶帳號除外）。	8. 抽查資通系統帳號及權限之適切性之審查紀錄，以確認該紀錄中是否包含權責主管簽名及審查日期，並確認審查結果中之資通系統閒置帳號皆已於系統中被停用。
（九）資通系統之特權帳號應進行申請並經適當管理階層或治理單位核准。	9. 檢查特權帳號之申請紀錄，以確認資通系統之特權帳號之申請皆經權責管理階層或治理單位核准。
（十）資訊安全人員應定期覆核特權帳號之使用紀錄。	10. 抽查特權帳號使用紀錄覆核之紀錄，以確認特殊權限存取紀錄是否經資訊安全人員定期覆核，且無審核人員覆核自己存取紀錄之情況。

（十一）使用者密碼於首次使用後應進行更改，使用者更改之密碼應符合密碼原則，系統預設之初始密碼應被停用或刪除。	11. 抽查使用者密碼之更改紀錄，以確認使用者密碼於首次使用後是否進行更改。 12. 觀察系統畫面，以確認系統預設之初始密碼是否已被停用或刪除。
（十二）帳號與密碼資訊應以加密方式保存。	13. 觀察保存帳號密碼之檔案是否以加密方式保存。
（十三）固定密碼之設定應訂定密碼原則機制。	14. 觀察系統之密碼設定參數，以確認是否符合密碼原則。
（十四）每次密碼變更時，系統應對該使用者之身分進行驗證。	15. 觀察使用者於變更密碼時，系統是否對使用者進行身分進行驗證。
（十五）系統於有帳號登入異常情事時應通知相關權責單位，相關權責單位應即時了解異常原因，並留存處理紀錄。	16. 抽查系統之帳號登入異常情事通知紀錄，比對至相關處理紀錄，以確認該等情事皆已被了解並處理。
（十六）VASP 應訂定並執行金鑰之安全管理規定。	17. 檢查金鑰安全管理規定，以確認 VASP 是否訂定金鑰之安全管理規定。 18. 觀察產生、儲存、封存、檢索、分發、汰除及銷毀密碼金鑰之管理流程，以確保 VASP 確實依金鑰之安全管理規定執行。
2.1.4.9 系統開發及維護作業	
（一）系統開發需求申請應經申請單位主管核准。	1. 抽查系統開發申請文件，以確認該等文件是否經權責主管核准。
（二）系統開發人員應對經核准之系統開發需求申請進行可行性評估，並將資訊安全納入考量，以確認符合	2. 抽查系統開發需求申請之評估紀錄，以確認系統開發人員是否對該需求進行可行性評估，並將資訊安全納入考量，以確認符合

VASP 資訊安全制度。	VASP 資訊安全制度。
（三）開發測試環境需與正式環境分離，且不應使用正式資料進行，如必須使用生產資料進行測試操作，則應考慮相關控制措施以保護資料的機密性。	3. 觀察開發環境是否與正式環境有所區隔，且測試環境資料非使用正式資料，如需使用正式資料則應有相關控制措施保護資料機密性。
（四）開發完成之系統應經申請單位測試驗收以符合申請單位需求，其中系統程式換版或產製比對報表不應由系統開發人員執行，並經資訊安全單位主管及系統相關權責單位或申請單位相關權責人員覆核。	4. 抽查系統驗收紀錄、程式換版紀錄及比對報表，以確認經資訊安全單位主管及系統相關權責單位或申請單位相關權責人員覆核，且非由系統開發人員進行換版及編製比對報表，以確認是否符合職能分工之要求。
（五）權責管理人員應對所檢測出來之系統弱點（包含弱點掃描、滲透測試及程式原碼覆核或安全檢測等資安檢測作業）進行維護並記錄，送交權責單位主管進行覆核。	5. 抽查系統弱點（包含弱點掃描、滲透測試及程式原碼覆核或安全檢測等資安檢測作業）之維護紀錄，以確認權責管理人員是否確實對系統弱點進行維護並經權責單位主管覆核。
2.1.4.10 營運持續管理作業	
（一）資訊安全管理單位應訂定系統故障復原程序並定期進行測試。	1. 檢查資訊安全管理單位是否訂定系統故障復原程序。 2. 抽查系統故障復原程序之測試紀錄，以確認資訊安全管理單位是否定期進行測試。
（二）資訊安全管理單位應訂定營運持續計畫。	3. 檢查資訊安全管理單位是否訂定營運持續計畫。
（三）營運持續計畫應定期（至少一年一次）完整演練並針對演練結果對營運持續計畫予以修正。	4. 抽查營運持續計畫演練紀錄，以確認該計畫是否定期演練（至少一年一次）並依據演練結果修正該計畫。

（四）資訊安全管理單位應定期評估營運系統及設備之事故應變措施。	5. 抽查核心營運系統及設備之事故應變措施之評估紀錄，以確認資訊安全管理單位是否定期評估核心營運系統及設備之事故應變措施。
2.1.4.11 資通系統或資通服務(錢包託管技術)委外辦理作業	
（一）業務單位承辦人員對擬委外業務之可行性及成本效益進行評估，該評估結果應由業務單位主管核准。	1. 抽查委外業務之評估結果，以確認該委外是否經評估，並經業務單位主管核准。
（二）業務單位承辦人員應依其規畫書之要求條件評估委外廠商，並將相關評估結果作成書面紀錄。	2. 檢查委外廠商之評估紀錄，以確認委外廠商是否每年皆重新進行評估。
（三）業務單位承辦人應訂定與委外廠商之契約，該契約條款應至少包含「服務水準協議(SLA)」、資通安全責任及保密規定、資安要求及對委外廠商資安稽核權，並經業務單位主管評估後核准。	3. 檢查與委外廠商簽訂之契約，以確認該契約條款是否包含「服務水準協議(SLA)」、資通安全責任及保密規定、資安要求及對委外廠商資安稽核權，以及是否經業務單位主管核准。
（四）委外作業人員之資料存取權限應經適當核准。	4. 檢查委外作業人員之權限申請紀錄，以確認委外作業人員之資料存取權限是否經核准。 5. 檢查資訊安全人員定期檢視委外作業人員系統操作之紀錄，以確認委外廠商依照申請需求執行。
（五）資訊安全人員應對委外廠商交付之服務系統檢查其未有植入後門程式等惡意程式，確保系統符合需求後始正式上線運作。	6. 檢查對委外廠商交付之服務系統之檢查紀錄，以確認資訊安全人員是否對委外廠商交付之服務系統檢查其未有植入後門程式等惡意程式。

（六）資訊安全人員應定期檢查委外作業系統之安全性。	7. 檢查對委外作業系統安全性之檢查紀錄，以確認資訊安全人員是否定期檢查委外作業系統之安全性。
（七）委外廠商應定期提出第三方獨立機構對其資通安全之審查報告。	8. 檢查委外廠商由第三方獨立機構對其進行資通安全之審查報告。
（八）合約中應訂定委外關係於終止、解除或結束後之相關作業。	9. 抽查與委外廠商之合約，以確認合約中是否訂定委外關係於終止、解除或結束後之程序。
2.1.4.12 新興科技應用作業	
（一）雲端服務申請者應對雲端服務之需求、適切性及可能涉及之資訊安全進行評估，該評估應包括與資訊安全單位討論。	1. 檢查雲端服務評估紀錄，以確認申請者是否對雲端服務的需求、適切性及可能涉及的資訊安全進行了評估，並與資訊安全單位進行過討論。
（二）雲端服務申請者對雲端服務提供廠商所提供雲端服務之購置申請，應檢附經確認之可行性評估結果，並經適當管理階層或治理單位核准。	2. 檢查雲端服務之購置申請，比對至雲端服務提供廠商評估紀錄，以確認該購置是否係依評估紀錄進行，並經權責管理階層或治理單位核准。
（三）合約中應訂定雲端服務提供廠商於雲端服務運作發生資訊安全事件時之資通安全事件通報程序及處理程序。	3. 檢查與雲端服務提供廠商之合約，以確認合約中是否訂定於雲端服務運作發生資訊安全事件時之資通安全事件通報程序及處理程序。
（四）應對傳輸及儲存至雲端服務提供廠商之客戶資料或敏感資料，採行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。	4. 檢查儲存至雲端服務廠商之客戶資料，以確認資料，採行資料加密或代碼化等有效保護措施。 5. 檢視是否已訂定加密金鑰管理機制。

（五）於終止雲端服務使用時，雲端服務申請者應確認雲端服務提供廠商應於一定期限內刪除其服務期間之所有用戶資訊。	6. 檢查與雲服務廠商之終止服務協議，若已有終止雲端服務使用之情形發生，則應抽查刪除用戶資訊之確認紀錄，以確認所有用戶資訊皆已被刪除。
（六）VASP 應訂定公務用行動裝置之申請、使用、更新、繳回與審核等相關資訊安全規範與管理辦法。	7. 檢查 VASP 之公務用行動裝置之資訊安全規範與管理辦法，以確認 VASP 是否對公務用行動裝置之申請、使用、更新、繳回與審核等訂定相關資訊安全規範與管理辦法。
（七）風險評鑑執行人員應對行動裝置可存取之資源進行風險評估作業，並依據風險評估結果採取適當之安全控管措施。	8. 抽查對行動裝置可存取之資源之風險評估紀錄及所採取安全控管措施，以確認風險評鑑執行人員已對行動裝置可存取之資源進行風險評估並依據評估結果採取安全控管措施。
（八）行動裝置應對未通過檢測之行動應用程式之安裝設定阻擋程式。	9. 觀察安裝未通過檢測之行動應用程式時，行動裝置是否確實阻擋。
（九）VASP 應訂定員工自攜行動裝置之資訊安全規範與管理辦法，包括裝置使用用途、限制裝置私接存取網際網路及行動裝置儲存機密資料之限制與管理方式等。	10. 檢查 VASP 之員工自攜行動裝置之資訊安全規範與管理辦 法，以確認 VASP 是否對自攜行動裝置之使用用途、限制裝置私接存取網際網路及行動裝置儲存機密資料之限制與管理方式等，訂定資訊安全規範與管理辦法。
（十）VASP 應建立物聯網設備管理清冊並至少每年更新一次。	11. 檢查物聯網設備管理清冊，以確認 VASP 是否至少每年更新一次。
（十一）物聯網設備應具備安全性更新機制且定期（每年一次）更新，如存在已知弱點無法更新時，VASP	12. 檢查物聯網設備更新紀錄，以確認該設備是否具備安全性更新機制且定期（每年一次）更新，如存在已知弱點無法更新時，應檢

應建立補償性控管機制。	查其實施補償性控管措施相關紀錄。
（十二）物聯網設備應具備身份驗證機制或配對綁定機制，並應變更該等設備之初始密碼。	13. 觀察物聯網設備，以確認該設備是否具備身份驗證機制或配對綁定機制。 14. 抽查物聯網設備之密碼變更紀錄，以確認是否變更該等設備之初始密碼。
（十三）VASP 與物聯網設備供應商簽訂採購合約時，其內容應包含資訊安全相關協議（如：服務承諾、安全性更新年限、主動通報設備已知資安漏洞並提出相關應變處置方案）。	15. 檢查與物聯網設備供應商簽訂之採購合約，以確認其內容是否包含資訊安全相關協議。
（十四）VASP 應對使用影像視訊方式進行身分驗證之客戶使用強化驗證並搭配其他驗證因子，並留存影像或照片。	16. 觀察進行身分驗證時，是否有進行強化驗證並搭配其他驗證因子（如上傳身分證件、手機簡訊 OTP）。 17. 抽查留存之影像，以確認 VASP 是否對客戶驗證之身分留存紀錄。
（十五）VASP 應對使用電話交易服務之客戶，訂定身分驗證程序（如語音密碼）避免非本人之假冒。	18. 觀察進行電話交易服務時，是否有身分驗證程序。
2.1.4.13 符合性	
（一）VASP 是否定期(每年至少乙次)辦理虛擬資產資訊安全管理查核作業(內部辦理或委託外部專業機構)。	1. 抽查虛擬資產資訊安全管理查核作業，以確認是否定期執行相關查核作業。

（二）針對前項查核作業所發現之缺失項目是否進行追蹤及改善。	2. 抽查前項查核作業，以確認缺失改善事項是否進行追蹤及改善。

2.2 會計師對 VASP 保管客戶資產內部控制制度執行協議程序之執行報告

協議程序執行報告

甲公司公鑒：

乙公司民國○○○年○○月○○日之資產分離保管（包括法定貨幣/虛擬資產餘額驗證、錢包管理、虛擬資產託管管理、虛擬資產資訊安全管理）之內部控制制度之妥適性，業經本會計師依協議程序執行完竣。該等程序之採用係由貴公司作最後決定，因此對其是否足夠，本會計師不表示意見。本次工作係依照其他相關服務準則 4400 號「財務資訊協議程序之執行」進行，其目的係為協助貴公司評估資產分離保管之內部控制制度，茲將執行之程序及所發現之事實分別列示於附件。

由於本會計師並非依照確信準則進行確信，因此對上述資產分離保管之內部控制制度之妥適性不提供任何程度之確信。若本會計師執行額外程序或依照確信準則進行確信，則可能發現其他應行報告之事實。

本報告僅供貴公司作為第一段所述目的之用，不可作為其他用途或分送其他人士。本報告僅與前述特定項目有關，因此不得擴大解釋為與任何乙公司之財務報表整體有關。

○○會計師事務所

會計師：（簽名及蓋章）

中華民國○○○年○○月○○日

附件

法定貨幣/虛擬資產餘額驗證之協議程序

法定貨幣入金作業

程序

1. 抽查權責人員針對入金之客戶進行風險控管檢核措施（如 AML 檢核、客戶資格權限比對及入金限額等）之紀錄，以確認已由權責人員進行檢核。
2. 抽查入金之客戶明細，比對至具備法定貨幣交易資格之客戶明細，以確認通過入金申請之客戶是否於具備法定貨幣交易資格之清單中。
3. 抽查出納人員之確認紀錄，以確認出納人員是否確實確認系統帳戶入金之金額與網銀明細或其他銀行傳輸之資料入金金額一致。
4. 抽查網銀明細或其他銀行傳輸之資料入金金額，比對至系統帳戶之入金紀錄，以確認網銀明細或其他銀行傳輸之資料入金金額與系統帳戶入金之金額是否一致。
5. 抽查出納人員確認當日法定貨幣退款明細與當日網銀或其他銀行傳輸之資料退款明細之紀錄，並確認該紀錄中是否包含出納人員之簽名及確認日期。
6. 抽查網銀或其他銀行傳輸之資料退款明細，比對至法定貨幣退款明細，以確認出納人員是否將相關款項正確地退還給應退款之客戶。
7. 檢查 VASP 內部控制制度文件，確認其內部控制制度中是否明確規定就虛擬資產交易及其款項代收付業務收受客戶之法定貨幣，應與其自有之法定貨幣分離保管。
8. 檢查信託合約或十足履約保證契約以確認 VASP 是否已將客戶之法定貨幣交付信託或取得銀行十足之履約保證。核對第三方信託合約銀行對帳單金額與 VASP 之客戶法定貨幣帳簿餘額，確認該帳簿餘額是否與對帳單金額一致以確定 VASP 是否確實將其客戶法定貨幣皆交付信託；或核對銀行對帳單與履約保證契約，確認 VASP 之客戶法定貨幣餘額皆未超過履約保證契約之額度。
9. 抽查 VASP 系統中之客戶法定貨幣變動紀錄，比對至客戶之虛擬資產交易相關法定貨幣變動申請及出金明細，確認對交付信託之法定貨幣之動用中無非屬客戶之虛擬資產交易相關法定貨幣及出金之動用，以確認明細餘額之正確性。
10. 抽查 VASP 系統中之客戶法定貨幣變動明細表中是否包含姓名及法定貨幣餘額。
11. 抽查客戶入金之銀行帳戶是否與 VASP 自身之銀行帳戶不同。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後

附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

<u>法定貨幣出金/退款作業</u>

程序

1. 抽查申請出金客戶之 AML 檢核與風險控管檢核紀錄，並確認該紀錄中是否包含檢核人員簽名及檢核日期，以確認 VASP 權責人員是否確認客戶確實具備法定貨幣交易之資格。
2. 抽查出金成功之客戶清單，比對至其 AML 檢核與風險控管檢核之紀錄，以確認該等客戶皆經 AML 檢核與風險控管檢核。
3. 抽查未通過 AML 檢核之客戶明細，比對至系統，以確認 VASP 是否已對該客戶進行對應之處理流程。
4. 抽查當日出金明細表之個別客戶出金明細，與客戶線上操作之出金指示核對，確認個別客戶出金金額正確。抽查當日出金明細表及信託指示書或同等效力文件之覆核紀錄，以確認該等文件是否經覆核人員確實簽核。
5. 抽查法幣出納人員確認網銀或其他銀行傳輸之資訊出金紀錄與當日出金明細表之紀錄，以確認法幣出納人員是否確認相關明細餘額之正確性並經覆核人員簽核。
6. 抽查當日退款明細表及信託指示書或同等效力文件之覆核紀錄，以確認該等文件是否經覆核人員確實簽核。
7. 抽查法幣出納人員確認網銀或其他銀行傳輸之資訊退款紀錄與當日退款明細表金額一致，以及已退款至客戶綁定之銀行帳號或原匯入之非綁定帳戶之紀錄，以確認法幣出納人員是否確認相關明細餘額之正確性並經覆核人員簽核。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

<u>虛擬資產入金與接收作業</u>

程序

1. 檢查VASP是否於虛擬資產買賣、接收、發送、移轉確實保存交易記錄。
2. 抽查VASP系統中保存之交易紀錄是否足以重建個別交易。
3. 抽查 VASP 是否紀錄所保管之客戶虛擬資產（應至少包括客戶錢包地址、姓名、虛擬資產種類、及數量等）。
4. 檢查 VASP 是否紀錄列管未完成實名制身分驗證者之虛擬資產後（包含無主入金），如發現異常時通報司法警察機關。
5. 抽查 VASP 收到黑名單或詐騙嫌疑等高風險客戶及地址所發送的虛擬資產時，是否依法向法務部調查局申報可疑交易。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

虛擬資產發送與提領作業

程序

1. 抽查 VASP 系統是否正確與完整紀錄虛擬資產發送與提領申請紀錄，包含客戶發送至外部之錢包接收地址、交易幣種、交易數量、交易時間、交易序碼（TxID）。
2. 抽查虛擬資產提領申請紀錄是否有 VASP 標註為黑名單或詐騙嫌疑等高風險客戶或外部錢包地址之申請。若有，檢查系統拒絕該等申請之紀錄。
3. 檢查VASP系統是否確認客戶提領申請後熱錢包內餘額是否足夠。
4. 檢查 VASP 系統是否於熱錢包餘額不足時（水位過低），推播通知錢包管理人員進行錢包移轉。
5. 抽查系統完成提領之紀錄，比對至客戶申請紀錄，以確認系統是否確實將虛擬資產移轉至客戶指定之錢包地址。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

法定貨幣餘額驗證作業

程序

1. 抽查合作之第三方信託銀行法定貨幣出入金變動明細與 VASP 帳上法定貨幣出入金金額之核對紀錄，以確認是否係由法幣出納人員核對且皆經覆核人員簽核。
2. 抽查合作之第三方信託銀行法定貨幣出入金變動明細，比對至 VASP 帳上法定貨幣出入金金額，以確認合作之第三方信託銀行法定貨幣出入金變動明細是否與 VASP 帳上法定貨幣出入金金額相符。
3. 抽查第三方信託銀行法定貨幣當日網銀或其他銀行傳輸資訊餘額與 VASP 法定貨幣帳簿餘額之核對紀錄，以確認是否係由法幣出納人員核對且皆經覆核人員簽核。
4. 抽查第三方信託銀行法定貨幣當日網銀或其他銀行傳輸資訊餘額，比對至 VASP 法定貨幣帳簿餘額，以確認第三方信託銀行法定貨幣當日網銀或其他銀行傳輸資訊餘額是否與 VASP 法定貨幣帳簿餘額相符。
5. 檢查調節表，以確認法幣出納人員是否編製調節表，並檢查各項調整項目是否有相應之支持文件，並經適當權責人員覆核調節表。
6. 檢查屬系統或人為疏失產生之錯誤之金額不一致紀錄，檢查其相對應之修正紀錄，以確認該等錯誤皆已被修正。
7. 檢查當期是否有無法查明原因或作適當修正之紀錄。若有，檢查對內部稽核部門之報告紀錄，以確認該等不一致已向內部稽核部門報告。對於該等報告紀錄中被標示為差異重大且無法查明原因者，檢查董事會會議紀錄，以確認該等差異重大且無法查明原因之不一致已向董事會報告。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

虛擬資產餘額驗證作業

程序

1. 由 VASP 提供各錢包地址，案件執行人員隨機指定錢包移轉之特定金額及特定時點，觀察錢包移轉是否符合案件執行人員之預期，以確認錢包是否係 VASP 所有。
2. 透過區塊鏈瀏覽器抽查確認錢包餘額。

3. 抽查屬於客戶及屬於 VASP 之各幣種錢包（包括冷、溫及熱錢包）之虛擬資產餘額表與錢包帳上餘額之核對紀錄，以確認是否係由錢包記帳人員核對且皆經覆核人員簽核。
4. 抽查屬於客戶及屬於 VASP 之各幣種錢包（包括冷、溫及熱錢包）之虛擬資產餘額表，比對至錢包帳上之餘額，以確認該等錢包之虛擬資產餘額表與錢包帳上之餘額是否相符。
5. 抽查各幣種錢包（包括冷、溫及熱錢包）之虛擬資產變動表與錢包帳上變動數之核對紀錄，以確認是否係由錢包記帳人員核對且皆經覆核人員覆核。
6. 抽查各幣種錢包（包括冷、溫及熱錢包）之虛擬資產變動表，比對至錢包帳上之變動數，以確認錢包之虛擬資產變動表與錢包帳上之變動數是否相符。
7. 檢查調節表，以確認錢包管理人員或錢包記帳人員是否編製調節表，並檢查各項調整項目是否有相應之支持文件。
8. 檢查屬系統或人為疏失產生之錯誤之金額不一致紀錄及相對應之修正紀錄，以確認該等錯誤皆已被修正。
9. 檢查當期是否有無法查明原因或作適當修正之紀錄。若有，檢查對內部稽核部門之報告紀錄，以確認該等不一致已向內部稽核部門報告。對於該等報告紀錄中被標示為差異重大且無法查明原因者，檢查董事會會議紀錄，以確認該等差異重大且無法查明原因之不一致已向董事會報告。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

錢包管理之協議程序

將虛擬資產由熱錢包移轉至溫錢包作業

程序

1. 檢查錢包管理相關職能與分工是否經公司之制度政策或文件予以定義，並確認該等職能已據此劃分予不同人員。
2. 檢查即時通知之水位設定是否係依照公司錢包水位之規定。
3. 檢查即時通知紀錄，以確認系統是否確實於達到門檻水位時發出通知。
4. 檢查公司是否建立錢包白名單，並定義白名單新增、修改、刪除之流程與授權規則。
5. 抽查系統之錢包移轉紀錄，以確認錢包移轉係經所有權責人員簽核。
6. 取得並檢視相關職能說明文件，以確認是否對保管私鑰或分片之人員有明確職能分配與權責敘述。
7. 抽查系統之錢包移轉紀錄，以確認所移轉之錢包地址是否皆是白名單錢包地址。
8. 檢查是否對移轉期限建立規定，並抽查交易以確認是否於期限內完成資產移轉。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

將虛擬資產由溫錢包移轉至冷錢包作業

程序

1. 檢查錢包管理相關職能與分工是否經公司之制度政策或文件予以定義，並確認該等職能已據此劃分予不同人員。
2. 檢查即時通知之水位設定是否係依照公司錢包水位之規定。
3. 檢查即時通知紀錄，以確認系統是否確實於達到門檻水位時發出通知。
4. 檢查公司是否建立錢包白名單，並定義白名單新增、修改、刪除之流程與授權規則。
5. 抽查系統之錢包移轉紀錄，以確認錢包移轉係經所有權責人員簽核。
6. 取得並檢視相關職能說明文件，以確認是否對保管私鑰或分片之人員有明確職能分配與權責敘述。
7. 抽查系統人員確認虛擬資產已移轉至指定之白名單錢包地址之紀錄。
8. 抽查系統之錢包移轉紀錄，以確認所移轉之錢包地址是否皆是白名單錢包地

址。

9. 檢查是否對移轉期限建立規定，並抽查交易以確認是否於期限內完成資產移轉。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

<u>將虛擬資產由溫錢包移轉至熱錢包作業</u>

程序

1. 檢查錢包管理相關職能與分工是否經公司之制度政策或文件予以定義，並確認該等職能已據此劃分予不同人員。
2. 檢查公司是否建立錢包白名單，並定義白名單新增、修改、刪除之流程與授權規則。
3. 抽查系統之錢包移轉紀錄，以確認錢包移轉係經所有權責人員簽核。
4. 取得並檢視相關職能說明文件，以確認是否對保管私鑰或分片之人員有明確職能分配與權責敘述。
5. 抽查系統之移轉紀錄，以確認所移轉之錢包地址是否皆是白名單錢包地址。
6. 檢查是否對移轉期限建立規定，並抽查交易以確認是否於期限內完成資產移轉。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

<u>將虛擬資產由冷錢包移轉至溫錢包作業</u>

程序

1. 檢查錢包管理相關職能與分工是否經公司之制度政策或文件予以定義，並確認該等職能已據此劃分予不同人員。
2. 檢查公司是否建立錢包白名單，並定義白名單新增、修改、刪除之流程與授

權規則。

3. 抽查系統之錢包移轉紀錄，以確認錢包移轉係經所有權責人員簽核。
4. 取得並檢視相關職能說明文件，以確認是否對保管私鑰或分片之人員有明確職能分配與權責敘述。
5. 抽查系統之移轉紀錄，以確認所移轉之錢包地址是否皆是白名單錢包地址。
6. 檢查是否對移轉期限建立規定，並抽查交易以確認是否於期限內完成資產移轉。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

<u>錢包與私鑰管理作業</u>

程序

1. 檢查董事會會議紀錄，以確認錢包水位設定是否經董事會或適當之治理單位通過。
2. 檢查董事會會議紀錄，以確認客戶之虛擬資產存放於冷錢包之比例或其變動是否經董事會或適當之治理單位通過。
3. 檢查 VASP 內部控制制度文件，確認內部控制制度中是否明確規定客戶之虛擬資產存放於冷錢包之比例。
4. 檢查 VASP 內部控制制度文件，確認內部控制制度中是否明確規定錢包之設立與調整規定。
5. 抽查錢包地址生成申請表之簽章紀錄，以確認監督人員是否監控操作過程。
6. 檢查冷錢包地址之更新紀錄，以確認錢包管理人員是否適時更新冷錢包地址。
7. 抽查冷錢包私鑰生成紀錄，以確認監督人員是否有監控操作過程。
8. 抽查移轉虛擬資產之相關紀錄是否妥善保存至少五年。
9. 取得對系統權限管理人員、私鑰管理人員及錢包管理人員之職能配置相關文件（例如職掌表、人員清冊或系統權限列表等），檢查系統權限管理人員、私鑰管理人員及錢包管理人員的權責是否在考量職能衝突風險下明確定義，且經管理階層核決。
10. 取得客戶冷錢包虛擬資產餘額表及客戶虛擬資產總額，計算客戶冷錢包之虛擬資產餘額是否達客戶虛擬資產總額 80%以上。
11. 取得客戶熱錢包虛擬資產餘額表及客戶虛擬資產總額，計算客戶熱錢包虛擬

資產餘額是否未超過客戶虛擬資產總額 20%。

12. 抽查客戶錢包（包含冷、溫及熱錢包）虛擬資產變動表，確認該等變動是否皆來自客戶發起之虛擬資產交易、系統因錢包儲存水位達門檻而發出之警示通知、因 2.1.2.6 作業流程第一項所述之營運目的所需或法令所訂之事由。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

客戶虛擬資產與 VASP 虛擬資產於相同錢包下之混合管理作業

程序

1. 抽查自 VASP 錢包移轉至客戶熱錢包之紀錄，以確認該紀錄中之移轉理由是否皆符合作業流程第一項之營運目的。
2. 檢查 VASP 是否建立辨認混同資產比例之管理機制。
3. 檢查 VASP 自有虛擬資產占客戶錢包（包含熱及冷錢包）內客戶虛擬資產之比例超過 20%之系統警示通知紀錄及相關錢包移轉紀錄，以確認每一系統警示通知是否皆有相關移轉紀錄（移轉理由應為依系統警示通知移轉），以及移轉紀錄是否依程序簽核。
4. 取得客戶錢包（包含熱及冷錢包）之虛擬資產餘額表，計算 VASP 存放至客戶錢包之虛擬資產餘額未超過客戶之虛擬資產餘額之 20%。
5. 檢查客戶冷錢包中之 VASP 虛擬資產之移轉紀錄，以確認該紀錄中之移轉理由是否僅為支付鏈上瓦斯費或因所存放之鏈上瓦斯費超過客戶之虛擬資產餘額之 20%。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

虛擬資產託管管理內部控制制度

程序

1. 檢查對第三方信託機構之評估紀錄，以確認 VASP 是否對第三方信託之資格及能力進行評估並記錄評估結果。
2. 檢查 VASP 對第三方信託機構之評估紀錄是否包含第三方信託機構對虛擬資產分離保管之政策，以確認該第三方信託機構在管理 VASP 託管之虛擬資產時，是否係與第三方信託機構之其他虛擬資產分離保管。
3. 檢查第三方信託機構之客戶虛擬資產保管紀錄，以確認第三方信託機構保管 VASP 之客戶虛擬資產之錢包中，是否包含 VASP 本身之虛擬資產。
4. 抽查錢包記帳人員核對委託第三方信託機構託管之虛擬資產之帳上數量與區塊鏈瀏覽器顯示之錢包餘額之紀錄，以確認錢包記帳人員是否定期核對。
5. 檢查當期是否有無法查明原因或作適當修正之紀錄。若有，檢查對內部稽核部門之報告紀錄，以確認該等不一致已向內部稽核部門報告。若該等報告紀錄中有差異重大且無法查明原因者，檢查董事會會議紀錄，以確認該等差異重大且無法查明原因之不一致已向董事會報告。
6. 檢查 VASP 之確認紀錄，以確認 VASP 託管之虛擬資產是否與第三方信託之其他虛擬資產分離保管。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

虛擬資產資訊安全管理之協議程序

風險評鑑與管理作業

程序

1. 抽查風險評鑑之紀錄，以確認風險評鑑執行人員是否每年對虛擬資產資訊系統中之各項資產進行風險評鑑。
2. 抽查風險評鑑之紀錄，以確認資訊資產是否依風險權值進行分級，並確認風險評鑑是否經風險評鑑單位主管或擁有資訊資產之單位主管核准。
3. 檢查 VASP 之風險評鑑清冊及風險處理計畫，以確認其是否依風險評鑑結果訂定控制措施。
4. 抽查 VASP 之控制措施評估紀錄，以確認風險評鑑執行人員是否定期評估該控制措施並依評估結果進行改善。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

資訊安全政策作業

程序

1. 檢查資訊安全管理組織是否訂定資訊安全政策、資訊安全作業程序。
2. 檢查資訊安全政策核准紀錄，以確認資訊安全政策是否經管理階層核准。
3. 檢查資訊安全政策發布紀錄，以確認資訊安全政策已發布。
4. 檢查 VASP 對資訊安全政策之審查紀錄，以確認權責單位是否每年至少一次對資訊安全政策進行審查。
5. 抽查 VASP 資安事件紀錄，以確認是否通報內部資安部門，如涉及客戶個人資料外洩，是否通報主管機關。
6. 檢查 VASP 之資訊安全管理系統驗證紀錄，以確認資訊安全管理系統是否定期通過公正第三方之驗證。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

安全組織設立作業

程序

1. 檢查 VASP 是否訂定相關人員之工作職掌與兼辦業務情形之規定。
2. 觀察 VASP 為執行資訊安全管理作業所配置之人力資源及設備，以確認 VASP 是否係依規定配置。
3. 檢查 VASP 之資訊安全管理組織成員名單是否建冊並適時更新。
4. 檢查 VASP 之資訊安全管理審查會議紀錄，以確認資訊安全推動小組是否每年召開資訊安全管理審查會議對現有資訊安全管理依實際狀況調整。
5. 檢查 VASP 之資訊安全課程訓練紀錄，以確認資訊安全人員主管是否接受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，及使用資訊系統之從業人員是否定期參加一小時以上資訊安全課程訓練。
6. 檢查 VASP 審查重要資訊處理人員保密協議之紀錄，以確認 VASP 是否定期（至少一年一次）審查並適時要求重要資訊處理人員簽署保密協議。
7. 檢查 VASP 內部控制制度文件，確認其內部控制制度是否依所屬資安分級（若尚無適用之資安分級，則依其所營事業規模與性質）規定應取得並維持之資通安全專業證照。
8. 檢查取得資通安全專業證照之資訊安全人員名單，以確認其是否依其內部控制制度取得並維持資通安全專業證照。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

資產分類與控制作業

程序

1. 檢查資訊安全推動小組確認資訊資產清冊之紀錄，並確認 VASP 是否每年至少進行一次資訊資產盤點。
2. 抽查資訊資產異動申請單，以確認資訊資產之異動是否經資訊資產權責單位主管核准。
3. 抽查資訊資產清冊維護紀錄，比對至資訊資產異動申請單，以確認各類資訊資產之異動是否已納入資訊資產清冊。
4. 抽查資訊資產異動申請單，比對至資訊資產清冊維護紀錄，以確認各類資訊資產之異動是否已納入資訊資產清冊。
5. 抽查資訊資產，以確認每一資訊資產之機密等級已明確標示。

6. 觀察資訊資產權責單位是否依其敏感程度確實執行資料保護措施。
7. 抽查資料類型資訊資產刪除與銷毀紀錄，以確認資訊資產保管者是否於資訊資產之保存期限到期後刪除與銷毀該資產。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

人員安全作業

程序

1. 抽查對員工之背景調查記錄，以確認 VASP 是否對員工進行背景調查。
2. 對涉及財務、虛擬資產管理、資訊安全...等職位之重要人員，於錄用或任職時應進行信用紀錄與犯罪紀錄審查。
3. 檢查合約，以確認員工是否知悉其應負擔之資訊安全責任，若具有機密維護責任，須另填具保密切結書。
4. 抽查人員異動紀錄，比對至系統之權限設定，以確認異動人員之資產存取及使用權限依 VASP 規定進行調整。
5. 檢查資訊安全與個資保護教育訓練紀錄，以確認全 VASP 員工是否每年依職務層級接受資訊安全與個資保護教育訓練。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

實體與環境安全作業

程序

1. 抽查電腦機房之門禁權限審查紀錄，以確認 VASP 是否每年定期審查電腦機房之門禁權限。
2. 觀察機房監控錄影設備是否正常運作，並確認監控是否 24 小時監控，且紀錄是否至少保存 30 天，監控僅特定人員可進行存取。

3. 抽查工作日誌，以確認電腦機房管理專員是否每日紀錄管理狀況、是否紀錄電腦機房內濕度及溫度等及該等紀錄是否保留至少六個月。
4. 抽查電腦機房內之安全設備之檢查紀錄，以確認 VASP 是否委託廠商定期檢查各項安全設備（至少一年一次）。
5. 抽查出入登記簿，比對至人員進出機房申請表，以確認未具電腦機房進出權限之人員於進入機房時是否皆經核准。
6. 檢查門禁系統中之權限設定，比對至具權限員工名單，以確認系統設定有權限之員工是否皆為 VASP 有開放權限之員工。
7. 觀察辦公室監控錄影設備是否正常運作，並確認監控紀錄是否至少保存 30 天，並且僅特定人員可進行存取。
8. 觀察不具權限之人員是否可進出辦公室。
9. 抽查伺服器或個人電腦，以確認是否已設定螢幕保護與密碼保護機制。
10. 抽查權責主管核准可攜式設備之使用分配及各項設備之保管人之紀錄。
11. 檢查 VASP 是否建立相關遺失通報程序。
12. 抽查可攜式設備使用軟體情形，並比對定期檢視紀錄，以確認未使用非法或未經核准之軟體。
13. 抽查報廢紀錄，比對至經簽核之報廢申請單，以確認將報廢之設備係依據設備報廢程序執行。
14. 抽查訪客進入登記表，並觀察訪客登記情形，以確認訪客進入皆有進行登記。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

<u>通訊與作業管理作業</u>

程序

1. 檢查網路系統安全之評估紀錄，以確認網路管理人員是否定期評估網路系統安全。
2. 檢查網路運作環境與作業系統之安全漏洞檢視紀錄，比對至該等安全漏洞修補紀錄，以確認網路管理人員是否將發現之安全漏洞皆予以修補，並確保安全防護工具為最新。
3. 觀察 VASP 網路是否有區隔機制。
4. 檢查公告紀錄，以確認網路安全相關事項已確實公告，並檢視機敏資料是否適當存放。

5. 檢查 VASP 之遠端連線管理辦法文件及進行相關安全防護之紀錄，以確認是否具有遠端連線管理辦法，以及是否依該辦法進行控管。
6. 觀察 VASP 是否建立防火牆。
7. 檢查防火牆之控管紀錄及防火牆規則覆核之紀錄，以確認網路管理人員是否有定期控管防火牆及是否定期檢視防火牆規則。
8. 檢查防火牆規則異動申請單，以確認對防火牆之異動皆經權責單位主管核准。
9. 檢查防火牆規則之異動紀錄，比對至經核准之防火牆異動申請單，以確認網路管理人員是否依經核准之防火牆異動申請單設定防火牆。
10. 檢查存取控制列表之檢視紀錄，比對至網路連線授權清單，以確認是否有未經授權之存取。
11. 觀察網路下單系統登入是否採用多因子驗證。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

存取控制作業

程序

1. 檢查 VASP 是否訂定資訊系統存取控制相關規定。
2. 抽查對存取權限之申請紀錄，以確認該申請是否經該資訊資產權責單位主管核准。
3. 抽查系統之權限設定紀錄，比對存取權限之申請紀錄，以確認資產保管人員是否依經核准之存取權限申請執行權限變更。
4. 抽查職務調動紀錄或離職申請紀錄，並比對系統權限設定紀錄，以確認於異動生效日即對存取權限進行停用。
5. 抽查委外作業人員之權限授予紀錄，以確認資訊安全人員是否核准授予委外作業人員之權限。
6. 抽查委外期間結束之委外人員清單，比對至系統中對該等人員之權限設定，以確認資產保管人員是否於委外人員之委外期間結束後確實取消委外作業人員之權限。
7. 抽查系統上線紀錄並比對人員存取及授權，以確認人員已依據職務性質進行區分。
8. 抽查資通系統帳號及權限之適切性之審查紀錄，以確認該紀錄中是否包含權

責主管簽名及審查日期，並確認審查結果中之資通系統閒置帳號皆已於系統中被停用。

9. 檢查特權帳號之申請紀錄，以確認資通系統之特權帳號之申請皆經權責管理階層或治理單位核准。
10. 抽查特權帳號使用紀錄覆核之紀錄，以確認特殊權限存取紀錄是否經資訊安全人員定期覆核，且無審核人員覆核自己存取紀錄之情況。
11. 抽查使用者密碼之更改紀錄，以確認使用者密碼於首次使用後是否進行更改。
12. 觀察系統畫面，以確認系統預設之初始密碼是否已被停用或刪除。
13. 觀察保存帳號密碼之檔案是否以加密方式保存。
14. 觀察系統之密碼設定參數，以確認是否符合密碼原則。
15. 觀察使用者於變更密碼時，系統是否對使用者進行身分進行驗證。
16. 抽查系統之帳號登入異常情事通知紀錄，比對至相關處理紀錄，以確認該等情事皆已被了解並處理。
17. 檢查金鑰安全管理規定，以確認 VASP 是否訂定金鑰之安全管理規定。
18. 觀察產生、儲存、封存、檢索、分發、汰除及銷毀密碼金鑰之管理流程，以確保 VASP 確實依金鑰之安全管理規定執行。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

<u>系統開發及維護作業</u>

程序

1. 抽查系統開發申請文件，以確認該等文件是否經權責主管核准。
2. 抽查系統開發需求申請之評估紀錄，以確認系統開發人員是否對該需求進行可行性評估，並將資訊安全納入考量，以確認符合 VASP 資訊安全制度。
3. 觀察開發環境是否與正式環境有所區隔，且測試環境資料非使用正式資料，如需使用正式資料則應有相關控制措施保護資料機密性。
4. 抽查系統驗收紀錄、程式換版紀錄及比對報表，以確認經資訊安全單位主管及系統相關權責單位或申請單位相關權責人員覆核，且非由系統開發人員進行換版及編製比對報表，以確認是否符合職能分工之要求。
5. 抽查系統弱點（包含弱點掃描、滲透測試及程式原碼覆核或安全檢測等資安檢測作業）之維護紀錄，以確認權責管理人員是否確實對系統弱點進行維護

並經權責單位主管覆核。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。(經執行上述程序，除後附建議書外，並未發現重大異常之情事)

建議事項：

發現事實	負責單位	建議	管理階層回應

營運持續管理作業

程序

1. 檢查資訊安全管理單位是否訂定系統故障復原程序。
2. 抽查系統故障復原程序之測試紀錄，以確認資訊安全管理單位是否定期進行測試。
3. 檢查資訊安全管理單位是否訂定營運持續計畫。
4. 抽查營運持續計畫演練紀錄，以確認該計畫是否定期演練（至少一年一次）並依據演練結果修正該計畫。
5. 抽查核心營運系統及設備之事故應變措施之評估紀錄，以確認資訊安全管理單位是否定期評估核心營運系統及設備之事故應變措施。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。(經執行上述程序，除後附建議書外，並未發現重大異常之情事)

建議事項：

發現事實	負責單位	建議	管理階層回應

資通系統或資通服務（錢包託管技術）委外辦理作業

程序

1. 抽查委外業務之評估結果，以確認該委外是否經評估，並經業務單位主管核准。
2. 檢查委外廠商之評估紀錄，以確認委外廠商是否每年皆重新進行評估。
3. 檢查與委外廠商簽訂之契約，以確認該契約條款是否包含「服務水準協議(SLA)」、資通安全責任及保密規定、資安要求及對委外廠商資安稽核權，以及是否經業務單位主管核准。
4. 檢查委外作業人員之權限申請紀錄，以確認委外作業人員之資料存取權限是否經核准。

5. 檢查資訊安全人員定期檢視委外作業人員系統操作之紀錄，以確認委外廠商依照申請需求執行。
6. 檢查對委外廠商交付之服務系統之檢查紀錄，以確認資訊安全人員是否對委外廠商交付之服務系統檢查其未有植入後門程式等惡意程式。
7. 檢查對委外作業系統安全性之檢查紀錄，以確認資訊安全人員是否定期檢查委外作業系統之安全性。
8. 檢查委外廠商由第三方獨立機構對其進行資通安全之審查報告。
9. 抽查與委外廠商之合約，以確認合約中是否訂定委外關係於終止、解除或結束後之程序。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

新興科技應用作業

程序

1. 檢查雲端服務評估紀錄，以確認申請者是否對雲端服務的需求、適切性及可能涉及的資訊安全進行了評估，並與資訊安全單位進行過討論。
2. 檢查雲端服務之購置申請，比對至雲端服務提供廠商評估紀錄，以確認該購置是否係依評估紀錄進行，並經權責管理階層或治理單位核准。
3. 檢查與雲端服務提供廠商之合約，以確認合約中是否訂定於雲端服務運作發生資訊安全事件時之資通安全事件通報程序及處理程序。
4. 檢查儲存至雲端服務廠商之客戶資料，以確認資料，採行資料加密或代碼化等有效保護措施。
5. 檢視是否已訂定加密金鑰管理機制。
6. 檢查與雲服務廠商之終止服務協議，若已有終止雲端服務使用之情形發生，則應抽查刪除用戶資訊之確認紀錄，以確認所有用戶資訊皆已被刪除。
7. 檢查 VASP 之公務用行動裝置之資訊安全規範與管理辦法，以確認 VASP 是否對公務用行動裝置之申請、使用、更新、繳回與審核等訂定相關資訊安全規範與管理辦法。
8. 抽查對行動裝置可存取之資源之風險評估紀錄及所採取安全控管措施，以確認風險評鑑執行人員已對行動裝置可存取之資源進行風險評估並依據評估結果採取安全控管措施。
9. 觀察安裝未通過檢測之行動應用程式時，行動裝置是否確實阻擋。

10. 檢查 VASP 之員工自攜行動裝置之資訊安全規範與管理辦法，以確認 VASP 是否對自攜行動裝置之使用用途、限制裝置私接存取網際網路及行動裝置儲存機密資料之限制與管理方式等，訂定資訊安全規範與管理辦法。
11. 檢查物聯網設備管理清冊，以確認 VASP 是否至少每年更新一次。
12. 檢查物聯網設備更新紀錄，以確認該設備是否具備安全性更新機制且定期（每年一次）更新，如存在已知弱點無法更新時，應檢查其實施補償性控管措施相關紀錄。
13. 觀察物聯網設備，以確認該設備是否具備身份驗證機制或配對綁定機制。
14. 抽查物聯網設備之密碼變更紀錄，以確認是否變更該等設備之初始密碼。
15. 檢查與物聯網設備供應商簽訂之採購合約，以確認其內容是否包含資訊安全相關協議。
16. 觀察進行身分驗證時，是否有進行強化驗證並搭配其他驗證因子（如上傳身分證件、手機簡訊 OTP）。
17. 抽查留存之影像，以確認 VASP 是否對客戶驗證之身分留存紀錄。
18. 觀察進行電話交易服務時，是否有身分驗證程序。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應

符合性

程序

1. 抽查虛擬資產資訊安全管理查核作業，以確認是否定期執行相關查核作業。
2. 抽查前項查核作業，以確認缺失改善事項是否進行追蹤及改善。

執行結果

發現事實：經執行上述程序，並未發現重大異常情形。（經執行上述程序，除後附建議書外，並未發現重大異常之情事）

建議事項：

發現事實	負責單位	建議	管理階層回應