SECURITIES AND FUTURES COMMISSION
證券及期貨事務監察委員會

外部評估報告的涵蓋範圍

2023 年 6 月

目錄

外部評估報告的涵蓋範圍

1. 在《證券及期貨條例》下的現行制度及／或《打擊洗錢條例》下的虛擬資產服務提供者制度中的每名虛擬資產交易平台營運者申請人均須(i)在提交其牌照申請時，提交一份外部評估報告；及(ii)在獲證監會原則上批准之後，提交另一份外部評估報告。本文件列明應提交的外部評估報告的涵蓋範圍。

程序

2. 平台營運者在提交其牌照申請時，應提交一份由外部評估專家對平台營運者的政策及程序的設計效能的評估報告（"**第一階段評估**"）。

3. 在牌照申請的評估過程中，證監會將邀請平台營運者就各主要風險範疇詳細講解流程及進行系統示範。

4. 在證監會原則上批准有關申請後，平台營運者可進而落實任何尚待實施的系統及監控措施，並委聘外部評估專家，對有關主要風險範疇所制訂的政策、程序、系統及監控措施的全面實施和成效作出評估，包括進行穿透及漏洞測試（"**第二階段評估**"）。視乎第二階段評估的結果，並在其他待處理的事宜（如適用）（例如安排保險、開設獨立的銀行帳戶、注資及就將予銷售的虛擬資產完成納入程序等）辦妥後，證監會才會授予最終批准。

5. 有關揀選及委任外部評估專家的規定：

   - 平台營運者可在適當的情況下，委聘不同的外部評估專家就不同範疇（例如網絡保安和保管）進行檢視，視乎個別評估專家在相關領域的專業知識、經驗和往績紀錄而定。
   - 外部評估專家應獨立於申請人、其集團或集團公司。
   - 某一特定系統的服務提供者不應同時擔任同一系統的外部評估專家。
   - 外部評估專家應具有所需的專業知識及技術知識，以進行所需的評估。
   - 外部評估專家的能力聲明應連同外部評估報告一併提交予證監會。證監會保留反對委任任何外部評估專家的權利。

6. 評估的涵蓋範圍

   a) <u>第一階段評估 ── 對設計效能的外部評估</u>

   第一階段評估應聚焦於虛擬資產交易平台建議的架構、管治、運作、系統及監控措施的設計效能。外部評估專家應檢視並評估平台營運者的政策和程序是否清楚地以書面記載下來，以及是否符合適用的法律及監管規定，包括（但不限於）《適用於虛擬資產交易平台營運者的指引》和《打擊洗錢及恐怖分子資金籌集指引（適用於持牌法團及獲證監會發牌的虛擬資產服務提供者）》。有關應涵蓋的範疇，請參閱附錄 1。

b) 第二階段評估 ── 對系統及監控措施的實施成效的外部評估

第二階段評估應聚焦於所規劃的政策、程序、系統及監控措施的實施安排以及實際採納成效。只有在（除其他條件外）第二階段評估的結果獲證監會信納的情況下，證監會才會就牌照申請授予最終批准。有關應涵蓋的範疇，請參閱附錄 2。

附錄 1

第一階段評估 —— 對設計效能的評估

評估報告的格式

1. 評估報告應涵蓋下列各項：

- 摘要
- 外部評估專家的專業知識、經驗和往績紀錄
- 評估的涵蓋範圍／範疇
- 評估的限制
- 評估方法
- 對於在特定範疇內經評估的相關架構／流程／政策／程序／系統／監控措施，以及外部評估專家所採用的方法及評估程序的描述
- 詳細評估結果和針對不符合適用法律及監管規定的範疇的建議，以及平台營運者為糾正有關事宜而採取的行動（或計劃採取的行動，連同具體時間表）

應涵蓋的範疇

2. 儘管第一階段評估應涵蓋的範疇實際上可能會視乎個別平台營運者的業務及運作情況而有所不同，但證監會期望第一階段評估至少應涵蓋下列範疇：

2.1 *A 部 —— 管治及人手編制*

(i) 提供組織架構圖，當中描述平台營運者的建議管理及管治架構，各業務及營運單位和主要的人力資源，以及其各自的匯報對象；

(ii) 經考慮虛擬資產交易活動的特定性質後，確認建議的企業管治方式及人力資源是否足夠及適當；

(iii) 在人員的勝任能力方面，評估及確認平台營運者的高級管理層成員具備相關的行業經驗、資歷、技術專業知識和在他們所負責的關鍵業務職能方面的專門技能；

(iv) 確認各業務職能將有足夠數量的具備合適資格及經驗的專業人員，且將監督和匯報職責指派予合適的職員執行；

(v) 識別關鍵人員，並確認將制定有效的計劃以減低關鍵人員風險；及

(vi) 確認高級管理層成員全面了解虛擬資產交易業務的性質和相關風險，適用法律及監管規定，以及他們本身的權限及責任範圍。

2.2 *B 部 —— 納入代幣*

(i) 確認將設立由所需成員組成的代幣納入及檢討委員會，並制定透明、公平及以文件妥為記錄的決策程序和為定期匯報及持續監察獲納入的虛擬資產而設的機制；及

(ii) 確認有關納入（例如代幣納入準則）、中止、暫停及撤銷虛擬資產和持續監察獲納入的虛擬資產的政策及程序將符合相關監管規定。

2.3 *C 部 —— 保管虛擬資產*

(i) 說明建議的錢包架構和系統，錢包管理政策和管治程序，以及在不同錢包之間進行虛擬資產轉帳的操作流程；

(ii) 確認將依照傳統金融機構應達到的標準，以相若方式保障客戶資產。尤其是，有關報告應確認：

(a) 將會設立有效的監控措施，以確保 98%的客戶虛擬資產將在線下儲存；

(b) 將制定詳盡規格及經證實的程序，闡述將如何對加密裝置或應用程式的存取予以授權及核實，範圍涵蓋密鑰的產生、分派、儲存、使用及銷毀，以及可如何按規定即時撤銷某簽署人的存取權；

(c) 將設有詳細的機制，當中就虛擬資產在線上、線下及其他儲存方式之間轉移訂立充分的制衡及監控措施，並清楚列明各個指定履行該等轉移中任何非自動過程的職能的職權範圍；及

(d) 將設有穩妥程序，以便從操作及技術角度處理硬分叉（hard fork）或空投（airdrop）等事件；

(iii) 確認在私人密鑰管理方面設有充分的內部監控措施及管治程序，藉以確保於香港安全地產生、儲存及備份所有加密種子及私人密鑰。有關確認尤其應闡明：

(a) 所產生的種子及私人密鑰將足以避免猜測或串通，且有關種子或私人密鑰的產生方式將可保證隨機性，及故此無法複製有關種子或私人密鑰；

(b) 與客戶虛擬資產有關的種子及私人密鑰的存取將會嚴格地局限於獲授權人士，而平台營運者當中將無人可管有有關種子、私人密鑰或後備密碼的完整資料，以及將會設立並落實監控措施，藉此紓減平台營運者的獲授權人士互相串通的風險；

(c) 將對存取後備種子或私人密鑰設立嚴謹的監控措施，而後備種子或私人密鑰的保存及派發方式將能減輕出現任何缺失的可能，以及確保不能單靠儲存於同一實際地點的後備種子或私人密鑰而重新建立該種子或私人密鑰；及

(d) 種子及私人密鑰將在香港儲存；

(iv) 提供就平台營運者將用作儲存客戶虛擬資產的儲存方式所進行的評估（當中應顧及保安威脅、技術及市況的最新發展），並確認將在採用錢包儲存技術前進行全面測試，以確保其可靠性；

(v) 確認將就安全地處理客戶虛擬資產的提存要求制定充分的程序，以防止有關過程中所涉及的風險（例如因盜竊、欺詐及其他不誠實行為、專業上的失當行為或不作為而引致的損失），並尤其確認：

(a) 設有清晰的程序，以評核有關發展的潛在影響和風險及處理針對分布式分類帳技術的欺詐行為；

(b) 設有機制，透過採用適當的確認方法來查核及監察客戶互聯網規約（IP）地址，以及允許客戶用作提存的錢包地址；

(c) 訂有政策及程序，以確保有關暫停客戶虛擬資產提取的任何決定都是在透明及公平的基礎上作出的，而平台營運者將在沒有延誤的情況下通知證監會及平台營運者的所有客戶；及

(d) 將設有程序，以防範欺詐性要求或在威迫下作出的要求；或設有監控措施，以防止平台營運者的人員將資產轉移至獲允許的地址以外的錢包地址；及

(vi) 確認設有嚴格的程序，以便適時及有效率地為客戶資產擬備、檢視及審批對帳，並將由適當的職員核對及檢視有關對帳，而重大差異及長期未獲處理的差額將適時地向高級管理層上報，以便採取適當行動。

2.4 *D 部 —— 認識你的客戶*

(i) 說明建議的"認識你的客戶"政策及程序（包括在有關過程中將採用的任何技術），並說明能顯示在"認識你的客戶"過程中的不同階段的相關運作流程（包括識別及核實身分、簽署客戶協議、向客戶作出披露、數據收集和使用，以及上報／匯報等）；

(ii) 確認建議的"認識你的客戶"政策及程序屬於相關監管要求下可接受的開立帳戶方式；

(iii) 確認已由合資格的獨立外部評估專家進行全面的實施前評估（當中涵蓋所需範圍），以評估在透過遙距程序與海外個人客戶建立業務關係方面所採納的程序及技術的合適性及成效；

(iv) 確認"認識你的客戶"程序在確立客戶的真實和全部身分、財政狀況、資金／財務來源、投資經驗及投資目標方面的成效；

(v) 確認設有程序，以在向客戶提供任何服務前評估有關客戶對虛擬資產的認識，並處理對虛擬資產並無認識的客戶；

(vi) 確認設有程序，以評估客戶的風險承受水平及風險狀況，並確定風險狀況，及評估客戶是否適合參與虛擬資產的交易；及

(vii) 確認設有程序，以為每名客戶設定上限，藉此在參照客戶的財政狀況及個人情況的前提下，確保客戶就虛擬資產所承擔的風險根據平台營運者的判斷是合理的。

2.5 *E 部 —— 打擊洗錢及恐怖分子資金籌集*

(i) 說明建議的打擊洗錢及恐怖分子資金籌集政策、程序及管控措施（打擊洗錢／恐怖分子資金籌集制度）；

(ii) 確認建議的打擊洗錢／恐怖分子資金籌集制度是充分及適當的，足以管理及減低洗錢及恐怖分子資金籌集（洗錢／恐怖分子資金籌集）風險和確保遵守監管規定，尤其是確認設有充分及適當的打擊洗錢／恐怖分子資金籌集制度，以遵從有關下列各項的規定：

(a) 客戶盡職審查措施（包括簡化盡職審查及斷定司法管轄權是否對等；涵蓋高度風險情況、沒有為身分識別的目的而現身的客戶及政治人物的所有特別規定；在適當情況下索取額外客戶資料的規定；及適用於跨境代理關係的額外盡職審查措施）；

(b) 持續監察（包括對虛擬資產交易及相關錢包地址進行篩查，以及監察附加的客戶資料）；

(c) 虛擬資產轉帳（當平台營運者進行虛擬資產轉帳及／或以匯款機構、中介機構或收款機構的身分行事時），以及相關制裁篩查規定；及

(d) 第三者存款及付款（包括確定客戶對在匯款或收款機構開設的戶口或非託管錢包（unhosted wallet）的擁有權或控制權）；及

(iii) 確認建議的打擊洗錢／恐怖分子資金籌集制度可讓平台營運者：

(a) 在進行機構風險評估及客戶風險評估時，採用風險為本的方法並顧及到有關監管規定（例如評估洗錢／恐怖分子資金籌集風險的風險指標示例清單（並非詳盡無遺））；及

(b) 充分參照可疑交易及活動指標示例清單（並非詳盡無遺），從而識別出可疑交易及活動。

2.6 *F 部 —— 市場監察*

(i) 說明並確認設有政策及監控措施來監察虛擬資產交易平台，以識別、預防及匯報任何市場操縱或違規交易活動；

(ii) 確認平台營運者所識別及監察的交易活動種類已涵蓋可能在其業務和活動範疇內出現的大部分操縱或違規交易活動；

(iii) 說明建議的外部監察系統的設定、指標和警示種類、相關門檻、監察方法及運作，以及如何對系統加以調改並將之用作識別、偵測及預防任何市場操縱或違規交易活動；及

(iv) 說明對建議的外部監察系統進行的任何測試，並確認建議的外部監察系統在識別、偵測及預防任何市場操縱或違規交易活動方面的成效。

2.7 *G 部 —— 風險管理*

(i) 說明並確認設有適當和有效的政策及程序，讓平台營運者得以識別、衡量、監察及管理該平台營運者、其有聯繫實體及其客戶所面對的風險（不論是財務或其他風險），當中包括但不限於對手方風險、市場風險、信貸風險、財務風險及運作風險；

(ii) 說明並確認設有有效及獨立的風險管理職能，聯合平台營運者的高級管理層一同界定風險政策，訂立和維持風險措施，以及監察並定期檢視風險管理政策及程序；

(iii) 說明並確認有就虛擬資產交易平台的運作制定風險管理及監督管制措施，例如系統監控措施（旨在防止出現"胖手指"（fat finger，意即錯誤操作鍵盤或滑鼠）錯誤的情況、阻止接納交易指示及取消交易指示等等）、自動化交易前監控措施及交易後監察。

2.8 *H 部 —— 網絡保安*

(i) 識別網絡保安風險，包括欺詐風險、錯誤及遺漏、服務中斷或其他運作或監控缺失；

(ii) 說明並確認建議的資訊科技預算和建議的資訊科技庫存清單，就支援業務活動和營運的規劃中資訊科技基礎設施、系統及保安監控措施的實施和運作而言，是足夠及完備的；

(iii) 確認所規劃的資訊科技基礎設施和系統符合相關規定及穩健的行業作業手法，並可達致高水平的資訊安全、系統穩定性和業務延續性；

(iv) 確認設有政策及程序以有效管理及充分監督虛擬資產交易平台（包括其交易系統及託管基礎設施）的設計、開發、應用及運作，及平台營運者將會因應市況及監管發展的變化，定期檢討這些政策及程序；

(v) 確認平台營運者將為虛擬資產交易平台的設計、開發、應用及運作調配具備足夠資格的職員、專才、技術設備及財政資源；

(vi) 確認平台營運者將就第三方服務提供者作出適當的盡職審查、持續的監察及適當的安排，確保其將遵守適用法律及監管規定；

(vii) 確認有就系統升級及維護訂立書面標準運作程序，當中載述（其中包括）(a)通訊的方式，以及如何處理仍在掛盤冊且有待執行的交易

指示；(b)有關在系統停機後及在恢復持續交易前有多少時間輸入、更改或取消交易指示的資料；及(c)適用於在預期及計劃之外，並對有序市場構成影響的系統故障的程序；

(viii) 確認設有政策及程序以確保交易系統及對系統的所有改動在應用前將會經過測試，並定期予以檢視，另亦會就交易系統的所有改動備存清晰的審計線索；

(ix) 確認設有政策及程序，一旦任何交易系統中斷以致申請人的客戶可能受到影響，可在切實可行的情況下盡早通知客戶；

(x) 確認申請人將採取充足、最新及適當的保安監控措施，以保護虛擬資產交易平台免被濫用。這些保安監控措施至少應包括：(a)藉著可靠的驗證方式及技術來確保只有限定人士可進入虛擬資產交易平台；(b)就客戶帳戶的登入實施雙重認證；(c)就密碼制訂有效的政策及程序；(d)設立嚴格的密碼政策及網頁超時監控措施；(e)就某些活動通知客戶；(f)對基礎設施實施足夠的保安監控措施；(g)採用最新數據加密及安全轉移技術；(h)採用最新的保安工具，以偵測、預防及阻止任何潛在的入侵、違反保安規定及網絡攻擊的情況；及(i)設有充足的內部程序及為申請人的職員提供培訓，並定期向其客戶提供警示及教材，以提高他們對網絡保安的重要性及需嚴格遵循系統保安規定的意識；

(xi) 確認設有政策及程序，訂明懷疑或確實的網絡保安事故將以何種方式向內和向外上報；

(xii) 確認設有政策及監管措施，以(a)定期監察虛擬資產交易平台的容量使用情況，並訂有適當的容量規劃；(b)對虛擬資產交易平台的容量定期進行壓力測試，以確定在不同的模擬市況下的系統表現，並以文件載明壓力測試的結果及為解決壓力測試所發現的問題而採取的任何行動；(c)確保平台的容量將足以處理在營業額及市場成交量方面任何可預見的增長；及(d)確保在必要時會作應變安排（並已將當中細節告知客戶）；

(xiii) 確認訂有應變計劃，以處理與虛擬資產交易平台有關的緊急情況及服務中斷事故，包括在系統復原後檢查及確保數據的完整性，及確保交易在系統恢復運作後可以公平和有序的方式進行；及

(xiv) 確認設有政策及程序，確保後備設施及應變計劃至少每年進行一次有關可行性及充足性方面的檢討、更新及測試。

附錄 2

第二階段評估 — 對實施成效的評估

評估報告的格式

1. 評估報告應涵蓋下列事項：

- 摘要
- 外部評估專家的專業知識、經驗和往績紀錄
- 評估的涵蓋範圍／範疇
- 評估的限制
- 評估方法
- 對經過評估的特定範疇及外部評估專家所採用的評估方法和程序的描述
- 清楚載列及說明任何偏離計劃之處，並評估有關偏差會否導致違反適用法律及監管規定
- 詳細評估結果和針對未有妥為或按計劃設置或落實的事宜的建議，以及平台營運者為糾正有關事宜而採取的行動

須涵蓋的範疇

2. 證監會預期第二階段評估應至少評估下列範疇的政策、程序、系統及監控措施有否妥為落實（如第一階段評估所述），經過測試或抽樣檢查並且（如適用）設有後備方案。任何偏離所規劃的政策及程序之處均須清楚地列出並加以說明。

2.1 *A 部 —— 納入代幣*

- 擬獲納入以供買賣的虛擬資產
- 代幣納入及檢討委員會

2.2 *B 部 —— 保管虛擬資產*

- 錢包系統及備份
- 錢包操作系統
- 保險庫及其他儲存方式
- 密鑰轉換
- 種子或私人密鑰的備份

- 對種子及私人密鑰以及有關備份的存取權及控制權
- 由線上轉至線下及由線下轉至線上的內部轉移、調整及充值
- 處理客戶的提存要求
- 將用作提存的錢包地址列於允許的範圍內
- 客戶資產對帳

2.3 *C 部 —— 認識你的客戶*

- 與客戶建立業務關係的程序
- 專業投資者評估
- 客戶的虛擬資產知識評估
- 客戶的風險承受水平評估
- 為客戶釐定風險狀況
- 設立風險承擔限額
- 客戶協議以及條款和條件
- 向客戶作出披露

2.4 *D 部 —— 打擊洗錢及恐怖分子資金籌集*

- 機構風險評估
- 客戶風險評估
- 客戶盡職審查措施
- 簡化盡職審查及斷定司法管轄權是否對等
- 涵蓋高度風險情況、沒有為身分識別的目的而現身的客戶及政治人物的所有特別規定
- 適用於跨境代理關係的額外盡職審查措施
- 確保客戶資料反映現況
- 交易監察
- 制裁篩查

- 可疑交易匯報
- 虛擬資產轉帳
- 第三者存款及付款

2.5 *E 部 —— 市場監察*

- 設定警示種類、指標及門檻
- 就所產生的警示／個案進行回溯測試及抽樣檢查
- 就所產生的警示／個案進行檢討及評估
- 持續檢討（例如管理層報告及趨勢分析）

2.6 *F 部 —— 交易系統及風險管理*

- 交易系統及配對引擎
- 系統監控措施
- 交易前監控措施
- 監察登入情況
- 監察預先注資的情況
- 有關員工存取交易資料的監控措施
- 應用程式介面
- 就預期及計劃之外的中斷事故而設的故障後復原及應變演習

2.7 *G 部 —— 網絡保安*

- 資訊科技系統及監控措施經過測試，務求在運作暢順程度、資訊安全水平、系統穩定性和業務延續性方面均有高度保證。

  (a) 平台的可靠性

  (b) 平台的安全性

  (c) 平台的容量及壓力測試（包括虛擬資產交易平台的容量）

  (d) 系統及數據備份

  (e) 數據的完整性及保密性

  (f) 用戶使用權管理

(g) 修補程式管理

(h) 端點防護

(i)硬件及軟件在未經授權的情況下被安裝

(j)應變措施

- 第二階段評估亦應涵蓋下列事項：

(a) 查核並確認所有外部服務提供者（例如市場監察工具、打擊洗錢及恐怖分子資金籌集工具以及"認識你的客戶"工具）已獲委聘，而由它們提供的相關系統已按計劃全面經過調改並投入運作。

(b) 進行漏洞評估，從而將那些一旦被人利用便可能會導致系統遭入侵（蓄意或非蓄意）的漏洞識別出來，並對這些漏洞進行評級及作出匯報。有關報告應列出已知漏洞（按照風險水平評級）所引致的潛在風險。漏洞評估應涵蓋外部及內部漏洞掃瞄。

(c) 對網絡裝置、防火牆、伺服器、數據庫、錢包及網站應用程式進行穿透測試。測試必須同時包括應用程式層面及網絡層面的評估。有關報告應描述經核證的每項漏洞及／或所發現的潛在問題。

(d) 確認已就在穿透及漏洞測試中所識別出的全部中高風險項目，採取重要／關鍵的糾正措施。