

就「虛擬資產交易平台營運者的建議監管規定的諮詢文件」提交意見書

UD 成立於1998年，早期以提供域名註冊、網頁寄存等雲端服務為主，及後逐漸發展成雲端管理、網絡方案及網絡安全管理服務供應商。我們擁抱創新，自2017年起，我們開拓區塊鏈業務，為客戶提供區塊鏈、NFT及加密貨幣服務，我們的專家團隊提供區塊鏈、NFT、元宇宙及加密貨幣等諮詢服務及一站式解決方案，致力為本港不同的企業通過創新區塊鏈技術進一步發展業務。

我們關注證券及期貨事務監察委員會發牌的虛擬資產交易平台營運者的監管規定，並提出我們的看法和建議。

針對問題6，有關如何有效地紓減和保管客戶虛擬資產風險（特別是線上儲存方式），我們認為平台營運方需要在平台設計階段就考慮網絡安全元素，包括日常運作程序、政策、管理和技術上的網絡安全考量。在技術方案方面，我們提出以下建議：

驗證平台營運方的措施是否符合網絡安全標準，例如OWASP或NIST等相關網絡安全框架。在採用線上儲存方式持有虛擬資產時，需要諮詢合格的網絡安全顧問，而核心系統需要進行定期漏洞掃描，以確保已排除所有已知漏洞。

以我們在網絡安全管理服務的多年經驗得知，大部分系統在設計時都針對程式漏洞下了功夫，因為往往事故都出現在系統運作一段時間後，從運作流程中出現邏輯漏洞。因此定期的滲透測試是必須的，可確保系統免於系統邏輯或更精密的攻擊。

除了技術方案，我們還建議平台營運方進行技術稽查，檢視現有的政策、控管和技術配置，例如是否有公司網絡安全守則，確保系統在應用層面以外也有多種防護政策。此外，獨立的網絡安全專家可以中立地評估平台營運方的網絡保安措施是否貼合實際情況。

證監會同時提出平台營運者應安排定期技術稽查及網絡保安評估，包括滲透測試，以確保平台營運方的網絡保安措施貼合實際需求，將攻擊層面減到最低。

我們強烈建議平台營運者採取積極態度，安排定期的技術稽查和網絡保安評估，以及滲透測試，以確保系統的安全性。每月掃描可以協助安全部門及時發現遺留的高風險系統和漏洞。滲透測試則建議至少每年進行一次，如果系統中保有敏感數據，建議在 DevSecOpS 程序中同時考慮。

在系統推出前，平台營運者應該進行安全測試，以確保系統的安全性。同時，在系統上線之前，應該確保系統已經達到安全規範。牽涉到私隱安全的新功能，更應該在推出前進行漏洞測試。

以上是我們作為資深網絡安全管理服務供應商的建議，希望能引起平台營運者的重視，並採取相應的措施，確保系統安全，以保障投資者的資產安全。如委員會對以上意見書有任何提問，歡迎與我們聯絡。

二零二三年三月二十三日



UD Blockchain

Tel: 2554 7545 | Fax: 2554 7215 | Email: service@ud.hk | ud.hk