

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
通訊與作業管理— 網路安全管理（適用網際網路下單證券商，另一、二、五項並適用於全體證券商）	<p>一、網路系統安全評估：</p> <p>(一) 是否定期評估自身網路系統安全(例如：作業系統、網站伺服器、瀏覽器、防火牆及防毒版本等)，並留存相關紀錄。</p> <p>(二) 是否定期或適時修補網路運作環境及作業系統之安全漏洞（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），並留存相關文件。</p> <p>(三) 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)之事項是否隨時對內部公告。</p> <p>(四) 各電腦主機、重要軟硬體設備是否有專人負責。</p> <p>(五) 公司網路是否依用途區分為 DMZ、營運環境、測試環境及其他環境，並有適當區隔機制(如防火牆、虛擬區域網路、實體隔離等)。</p> <p>(六) 個人資料及機敏資料是否存放於安全的網路區域。</p> <p>(七) 系統是否僅開啟必要之服務及程式，未使用之服務功能應關閉。</p>				
備 註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員

日 期

證券股份有限公司

作業週期：每月至少查核乙次

電腦作業與資訊提供查核明細表

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
通訊與作業管理— 網路安全管理（適 用網際網路下單證 券商，另一、二、 五項並適用於全體 證券商）	<p>(八) 公司是否建立遠端連線管理辦法，對使用外部網路遠端連線至公司內部作業進行控管，留存相關維護紀錄並由權責主管定期覆核。</p> <p>二、 防火牆之安全管理：</p> <p>(一) 是否建立防火牆。</p> <p>(二) 防火牆是否有專人管理。</p> <p>(三) 防火牆進出紀錄及其備份是否至少保存三年。</p> <p>(四) 重要網站及伺服器系統(如網路下單系統等) 是否以防火牆與外部網際網路隔離。</p> <p>(五) 防火牆系統之設定是否經權責主管之核准。</p> <p>(六) 是否每年定期檢視並維護防火牆存取控管設定，並留存相關紀錄。</p>				
備 註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員

日 期

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
通訊與作業管理— 網路安全管理（適 用網際網路下單證 券商，另一、二、 五項並適用於全體 證券商）	<p>三、 網路傳輸安全管理：</p> <p>(一) 網路下單畫面是否採加密方式(例如：SSL)處理。</p> <p>(二) 公司是否每日針對核心系統之帳號登入失敗紀錄、非客戶帳號嘗試登入紀錄等進行監控及分析，發現有帳號登入異常情事(如密碼輸入錯誤達三次、一定時間內大量帳號登入失敗、帳戶申請或更新憑證下載異常)，是否即時了解異常原因，並留存相關紀錄。</p> <p>(三) 網路下單登入時是否採多因子認證方式(例如：下單憑證、綁定裝置、OTP、生物辨識等機制，以確保為客戶本人登入。</p> <p>四、 CA 認證與憑證管理：</p> <p>(一) 網路下單是否訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，是否採用多因子(如：下單憑證、綁定裝置、OTP、生物辨識及 SIM 認證等)驗證方式，且與登入帳戶時使用之因子不同，確實辨認客戶身分並留存紀錄。</p> <p>(二) 網路下單是否全面使用認證機制。</p> <p>五、 電腦病毒及惡意軟體之防範：</p> <p>(一) 是否安裝防毒軟體，並及時更新程式及病毒碼。</p> <p>(二) 是否定期對電腦系統及資料儲存媒體進行病毒掃瞄(含電子郵件)。</p>				
備 註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員

日 期

證券股份有限公司

電腦作業與資訊提供查核明細表

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
通訊與作業管理— 網路安全管理（適 用網際網路下單證 券商，另一、二、 五項並適用於全體 證券商）	<p>(三) 防毒是否涵蓋個人端（含攜帶型及營業處所內供投資人共用之電腦等）及網路伺服器端電腦。</p> <p>(四) 是否對於電子郵件中帶電腦病毒之附件或網頁連結，進行掃毒作業或阻擋。</p> <p>(五) 為防範電腦病毒擴散，影響電腦安全，公司是否訂定電子郵件使用安全相關規定及建立郵件過濾機制。</p> <p>(六) 公司是否建立上網管制措施，以避免下載惡意程式。</p> <p>(七) 公司是否偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。</p> <p>(八) 公司是否每年定期辦理社交工程演練，並對誤開啟信件或連結之人員進行教育訓練，並留存相關紀錄。</p> <p>六、 網路下單系統功能檢查：</p> <p>(一) 是否定期檢查網路下單系統提供之功能，並留存紀錄。</p> <p>(二) 是否就提供外部連線使用網路下單系統偵測網頁與程式異動、記錄並通知相關人員處理。</p>				
備 註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員

日期

證券股份有限公司

電腦作業與資訊提供查核明細表

項 目	查 核 程 序	查 核 結 果			底 稿 索 引
		是	否	不適用	
通訊與作業管理— 網路安全管理（適 用網際網路下單證 券商，另一、二、 五項並適用於全體 證券商）	<p>七、公司提供 API 服務規範： 公司提供客戶使用應用程式介面(API)服務，是否於首次下單前就相關傳輸設定進行連線測試，並留存相關測試紀錄。</p> <p>八、網際網路下單服務品質相關標準： 公司提供網際網路下單業務時，兼顧客戶服務品質，是否訂定網際網路下單服務品質相關標準，並包含下列重點如：交易之安全性、交易之穩定及系統可用性、提供客戶服務。</p> <p>九、帳號登入或異常態樣通知： 公司對於客戶帳號登入時宜進行通知，如有符合以下異常態樣是否即通知客戶，並留存紀錄，避免非客戶本人登入情事：(1)密碼輸入錯誤或帳戶被鎖定；(2)申請或更新憑證；(3)變更基本資料；(4)異常來源或行為嘗試登入等；(5)密碼申請異動或補發時。</p> <p>十、異常 IP 登入之監控與預警： 公司應依其所屬資安分級對於嘗試登入帳號之異常及不明來源 IP，如發現下列情形，是否有警示機制，進行監控分析及留存紀錄，並定期檢視以確認機制有效運作：(1)同一來源 IP 登入不同帳號達一定次數以上；(2)同一帳號在一定時間內由不同國家登入；(3)發現異常 IP(如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單)或國外 IP 嘗試登入。</p>				
備 註：使用主機共置服務者，稽核人員應另就屬主機共置服務業務之查核程序再進行查核，並同時作成查核報告。					

稽核人員

日期