證券商內部控制制度標準規範—內部稽核實施細則修訂對照表（111 年）

編號	作業項目	修　訂　後　內　容	修　訂　前　內　容	修訂說明
AC-12000	資訊安全政策之稽核 目的： 確定上述作業是否符合規定辦理	(一)~(六)略 (七)、公司每年是否將前一年度資訊安全整體執行情形，由**資訊安全長或**負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具**「證券暨期貨市場各服務事業建立內部控制制度處理準則」第二十四條規定之內部控制制度聲明書，於會計年度終了後三個月內提報董事會通過，並將該聲明書內容揭露於主管機關指定之申報網站。** （以下略）	(一)~(六)略 (七)、公司每年是否將前一年度資訊安全整體執行情形，由負責資訊安全之最高主管與董事長、總經理、稽核主管聯名出具資訊安全整體執行情形聲明書，並提報董事會通過，於會計年度終了後三個月內將該聲明書內容揭露於公開資訊觀測站。 （以下略）	**配合內部控制制度 CC-12000 之修訂，並同時修訂查核明細表(I-140-2)。**

AC-17010（適用網際網路下單證券商，另1、2、3、4、5、8、9、10、15、16、18、19、20、21項並適用於所有證券商）	通訊與作業管理－網路安全管理之稽核目的：確定上述作業是否符合規定辦理	（一）、網路安全管理： 1.~6.(略) 7.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。 8.~27.(略) 28.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。 29.略。 30.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	（一）、網路安全管理： 1.~6.(略) 7.網路下單是否訂定憑證交付程序，避免非本人取得憑證。 8.~27.(略) 28.公司是否每日針對核心系統之帳號登入失敗紀錄、非客戶帳號登入嘗試紀錄等進行監控及分析，並留存相關紀錄。 29.略。 30.(新增)	配合內部控制制度 CC-17010之修訂，並同時修訂查核明細表(I-91-1)。

		行為嘗試登入等；(5)密碼申請異動或補發時。 31.公司是否依其所屬資安分級對異常及不明來源 IP 連線進行監控分析及留存紀錄，如有發現下列情形，應設有警示機制，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) 異常來源（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。	31.(新增)	
AC-18000	存取控制之稽核目的：確定上述作業是否符合規定辦理	(一)~(七) 略 (八)、密碼是否~~以亂碼方式儲存~~使用公開安全且未遭破解之演算法(例如：雜湊演算法等不可逆運算式)產生亂碼並加密儲存。；初始密碼是否隨機產生，並與使用者或客戶身分無關。(本項不適用採自行訂定交付電子式交易密碼條之方式) (九)、密碼輸入錯誤次數達三次者，是否予中斷連線且鎖定該帳號，並留存紀錄。公司於接獲客戶聯繫申請解除鎖定時，是否確實辨認身分(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，並留存相關紀錄後，始得辦理之。 (十)、對於使用者及客戶忘記密碼之處理，公司	(一)~(七)略 (八)、密碼是否以亂碼方式儲存；初始密碼是否隨機產，並與使用者身分無關。 (九)、密碼輸入錯誤次數達三次者，是否予中斷連線。。 (十)、對於使用者忘記密碼之處理，是否有	配合內部控制制度 CC-18000 之修訂，並同時修訂查核明細表(I-91-2)。

AC-19000	系統開發及維護之稽核 目的： 確定上述作業是否符合規定辦理	是否有嚴格的身分確認程序(如聯繫客服驗證基本資料、OTP、臨櫃辦理等方式)，方可再次使用系統。 (十一)、除語音按鍵下單~~輸入介面僅可輸入數字外（例如：語音按鍵下單）~~，公司是否使用優質密碼設定(長度六個字元(含)以上，且具有文數字或符號)並進行管控。 (十二)、客戶密碼超過一年未變更或變更密碼與前一代相同，公司是否做妥善處理。除客戶外，公司其他使用者之密碼是否至少每三個月變更一次。 （以下略） (一)~(四十八)略 (四十九)、委外系統如涉及機敏性資料傳送(如：客戶帳號密碼或交易資料等)是否檢驗相關資料流，傳遞對象之妥適性並留存相關紀錄	嚴格的身分確認程序，方可再次使用系統。 (十一)、除輸入介面僅可輸入數字外（例如：語音按鍵下單），公司是否使用優質密碼設定(長度六個字元(含)以上，且具有文數字或符號)並進行管控。 (十二)、除客戶外，公司其他使用者之密碼是否至少每三個月變更一次。 （以下略） (一)~(四十八)略 (四十九)、(新增)	配合內部控制制度 CC-19000之修訂，並同時修訂查核明細表(I-130-3)。