建立證券商資通安全檢查機制部分條文修正對照表（115 年）

修正條文	現行條文	說明
1.略	1.略	
2.略	2.略	
3.略	3.略	
4.資產分類與控制（CC-14000，半年查核）	4.資產分類與控制（CC-14000，半年查核）	
（1）~（5）略	（1）~（4）略	
	（5）公司應避免使用危害國家資通安全產品。	
（6）應定期盤點使用之應用程式介面(API)，並建立適當安全控管機制。	(新增)	增訂檢查重點
5.(略)	5.略	
6.實體與環境安全（CC-16000，半年查核）	6.實體與環境安全（CC-16000，半年查核）	
（1）電腦機房應設有門禁管制~~（例如：刷卡）~~。	（1） 電腦機房應有門禁管制（例如：刷卡）。	避免限縮實務執行方式，爰刪除例示文字，以採原則性規範。
（2）~（6）略	（2）~（6）略	
（7）公司自有及租用之機房或機櫃，除公司之期貨商關係企業且設有網路區隔，始得與其共同使用同一機房或	(新增)	增訂檢查重點

機櫃外，均不得將機房或機櫃空間分租、轉租、出借或以任何方式提供第三方使用。		
7.通訊與作業管理（CC-17000） （1） 網路安全管理（CC-17010，適用網際網路下單證券商，另 a、b、f、m 項並適用於所有證券商，每月查核） a.網路系統安全評估： （a） ~ （j）略 （k）公司應就所接收資安情資，辨識其來源之可靠性及時效性，及時進行威脅與弱點分析及研判潛在風險，並採取對應之預防或應變措施。 b 網路設備之安全管理： （a） ~ （c）略 （d）重要網站及伺服器系統（如網際網路下單系統等）應以防火牆與外部網際網路隔離。 （e） ~ （h）略	7.通訊與作業管理（CC-17000） （1） 網路安全管理（CC-17010，適用網際網路下單證券商，另 a、b、f、m 項並適用於所有證券商，每月查核） a.網路系統安全評估： （a）~（j）略 (新增) b 網路設備之安全管理： （a） ~ （c）略 （d）重要網站及伺服器系統（如網路下單系統等）應以防火牆與外部網際網路隔離。 （e） ~ （h）略	參酌「證券商辦理資通系統資通安全評估作業程序」，增訂情資評估及處理之規定。 調整用字一致性

c. 網路傳輸安全管理： （a）網際網路下單畫面應採加密方式(例如：TLSSSL)處理。 （b）略 （c）公司提供網際網路下單服務，應於網際網路下單登入時採多因子認證方式（例如：固定密碼、圖形鎖、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。 （d）略 d 略 e.身分認證與憑證管理 （a）網際網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，必須採用多因子（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。 （b）網際網路下單證券商應全面使用認證機制。	c. 網路傳輸安全管理： （a）網路下單畫面應採加密方式(例如：SSL)處理。 （b）略 （c）公司提供網路下單服務，應於網路下單登入時採多因子認證方式（例如：固定密碼、圖形鎖、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。 （d）略 d 略 e.身分認證與憑證管理 （a）網路下單證券商應訂定憑證交付程序，避免非本人取得憑證。客戶申請或更新憑證下載，必須採用多因子（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。 （b）網路下單證券商應全面使用認證機制。	調整用字一致性及範例，避免使用安全性不足之協議 調整用字一致性 調整用字一致性 調整用字一致

（c）~（d）略 f.電腦病毒及惡意軟體之防範： （a）~（e）略 （f）公司應建立軟體白名單及上網控管機制。 （g）~（h）略 g. 網路系統功能檢查： （a）應定期檢查網際網路下單系統提供之功能，並留存紀錄。 （b）略 h~m 略 （2）略 8.存取控制（CC-18000，每月查核） （1）~（2）略 （3） 密碼管理： a~e 略 f.除語音按鍵下單外，公司應使用優質密碼設定（長度 6 個字元（含）以上，且具有文數字或符號）並進行管控，及加強宣導客戶定期更新密碼以不超過三個月為宜，如客戶密碼超過一年未變	（c）~（d）略 f.電腦病毒及惡意軟體之防範： （a）~（e）略 （f）公司應建立軟體白名單控管機制。 （g）~（h）略 g. 網路系統功能檢查： （a）應定期檢查網路下單系統提供之功能，並留存紀錄。 （b）略 h~m 略 （2）略 8.存取控制（CC-18000，每月查核） （1）~（2）略 （3） 密碼管理： a~e 略 f.除語音按鍵下單外，公司應使用優質密碼設定（長度 6 個字元（含）以上，且具有文數字或符號）並進行管控，及加強宣導客戶定期更新密碼以不超過三個月為宜，如客戶密碼超過一年未變更或變更密碼與前一代相同，公司應做妥善處	性 增訂上網連線管控機制規定 調整用字一致性 增訂系統使用帳號密碼之例外管理規定

更或變更密碼與前一代相同，公司應做妥善處理。~~除客戶外，~~公司~~其他~~使用者之密碼除提供系統使用之帳號應採定期變更或適當安全控管措施（如限制人工登入、監控告警等）外，應至少每三個月變更一次。 g~h 略 （4）電腦稽核紀錄管理： a. 對重要系統（如主機連線系統、網際網路下單系統等）之稽核日誌記錄內容應包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項。 b~d 略 （5）略 （6） 資料輸出管理： a~b 略 c. 投資人於公司網站查詢個人資料應具有加密傳輸機制（例如：TLS~~SL~~）。 d 略 9.系統開發及維護（CC-19000，半年查核） （1）~（3）略	理。除客戶外，公司其他使用者之密碼應至少每三個月變更一次。 g~h 略 （4）電腦稽核紀錄管理： a. 對重要系統（如主機連線系統、網路下單系統等）之稽核日誌記錄內容應包括使用者識別碼、登入之日期時間、電腦的識別資料或其網址等事項。 b~d 略 （5）略 （6） 資料輸出管理： a~b 略 c. 投資人於公司網站查詢個人資料應具有加密傳輸機制（例如：SSL）。 d 略 9.系統開發及維護（CC-19000，半年查核） （1）~（3）略 （4） 委外廠商管理：	調整用字一致性 調整範例，避免使用安全性不足之協議

（4） 委外廠商管理： a~b 略 c.資訊服務供應商應提供安全性檢測證明（如行動應用程式資安檢測、源碼~~檢測~~掃描、弱點掃描等），並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過源碼掃描或黑箱測試。 d~l 略 （5）~（7）略 （8） 應用系統異動管理： a~b 略 c. 程式~~系統~~變更上線前應進行完整測試，變更完成後須檢核與申請內容是否相符，並進行~~必要~~驗證以確認變更作業之可用性及正確性。 （9）~（11）略 （12）核心系統~~發生錯誤時，應針對風險評估~~使用者頁面應僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 （13）~（14）略	a~b 略 c.資訊服務供應商應提供安全性檢測證明（如行動應用程式資安檢測、源碼檢測、弱點掃描等），並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過源碼掃描或黑箱測試。 d~l 略 （5）~（7）略 （8） 應用系統異動管理： a~b 略 c.系統變更完成後須檢核與申請內容是否相符，並進行必要驗證以確認變更作業之正確性。 （9）~（11）略 （12）核心系統應針對風險評估使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。 （13）~（14）略 10. 營運持續管理（CC-20000，半年查核）	調整用字一致性 增訂程式更版上線前驗證之規定 調整文字，以清楚規範適用範圍。

10.營運持續管理（CC-20000，半年查核） （1）~（2）略 （3）公司應每年至少執行一次營運衝擊分析，評估核心系統可容忍中斷時間、復原時間目標（RTO ）、資料復原點目標（RPO ），並擬訂營運持續計畫（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，依其所屬資安分級定期辦理業務持續運作演練，且視演練範圍是否涉及第三方，邀請相關廠商參與演練。網際網路下單證券商應依經紀業務規模市占率暨自然人客戶數比率分級，訂定核心系統可容忍中斷時間。 （4）公司應依所屬資安分級建置異地備援機房，並依營運衝擊分析結果於異地備援機房建置對營運具重大影響之核心系統，以維持營運持續運作能力。（註：異地備援機房建置範圍由交易主機擴大至對營運具重大影響之核心系統，自 116 年 12 月底生效。）	（1）~（2）略 （3）證券經紀商之交易主機應有備援措施，並依所屬資安分級建置異地備援機房。 （4）公司應執行營運衝擊分析，評估核心系統可容忍中斷時間、復原時間目標（RTO ）、資料復原點目標（RPO ），並擬訂營運持續計畫（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，依其所屬資安分級定期辦理業務持續運作演練，且視演練範圍是否涉及第三方，邀請相關廠商參與演練。網路下單證券商應依經紀業務規模市占率暨自然人客戶數比率分級，	原條文(4)前移至(3)，增訂辦理頻率每年至少一次。 調整用字一致性 原條文(3)後移至(4)，為維持營運韌性，擴大異地備援機房建置範圍至對營運具重大影響之前端交易系統、中台

（5）~（6）略 （7）公司應明確訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序，並每年進行演練。 (以下略)	訂定核心系統可容忍中斷時間。 （5）~（6）略 （7）公司應明確訂定分散式阻斷服務攻擊（DDoS）防禦與應變作業程序。 (以下略)	等核心系統。 增訂週期性演練規定