建立證券商資通安全檢查機制部分條文修正對照表

修正條文	現行條文	說明
1 風險評鑑與管理（CC-11000，適用網際網路下單證券商，不適用語音下單及傳統下單之證券商，年度查核） (1)~(3)略 (4)應評估核心系統可容忍中斷時間。 2.資訊安全政策(CC-12000，年度查核) (1)~(6)略 (7)公司應參考「建立證券商資通安全檢查機制-分級防護應辦事項附表」辦理資訊安全分級防護應辦事項。 (8)公司應依其所屬資安分級辦理核心系統導入資訊安全管理系統，並通過公正第三方之驗證，且持續維持驗證有效性。(111 年 1 月底導入生效，112 年 1 月底驗證生效) 3.安全組織（CC-13000，半年查核） (1)-(2)略 (3)公司應視資訊安全管理需要及所屬資安分級，指定專人或專責單位負責規劃與執行資訊安全工作，且資訊安全專責人員及專責主管每年應定期參加十五小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。 (4)-(5)略 (6)公司應依其所屬資安分級要求資安專責人員取得並維持相當資通安全專業證照。(112 年 1 月底生效)	1.風險評鑑與管理（CC-11000，適用網際網路下單證券商，不適用語音下單及傳統下單之證券商，年度查核） (1)~(3)略 (4)新增 2.資訊安全政策(CC-12000，年度查核) (1)~(6)略 (7)新增 (8)新增 3.安全組織（CC-13000，半年查核） (1)-(2)略 (3)公司應視資訊安全管理需要，指定專人或專責單位負責規劃與執行資訊安全工作，且每年應定期參加十五小時以上資訊安全專業課程訓練或職能訓練並通過評量。其他使用資訊系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。 (4)-(5)略 (6)新增	奉金融監督管理委員會證券期貨局 108 年 10 月 14 日證期(券)字第 1080360522 號函囑參酌銀行金融機構辦理電子銀行安全控管作業基準之相關規定，檢視現行證券規範不足並研議強化修正。 奉金融監督管理委員會證券期貨局 109 年 7 月 15 日證期(券)字第 1090363177 號函囑邀集證券商業同業公會及財團法人中華民國證券櫃檯買賣中心開會共同研商資安應辦事項及推

4.資產分類與控制（CC-14000，半年查核） (1)~(2)略 (3)公司應對自行或委外開發之資訊系統完成資訊系統分級，資訊系統等級應至少區分核心與非核心系統，每年應至少檢視一次資訊系統分級妥適性。(111年1月底生效) (以下略) 6.實體環境與環境安全(CC-16000，半年查核） (1)~(5)略 (6)公司應定期審查資訊機房門禁管制權限。 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、e 項，適用於所有證券商，每月查核） a.網路系統安全評估： (a)~(d)略 (e)公司網路應依用途區分為 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)。 (f)個人資料及機敏資料應存放於安全的網路區域，不得存放於網際網路等區域。 (g)系統應僅開啟必要之服務及程式，未使用之服務功能應關閉。 (h)公司應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。 (i)公司應防止未經授權設備使用內部網路。	4.資產分類與控制（CC-14000，半年查核） (1)~(2)略 (3)新增。 (以下略) 6.實體環境與環境安全 CC-16000，半年查核） (1)~(5)略 (6)新增 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、e 項並適用於所有使用競價終端設備連結公眾網路之證券商，每月查核） a.網路系統安全評估 (a)~(d)略 (e)新增 (f)新增 (g)新增	動時程。

b. 防火牆之安全管理 (a)~(e)略 (f)公司應每年定期檢視並維護防火牆存取控管設定，並留存相關檢視紀錄。 (g)公司交易相關網路直接連線之設備不得使用危害國家資通安全產品。 (以下略) e.電腦病毒及惡意軟體之防範 (a)~(d)略 (e) 為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定及建立郵件過濾機制。 (f) 公司應建立上網管制措施，以避免下載惡意程式。 (g) 公司應偵測釣魚網站及惡意網站連結並提醒客戶防範網路釣魚。 (h) 公司宜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。 f~h 略 i.網路攻擊防護機制導入及安全性檢測 (a)公司應依其所屬資安分級定期對提供網際網路服務之核心系統辦理滲透測試，並依測試結果進行改善。(111 年 1 月底生效) (b)公司應依其所屬資安分級定期辦理資通安全健診(應含網路架構檢視、網路惡意活動檢視、使用者端電腦惡意活動檢視、伺服器主機惡意活動檢視、目錄伺服器設定及防火牆連線設定檢視)。(112 年 1 月底生效)	(h)新增 (i)新增 b.防火牆之安全管理 (a)~(e)略 (f)新增 (g)新增 (以下略) e.電腦病毒及惡意軟體之防範 (a)~(d)略 (e)為防範電腦病毒擴散，影響電腦安全，公司應訂定電子郵件使用安全相關規定 (f)新增 (g)新增 (h)新增 f~h 略 i.新增	奉金融監督管理

(c)公司應依其所屬資安分級建立資通安全威脅偵測管理機制(應含括事件收集、異常分析、偵測攻擊並判斷攻擊行為) (112 年 1 月底生效) (d)公司應依其所屬資安分級建立入侵偵測及防禦機制。(112 年 1 月底生效) (e)公司應依其所屬資安分級設置應用程式防火牆。(112 年 1 月底生效) (f)公司應依其所屬資安分級辦理進階持續性威脅攻擊防禦措施。(112 年 1 月底生效) (2)電腦系統及作業安全管理（CC-17020，半年查核） a.略 b.電腦作業系統環境設定及使用權限設定： (a)~(b)略 (c)公司應建立系統最高權限帳號管理辦法(含作業系統及應用系統)，如需使用最高權限帳號時須取得權責主管同意，並留存相關紀錄。 (d)公司應建立並落實個人電腦、伺服器及網路通訊設備之安全性組態基準(如密碼長度、更新期限等)。 (e)公司透過網際網路使用管理帳號登入重要系統時，應採用多因子認證機制。 (以下略) 8.存取控制（CC-18000，每月查核） (1)~(2)略 (3)密碼管理 a.~c.略 d. 初始密碼應隨機產生，並與使用者身分無關。(本項不適用採自行訂定交付電子式交易密碼條之方式)	(c)新增 (d)新增 (e)新增	委員會證券期貨局 109 年 7 月 17 日證期(券)字第 1090345141 號函囑邀集證券商業同業公會及財團法人中華民國證券櫃檯買賣中心開會研議強化物聯網設備資安管理。 證交所 108 年

e.~g.略 h. 客戶申請採電子式交易型態者，公司得以一般或自訂電子方式交付電子密碼條，應依下列說明辦理： (a)採一般電子方式交付電子密碼條，應傳送 OTP（One Time Password）密碼至客戶開戶留存之手機號碼，及將加密後之電子密碼條以電子方式傳送至客戶留存之電子信箱，此流程相關系統紀錄應留存。 (b)採自訂交付電子密碼條方式，應訂定交付電子式交易密碼之作業程序及安全控管機制，並辦認電子式交易密碼交付對象為本人及留存相關紀錄。 (以下略) 9.系統開發及維護（CC-19000，半年查核） (1)~(8)略 (9) 公司應定期（至少每半年乙次）辦理資訊系統弱點掃描作業，針對所辨識出之潛在系統弱點，應評估其相關風險或安裝修補程式，並留存紀錄（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商）。 (以下略) 10.營運持續管理(CC-20000，半年查核) (4)、公司應擬訂營運持續計畫（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，並擬訂關鍵性業務及其衝擊影響分析，再依其所屬資安分級定期辦理業務持續運作演練。(111 年 1 月底生效) (以下略) 12.新興科技應用（CC-21100，年度查核）	(以下略) 8.存取控制（CC-18000，每月查核） (1)~(2)略 (3)密碼管理 a.~c.略 d. 初始密碼應隨機產生，並與使用者身分無關。 e.~g.略 h. 客戶申請採電子式交易型態者，公司以電子方式交付電子密碼條時，應傳送 OTP（One Time Password）密碼至客戶開戶留存之手機號碼，及將加密後之電子密碼條以電子方式傳送至客戶留存之電子信箱，此流程相關系統紀錄應留存。 (a)新增 (b)新增 (以下略) 9.系統開發及維護（CC-19000，半年查核） (1)~(8)略 (9) 公司應定期（至少每半年乙次）辦理資訊系統弱點掃描作業，針對所辨識出之潛在系統弱點，宜評估其相關風險或安裝修補程式，並留存紀錄（適用網際網路下單證券商，不適用語音下單及傳統下單之證券商）。	5 月 28 日臺證輔字第 1080008630 號函

(1)~(3)略 (4)物聯網： a.~d.(略) e.公司採購物聯網設備時，宜優先採購取得資安標章之物聯網設備。 f.公司應定期辦理物聯網設備使用及管理人員資安教育訓練。	(以下略) 10. 營運持續管理(CC-20000，半年查核) (4)、公司宜擬訂營運持續計畫（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，並擬訂關鍵性業務及其衝擊影響分析。 (以下略) 12.新興科技應用（CC-21100，年度查核） (1)~(3)略 (4)物聯網： a.(略) ~d.(略) e.新增 f.新增	