建立證券商資通安全檢查機制部分條文修正對照表(112 年)

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、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）	依據主管機關112 年 8 月 15 日金管證券字第11203447331 號函同意辦理，爰修訂左列條文。
(1)~(3)略	(1)~(3)略	
(4)應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)。	(4) 應評估核心系統可容忍中斷時間。	參考資訊作業韌性自律規範修訂
2~6、略	2~6、略	
7、通訊與作業管理（CC-17000）	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 項並適用於所有證券商，每月查核）	（1）網路安全管理（CC-17010，適用網際網路下單證券商，另 a、b、e 項並適用於所有證券商，每月查核）	
a. 網路系統安全評估：	a. 網路系統安全評估：	
(a)~(g)略	(a)~(g)略	
(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及身分認證，並留存	(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，並留存相關維護紀	

相關維護紀錄並由權責主管定期覆核。 (i)略 (j)應避免使用生命週期終止(End of Service, EOS/End of Life, EOL)之網路設備，並針對 EOS/EOL 之網路設備擬定汰除相關計畫。	錄並由權責主管定期覆核。 (i)略 (新增)	參考資通系統安全防護基準自律規範修訂 參考網路安全防護自律規範修訂
b.~~防火牆~~網路設備之安全管理： (a)~(g)略 (h)公司建立網路設備規則應以最小授權及正面表列為原則。 (i)公司應至少每年檢視一次對外網路設備規則，並留存相關紀錄。	b.防火牆之安全管理： (a)~(g)略 (新增) (新增)	同上
c 網路傳輸及連線安全管理： (a)~(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。	c 網路傳輸及連線安全管理： (a)~(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：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。	同上 參考新興科技資通安全自律規範修訂
d.多因子驗證： 公司使用多因子驗證應具下列三項之任兩項技術： (a)公司所約定之資訊，且無第三人知悉（如固定密碼、圖形鎖或手勢等）。	(新增) (新增)	參考新興科技資通安全自律規範

(b)客戶所持有之實體設備（如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等），公司應確認該設備為客戶與公司所約定持有之設備。	(新增)	修訂
(c)客戶提供給公司其所擁有之生物特徵（如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等），公司應直接或間接驗證該生物特徵。	(新增)	
e.身分~~CA~~認證與憑證管理	d.CA 認證與憑證管理：	項次調整
(a)~(b)略	(a)~(b)略	
(c)公司應於伺服器端驗證客戶交易身分及使用者帳號。	(新增)	同上
(d)公司對電子交易身分之申請、交付、使用、更新與驗證應訂定相關規範。	(新增)	同上
f.電腦病毒及惡意軟體之防範：	e.電腦病毒及惡意軟體之防範：	項次調整
略	略	
g.網路系統功能檢查：	f.網路系統功能檢查：	項次調整
略	略	
h.公司提供 API 服務規範：	g.公司提供 API 服務規範：	項次調整
略	略	
i.網際網路下單服務品質相關標準：	h.網際網路下單服務品質相關標準：	項次調整
略	略	

j.網路攻擊防護機制導入及安全性檢測~~（112 年 2 月 28 日生效）~~ (a)~(f)略 (g) 核心系統身分驗證機制應防範自動化程式之登入或密碼更換嘗試，非核心系統宜防範自動化程式之登入或密碼更換嘗試。	i.網路攻擊防護機制導入及安全性檢測（112 年 2 月 28 日生效） (a)~(f)略 (新增)	項次調整，移除生效日期 參考資通系統安全防護基準自律規範修訂
k.帳號登入或異常態樣通知~~（112 年 2 月 28 日生效）：~~略	j.帳號登入或異常態樣通知（112 年 2 月 28 日生效）：略	項次調整，移除生效日期
l.異常IP登入之監控與預警：~~（112 年 2 月 28 日生效）：~~略	k.異常 IP 登入之監控與預警：（112 年 2 月 28 日生效）：略	項次調整，移除生效日期
（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)~(e)略 (f) 資通系統內部時鐘應定期與基準時間源進行同步。	（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)~(e)略	
(g) 公司應依其所屬資安分級對核心系統重要組態設定檔案及其他具保護需求之資訊進行加密或以其他適當方式儲存。	(新增)	參考資通系統安全防護基準自律
(h) 公司應依其所屬資安分級訂定對核心系統之閒置	(新增)	

時間或可使用期限與核心系統之使用情況及條件(如：帳號類型與功能限制、操作時段限制、來源位址限制、連線數量及可存取資源等)。	(新增)	規範修訂 同上
c. 電腦媒體之安全管理： (a)~(e)略 (f) 公司應依據系統特性與資料復原點目標（RPO），考量備份頻率、儲存媒體類型（光碟、外接硬碟、磁帶）、資料類型（虛擬機映像檔、系統源碼、資料庫與組態設定檔等）、備份類型（完整備份、增量備份與差異備份）、備份方式（網路同步寫入、網路非同步寫入與離線備份）等，制定適當之資料備份機制，如採離線備份應依備份類型建立適當的備份基準(baseline)，以確保資料可正確回存。 (g)公司制定資料備份機制時，宜考量「3-2-1 備份原則」，至少製作三份備份；將備份分別存放在兩套獨立不同儲存設備；至少一份放在異地保存。	c.電腦媒體之安全管理： (a)~(e)略 (新增)	同上 參考資訊作業韌性參考指引修訂
d~f 略	(新增)	
8.存取控制 (1)略		參考資訊作業韌性自律規範修訂

(2)權限管理 a~e 略 f. 應定期（至少每半年一次）審查~~並檢討久未使用之使用者權限~~資通系統帳號及權限之適切性，並視審查結果停用資通系統閒置帳號。（~~使用者為~~客戶帳號~~者~~除外）。 g. 公司應建立資通系統帳號管理機制，包含帳號之申請、建立、修改、啟用、停用及刪除之程序。 h. 資通系統帳號應定義人員角色及責任，授權應採最小權限原則，僅允許使用者(或代表使用者行為之程序)依公司部門權責及業務功能，完成作業所需之授權存取。 (3)略 (4) 電腦稽核紀錄管理： a~c 略 d.核心系統電腦稽核紀錄(日誌)應建立監控機制，處理失效時，應採取適當之行動。 (5) 資料輸入管理： a~g(略) h.公司應依「個人資料保護法」妥善處理公司保有之個	d~f 略 8.存取控制 (1)略 (2)權限管理 a~e 略 f. 應定期（至少每半年一次）審查並檢討久未使用之使用者權限（使用者為客戶者除外）。 (新增) (新增) (3)略 (4) 電腦稽核紀錄管理： a~c 略 (新增)	 參考資通系統安全防護基準自律規範修訂 同上 同上

人資料，並定期或不定期稽核依「個人資料保護法」定義之個人資料管理情形。 i.~j.略 k.應留存個人資料使用稽核軌跡（如登入帳號、系統功能、時間、系統名稱、查詢指令或結果）或辨識機制，以利個人資料外洩時得以追蹤個人資料使用狀況。	(5) 資料輸入管理： a~g(略) h.公司應定期或不定期稽核依「個人資料保護法」定義之個人資料管理情形。 i.~j.略	同上 同上
9. 系統開發及維護（CC-19000，半年查核） (1)~(3)略 (4)委外~~作業應簽訂契約，委外作業契約內容應包含資訊安全協定與對委外廠商資安稽核權等條款。~~廠商管理： a. 公司與委外資訊服務供應商提供服務應訂定合約，合約所含內容應包含以下內容：合約期限、服務範圍、服務交付日期、服務水準要求、服務變更規範、服務驗收之標準、資通安全事件通報及應變處理作業程序、對資訊服務供應商之稽核權條款、合約轉讓或同意分包之規範、保密義務條款、罰則與損害賠償條款、爭議處理程序、違約處理條款、合約終止規範、合約終止後之處理、保固、權利及責任。 b. 證券商應評估資訊服務供應商之集中度，包括評估資訊服務供應商作業能力，採取適當風險管控措	(新增) 9. 系統開發及維護（CC-19000，半年查核） (1)~(3)略 （4）委外作業應簽訂契約，委外作業契約內容應包含資訊安全協定與對委外廠商資安稽核權等條款。 (新增) (新增)	同上 參考供應鏈風險管理自律規範修訂 同上

施，確保作業委外處理之品質，並注意作業委託資訊服務供應商之適度分散以控管作業風險。		
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程式碼掃描或黑箱測試。	(新增)	
d. 公司應訂定相關規範管控，與資訊服務供應商資訊委外關係於終止、解除或結束後之相關作業。		同上
e. 委外資訊服務供應商應揭露第三方程式元件之來源與授權證明。	(新增)	
f. 公司應管控資訊服務供應商存取權限，對於電腦通行使用權利進行適當控管。		同上
g. 公司應對資訊服務供應商服務內容變更進行風險評估。	(新增)	
h. 公司對於委外資訊服務供應商於委外關係所涉及公司資訊資產，應於委外關係終止、解除或結束時完整歸還、確保銷毀或轉交予其他資訊服務供應商，並要求資訊服務供應商持續遵守保密承諾。	(新增)	同上
i. 委外資訊服務供應商如自行發現程式漏洞、版本老舊，或於使用相同服務之其他證券商應用系統發生	(新增)	同上

故障或異常時，應儘速瞭解原因，並主動轉知及提供因應措施。	(新增)	同上
j. 委外資訊系統之服務規格書應包括硬體規格、軟體版本、作業環境變動、作業系統底層架構及系統程式相容性等，並包含維持委外廠商服務水準之要求與橫向溝通機制。	(新增)	同上
	(新增)	同上
(5)~(10)略		強化委外廠商管理
(11) 行動應用程式安全管理（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）： a~b 略 c. 行動應用程式檢測： (a)涉及投資人使用之行動應用程式於初次上架前及每年應委由經財團法人全國認證基金會（ TAF）認證合格之第三方檢測實驗室進行並完成通過資安檢測，檢測範圍以目的事業主管機關~~經濟部工業局~~委託執行單位「行動應用資安聯盟」公布之行動應用程式基本資安檢測基準項目進行檢測。如通過實驗室檢測後一年內有更新上架之需要，應於每次上架前就重大更新項	(新增)	強化委外廠商管理
	(5)~(10)略 (11) 行動應用程式安全管理（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）： a~b 略	

目進行委外或自行檢測；所謂重大更新項目為與「下單交易」、「帳務查詢」、「身份辨識」及「客戶權益有重大相關項目」有關之功能異動。檢測範圍以 OWASP MOBILE TOP10 之標準為依據，並留存相關檢測紀錄。 (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)提供網際網路下單服務之核心系統上架前及系統更新時應執行「源碼掃描」安全檢測。 10. 營運持續管理（CC-20000，半年查核） (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，評估核心系統中斷造成之衝擊程度，並依核心系統之復原時間目標(RTO)、資料復原點目標(RPO)，作為恢復核心系統、備份備援規劃及執行復原作業之依據，再	c. 行動應用程式檢測： (a)涉及投資人使用之行動應用程式於初次上架前及每年應委由經財團法人全國認證基金會（ TAF）認證合格之第三方檢測實驗室進行並完成通過資安檢測，檢測範圍以經濟部工業局委託執行單位「行動應用資安聯盟」公布之行動應用程式基本資安檢測基準項目進行檢測。如通過實驗室檢測後一年內有更新上架之需要，應於每次上架前就重大更新項目進行委外或自行檢測；所謂重大更新項目為與「下單交易」、「帳務查詢」、「身份辨識」及「客戶權益有重大相關項目」有關之功能異動。檢測範圍以 OWASP MOBILE TOP10 之標準為依據，並留存相關檢測紀錄。 (新增) (新增) 10. 營運持續管理（CC-20000，半年查核） (1)~(2)(略)	配合機關名稱調整 參考資通系統安全防護基準自律規範 同上

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）~~	(3) 證券經紀商之交易主機應有備援措施。	
(5) 公司應訂定資訊安全訊息通報機制（例如：正式之通報程序及資安事件通報聯絡人），針對與資訊系統有關之資訊安全或服務異常事件應依「證券期貨市場資通安全事件通報應變作業注意事項」及「證券商通報重大資安事件之範圍申報程序及其他應遵循事項」辦理，並採取適當矯正程序，留存紀錄。	(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）	參考資訊作業韌性自律規範修訂
(6)~(8)略		同上
(9)公司應辨識風險情境，就各項風險情境當災害發生造成資訊作業異常或中斷時，擬定各系統之應變、減災或復原措施 相關作業流程。 (10)核心系統原服務中斷時，應於可容忍時間內，由備援設備或其他方式取代並提供服務。	(5) 公司應訂定資訊安全訊息通報機制（例如：正式之通報程序及資安事件通報聯絡人），針對與資訊系統有關之資訊安全或服務異常事件應依「證券期貨市場資通安全事件通報應變作業注意事項」辦理，並採取適當矯正程序，留存紀錄。	依據臺證輔字第 1120503153 號函增訂重大資安事件申報
11.略		
12、新興科技應用（CC-21100，年度查核）		
(1) 雲端服務： 應事先評估使用雲端運算服務之風險，若雲端運算服務涉及關鍵性系統、資料或服務者，應訂定雲端運算服務相關運作安全規範。	(6)~(8)略 (新增)	參考資訊作業韌

a. 公司為雲端服務使用者時，應訂定雲端~~運算服務運作安全規範內含雲端~~服務提供者之遴選機制、查核措施、備援機制、服務水準（含資訊安全防護）、~~與~~復原時間及服務終止措施要求等，如有不符需求之處，需有其它補償性措施。 b. 略 (2) 社群媒體： c. 公司應訂定經營官方社群媒體資訊安全規範與管理辦法，並包含以下內容： (a)~(b)略 (c) 對經營之社群媒體應標示證券商名稱、聯絡方式、許可證字號、客戶申訴聯繫方式及處理窗口，以區別為官方經營之社群媒體。 (3)略 (4)物聯網 a~f 略 g.應建立物聯網設備存取權限控管措施。 (5)略 (6) 深度偽造(Deepfake) a.使用影像視訊方式進行身分驗證時應強化驗證並搭配其他驗證因子(如上傳身分證件、手機簡訊OTP)。	(新增) 11.略 12、新興科技應用（CC-21100，年度查核） （1） 雲端服務： a. 公司為雲端服務使用者時，應訂定雲端運算服務運作安全規範內含雲端提供者之遴選機制、查核措施、備援機制、服務水準（含資訊安全防護）與復原時間要求等，如有不符需求之處，需有其它補償性措施。 b. 略 (2) 社群媒體： c. 公司應訂定經營官方社群媒體資訊安全規範與管理辦法，並包含以下內容： (a)~(b)略 (c) 對經營之社群媒體應標示證券商名稱、聯絡方式，以區別為官方經營之社群媒體。	性自律規範修訂 參考資通系統安全防護基準自律規範 參考新興科技資通安全自律規範修訂 同上

b.應定期辦理涵蓋深度偽造認知及防範議題之資訊安全教育訓練。 (以下略)	(3)略 (4)物聯網 a~f 略 (新增) (5)略 (新增) (以下略)	 同上 同上 同上 同上 同上