建立證券商資通安全檢查機制部分條文修正對照表 (114 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）~（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），並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。~~ 2.資訊安全政策（CC-12000，年度查核） （1）~（2）略 （3）公司所訂定之資訊安全政策，應經管理階層核准，並應正式發布要求所有員工共同遵守，並轉知與公司~~連線作業~~合作之公私機關（構）、提供資訊服務之廠商共同遵行。 （4）~（8）略 3.安全組織（CC-13000，年度查核） （1）~（2）略	2.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、復原時間目標（RTO）、資料復原點目標（RPO），並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。 2.資訊安全政策（CC-12000，年度查核） （1）~（2）略 （3）公司所訂定之資訊安全政策，應經管理階層核准，並應正式發布要求所有員工共同遵守，並轉知與公司連線作業之公私機關（構）、提供資訊服務之廠商共同遵行。 （4）~（8）略 3.安全組織（CC-13000，年度查核） （1）~（2）略	調整適用範圍為全體證券商。 調整可容忍中斷時間規定至營運持續管理章節。 調整範圍不限於連線之公私機關(構)。

（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，且資訊安全人員及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~~通系統之從業人員，每年應至少接受三小時以上資訊安全宣導課程。	（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，且資訊安全人員及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。	調整用字一致性。
（4）~（6）略	（4）~（6）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）資訊資產應列有清冊且包含軟體、硬體、場地及資料等類別，~~清冊~~並應加以維護。	（1）資訊資產應列有清冊，清冊並應加以維護。	增加盤點類別之要求。
（2）略	（2）略	
（3）公司應對自行或委外開發之資~~訊~~通系統完成資~~訊~~通系統分級，資~~訊~~通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~~通系統分級妥適性。~~（111 年 1 月底生效）~~	（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）	調整用字一致性，並移除生效日。
（4）略	（4）略	
（5）公司應避免使用危害國家資通安全產品。	(新增)	增訂資通安全產品管理條款，說明不可使用危害國家資通安全軟硬
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）~（5）略	（1）~（5）略	

		體之要求。
（6）公司應定期審查~~資訊~~電腦機房門禁管制權限。	（6）公司應定期審查資訊機房門禁管制權限。	調整用字一致性。
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、m 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、f 項並適用於所有證券商，每月查核）	新增無線網路管理適用全體證券商。
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多因子身分認證，並留存相關維護紀錄並由權責主管定期覆核。	(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，並留存相關維護紀錄並由權責主管定期覆核。	調整遠端連線須使用多因子之身分認證機制。
(i)略	(i)略	
(j)應避免使用生命週期終止（End of Service, EOS／End of Life, EOL）之軟體及網路設備，且於到期前擬定汰除計畫，並視情況建立補償性措施~~並針對 EOS／EOL 之網路設備擬定汰除相關計畫~~。	(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。	調整範圍須包含軟體，並說明應有配套措施。
b.網路設備之安全管理：	b.網路設備之安全管理：	
(a)~(e)略	(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，每半年檢視 DMZ 區之防火牆規則，包含評估高風險設定及六個月內無流量之防火牆之必要性，及針對已下線資通系統於六個月內調整或停用該規則，並留存相關檢視紀錄。	(f)公司應每年定期檢視並維護防火牆存取控管設定，每半年檢視 DMZ 區之防火牆規則，並留存相關檢視紀錄。	參酌「金融機構資通安全防護基準」第十三條第三項，增訂防火牆應檢視之項目。
~~(g)公司交易相關網路直接連線之設備應避免使用危害國家資通安全產品。~~	(g)公司交易相關網路直接連線之設備應避免使用危害國家資通安全產品。	整併至資產分類與控制章節。
(g)公司建立網路設備規則應以最小授權及正面表列為原則。	(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。	條號調整。
(h)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。	(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。	條號調整。
c.網路傳輸及連線安全管理：	c.網路傳輸及連線安全管理：	
(a)~(c)略	(a)~(c)略	
(d)公司加密機制應優先考慮使用公開、國際機構驗證且未遭破解之演算法。	(新增)	增訂加密安全性之要求，說明加密機制需符合現行國際標準。
d.~e.(略)	d.~e.(略)	
f.電腦病毒及惡意軟體之防範：	f.電腦病毒及惡意軟體之防範：	
(a)略	(a)略	

(b)應定期對~~電腦~~資通系統及資料儲存媒體進行病毒掃~~瞄~~描（含電子郵件）。 (c)~(e)略 (f)公司應建立軟體白名單控管機制~~上網管制措施，以避免下載惡意程式~~。 (g)略	(b)應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）。 (c)~(e)略 (f)公司應建立上網管制措施，以避免下載惡意程式。 (g)略	調整用字一致性。 修訂軟體控管方式，說明須建立白名單以進行存取管理。
(h)公司~~宜~~應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。 g.~i. (略) j. 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	(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。 g.~i. (略) j. 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	調整規範強度，說明社交工程演練須每年定期辦理。 刪除生效日 刪除生效日

伺服器設定及防火牆連線設定檢視）。~~（112 年 1 月底生效）~~	伺服器設定及防火牆連線設定檢視）。（112 年 1 月底生效）	
(c)~(e)略	(c)~(e)略	
(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）~~	(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）	刪除生效日
(g)略	(g)略	
k.~l.(略)	k.~l.(略)	
m. 無線網路管理：	(新增)	參酌證券商公會「網路安全防護自律規範」第三條第三項無線網路管理增訂此構面。
(a)公司設置無線網路應採用現行公開資訊已認可且無弱點之安全協定。	(新增)	
(b)公司提供內部無線網路使用應限內部人員公務用或資訊服務供應商申請核准後使用。	(新增)	
（2）電腦系統及作業安全管理（CC－17020，半年查核）略	（2）電腦系統及作業安全管理（CC－17020，半年查核）略	
8.存取控制（CC-18000，每月查核）	8.存取控制（CC-18000，每月查核）	
（1）公司應訂定資~~訊~~通系統存取控制相關規定，並以書面、電子或其他方式告知員工遵守。	（1）公司應訂定資訊系統存取控制相關規定，並以書面、電子或其他方式告知員工遵守。	調整用字一致性。
（2）略	（2）略	
（3）密碼管理：	（3）密碼管理：	
a.~e. (略)	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。~~（111年11月30日生效）~~ g.~h. (略) （4）~（6）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： a.(略) b. 證券商應針對資訊委外業務項目之資通安全風險與委外作業可行性，及資訊服務供應商作業能力及集中度，由相關資訊單位共同執行風險評估，評估結果應提報適當管理層級並取得同意。~~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。~~	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。（111年11月30日生效） g.~h. (略) （4）~（6）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： a.(略) 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。	刪除生效日 參酌「證券商資通系統與服務供應鏈風險管理自律規範」第三條第一項供應商遴選原則修訂。

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~~源碼掃描或黑箱測試。	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。	調整用字一致性。
d.~i.(略)	d.~i.(略)	
j. 委外資~~訊~~通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。	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。	調整用字一致性。
k. 公司應載明資訊服務供應商配合進行壓力測試及調整服務負載量之義務，並於市場交易量、業務變化及客戶屬性等發生顯著異動時發動辦理，俾憑評估系統資源調配或擴增。	(新增)	增訂委外服務壓力測試之要求，說明資訊服務供應商應配合組織因應內外在環境變化執行壓力測試。

l. 公司於資訊服務委外期間應定期對資訊服務供應商進行稽核，並應要求資訊服務供應商定期提交服務水準報告，相關結果應提報適當管理層級審查。 （5）~（7）略	(新增) （5）~（7）略	參酌「證券商資通系統與服務供應鏈風險管理自律規範」第七條第一項及第二項審核資訊服務供應商服務修訂。
（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。	（8）應用系統異動管理： a.~b.(略) (新增)	增訂程式變更正確性管理之條款，說明程式上線後應確認變更正確性。
（9）公司應定期（至少每半年乙次）辦理資~~訊~~通系統弱點掃描作業，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	（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	調整用字一致性。

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）。	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）。	
（10）程式~~原始~~源碼安全規範（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）：	（10）程式原始碼安全規範（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）：	調整用字一致性。
a.~e.(略)	a.~e.(略)	
f. 公司應依上開安全事項檢驗程式~~原始~~源碼並符合安全事項之要求；無法取得程式~~原始~~源碼時，應要求程式提供者符合上開前五項安全事項（a、b、c、d、e） 之佐證。	f. 公司應依上開安全事項檢驗程式原始碼並符合安全事項之要求；無法取得程式原始碼時，應要求程式提供者符合上開前五項安全事項（a、b、c、d、e） 之佐證。	調整用字一致性。
（11）~（14）略	（11）~（14）略	
10.營運持續管理（CC-20000，半年查核）	10.營運持續管理（CC-20000，半年查核）	
（1）~（3）略	（1）~（3）略	
（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，~~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~~	（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，再依其所屬資安分級定	整併可容忍中斷時間規定至營運持續管理章節。

~~復核心系統、備份備援規劃及執行復原作業之依據，再~~依其所屬資安分級定期辦理業務持續運作演練~~。公司應~~，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，訂定核心系統可容忍中斷時間。	期辦理業務持續運作演練。公司應視演練範圍是否涉及第三方，邀請相關廠商參與演練。	
（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~~通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。	（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。	調整用字一致性。
（6）~（11）略	（6）~（11）略	
11.(略)	11.(略)	
12.新興科技應用（CC-21100，年度查核）	12.新興科技應用（CC-21100，年度查核）	
（1）~（4）略	（1）~（4）略	
（5）遠距辦公：	（5）遠距辦公：	
a. (略)	a. (略)	

b. 公司應依業務範圍及控管權限設定~~居家~~遠距辦公員工之系統功能權限，且妥善設定遠距辦公軟體(如禁止連接至本機印表機、跨端剪貼資料等)。	b. 公司應依業務範圍及控管權限設定居家辦公員工之系統功能權限。	參酌「金融機構資通安全防護基準」第十二條第四項，增訂遠距設備使用管理要求。
c. 公司應依員工執行業務內容訂定連線時段限制及相關規範，並設定閒置時間螢幕鎖定或中斷連線機制。	c.公司應依員工執行業務內容訂定連線時段限制及相關規範。	同上。
d.~i.(略)	d.~i.(略)	
（6）~（7）略	（6）~（7）略	
（7）人工智慧(AI)：	(新增)	參酌「證券商運用人工智慧技術自律規範」增訂人工智慧使用條款。
a. 使用人工智慧技術應列有清冊並加以維護，且應遵循資通安全、個人資料保護、智慧財產權等金融法規及其他法律規範與相關資訊使用規定。	(新增)	
b. 使用人工智慧技術與客戶直接互動時，應告知該互動或服務係利用人工智慧技術自動完成，或揭露其適用人群、場景或用途。	(新增)	同上。
13.(略)	13.(略)	

14.主機共置（Co_Location ）服務管理（CC-23000，適用使用主機共置服務之證券商，月或半年查核） （1）略 （2）配合定期盤點主機共置機房之資訊資產，且應包含軟體、硬體、場地及資料等類別~~機櫃內主機與網路設備~~（半年查核）。 (以下略)	14.主機共置（Co_Location ）服務管理（CC-23000，適用使用主機共置服務之證券商，月或半年查核） （1）略 （2）配合定期盤點主機共置機房機櫃內主機與網路設備（半年查核）。 (以下略)	增加盤點類別之要求。