證券商內部控制制度標準規範—內部控制制度修訂對照表（111 年）

編號	作業項目	修 訂 後 內 容	修 訂 前 內 容	修訂說明
CC-12000	資訊安全政策	(一)~(七)略 (八)、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 112 年 1 月底通過驗證(1~2 級證券商)112 年 12 月底通過驗證(第 3 級證券商))	(一)~(七)略 (八)、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 112 年 1 月底通過驗證)	依據金融監督管理委員會 111 年 3 月 8 日發布之「證券期貨業永續發展轉型執行策略」架構一/策略 2/具體措施 6、7 等事項辦理。

CC-13000	安全組織	(一)、公司應依規定配置適當人力資源及設備負責資訊安全制度之規劃、監控及執行資訊安全管理作業，所稱配置適當人力資源之規定如下： 1. 實收資本額達新臺幣二百億元以上之公司，應設置資訊安全專責單位，該單位應配置專責主管及至少三名專責人員，專門負責資訊安全相關工作或職務，不得兼辦資訊或其他與職務有利益衝突之業務。 2. 實收資本額達一百億元以上，未達二百億元者，應配置資訊安全主管及至少三名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務；如已設置資訊安全專責單位者，得配置專責主管及二名專責人員，且專門負責資訊安全相關工作或職務，不得兼辦資訊或其他與職務有利益衝突之業務。 3. 實收資本額達四十億元以上，未達一百億元者，應配置資訊安全主管及至少二名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。	(一)、公司應配置適當人力資源及設備負責資訊安全制度之規劃、監控及執行資訊安全管理作業，所稱配置適當人力資源之規定如下： 1. 實收資本額達新臺幣二百億元以上之公司，應設置資訊安全專責單位，該單位應配置專責主管及至少二名專責人員，專門負責資訊安全相關工作或職務，不得兼辦資訊或其他與職務有利益衝突之業務。 2. 實收資本額達一百億元以上，未達二百億元者，應配置資訊安全主管及至少二名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務 。 3. 實收資本額達四十億元以上，未達一百億元者，應配置資訊安全主管及至少一名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。	依據金融監督管理委員會111年11月3日金管證券字第11103845963號令辦理，調整資安人力配置。

		4. 實收資本額未達四十億元者，應配置至少一名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。 5. 外國金融機構、證券商及信用評等事業依證券商設置標準，在國內設立分支機構經營或兼營證券者，將實收資本額改按指撥營運資金計算。 (二)略 (三)、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。 (四)~(六)、略 (七)、公司應依其所屬資安分級要求資安人員取得並維持相當資通安全專業證照。	4. 實收資本額未達四十億元者，應配置至少一名資訊安全人員，除兼辦資訊職務外，不得兼辦其他與職務有利益衝突之業務。 5. 外國金融機構、證券商及信用評等事業依證券商設置標準，在國內設立分支機構經營或兼營證券者，將實收資本額改按指撥營運資金計算。 (二)略 (三)、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。 (四)~(六)、略 (七)、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。	依據金融監督管理委員會111年11月3日金管證券字第11103845963號令辦理，調整資安人力配置。 依據金融監督管理委員會111年3月8

		(以下略)	(以下略)	日發布之「證券期貨業永續發展轉型執行策略」架構一/策略 2/具體措施 6、7 等事項辦理。

CC-17010	網路安全管理	作業程序及控制重點： (一)~(五)略 (六)、網路系統功能檢查： 1、 略。 2、 公司應就提供外部連線使用網路系統偵測網頁與程式異動、記錄並通知相關人員處理。（112年6月底生效）。 (七)~(八)略 (九)、網路攻擊防護機制導入及安全性檢測 1~2略 3、 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)	作業程序及控制重點： (一)~(五)略 (六)、網路~~干單~~系統功能檢查： 1、 略。 2、 應就網路~~干單~~系統偵測網頁與程式異動、記錄並通知相關人員處理~~（註：本項目自107年8月1日起實施）~~。 (七)~(八)略 (九)、網路攻擊防護機制導入及安全性檢測 1~2略 3、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)~~	依據金融監督管理委員會證券期貨局111年10月4日證期(券)字第11103841521號函辦理，強化外部連線系統監控。 依據金融監督管理委員會證券期貨局111年10月3日證期(券)字第1110350967號函。

		4、公司應依其所屬資安分級建立入侵偵測及防禦機制。 5、公司應依其所屬資安分級設置應用程式防火牆。 6、(略) (十)略 (十一)異常 IP 登入之監控與預警： 公司應對異常及不明來源 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. 發現異常來源 (如金融資安資訊分享與分析中心 F-ISAC 公布之黑名單或國	4、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)~~ 5、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)~~ 6、(略) (十)略 (十一)異常 IP 登入之監控與預警： 公司應~~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. 發現異常來源 (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。 (111 年 12 月底生效) (以下略)	外 IP)嘗試登入。 (111 年 ~~9 月 30 日~~生效) (以下略)	

CC-17020	電腦系統及作業安全管理	作業程序及控制重點： (一)略 (二)、電腦作業系統環境設定及使用權限設定： 1.~6.(略) 7.公司透過網際網路使用帳號登入系統時，應採用多因子認證機制。(112年6月底生效) (以下略)	作業程序及控制重點： (一)略 (二)、電腦作業系統環境設定及使用權限設定： 1.~6.(略) 7.公司透過網際網路使用管理~~重要~~帳號登入系統時，應採用多因子認證機制。 (以下略)	依據主管機關111年10月4日證期(券)字第11103841521號函辦理，強化外部連線系統監控。