建立證券商資通安全檢查機制部分條文修正對照表（111 年)

修正條文	現行條文	說明
1. (略)	1. (略)	
2. 資安政策(CC-12000，年度查核)	2. 資安政策(CC-12000，年度查核)	
(1)~(7)略	(1)~(7)略	
(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。	(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）~~	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」辦理
3、安全組織（CC-13000，年度查核）	3、安全組織（CC-13000，年度查核）	
(1)~(2)略	(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。	(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。	依據金融監督管理委員會 111 年 11 月 3 日金管證券字第 1110384596 號令辦理
(4)~(5)略	(4)~(5)略	
(6)公司應依其所屬資安分級要求資訊安全人員取得並維持相當資通安全專業證照。	(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）~~	

4.~6.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、e 項並適用於所有證券商，每月查核）a.~e.略 f. 網路系統功能檢查： (a)略 (b)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。 g. ~h.(略) i.網路攻擊防護機制導入及安全性檢測 (a).~(b).略 (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） (d). 公司應依其所屬資安分級建立入侵偵測及防禦機制。 (e). 公司應依其所屬資安分級設置應用程式防火牆。 (f).略 k.異常 IP 登入之監控與預警：	4.~6.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、e 項並適用於所有證券商，每月查核）a.~e.略 f. 網路~~下單~~系統功能檢查： (a)略 (b)應就網路~~下單~~系統偵測網頁與程式異動、記錄並通知相關人員處理。 g.~h.(略) i.網路攻擊防護機制導入及安全性檢測 (a).~(b).略 (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).略 k.異常 IP 登入之監控與預警~~（111 年 9 月 30 日生效）~~： 公司應~~依其所屬資安分級~~對異常及不明來源 IP 連線進行	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，為提升證券商提供外部連線使用系統之資訊安全。 依據金融監督管理委員會證

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： (a)同一來源 IP 登入不同帳號達一定次數以上。 (b)同一帳號在一定時間內由不同國家登入。 (c)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。 (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)~(d)略 (e) 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。 (以下略)	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： (a)同一來源 IP 登入不同帳號達一定次數以上。 (b)同一帳號在一定時間內由不同國家登入。 (c)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。 (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)~(d)略 (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)	券期貨局 111 年 10 月 3 日證期（券）字第 1110350967 號函辦理，為強化資安防護研議網路資安防禦設備擴大適用至第四級證券商之可行性。 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，為提升證券商提供外部連線使用系統之資訊安全。