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.略 2.略 3.略 4.資產分類與控制（CC-14000，半年查核） （1）~（4）略 （5）公司交易相關網路直接連線之設備不得~~應避免~~使用危害國家資通安全產品。 （6）略 5.略 6.略 7.略 8.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~d 略 e. 公司與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。	1.略 2.略 3.略 4.資產分類與控制（CC-14000，半年查核） （1）~（4）略 （5）公司應避免使用危害國家資通安全產品。 （6）略 5.略 6.略 7.略 8.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~d 略 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。	參酌資通安全管理法第十一條及第二十七條，調整為不得使用危害國家資通安全產品，範圍為交易相關網路直接連線之設備。

f~l 略 （5）~（9）略 （10） 應用系統異動管理：程式源碼安全規範(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)： a~c 略 d. 程式應針對使用者輸入之資料，於應用系統伺服器端~~字串，~~進行安全檢查並提供相關注入攻擊防護機制。 e~f 略 （11）~（14）略 10.營運持續管理（CC-20000，半年查核） （1）~（3）略 （4）公司應依所屬資安分級建置異地備援機房，並依營運衝擊分析結果於異地備援機房建置對營運具重大影響之核心系統，以維持營運持續運作能力，且應每年定期或於市場交易發生顯著變化時，檢視異地備援系統清單之完整性。 (註：異地備援機房建置範圍由交易主機擴大至對營運具重大影響之核心系統，自 116 年 12 月底生效。) (以下略)	f~l 略 （5）~（9）略 （10） 應用系統異動管理：程式源碼安全規範(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)： a~c 略 d. 程式應針對使用者輸入之字串，進行安全檢查並提供相關注入攻擊防護機制。 e~f 略 （11）~（14）略 10.營運持續管理（CC-20000，半年查核） （1）~（3）略 （4）公司應依所屬資安分級建置異地備援機房，並依營運衝擊分析結果於異地備援機房建置對營運具重大影響之核心系統，以維持營運持續運作能力。 (註：異地備援機房建置範圍由交易主機擴大至對營運具重大影響之核心系統，自 116 年 12 月底生效。) (以下略)	增加使用第三方程式元件之識別範圍。 參酌資通安全責任等級分級辦法附表十、資通系統防護基準修正內容，新增使用者輸入資料合法性檢查應置放於應用系統伺服器端。 增訂檢視異地備援系統清單之頻率。