證券商內部控制制度標準規範—內部控制制度修正對照表

編號	作業項目	修正後內容	修正前內容	修正說明
CC-20000	營運持續管理	作業程序及控制重點： (一)研擬備援及回復計畫，其內容至少包含下列項目之說明： 1.資料庫、檔案及程式之備援回復。 2.電腦作業系統備援及回復。 3.電腦設備備援及設備故障回復。 4.通訊設備及線路之備援及回復。 5.電力系統備援及回復。 (二)與業務單位人員研討於重大異常狀況發生時，根據下列時間點(１、開盤前機器無法啟動。２、盤中交易期間機器停頓。３、收盤後資料未核對完成前系統發生異常情形。４、所有交割或清算之作業未完成時系統發生異常。５、每日日結作業時系統發生異常。)考慮當時系統發生的作業需求型態、影響的業務層面及相關人員應採的應變措施，訂定人工配合之備援計畫，以及需包含電腦系統等故障復原標準作業程序，並落實執行且留存紀錄。 (三)核定之備援及回復計畫由下列人員執行： 1.非人工備援作業由資訊單位人員為之。 2.人工備援作業由使用該應用系統之業務單位人員為之。 (四)重大異常狀況發生時，資訊單位人員應立即檢視電腦系統無法正常運作原因，判定災害等級，影響業務範圍，估計回覆作業	作業程序及控制重點： (一)研擬備援及回復計畫，其內容至少包含下列項目之說明： 1.資料庫、檔案及程式之備援回復。 2.電腦作業系統備援及回復。 3.電腦設備備援及設備故障回復。 4.通訊設備及線路之備援及回復。 5.電力系統備援及回復。 (二)與業務單位人員研討於重大異常狀況發生時，根據下列時間點(１、開盤前機器無法啟動。２、盤中交易期間機器停頓。３、收盤後資料未核對完成前系統發生異常情形。４、所有交割或清算之作業未完成時系統發生異常。５、每日日結作業時系統發生異常。)考慮當時系統發生的作業需求型態、影響的業務層面及相關人員應採的應變措施，訂定人工配合之備援計畫，以及需包含電腦系統等故障復原標準作業程序，並落實執行且留存紀錄。 (三)核定之備援及回復計畫由下列人員執行： 1.非人工備援作業由資訊單位人員為之。 2.人工備援作業由使用該應用系統之業務單位人員為之。 (四)重大異常狀況發生時，資訊單位人員應立即檢視電腦系統無法正常運作原因，判定災害等級，影響業務範圍，估計回覆作業	1. 原條文(八)前移至(七)，增訂辦理頻率每年至少一次，並調整用字一致性； 2.原條文(七)後移至(八)，為維持營運韌性，擴大異地備援機房建置範圍至對營運具重大影響之前端交易系統、中台等核心系統； 3.增訂週期性演練規定

編號	作業項目	修正後內容	修正前內容	修正說明
		時間，衡量當時作業狀況，通知相關人員根據備援及回復計畫所應採取之配合措施。 (五)不管是電腦系統或是電力、空調、消防系統發生異常，事後相關人員應確實檢討原因，並謀求改進與對應預防措施。 (六)所訂定之重大異常狀況系統復原計劃應定期模擬演練，以使相關人員熟悉重大異常狀況發生時，系統之應變措施及復原程序。 (七)公司應每年至少執行一次營運衝擊分析，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，依其所屬資安分級定期辦理業務持續運作演練，且視演練範圍是否涉及第三方，邀請相關廠商參與演練。網際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。 (八) 公司（證券經紀商）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	時間，衡量當時作業狀況，通知相關人員根據備援及回復計畫所應採取之配合措施。 (五)不管是電腦系統或是電力、空調、消防系統發生異常，事後相關人員應確實檢討原因，並謀求改進與對應預防措施。 (六)所訂定之重大異常狀況系統復原計劃應定期模擬演練，以使相關人員熟悉重大異常狀況發生時，系統之應變措施及復原程序。 (七)公司（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。 (八)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、	

編號	作業項目	修正後內容	修正前內容	修正說明
		大至對營運具重大影響之核心系統，自 116 年 12 月底生效。)	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，依其所屬資安分級定期辦理業務持續運作演練，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。	
		(九)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），及針對與資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。	(九)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），及針對與資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。	
		(十)公司發生個人資料之竊取、竄改、毀損、滅失、或洩漏等資安事故者，應即函報證交所(或櫃檯買賣中心、券商公會)轉陳主管機關。	(十)公司發生個人資料之竊取、竄改、毀損、滅失、或洩漏等資安事故者，應即函報證交所(或櫃檯買賣中心、券商公會)轉陳主管機關。	
		(十一)公司應明確訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序，並每年進行演練。	(十一)公司應明確訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序。	
		(十二)故障復原程序應定期測試，測試後應召開檢討會議，針對測試缺失謀求改進，並留存紀錄。	(十二)故障復原程序應定期測試，測試後應召開檢討會議，針對測試缺失謀求改進，並留存紀錄。	
		(十三)公司應辦理下列資安防護事宜： 1.指定人員及部門統籌並協調聯繫各有關	(十三)公司應辦理下列資安防護事宜： 1.指定人員及部門統籌並協調聯繫各有關	

編號	作業項目	修正後內容	修正前內容	修正說明
		部門。 2.定期評估核心營運系統及設備,對評估結果採取適當措施，並提報董事會，以確保營運持續及作業韌性之能力。 3.於永續報告書、年報、財務報告或公司網站，揭露年度內公司持續核心營運系統及設備營運所需之資源及落實於年度預算或教育訓練計畫等項目。 (十四)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。 (十五)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。 (十六)公司資訊委外作業如涉及核心資通系統與資通服務，資訊服務供應商應定期提供資通系統與資通服務之回復計畫，回復計畫可以災難復原計畫、備援演練、營運持續計畫等形式呈現。	部門。 2.定期評估核心營運系統及設備,對評估結果採取適當措施，並提報董事會，以確保營運持續及作業韌性之能力。 3.於永續報告書、年報、財務報告或公司網站，揭露年度內公司持續核心營運系統及設備營運所需之資源及落實於年度預算或教育訓練計畫等項目。 (十四)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。 (十五)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。 (十六)公司資訊委外作業如涉及核心資通系統與資通服務，資訊服務供應商應定期提供資通系統與資通服務之回復計畫，回復計畫可以災難復原計畫、備援演練、營運持續計畫等形式呈現。	