證券商內部控制制度標準規範—內部稽核實施細則修正對照表

編號	作業項目	修正後內容	修正前內容	修正說明
AC-20000	營運持續管理之稽核 目的： 確定上述作業是否符合規定辦理	不定期（每半年至少查核乙次） (一)故障復原程序（例如：電腦設備、通訊設備、電力系統、資料庫、電腦作業系統等備援及回復計畫）是否明確訂定，並製成文件。 (二)故障復原程序是否週期性測試，測試後是否召開檢討會議，針對測試缺失謀求改進，並留存紀錄 (三)公司是否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，且是否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。 (四)公司（證券經紀商）是否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。(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	不定期（每半年至少查核乙次） (一)故障復原程序（例如：電腦設備、通訊設備、電力系統、資料庫、電腦作業系統等備援及回復計畫）是否明確訂定，並製成文件。 (二)故障復原程序是否週期性測試，測試後是否召開檢討會議，針對測試缺失謀求改進，並留存紀錄 (三)公司（證券經紀商）之交易主機是否有備援措施，並依所屬資安分級建置異地備援機房。 (四)公司是否執行營運衝擊分析，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	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
		心系統，自 116 年 12 月底生效。)	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，且是否視演練範圍是否涉及第三方，邀請相關廠商參與演練。網路下單證券商是否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。	
		(五)公司是否訂定資訊安全訊息通報機制。	(五)公司是否訂定資訊安全訊息通報機制。	
		(六)公司針對與資通系統有關之資訊安全或服務異常事件，是否依「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。	(六)公司針對與資通系統有關之資訊安全或服務異常事件，是否依「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。	
		(七)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，是否立即函報證交所(或櫃檯買賣中心、券商公會)轉陳主管機關。	(七)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，是否立即函報證交所(或櫃檯買賣中心、券商公會)轉陳主管機關。	
		(八)公司是否明確訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序，並是否每年進行演練。	(八)公司是否明確訂定分散式阻斷服務攻擊(DDoS)防禦與應變作業程序。	
		(九)公司是否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	(九)公司是否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	

編號	作業項目	修正後內容	修正前內容	修正說明
		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)公司是否辨識風險情境，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。 (十一)核心系統原服務中斷時，是否於可容忍時間內，由備援設備或其他方式取代並提供服務。 (十二)公司資訊委外作業如涉及核心資通系統與資通服務，資訊服務供應商是否定期提供資通系統與資通服務之回復計畫(如災難復原計畫、備援演練、營運持續計畫等)。	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)公司是否辨識風險情境，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。 (十一)核心系統原服務中斷時，是否於可容忍時間內，由備援設備或其他方式取代並提供服務。 (十二)公司資訊委外作業如涉及核心資通系統與資通服務，資訊服務供應商是否定期提供資通系統與資通服務之回復計畫(如災難復原計畫、備援演練、營運持續計畫等)。	