證券商內部控制制度標準規範—內部稽核實施細則修訂對照表(113 年)

編號	作業項目	修 訂 後 內 容	修 訂 前 內 容	修訂說明
AC-11000	風險評鑑與管理之稽核 目的： 確定上述作業是否符合規定辦理	(一)~(二)略 (三)、是否定期（每年至少乙次）對全公司之資訊資產及各項作業辦理資訊安全風險評鑑（風險評估範圍應包含營運相關之重大風險與控管措施，如新產品、新興技術和資訊系統風險），並留存紀錄。 (四) 略 (AC-12000 ~ AC-13000 略)	(一)~(二)略 (三)、是否定期（每年至少乙次）對全公司之資訊資產及各項作業辦理資訊安全風險評鑑，並留存紀錄。 (四)略 (AC-12000 ~ AC-13000 略)	配合內部控制制度 CC-11000 之修訂，並同時修訂查核明細表(FC-11000-A)。

AC-14000	資訊分類與控制之稽核目的：確定上述作業是否符合規定辦理	(一)~(三)略 (四)、公司是否對資訊資產之資料與文件的保存期限進行規範，並於保存期限到期後進行刪除與銷毀。 (AC-15000 ~ AC-16000 略)	(一)~(三)略 (新增) (AC-15000 ~ AC-16000 略)	配合內部控制制度 CC-14000 之修訂，並同時修訂查核明細表(FC-14000-S)。

AC-17000 17010 網路安全管理（適用網際網路下單證券商，另1~7、9、13~15、20~26項並適用於所有證券商）	網路安全管理之稽核目的：確定上述作業是否符合規定辦理	(一)、網路安全管理 1、~23、略 24、是否每年定期檢視並維護防火牆存取控管設定，每半年檢視 DMZ 區之防火牆規則，並留存相關紀錄。 25、~38、略 (AC-18000 ~ AC-19000 略)	(一)、網路安全管理 1、~23、略 24、是否每年定期檢視並維護防火牆存取控管設定，並留存相關紀錄。 25、~38、略 (AC-18000 ~ AC-19000 略)	配合內部控制制度 CC-17000之修訂，並同時修訂查核明細表(FC-17000-17010-M)。

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	(一)~(三)略 (四)、公司是否擬訂營運持續計畫（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，並擬訂關鍵性業務及其衝擊影響分析，評估核心系統中斷造成之衝擊程度，並依核心系統之復原時間目標(RTO)、資料復原點目標(RPO)，作為恢復核心系統、備份備援規劃及執行復原作業之依據，再依其所屬資安分級定期辦理業務持續運作演練。公司是否視演練範圍是否涉及第三方，邀請相關廠商參與演練。 (五)~(十一)略 (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)。 (AC-21000 略)	(一)~(三)略 (四)、公司是否擬訂營運持續計畫（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，並擬訂關鍵性業務及其衝擊影響分析，評估核心系統中斷造成之衝擊程度，並依核心系統之復原時間目標(RTO)、資料復原點目標(RPO)，作為恢復核心系統、備份備援規劃及執行復原作業之依據，再依其所屬資安分級定期辦理業務持續運作演練。 (五)~(十一)略 (新增) (AC-21000 略)	配合內部控制制度 CC-20000之修訂，並同時修訂查核明細表(FC-20000-S)。

AC-21100	新興科技應用之稽核目的：確定上述作業是否符合規定辦理	(一)~(二)略 (三)行動裝置 是否訂定行動裝置之資訊安全規範與管理辦法，並包含以下項目： (1)公務用行動裝置設備管理辦法： A.~C.略 D.公務用行動裝置管理辦法內容應包含行動裝置儲存機密資料之限制與管理方式。 (2)員工自攜行動裝置設備管理辦法： A.~C.略 D.員工自攜行動裝置管理辦法內容應包含行動裝置儲存機密資料之限制與管理方式。 (以下略)	(一)~(二)略 (三) 行動裝置 是否訂定行動裝置之資訊安全規範與管理辦法，並包含以下項目： (1)公務用行動裝置設備管理辦法： A.~C.略 (新增) (2)員工自攜行動裝置設備管理辦法： A.~C.略 (新增) (以下略)	配合內部控制制度 CC-21100之修訂，並同時修訂查核明細表(FC-21100-A-2及FC-21100-A-3)。