證券商內部控制制度標準規範—內部控制制度修訂對照表（113 年）

編號	作業項目	修 訂 後 內 容	修 訂 前 內 容	修訂說明
CC-11000（適用網際網路下單證券商） CC-140	風險評鑑與管理	CC-11000 風險評鑑與管理（網際網路下單證券商適用） (一)~(二)略 (三)、~~公司應有書面的資訊安全風險評鑑報告，每年至少評估乙次，並留存相關紀錄~~公司應至少每年進行一次資訊安全風險評鑑，並留存相關紀錄，營運相關的重大風險與控管措施議題（包括新產品、新興技術和資訊系統的風險）應納入風險評估範圍，以確保公司政策、程序和控管措施之有效性。 (四)略 CC-12000~CC-13000 略	CC-11000 風險評鑑與管理（網際網路下單證券商適用） (一)~(二)略 (三)、公司應有書面的資訊安全風險評鑑報告，每年至少評估乙次，並留存相關紀錄。 (四)略 CC-12000~CC-13000 略	依據主管機關 112 年 7 月 5 日證期(券)字第 1120382968 號函辦理，就資安治理成熟度評估內容，爰增修資安規範。 調整：風險評估範圍應包含營運相關的重大風險與控管措施議題（包括新產品、新興技術和資訊系統的風險）

00 CC-170	資產分類與控制	CC-14000 資產分類與控制 (一)~(三)略 (四)、公司應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。 CC-15000~CC-16000 略	CC-14000 資產分類與控制 (一)~(三)略 (新增) CC-15000~CC-16000 略	 新增

10（適用網際網路下單證券商，另(一)、(二)、(六)項並適用於所有證券商） CC-20000	網路安全管理	CC-17000 通訊與作業管理 17010 網路安全管理 (一)略 (二)、防火牆之安全管理 1~5 略 6、公司應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，並留存相關檢視紀錄。 7 略 (三)~(十一)略 CC-18000~CC-19000 略	CC-17000 通訊與作業管理 17010 網路安全管理 (一)略 (二)、防火牆之安全管理 1~5 略 6、公司應每年定期檢視並維護防火牆存取控管設定，並留存相關檢視紀錄。 7 略 (三)~(十一)略 CC-18000~CC-19000 略	調整：DMZ 區防火牆規則應每半年檢視

	營運持續管理	CC-20000 營運持續管理 (一)~(七)略 (八)、公司應擬訂營運持續計畫（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。公司應視演練範圍是否涉及第三方，邀請相關廠商參與演練。 (九)~(十三)略 (十四)、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	CC-20000 營運持續管理 (一)~(七)略 (八)、公司應擬訂營運持續計畫（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。 (九)~(十三)略 (新增)	評估第三方廠商配合演練 新增

CC-21100		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。 CC-21000 略	CC-21000 略	

	新興科技應用	CC-21100 新興科技應用 (一)~(二)略 (三)行動裝置 1、應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)	CC-21100 新興科技應用 (一)~(二)略 (三)行動裝置 1、應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)	新增 新增