建立證券商資通安全檢查機制部分條文修正對照表(113 年)

修正條文	現行條文	說明
1、風險評鑑與管理（CC-11000，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，年度查核） (1)、(2)略 (3)公司~~應有書面的資訊安全風險評估報告，每年至少評估一次，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。 (4)略	1、風險評鑑與管理（CC-11000，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，年度查核） (1)、(2)略 (3)公司應有書面的資訊安全風險評估報告，每年至少評估一次，並留存相關紀錄。 (4)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）
2~3、略	2~3、略	
4、資產分類與控制（CC-14000，半年查核） (1)~(3)略 (4) 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。	4、資產分類與控制（CC-14000，半年查核） (1)~(3)略	新增

5~6、略	5~6、略	
7、通訊與作業管理（CC-17000）	7、通訊與作業管理（CC-17000）	
（1）網路安全管理（CC-17010，適用網際網路下單證券商，另 a、b、e、f 項並適用於所有證券商，每月查核） a. 略 b. 網路設備之安全管理 (a) ~ (e) 略 (f) 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。 (g) ~ (i) 略 c. ~ l. 略	（1）網路安全管理（CC-17010，適用網際網路下單證券商，另 a、b、e、f 項並適用於所有證券商，每月查核） a. 略 b. 網路設備之安全管理 (a) ~ (e) 略 (f) 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。 (g) ~ (i) 略 c. ~ l. 略	調整：DMZ 區防火牆規則應每半年檢視
（2）略	（2）略	
8~9、略	8~9、略	
10、營運持續管理（CC-20000，半年查核）	10、營運持續管理（CC-20000，半年查核）	
（1）~（3）略	（1）~（3）略	

（4）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。	（4）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。	評估第三方廠商配合演練
（5）~（10）略	（5）~（10）略	
（11）證券商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。		新增
11、略	**11、略**	
12、新興科技應用（CC-21000，年度查核）	**12、新興科技應用（CC-21000，年度查核）**	
（1）~（2）略	（1）~（2）略	
（3）行動裝置		

a. 公司應訂定公務用行動裝置之資訊安全規範與管理辦法，須包含以下項目： (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。 b. 公司應訂定員工自攜行動裝置之資訊安全規範與管理辦法，須包含以下項目： (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。 （4）~（6）略 **(以下略)**	（3）行動裝置 a. 公司應訂定公務用行動裝置之資訊安全規範與管理辦法，須包含以下項目： (a) ~ (c) 略 b. 公司應訂定員工自攜行動裝置之資訊安全規範與管理辦法，須包含以下項目： (a) ~ (c) 略 （4）~（6）略 **(以下略)**	新增 新增