**中華民國證券商業同業公會**

**「資訊作業韌性自律規範」修正條文對照表**

| **修正條文** | **現行條文** | **說明** |
| --- | --- | --- |
| **第二條 名詞定義**  一、～七、（略）  八、第一類證券商：係指依「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之證券商。 | **第二條 名詞定義**  一、～七、（略）  八、第一類證券商：係指依「證券暨期貨市場各服務事業建立內部控制制度處理準則」第三十六條之二條文指派資訊安全長之證券商~~或「建立證券商資通安全檢查機制-分級防護應辦事項附表」所列第一級、第二級、第三級證券商。~~ | 一、參考臺灣證券交易所114年2月13日臺證輔字第1140500496號函，公告「證券暨期貨市場各服務事業資訊作業韌性參考指引」(下稱參考指引)第二條及金管會113年1月4日金管證券字第1120385996號函令，有關設立資訊安全長條件調整，刪除分類之條件。 |
| **第三條 營運持續管理及營運持續計畫演練**  **一**、證券商營運持續管理應參考證交所「建立證券商資通安全檢查機制」之營運持續管理相關規定辦理。  二、證券商應針對各情境、各業務狀況進行演練並可參考「核心系統備援演練參考程序」(附件)，進行事前準備、演練實施及演練後檢討之各階段檢核作業，以確認演練及測試程序之有效運作，並依據「建立證券商資通安全檢查機制－分級防護應辦事項附表」第十四項所規定之業務持續運作演練辦理。  (一)應針對已辨識可能造成核心業務中斷之風險情境(包含天然災害、人為災害與資通訊安全事件)設計演練情境並宜規劃針對所有情境或輪流針對部分情境進行演練。  (二)應進行模擬災害或意外發生時之情境操作，考量納入核心系統復原負責人員、核心業務執行人員與復原所需供應商；並規劃演練之系統相關資訊。  (三)應於演練前辨識可能造成之風險，並事先擬定保護措施。  (四)演練內容應驗證各項核心系統所制定之標準作業程序。  (五)應定期演練並驗證其核心系統可用性，依需求規劃為同異地系統備援演練或同異地資料備份回存測試，以確保人員熟悉程度與程序有效性，並應留存相關演練紀錄。  (六)第一類證券商應於異地系統備援演練時，納入實際業務運作驗證，以實證最小可接受服務水準所仰賴之內部資源配置及人力調度、外部夥伴之協同作業及資訊網路調整介接等作業，於關鍵時刻皆能有效運作。並鼓勵第二類證券商執行。  (七)應於演練後召開檢討會議，確認復原機制與演練結果是否符合所制定的復原時間目標(RTO)及資料復原點目標(RPO)要求，並檢視核心系統現有同異地系統備援機制與同異地資料備份機制是否符合核心業務之需求。 | **第三條 營運持續管理**  證券商營運持續管理應參考證交所「建立證券商資通安全檢查機制」之營運持續管理相關規定辦理。 | 依據參考指引第十二條(營運持續計畫演練)，增修制定風險情境之營運持續計畫應輪流進行演練，以測試程序之有效性，並增列「核心系統備援演練參考程序」(附件)強化核心系統演練作業確實性。 |
| **第五條 備份備援機制**  一、～二、（略）  三、應針對機密與敏感性資料，實施妥善之防護措施。 | **第五條 備份備援機制** | 一、新增本條第三點。  二、依據參考指引第八條(備份備援機制) ，增修制定資料備份機制時機敏資料應妥善防護。 |
| **第九條 核心系統委外之管理**  一、核心系統委外時，證券商應依委外服務範圍及特性確保供應商因下列原因而造成營運中斷後，核心系統之復原水準可滿足系統復原時間目標(RTO)及資料復原點目標(RPO)，以支持核心業務回復至最小可接受服務水準，並要求供應商配合證券商或自行辦理演練以驗證核心系統可用性。  (一)因天然災害、人為災害與資通訊安全事件而中斷。  (二)未預期之設備故障或變更。  (三)系統功能調整或重大性架構變更 。  (四)產品生命週期結束且不再提供技術協助服務，或不具可用性。  二、證券商應將上述營運持續管理相關要求納入委外契約。 |  | 依據參考指引第十四條(核心系統委外之管理)增訂核心系統委外之管理，列舉供應商可能面臨導致營運中斷之原因，並要求供應商應配合證券商辦理演練以驗證系統可用性。 |
| **第十條 施行程序**  本自律規範經本公會理事會會議通過，並報奉主管機關備查後實施，修正時亦同。 | **第九條 施行程序**  本自律規範經本公會理事會會議通過，並報奉主管機關備查後實施，修正時亦同。 | 條次調整。 |