**中華民國證券商業同業公會資訊作業韌性自律規範**

金融監督管理委員會112年8月15日金管證券字第1120344733號函准予備查

中華民國證券商業同業公會112年8月17日中證商業一字第1120004366號公告實施

金融監督管理委員會114年6月26日金管證券字第1140346614號函准予備查

中華民國證券商業同業公會114年6月月30日中證商業一字第1140003295號號公告實施

# 第一條 目的

為協助證券商於核心系統遭受中斷事故時，能有效執行應變措施並將損害降低至可承受範圍，爰訂定本自律規範。

# 第二條 名詞定義

1. 資訊作業韌性：資訊作業面臨損害、異常或中斷服務時的處理能力與應變彈性。
2. 核心業務：係指直接提供客戶交易或支持交易業務持續運作之必要業務。
3. 核心系統：係指直接提供客戶交易或支持交易業務持續運作之必要系統，其餘皆為非核心系統。
4. 營運衝擊分析(Business Impact Analysis，BIA)：評估核心系統中斷時可能對組織造成之衝擊。
5. 復原時間目標(Recovery Time Objective，RTO)：中斷事故發生後，核心系統從中斷事故發生到回復至最小可接受服務水準之目標時間。
6. 資料復原點目標(Recovery Point Objective，RPO)：中斷事故發生時，核心系統可承受之資料損失量所訂之值。
7. 最小可接受服務水準：核心業務於復原時間目標(RTO)內回復之最低限度運作水準。
8. 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。
9. 第二類證券商：係指非屬第一類證券商之證券商。
10. 外國證券商：係指外資集團在台子公司或分公司。外國證券商如有標準較佳之規範則從其規範；若無，則應遵守本國的規範。

# 第三條 營運持續管理及營運持續計畫演練

1. 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。
2. **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。**

# 第四條 資訊作業韌性管理組織

證券商就資訊作業韌性進行任務編組及配置適當人力，辦理下列事項：

一、識別核心業務及其對應之核心系統。

二、執行營運衝擊分析，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。

# 第五條 備份備援機制

一、制定資料備份機制時，宜考量「3-2-1 備份原則」。

(一)至少製作三份備份。

(二)將備份分別存放在兩種不同儲存媒體。

(三)至少一份放在異地保存。

二、依據核心系統特性、業務單位需求與復原時間目標(RTO)，制定適當之系統備援架構。

**三、應針對機密與敏感性資料，實施妥善之防護措施。**

# 第六條 機房設置規劃

一、規劃備援機房時應遵循政府建築及消防相關法令法規，考量支援設施包含電力供給、空調配置、環境監控與告警等配置。

二、第一類證券商應設置異地備援機房。

三、證券商規劃主/備援中心搬移或新建規劃時，異地備援機房地點與場所之選擇，宜考量與主機房非同一災難或失效影響之地理位置為原則。

# 第七條 災害應變機制

當災害發生造成資訊作業異常或中斷時，應辨識風險情境，就各項風險情境擬定各系統之應變、減災或復原措施相關作業流程。

一、應辨識可能造成中斷之風險情境，依據證交所「天然災害侵襲處理措施」、證交所「建立證券商資通安全檢查機制」及「證券期貨市場資通安全事件通報應變作業注意事項」制定緊急應變措施及緊急處理程序。

二、針對與資訊系統有關之資訊安全或服務異常事件，依據「證券期貨市場資通安全事件通報應變作業注意事項」制定緊急通報程序。

# 第八條 資訊作業韌性之認知及能力訓練

證券商就資訊作業韌性之任務編組人員，依據證交所「建立證券商資通安全檢查機制」所屬資安分級，應定期辦理資訊作業演練並留存紀錄。

# 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。**

# 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。