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

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

一、 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。

二、 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。

三、 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。

四、 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。

五、 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。

六、 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。

七、 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。

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。

九、 第二類證券商：係指非屬第一類證券商之證券商。

十、 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

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。

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。。

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 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。