**中華民國證券商業同業公會
證券商資通系統與服務供應鏈風險管理自律規範**

**修正條文對照表**

| **修正後條文** | **現行條文** | **說明** |
| --- | --- | --- |
| **第二條**五、資訊服務：指提供與系統軟體或硬體有關之服務形態，包含系統發展類、維運管理類及雲端服務類。 | **第二條**五、資訊服務：係指與資訊之蒐集、控制、傳輸、儲存、刪除、其他處理、使用或分享相關之服務。 | 參考「金融機構資通系統與服務供應鏈風險管理規範」第二條規定，重新定義資訊服務。 |
| **第三條 資訊服務供應商遴選原則**1. 證券商應評估資訊委外業務項目之資通安全可行性，及資訊服務供應商作業能力，採取適當風險管控措施，確保業務項目委外處理之品質，並應注意委託資訊服務供應商之適度分散以控管作業風險，相關事項請參閱附件：「證券商資訊委外之資安應注意事項檢查表」進行檢核；倘集中度過高疑慮者（包括單一資訊服務供應商對組織或單一資訊服務供應商於市場整體之集中度），資訊服務供應商選定，應由相關資訊單位共同執行風險評估，評估結果應提報適當管理層級並取得同意。

（以下略。） | **第三條 資訊服務供應商遴選原則**1. 證券商應評估資訊服務供應商之集中度，包括評估資訊服務供應商作業能力，採取適當風險管控措施，確保作業委外處理之品質，並應注意作業委託資訊服務供應商之適度分散以控管作業風險。資訊服務供應商選定之評估結果送交資訊部門主管核可，並依公司分層負責核決權限處理。

（以下略。） | 1. 依據主管機關113年8月22日證期(券)字第1130348556號函辦理。
2. 考量資訊服務供應商作業能力僅為證券商資訊業務委外之風險評估項目之一，爰參考集保結算所112年11月13日公告「證券暨期貨市場各服務事業資通系統與服務供應鏈風險管理參考指引」（以下稱供應鏈風險管理參考指引）第四條增列評估項目。

二、考量現今業者資訊委外作業量大幅增加，作業風險亦大幅提升，證券商應針對資訊委外各階段進行資安風險因素評估及執行相對應管控措施，爰依據集保結算所訂定「資訊委外之資安應注意事項檢查表」，增訂附件「證券商資訊委外之資安應注意事項檢查表」，供證券商進行委外各階段應注意事項之檢核。三、證券商作業委外係由各業務部門提出，非資訊部門主管負責，對於資訊服務供應商之集中度風險評估核決，爰引用供應鏈風險管理參考指引第4條第一項評估結果應提報適當管理層級並取得同意之條文。 |
| **第四條 證券商與資訊服務供應商之合約**一、證券商與資訊服務供應商之合約內容應依服務範圍的不同，宜包含下列各項：(一)基本要求1. 合約期限。2. 服務範圍。3. 服務交付日期。4. 服務水準要求（如為 一年期以上提供性質 者，如：軟硬體維護 合約、系統委外管理 等，資訊服務供應商 應依合約要求，定期 提交服務水準報告）。(5.至 17.略。)（(二)至(四)略。）(五)資訊服務供應商資安要求(1.至 5.略。)6.證券商應載明要求資訊服務供應商於知悉存有任何潛在問題和危害(如：於其他客戶端發生重大系統異常) ，且其可能影響受託業務時，立即通知證券商並採取相關補救措施。7.證券商電子交易之即時報價，如採用不同資訊服務供應商互為備援外，與資訊服務供應商之契約，應要求提供備援主機與備援系統相關證明文件，每年應與證券商進行一次主備援切換測試演練並保存相關演練記錄文件。8.第一類證券商之資訊服務供應商應提供取得之資安及品質證照。 | **第四條 證券商與資訊服務供應商之合約**一、證券商與資訊服務供應商之合約內容應依服務範圍的不同，宜包含下列各項：(一)基本要求1. 合約期限。2. 服務範圍。3. 服務交付日期。4. 服務水準要求。(5.至 17.略。)（(二)至(四)略。）(五)資訊服務供應商資安要求(1.至 5.略。)6.第一類證券商之資訊服務供應商應提供取得之資安及品質證照。 | 1. 參考供應鏈風險管理參考指引第七條修正。
2. 為了確保資訊委外服務的品質與可靠性，降低證券商風險，爰增列服務期間為一年期以上，供應商定期提交服務水準報告。
3. 考量近期業者發生委外資訊廠商應用系統錯誤，造成交易系統故障，建議業者強化管控，爰增列第6點。
4. 依據主管機關112年7月5日證期(券)字第1120339855號函及參考期貨公會113年1月24日公告資通系統安全防護基準自律規範第五條修正，為避免因即時行情中斷，影響委託人權益，於本條新增第7點，明訂應請電子交易即時報價之資訊服務供應商出示系統備援相關聲明。自行每年與證券商進行一次主備援切換測試演練及留存相關文件，以加強資安。
5. 前開規定，排除與不同即時報價資訊服務供應商簽約可互為備源之證券商。

六、條次配合變更。 |