**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**

| **修正條文** | **現行條文** | **說明** |
| --- | --- | --- |
| **第二條 名詞定義**  (一至三略)  四、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。  五、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。  六、資通服務：係指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。  七、資訊服務：係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。  八、雲端服務：透過網路技術達成共享運算資源之前提下，提供使用者具備彈性、可擴展及可自助之服務，如下列雲端服務模式：  (一)基礎架構即服務（Infrastructure as a Service，簡稱 IaaS）：雲端服務提供者通過網路向雲端服務使用者提供資訊科技基礎設施。  （二）平台即服務（Platform as a Service，簡稱 PaaS）：雲端服務提供者向雲端服務使用者提供平台工具。  （三）軟體即服務（Software as a Service，簡稱 SaaS）：雲端服務提供者利用網際網路向雲端服務使用者提供應用程式服務。  (九至十七略) | **第二條 名詞定義**  (一至三略)  四、資通服務：係指與資訊之蒐集、控制、傳輸、儲存、流通、刪除、其他處理、使用或分享相關之服務。  五、資訊服務：係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。  六、雲端運算服務：透過網路技術達成共享運算資源之前提下，提供使用者具備彈性、可擴展及可自助之服務。  (七至十五略) | 一、參酌臺灣集中保管結算所「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」(下稱供應鏈參考指引)第三條，增列核心業務及核心系統名詞定義。  二、第八項參酌供應鏈參考指引第三條第七項，修正雲端服務名詞定義。  三、編號調整。 |
| **第三條** **資訊服務供應商遴選原則**   1. 證券商應針對資訊委外業務項目之資通安全風險與委外作業可行性，及資訊服務供應商作業能力及集中度，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。內容應包含:   (一)分析資訊委外業務項目受影響之範圍(如：可能受影響之資訊資產、流程及作業環境)。  (二)將資訊委外業務項目之資通安全要求列入成本估算(如：安全性檢測行動應用程式資安檢測、源碼檢測、弱點掃描等)。  (三)資訊服務供應商對資訊委外業務項目之資通安全管控機制(如：資料管理、權限控管、設備管理等)。  (四)資訊服務供應商之服務集中度（包括單一資訊服務供應商對證券商或單一資訊服務供應商於市場整體之集中度）。  (五)資訊服務供應商與其提供產品或服務位置。  (六)資訊委外業務項目屬核心系統或跨機構資訊服務，應分析資訊服務供應商配合證券商營運持續與資通安全事件處理之目標與要求。  二、證券商應依前項風險評估結果採取適當風險管控措施，確保業務項目委外處理之品質， 並應注意作業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。  三、資訊委外業務項目屬核心系統，證券商與資訊服務供應商應有資訊安全人員參與，以協助管理資訊安全風險。  四、證券商評選資訊服務供應商之原則如下，並應留存相關文件紀錄：  (一)資訊服務供應商之維運能力(如財務能力、專業能力及經驗實績等)。  (二)雲端服務供應商應具備完善之雲端資通安全管理措施或通過第三方驗證。  ((三)第一類證券商之資訊服務供應商應具備完善之資通安全管理措施(提供管理措施與執行情形說明)或通過第三方驗證。  五、選商過程中如存在資訊資產交換，證券商應備妥保密協議書，並於交換與採購產品或服務相關之機敏性資訊前簽署。  六、第一類證券商之資訊服務供應商提供之建議書應包含下列項目：  (一)證券商採購需求產品/服務。  (二)資訊服務供應商應符合證券商資安要求與服務水準要求(例如：證券商資安政策、本公會資通系統安全防護基準自律規範)。  (三)資訊服務供應商之專案管理能力(例如，具有至少一張有效期間內之專案管理相關證照或相關成功專案簡述)。 | **第三條 資訊服務供應商遴選原則**  一、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，並應注意作業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。  二、證券商評選資訊服務供應商之原則如下，並應留存相關文件紀錄：  (一)資訊服務供應商之維運能力(如財務能力、專業能力及經驗實績等)。  (二)雲端運算服務供應商應具備完善之雲端運算資通安全管理措施或通過第三方驗證。  (三)第一類證券商之資訊服務供應商應具備完善之資通安全管理措施(提供管理措施與執行情形說明)或通過第三方驗證。  三、選商過程中如存在資訊資產交換，證券商應備妥保密協議書，並於交換與採購產品或服務相關之機敏性資訊前簽署。  四、第一類證券商之資訊服務供應商提供之建議書應包含下列項目：  (一)證券商採購需求產品/服務。  (二)資訊服務供應商應符合之資安要求(例如：證券商資安政策、本公會資通系統安全防護基準自律規範)。  (三)資訊服務供應商之專案管理能力(例如，具有至少一張有效期間內之專案管理相關證照或相關成功專案簡述)。 | 一、第一項第一款至第六款，參酌供應鏈參考指引第四條，增列執行風險評估項目。  二、第一項第一款與第二款，說明委外實務中，應先評估資訊委外業務項目之資訊安全風險與委外可行性，依據資訊安全要求進行成本估算。  三、第一項第三款，說明應評估資訊服務供應商需符合之專業資格、資訊安全要求，以及資訊安全要求之服務水準(如： 資料管理、權限控管、設備管理等)。  四、第一項第四款，說明資訊服務供應商之服務集中度。  五、第一項第五款，考量地緣政治要求，說明證券商應評估資訊服務供應商與提供產品或服務之位置(各國家可能有其不同地區適用之法規)，確認其所適用之當地法令法規，對於資訊安全要求與合約關係是否存在不利衝擊。  六、第一項第六款，參酌供應鏈參考指引第四條第一項第六款，說明證券商應評估核心系統或跨機構資訊服務供應商之營運持續與資通安全事件處理應符合證券商資訊安全要求，爰增核心資訊系統供應商及跨機構資訊服務之風險評估項目。  七、第三項參酌供應商參考指引第三條第三項，說明證券商委託供應商提供核心系統之應用系統開發案時，專案成員應有資訊安全人員參與，以協助第一道防線管理資訊安全風險與評估資訊安全作業執行情形。  八、第四項第二款配合第二條名詞修正，修正雲端服務名詞。  九、第六項第二目配合第一項第三款說明應評估資訊服務供應商需符合之專業資格、資訊安全要求，以及資訊安全要求之服務水準(如：資料管理、權限控管、設備管理等)，爰增建議書徵求文件包含服務水準要求。 |
| **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.服務變更規範。  6.服務驗收之標準。  7.資通安全事件通報及應變處理作業程序（含當發生資安事故時，資訊服務供商應主動、即時或於時限要求內通知證券商）。  (8.至 17.略。)  (二)證券商與資訊服務供應商之服務與產品應載明事項：  1.載明資訊委外服務或產品之智慧財產權及其授權範圍。  2.資訊服務供應商如分包予其他供應商應載明(異動亦同)。  3.應載明資訊服務供應商配合進行壓力測試及調整服務負載量之義務，並於市場交易量、業務變化及客戶屬性等發生顯著異動時發動辦理，俾憑評估系統資源調配或擴增。  4.第一類證券商應載明採購之服務與產品於規劃設計時納入服務與產品之機敏資料保護、授權與認證、安全性更新等。  5.第一類證券商應載明採購之服務與產品於規劃設計時納入隱私保護機制(Privacy by design)之要求  (三)資訊服務供應商服務範圍涉及資通系統開發、維護與監控，應遵循「本公會資通系統安全防護基準自律規範」。  (四)服務範圍涉及使用雲端服務，資訊服務供應商應遵循「本公會新興科技資通安全自律規範」。  (五)資訊服務供應商之資安應符合下列要求：  (1.至 6.略。)  7.證券商應載明資訊服務供應商在應用程式上線前應完整測試。交易主機應設立備援機制，並禁止於開盤前及開盤期間進行系統更新及下載，避免客戶端發生重大系統異常。  8.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。  9.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。(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.服務變更規範。  6.服務驗收之標準。  7.資通安全事件通報及應變處理作業程序。  (8.至 17.略。)  (二)證券商與資訊服務供應商之服務與產品應載明事項：  1.載明資訊委外服務或產品之智慧財產權及其授權範圍。  2.資訊服務供應商如分包予其他供應商應載明(異動亦同)。  3.第一類證券商應載明採購之服務與產品於規劃設計時納入服務與產品之機敏資料保護、授權與認證、安全性更新等。  4.第一類證券商應載明採購之服務與產品於規劃設計時納入隱私保護機制(Privacy by design)之要求。  (三)資訊服務供應商服務範圍涉及資通系統開發、維護與監控，應遵循「本公會資通系統安全防護基準自律規範」。  (四)服務範圍涉及使用雲端運算服務，資訊服務供應商應遵循「本公會新興科技資通安全自律規範」。  (五)資訊服務供應商之資安應符合下列要求：  (1.至 6.略。)  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。 | 一、第一項第一款第七目考量證券商資通安全事件處置時限需求，以利資訊服務供應商配合，爰增時限要求說明。  二、考量資訊服務供應商應配合證券商因應內外在環境變化執行壓力測試及相關負載調整，以維持服務與產品之可用性，爰增列第一項第二款第三目。  三、配合第二條名詞修正，修正雲端服務名詞。  四、邇來發生資訊服務供應商系統變更測試不完整，致開盤期間出現系統異常情形，影響交易秩序及投資人權益。為避免再發生類似情事，除明文禁止資訊服務供應商於開盤前及開盤期間進行系統更新及下載，並請證券商應落實委外廠商管理，確實要求廠商應用程式上線前測試之完整性，並參酌「建立證券商資通安全檢查機制」，要求交易主機應有備援措施，爰增列第一項第五款第七目。 |
| **第五條 資訊服務供應商存取權限**  一、專案負責人應向資訊服務供應商告知證券商之資通安全相關規範，為保護證券商資訊資產，資訊服務供應商經向證券商申請同意後，始有存取證券商資訊資產權限。  (以下略) | **第五條 資訊服務供應商存取權限**  一、專案負責人應向資訊服務供應商告知組織之資訊安全相關規範，為保護證券商資訊資產，資訊服務供應商經向證券商申請同意後，始有存取證券商資訊資產權限。  (以下略) | 一、配合第二條名詞定義，修正文字。 |
| **第七條 資訊服務供應商服務****審核與稽核**  一、證券商於資訊委外期間應每年至少一次或於知悉資訊服務供應商發生可能影響其委託業務之資通安全事件時，證券商得自行或授權第三方得對資訊服務供應商進行稽核。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。  (二至三略)  四、證券商應建立對資訊服務供應商之資訊委外服務資通安全監督之程序；倘資訊委外作業屬核心系統，應明訂資通安全稽核之方式、頻率，與稽核結果之改善追蹤機制。 | **第七條 審核資訊服務供應商服務**   1. 證券商於資訊委外期間應每年至少一次與認為有稽核之必要時，證券商得自行或授權第三方得對資訊服務供應商進行稽核。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。   (二至三略) | 一、參酌供應鏈參考指引第十二條，將核心資訊系統供應商及跨機構資訊服務之風險評估及查核等管理機制，爰增稽核文字。  二、第一項參酌供應鏈參考指引第十二條第三項，證券商應依據第四項建立之資通安全稽核程序，自行定義定期稽核頻率，另說明稽核之必要情境為知悉資訊服務供應商發生可能影響證券商所委託業務之資通安全事件。  三、第四項參酌供應鏈參考指引第十二條第二項，說明證券商應建立對資訊服務供應商資通安全稽核之程序針對核心系統供應商，應明訂執行資通安全稽核之方式與頻率爰增列第四項。 |