中華民國證券商業同業公會供應鏈風險管理自律規範

金融監督管理委員會 111 年 12 月 22 日金管證券字第 1110365208 號函准予備查
中華民國證券商業同業公會 111 年 12 月 23 日中證商業一字第 1110008167 號函公告實施

第一條 目的

為強化證券商對資通系統之資訊服務供應商遴選、管理、終止與解除之風險管理，特定本自律規範。

第二條 名詞定義

一、資訊委外：係指證券商將部分或全部之資通服務由組織外之軟硬體供應與維運商、跨機構合作夥伴提供。

二、資訊資產：係指與資訊處理相關之資產，包括硬體、軟體、資料、文件及人員等。

三、資通系統：係指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。

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。

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、營業秘密：係指方法、技術、製程、配方、程式、設計或其他可用於生產、銷售或經營之資訊，而符合下列要件者：

(一)非一般涉及該類資訊之人所知者。

(二)因其秘密性而具有實際或潛在之經濟價值者。

(三)所有人已採取合理之保密措施者。

八、存取：係指存取資訊資產的各種方式，包含取得、使用、保管、查詢、修改、調整、銷毀等。

九、專案負責人：係指專案經理或該項業務權責部門主管或其指派之人員。

十、資通安全機制（Security by design）：係指服務與產品規劃設

計時即融入資通安全的概念，於開發流程中的設計階段，列出安全需求、辨識安全風險及套用控制措施，以作為後續安全功能驗證的基礎，落實安全的軟體生命週期。

十一、隱私保護機制 (Privacy by design)：係指服務與產品規劃設計時即融入隱私保護機制的概念，於開發流程中的設計階段，列出隱私保護需求、辨識相關風險及套用控制措施，以作為後續安全功能驗證的基礎。

十二、資通安全事件：係指系統、服務或網路狀態經鑑別而顯示可能有違反資通安全政策或保護措施失效之狀態發生，影響資通系統機能運作，構成資通安全政策之威脅。

十三、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。

十四、第二類證券商：係指非屬第一類證券商之證券商。

十五、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 資訊服務供應商遴選原則

一、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。

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)。

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. 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. 對資訊服務供應商之稽核權條款。
9. 合約轉讓或同意分包之規範。
10. 保密義務條款。
11. 罰則與損害賠償條款。
12. 爭議處理程序。
13. 違約處理條款。
14. 合約終止規範。
15. 合約終止後之處理。
16. 保固。
17. 權利及責任。

(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. 資訊服務供應商應遵循之資安要求事項、個人資料保護法與其他相關法規遵循與保密義務。

2. 資訊服務供應商應提供安全性檢測證明 (如行動應用程式資安檢測、源碼檢測、弱點掃描等)，並應確保交付之系統或程式無惡意程式及後門程式，其放置於網際網路之程式應通過程式碼掃描或黑箱測試。

3. 資訊服務供應商揭露第三方程式元件之來源與授權證明。

4. 資訊服務供應商處理證券商委託服務各項範圍資訊，能於證券商要求期限內提供。

5. 資通(訊)服務供應商於處理證券商資料應有明確區隔，並應予以加密保護。

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。

二、證券商應於簽約程序中確認資訊服務供應商保密切結事宜。

三、資訊服務供應商發生資安事件致證券商受到影響時，資訊服務供應商的處置程序及責任。

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。

二、證券商應對資訊服務供應商人員電腦通行使用權利進行適當控管；證券商應於委外合約期間結束後立即收回該項權利。

三、資訊服務供應商之保護責任：

(一)資訊服務供應商對於資訊之存取控制措施不得低於與證券商協議之規定及「營業秘密法」第七條第一項及第二項。

(二)資訊服務供應商應保證該資訊資產、營業秘密之使用，僅限於原申請範圍。

四、證券商應管理並至少每半年一次檢視資訊服務供應商之駐點作業、實體與邏輯存取權限，包含作業地點的配置、網路設備及主機連線、電腦的使用、電腦機房的進出、門禁臨時卡的申請等。

第六條 服務變更管理

資訊服務供應商服務內容變更，證券商之專案負責人應重新對資訊服務供應商變更之服務內容進行風險評估。

第七條 審核資訊服務供應商服務

一、 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、 證券商資訊委外作業如為一年期以上，資訊服務供應商應定期或每年至少一次提交服務水準報告，交由證券商審核備查。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。

第八條 證券商與資訊服務供應商終止、解除、結束資訊委外關係

證券商與資訊服務供應商之資訊委外關係於終止、解除或結束後，證券商應立即停止資訊服務供應商所涉及之實體與邏輯存取權限，並回收或請資訊服務供應商銷毀屬於組織之資訊資產、營業秘密，必要時可要求資訊服務供應商出具銷毀證明，另要求：

(一)證券商若決定將產品或服務由原資訊服務供應商移轉回證券商或至其他資訊服務供應商時，原資訊服務供應商與證券商雙方應遵循之資安要求事項。

(二)資訊服務供應商於資訊委外關係所涉及證券商之資訊資產，應於委外關係終止、解除或結束時完整歸還、確保銷毀或轉交予其他資訊服務供應商。

(三)證券商與資訊服務供應商之資訊委外關係於終止、解除或結束後，資訊服務供應商應持續遵守保密承諾。

(四)終止程序執行之時限。

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。