# 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

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

金融監督管理委員會 113 年 10 月 1 日金管證券字第 1130355627 號函准予備查

中華民國證券商業同業公會 113 年 10 月 7 日中證商業一字第 1130005103 號函公告實施

金融監督管理委員會 113 年 11 月 22 日金管證券字第 1130361930 號函准予備查

中華民國證券商業同業公會 113 年 11 月 27 日中證商業一字第1130006165號函公告實施

金融監督管理委員會 114 年 2 月 26 日金管證券字第1140331935號函准予備查

中華民國證券商業同業公會 114 年 3 月 3 日中證商業一字第1140000918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、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。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、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。

十、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。

十一、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。

十二、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。

十三、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。

十四、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。

十五、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。

十六、第二類證券商：係指非屬第一類證券商之證券商。

十七、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

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。

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.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.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.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。

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。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 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、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。

三、證券商資訊委外作業如涉及核心資通系統與資通服務，資訊服務供應商應定期提供資通系統與資通服務之回復計畫，回復計畫可以災難復原計畫、備援演練、營運持續計畫等形式呈現。

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。