Deloitte.

勤業眾信

證券暨期貨市場各服務事業供應鏈風險管理參考指引說明

Deloitte Risk Advisory、2022/04

Agenda

- 目的 & 總說明
- 條文說明
- 問題與討論

目的 & 總說明

目的 & 總說明

目的

為協助證券商、期貨商及投信投顧業者安全有效的管理資訊服務供應鏈風險，依據金融監督管理委員會「金融資安行動方案」強化金融業資通系統供應商及跨機構資訊服務之風險評估及稽核等管理機制之議題，特針對資通系統之資訊服務供應商遴選、資訊服務供應商管理以及資訊服務供應商終止與解除等議題，擬定供應鏈風險管理參考指引。

總說明

本參考指引係參考資通安全管理法、營業秘密法、政府資訊作業委外資安參考指引、金融機構作業委託他人處理內部作業制度及程序辦法、證券暨期貨市場各服務事業建立內部控制制度處理準則、證券商內部控制制度標準規範、期貨商內部控制制度標準規範、建立證券商資通安全檢查機制、建立期貨商資通安全檢查機制、中華民國證券商業同業公會新興科技資訊安全自律規範、證券商資訊委外契約注意事項參考守則等，經蒐集實務做法併邀集業者共同研議相關參考指引，以維護供應鏈風險管理資訊安全。

本指引共十三條，其要點如下：

一、 說明本指引之立法意旨。(第一條)

二、 說明本指引之適用範圍。(第二條)

三、 明訂本指引提及之名詞解釋。(第三條)

四、 明定資訊服務供應商遴選要求。(第四條至第六條)

五、 明定資訊服務供應商合約要求與服務期間之資安管理。(第七條至第十二條)

六、 明定資訊服務供應商服務終止與解除要求。(第十三條)

七、 說明本指引之參考文獻。

條文說明

概要說明

供應鏈風險管理參考指引適用對象

適用對象		
本指引適用對象包含證券商、期貨商、證券投資信託事業及證券投資顧問事業		
適用對象分類		
第一類	**第二類**	**外資**
（一）「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組織。 （二）「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。 （三）「建立期貨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、第三級期貨商。	非屬第一類範圍之組織。	外資集團在台子公司或分公司，其資安管理政策由外國母公司或總公司控制與建置者，如其母公司或總公司已建置或設立相關控制措施，且有較佳之規範，則從其規範；若無，則應遵循本國法令法規規範。

「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36條之2條文

一、 證券商實收資本額達新臺幣(以下同)一百億元以上或電子下單達一定比率；電子下單一定比率為網際網路下單加計電子式專屬線路下單(Direct Market Access，以下簡稱DMA)成交金額達公司成交金額百分之六十，經紀業務成交金額市占率達全市場百分之二，且自然人客戶數達公司客戶數百分之五十者。

二、 期貨商實收資本額達二十億元以上，且電子下單達一定比率；電子下單一定比率為網際網路下單加計DMA下單成交口數達公司成交口數百分之六十，經紀業務成交口數市占率達全市場百分之二，且自然人客戶數達公司客戶數百分之五十者。

三、 證券投資信託事業及證券投資顧問事業前一年度月平均境內外管理資產規模達六千億元以上者。

註1：參考資料為「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36條之2條文

註2：以下參考指引如無特別說明，皆為第一類及第二類組織應遵循之事項。

供應鏈風險管理週期

供應商遴選	供應商合約	供應商管理	供應商服務終止與解除
第四~六條	第七條	第八~十二條	第十三條
• 應評估資訊服務供應商作業能力，採取適當風險管控措施。 • 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。 • 集中度過高疑慮者，資訊服務供應商選定，應執行風險評估，評估結果應提報總經理層級並取得同意。 • 應有評選資訊服務供應商之準則，並留存相關文件紀錄備查。 • 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。 • 大型採購案應要求資訊服務供應商提供建議書，並確認建議書內容是否符合採購需求(第一類)	• 應協議並確定合約內容。	• 存取管理。 • 存取風險之辨識。 • 安全管理。 ◆ 集中度過高者應造冊以利管理。 ◆ 外資組織因內部分工將資訊委外至總公司、國外分支機構境外處理者應辦理項目。 ◆ 應管理並定期(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等。 ◆ 應將進駐於組織內之資訊服務供應商人員納入組織安全管理。 ◆ 應要求資訊服務供應商提供駐點人員清單。 • 服務變更管理。 • 供應商服務審核。 ◆ 稽核權行使。 ◆ 服務水準報告。	• 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。 • 應定義資訊委外關係終止執行之服務持續性要求事項。

此處為概要，詳細條文會於後續章節說明

條文說明

供應鏈風險管理參考指引-第四、五、六條

條文	內容
第四條	（資訊服務供應商評選） 一、組織應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；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，應執行風險評估，評估結果應提報總經理層級並取得同意。 二、組織評選資訊服務供應商之準則應包含下列各項，並留存相關文件紀錄備查： （一）資訊服務供應商之財務能力、管理能力、專業能力、維運能力及經驗實績。 （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(提供管理措施與執行情形說明)或通過第三方驗證(例如：CSA STAR、ISO 27017、ISO 27018)。 （三）第一類組織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(例如：ISO 27001)。
第五條	（保密協議書準備與簽訂） 當選商過程中存在資訊資產交換，組織應備妥保密協議書，並於交換與採購產品或服務相關之機敏性資訊前簽署。
第六條	（建議書徵求文件） 第一類組織對其所規定之大型採購案應要求資訊服務供應商提供建議書，並確認建議書內容是否符合採購需求。建議書中應包含下列項目： 一、組織採購需求產品/服務。 二、資訊服務供應商應符合之組織資安要求(例如：組織資安政策)。 三、資訊服務供應商之專案管理能力。

集中度過高: 此為主管機關要求，考量之前發生撞庫事件，業者選商應考量供應商集中度，可能事件發生時供應商資源調配與即時因應是否充足。

供應鏈風險管理參考指引-第七條(1/2)

條文	內容
第七條	（資訊服務供應商合約安全控管） 一、組織選定資訊服務供應商後，雙方應協議並確定合約內容。合約應包含下列各項： （一）合約基本要求 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.資通安全事件處置程序（含當發生資安事故時，受託廠商應主動、即時通知委託人）。 8.對資訊服務供應商之稽核權條款（含受委託機構就受託事項範圍，同意主管機關及中央銀行得取得相關資料或報告，及進行金融檢查，或得命令其於限期內提供相關資料或報告）。 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（含合約終止之重大事由，應包括主管機關通知依契約終止或解約之條款）。 15.合約終止後之處理。 16.保固。 17.權利及責任。

供應鏈風險管理參考指引-第七條(2/2)

條文	內容
第七條	（二）資訊服務供應商服務與產品要求 1.組織應載明資訊委外服務或產品之智慧財產權。 2.組織應載明是否允許資訊委外服務或產品分包予其他供應商，如允許，資訊服務供應商應提供分包計畫並經組織同意後始可進行。 3.第一類組織應載明採購之服務與產品於規劃設計時納入資通安全機制(Security by design)之要求。資通安全機制設計應包含服務與產品之機敏資料保護、授權與認證、安全性更新等。 4.第一類組織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）服務範圍涉及資通系統開發、維護與監控，組織應載明要求資訊服務供應商應遵循「證券暨期貨市場各服務事業資通系統安全防護基準參考指引」辦理。 （四）服務範圍涉及使用雲端運算服務，組織應載明要求資訊服務供應商應遵循「證券期貨市場相關公會新興科技資訊安全管控指引」辦理。 （五）資訊服務供應商資安要求 1.組織應載明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.組織應載明資訊委外作業範圍內，組織與資訊服務供應商雙方之資安角色與責任。 3.組織應載明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。 4.組織應載明要求資訊服務供應商揭露第三方程式元件之來源與授權證明。 5.組織應載明要求資訊服務供應商處理之組織委託服務各項範圍資訊，能於組織要求期限內提供。 6.組織應載明服務變更或資通安全事件之資訊服務供應商處置程序。 7.第一類組織應載明資訊委外作業範圍內，組織之資訊應與資訊服務供應商及其處理其他組織之資料有明確區隔，並應予以加密保護。 8.第一類組織應載明資訊服務供應商應取得之資安及品質證照。 二、組織應於簽約程序中確認資訊服務供應商保密切結事宜之完成度。

供應鏈風險管理參考指引-第八、九、十條

條文	內容
第八條	(資訊服務供應商存取管理) 一、組織之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，並經組織權限申請程序申請，始可賦予資訊服務供應商存取組織之資訊資產權限，以保護組織資訊資產。 二、組織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；組織應於委外期間結束後立即收回該項權利。
第九條	(資訊服務供應商存取風險之辨識) 資訊服務供應商需存取組織資訊資產、營業秘密時，專案負責人應考慮以下各項因素評估風險： 一、應符合法規或主管機關之規定，並依據委託事項所需以最小權限及資訊最小揭露原則進行安全管控設計。 二、組織資訊資產與營業秘密之存取控管，應考慮取得、使用、保管、查詢、修改、調整、銷毀之管控措施。 三、資訊服務供應商之保護責任： （一）組織應要求資訊服務供應商對於資訊之存取控制措施不得低於與組織協議之規定，及「營業秘密法」第七條第一項及第二項。 （二）組織應要求資訊服務供應商保證該資訊資產、營業秘密之使用，僅限於原申請範圍。
第十條	(安全管理) 組織於專案進行中應注意下列事項： 一、資訊服務供應商集中度過高者應造冊以利管理，並確認其執行資安事件識別、回應和緩解風險之機制。 二、外資組織因內部分工將資訊委外至總公司、國外分支機構境外處理者（以下稱受委託機構），應依以下辦理： （一）組織應充分瞭解及掌握受委託機構對客戶資訊之蒐集、處理、利用、國際傳輸及控管情形。 （二）組織提供予受委託機構之客戶資訊僅限與受託事項直接相關之必要資訊。 （三）組織應要求受委託機構確實遵守以下事項： 1.組織之客戶資訊僅限由受委託機構之獲授權人員於受託事項範圍內使用及處理。 2.組織之客戶資訊應與受委託機構及其處理其他機構之資料有明確區隔。 3.受委託機構處理之組織客戶資訊應能及時提供予組織。 （四）如有國際傳輸機敏資料，組織應建立加密傳輸機制且應就受委託機構對客戶資訊之蒐集、處理、利用、國際傳輸及控管情形確認符合我國個人資料保護法相關規定，傳輸前應取得當事人授權且不違反主管機關對國際傳輸之限制，並留存完整稽核紀錄。 三、組織應管理並定期(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、電腦與電話的使用、電腦機房的進出、門禁臨時卡的申請等。 四、組織應將進駐於組織內之資訊服務供應商人員納入組織安全管理，如欲使用內部網路資源時，應有安全管制措施（如透過轉接方式或另建網路者，應與內部網路作實體隔離）。 五、組織應要求資訊服務供應商提供駐點人員清單。

供應鏈風險管理參考指引-第十一、十二條

條文	內容
第十一條	(服務變更管理) 資訊服務供應商服務內容變更若對資訊安全有所衝擊時，組織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。(例如：機密性、完整性、可用性之衝擊分析、ISO 27001 風險評鑑)
第十二條	(資訊服務供應商服務審核) 一、組織於資訊委外期間應定期(每年至少一次)與認為有進行監控與稽核之必要時，組織或組織授權之第三方得對資訊服務供應商進行稽核。 二、組織資訊委外作業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，交由組織審核備查。

供應鏈風險管理參考指引-第十三條

條文	內容
第十三條	(專案終止、解除或結束後) 一、於專案終止、解除或結束後，組織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。 二、組織應定義資訊委外關係終止執行之服務持續性要求事項，其應包含下列各項： （一）若決定將產品或服務由原資訊服務供應商移轉回組織或至其他資訊服務供應商時，原資訊服務供應商與組織雙方應遵循之資安要求事項。 （二）明列使用於資訊委外專案中所涉及組織擁有之資訊資產，以利於專案終止時得以完整歸還於組織、確保銷毀或轉交予其他資訊服務供應商。 （三）承上，明列歸還、轉交或銷毀之程序，必要時要求其落實之證明文件。 （四）當資訊委外關係終止後，保密承諾之持續性。 （五）終止程序執行之時限。

問題與討論

Deloitte.

勤業眾信