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
部分條文修正條文對照表

修正條文	現行條文	說明
第一條（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**(以下稱金管會)**「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。	第一條（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。	一、為指引說明簡要與便利，爰增文字說明。
第二條（適用範圍與對象） 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。適用對象分為以下兩類說明： 一、第一類： 「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。	第二條（適用範圍與對象） 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。適用對象分為以下兩類說明： 一、第一類： **(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**	一、依金管證券字第1120385996號函令，有關設立資訊安全長條件調整，刪除(二)、(三)分類之條款。

修正條文	現行條文	說明
	貨商。	
四、金管會周邊相關單位提供之資訊服務與受相關主管機關監督之金融資訊交換基礎設施(如 SWIFT)非屬適用範圍。 **五**、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。	**四**、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。	二、參照「金融機構作業委託他人處理內部作業制度及程序辦法」相關問題適用解說問答集，四、交易所、集中清算、結算與交割機構及其成員間之清算、結算及交割。五、受相關主管機關監督之全球金融資訊交換基礎設施(如SWIFT)之情形非屬金融機構作業委託他人處理之範疇，考量情形適用資通系統與服務供應鏈風險管理，爰增第四項。
第三條（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**、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：**	第三條（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**、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。 （以下略。）	一、第四、五項參酌金融資安行動方案執行表，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，納入供應鏈風險管理參考指引，並參酌現行「資通系統安全防護基準參考指引」與「資訊作業韌性參考指引」，增列核心業務及核心系統名詞定義。 二、第七項參照重大性作業委託雲端服務業者處理應注意事項，修正雲端服務名詞定義。

修正條文	現行條文	說明
（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。** （以下略。）		
第四條（資訊服務供應商評選） 一、組織應**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**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**	第四條（資訊服務供應商評選） 一、組織應**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：「資訊委外之資安應注意事項檢查表」；**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**	一、第一項第一款至第六款，參酌中華民國銀行商業同業公會全國聯合會「金融機構資通系統與服務供應鏈風險管理規範」，爰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，組織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。

修正條文	現行條文	說明
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組織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組織營運持續與資通安全事件處理之目標與要求。** 二、**組織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，相關事項請參閱附件：「資訊委外之資安應注意事項檢查表」。 **三、組織資訊委外業務項目屬**	**供應商選定，應執行風險評估**，評估結果應提報適當管理層級並取得同意。	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，調整敘述。 五、第一項第五款，考量地緣政治要求，說明組織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，參酌金融資安行動方案執行表，說明組織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組織資訊安全要求，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、第三項參酌中華民國

修正條文	現行條文	說明
核心系統，組織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**、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）雲端服務供應商應具備完善之雲端資通安全管理措施(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)。	**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)。	銀行商業同業公會全國聯合會「金融機構資通系統與服務供應鏈風險管理規範」，說明組織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三條名詞修正，修正雲端服務名詞。
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： (一略。) 二、資訊服務供應商應符合之組織資安要求**與服務水準要求**(例如：組織資安政策)。	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： (一略。) 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）。	一、配合第四條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。

修正條文	現行條文	說明
(以下略。)	(以下略。)	
第七條(資訊服務供應商合約安全控管) 一、組織與資訊服務供應商，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.至6.略。) 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**或於時限要求內**通知委託人)。 (8.至17.略。) (二)資訊服務供應商服務與產品要求 (1.至2.略。) **3.組織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。 5.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。 (四)服務範圍涉及使用雲端	第七條(資訊服務供應商合約安全控管) 一、組織與資訊服務供應商，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.至6.略。) 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.至17.略。) (二)資訊服務供應商服務與產品要求 (1.至2.略。) 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。 (四)服務範圍涉及使用雲端	一、第一項第一款第七目，考量組織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組織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、配合第三條名詞修

修正條文	現行條文	說明
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。	**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。	正，修正雲端服務名詞。
(五)資訊服務供應商資安要求 (1.至7.略。) **8.組織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。** 9.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。 10.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。 (以下略。)	(五)資訊服務供應商資安要求 (1.至7.略。) 8.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。 9.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。 (以下略。)	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」與「建立期貨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八目。
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**通**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。	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。	一、配合第三條名詞定義，修正文字。

修正條文	現行條文	說明
(以下略。)	(以下略。)	
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**通**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)	一、配合第三條名詞定義，修正文字。
第十二條(資訊服務供應商服務審核**與稽核**) 一、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。 二、**組織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。** 三、組織於資訊委外期間應定期**或於知悉資訊服務供應商發生可能影響受託業務之資通安全事件時**，組織或組織授權之第三方**以稽核或其他適當方式確認受託業務之執行情形**。	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。	一、參酌金融資安行動方案執行表，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、調整編號，原第二項調整為第一項。 三、第二項參酌中華民國銀行商業同業公會全國聯合會「金融機構資通系統與服務供應鏈風險管理規範」，說明組織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，爰增列第二項。 四、調整編號，原第一項調整為第三項。 組織應依據第二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

修正條文	現行條文	說明
		訊服務供應商發生可能影響受託業務之資通安全事件。 資通安全稽核作業得自行辦理或委託獨立第三方執行，或以其他適當方式（如：審查由資訊服務供應商提供公正第三方之驗證報告 ISO/CNS 27001 資訊安全管理系統標準及其他具有同等或以上效果之標準)監督資訊服務供應商遵循組織資通安全要求，爰增列第三項。