證券暨期貨市場各服務事業供應鏈風險管理參考指引
第四條、第七條、第十條修正草案對照表

修正名稱	現行名稱	說明
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	證券暨期貨市場各服務事業供應鏈風險管理參考指引	本指引係作為資通系統之建置、維運或資通服務提供之參考，為明確適用範圍，爰修正本指引名稱。
修正條文	**現行條文**	**說明**
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。 （以下略。）	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。 （以下略。）	一、考量供應商作業能力僅為組織資訊業務委外之風險評估項目之一，爰增列評估項目。 二、考量現今業者資訊委外作業量大幅增加，作業風險亦大幅提升，組織應針對資訊委外各階段進行資安風險因素評估及執行相對應管控措施，爰依據「金融機構資訊委外之資安應注意事項」，增列附件「資訊委外之資安應注意事項」，供組織進行委外各階段應注意事項之檢核。 三、考量各組織環境不同，風險評估結果提報層級可依組織訂定，爰酌修文字。

修正條文	現行條文	說明
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. 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.至17.略。) ((二）至（四）略。） （五）資訊服務供應商資安要求 (1.至6.略。) 7.組織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，立即通知組織並採取相關補救措施。 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	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.至17.略。) ((二）至（四）略。） （五）資訊服務供應商資安要求 (1.至6.略。) 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	一、考量合約制定與供應商選擇，二項作業得同時運作，爰酌修文字。 二、為了確保資訊委外服務的品質與可靠性，降低組織風險，爰增列服務期間為一年期以上，供應商定期提交服務水準報告。 三、考量近期業者發生委外資訊廠商應用系統錯誤，造成交易系統故障，建議業者強化管控，爰增列第7點。 四、編號調整。

修正條文	現行條文	說明
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。	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。	
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，應確認其執行資安事件識別、回應和緩解風險之機制。 （以下略。）	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。 （以下略。）	考量各組織環境不同，資訊服務供應商集中度過高者之管理方式由組織訂定，爰酌修文字。