銀行全面性洗錢及資恐風險評估作業之實務參考做法

金融監督管理委員會 107 年 10 月 18 日
金管銀法字第 10701166430 號函洽悉

一、緣起

全面性洗錢及資恐風險評估作業係透過辨識所面臨之一般性及特定洗錢、資恐風險，評估銀行之相關風險管控措施，以瞭解剩餘風險(residual risk) 之機制，俾進一步採取適當措施，以有效管理洗錢及資恐風險。

全面性洗錢及資恐風險評估結果有助於檢視銀行的資源配置與管控措施是否適切，以及有無調整必要，也呼應 FATF 在 2012 年新頒布之 40 項建議，強調在資源有限性下，以「風險為基礎」在防制洗錢與打擊資恐工作上的重要性。

就全面性洗錢及資恐風險評估作業，銀行應依據金融監督管理委員會（以下簡稱金管會）「銀行業及電子支付機構電子票證發行機構防制洗錢及打擊資恐內部控制要點」、本會「銀行防制洗錢及打擊資恐注意事項範本」及其附件「銀行評估洗錢及資恐風險及訂定相關防制計畫指引」等規定辦理之。

本文件係協助銀行就辨識、評估、執行其全面性洗錢及資恐風險評估作業，提供實務執行說明與做法供會員銀行參考，非屬本會制定之自律規範，不具有實質拘束力。會員銀行在符合現行防制洗錢及打擊資恐相關規範下，亦得按個別公司業務特性、風險程度及集團政策，自行辦理其風險評估作業並製作風險評估報告。本文件亦提供將國家風險評估 (National Risk Assessment, NRA) 與產業風險評估 (Sectoral Risk Assessment, SRA) 之方法論與結果，納入銀行全面性洗錢及資恐風險評估作業之參考。

二、全面性洗錢及資恐風險評估作業之原則性說明

（一）執行全面性洗錢及資恐風險評估作業有許多不同的方法論，

銀行執行風險評估作業應依照各自業務之性質、規模、多元性、複雜度、全球化程度等指標而採用最適宜之方法論，無法以單一方法論套用於所有銀行。

銀行兼營其他業務時，應將兼營業務納入全面性洗錢及資恐風險評估作業之範圍，惟評估方式仍應依據銀行各自之方法論；以單一兼營業務為評估之對象或出具單一兼營業務之評估報告結果非為必要。

（二）對較小型或業務較單純之銀行，較為簡化之風險評估即足夠；惟對於產品與服務較複雜之銀行、有多家分公司（或子公司）提供廣泛多樣之產品、或其客戶群較多元者，則需進行較高度的風險評估程序。

（三）銀行開始執行定期之風險評估作業前應訂定明確之評估方法，並於風險評估結果報告中明確說明其風險評估方法論。

（四）風險評估方法論應包括評估之因素、評分或評級標準（包含所使用之權重或矩陣）、人工調整評分之其他因素、理由或特定參數等。

（五）風險評估機制應與其規模、複雜度及業務性質等相當，並須納入所有國外分公司（或子公司）為全面性洗錢及資恐風險評估之範疇。

若在臺之外國金融機構集團分公司或子公司，其母集團之風險評估作業不低於我國規定且不違反我國法規情形、評估作業涵蓋在臺分公司或子公司，且評估結果業已適切地辨識在臺分公司或子公司之風險者，在臺分公司或子公司得援用其母集團之風險評估方法論及結果。

（六）辦理風險評估作業得輔以內部及外部來源取得之資訊，如銀行內部管理階層（如事業單位主管、客戶關係經理等）所提供的管理報告、國際防制洗錢組織與他國所發布之防制洗錢及打擊資恐相關報告、或各主管機關發布之洗錢及資恐風險

資訊(如我國國家風險評估報告、產業或部門風險評估報告)等，透過量化資訊輔以質化評估結果以進行之。

（七）風險評估頻率由各銀行自行決定，未有強制規定。而本會防制洗錢及打擊資恐注意事項範本之問答集建議銀行應每 1-1.5 年間至少辦理一次全面性洗錢及資恐風險評估作業。

（八）除定期評估外，銀行應於內外部環境有重大改變時(如發生重大事件、管理及營運上有重大發展、或有相關新威脅產生)，重新進行評估作業。

（九）銀行應定期檢視並檢討風險評估方法論，以確保風險評估方法均考量內部及外部變動之影響。

變更風險評估方法論時，建議考量跨年度間之可比較性，並應清楚說明方法論改變之理由。

（十）風險評估作業與結果應予以適當記錄、保存，且評估過程中應依內部流程與銀行內部高階管理階層充分溝通。

三、全面性洗錢及資恐風險評估作業之流程

實務上，全面性洗錢及資恐風險評估作業包含下列主要流程：

（一）風險評估作業之設計及規劃

（二）風險評估之資料蒐集

（三）風險計分及評級作業

（四）風險等級審核作業

（五）最終風險評等之檢閱及相關單位之核准程序

（六）最終風險評估結果依內部流程提供予相關單位或高階管理階層

四、全面性洗錢及資恐風險評估作業之評估方式

風險評估作業得先辨識全行之固有風險，評估管控環境、風險抵減措施之有效性，再評估剩餘風險，可依據下列階段進行之：

（一）辨識全行之固有風險：固有風險係指未考慮任何控制措施

下，銀行面臨被利用於洗錢及資恐之風險。

1、決定固有風險因素之類型、權重或評級依據。

（1）固有風險因素至少應包含客戶、地域、產品與服務，以及交易或服務管道。

（2）權重或評級之依據，得考慮風險因素之不同面向及其特性所產生的風險與控制對該銀行可能產生的影響、或以平均、依風險基礎方法等原則以決定之。

2、定義各固有風險因素類型之細部因子或評估指標，並依評估指標蒐集相關資料。

固有風險因素類型之指標及資料蒐集舉例如下：

（1）客戶風險：可考量客戶類型、地域、職業或產業等指標，並蒐集各指標之客戶數等相關資料。

（2）地域風險：蒐集各地域風險等級之客戶數或交易量等相關資料。

（3）產品與服務：可根據與現金關聯程度、是否具匿名效果、是否具金錢或價值移轉能力、收到款項是否可來自於未知或無關係之第三者等指標，並蒐集各指標之業務規模或交易量等相關資料。

（4）交易或服務管道：可考量是否透過非面對面開戶、是否透過非面對面交易及是否涉及第三方或中介者等指標，並蒐集各指標之業務規模或交易量等相關資料。

3、上開資料得透過資訊系統依部門別或業務線蒐集，並對所蒐集之資料適度地確認其正確性。

4、對各固有風險評估指標評分或評級，據以計算各固有風險類型及總固有風險之得分及評等。

5、風險評估之設計及執行，得適度納入主管機關發布之風險評估報告中與金融機構業務相關者。例如：參考國家洗錢及資恐風險評估之方法論及結果，作為設計固有風險評估因素或

指標之參考依據之一。以 2018 年所公布之我國「國家洗錢及資恐風險評估報告」為例，其對各產業及部門之洗錢與資恐弱點評估，風險因素類型包括固有特徵、產品和服務的本質、業務關係的本質、產業活動的地理範圍及產品和服務提供的管道等五項。

（二）評估管控環境、風險抵減措施（包含設計及執行效能）之有效性

1、管控措施係指包含防止洗錢風險發生並確保及時辨識潛在風險之政策、程序及行動、以及確保持續遵循相關法規之機制、作為等。

2、一般實務上，評估管控環境、風險抵減措施之有效性包含評估防制洗錢與打擊資恐制度之設計、政策之遵循程度、執行管控之程度與有效性、作業之自動化程度、以及內外部查核與測試之結果等。

3、定義管控措施之類型及權重或評級依據，實務上主要之管控措施包含如防制洗錢之公司治理、確認客戶身分、姓名及名稱檢核、帳戶及交易之持續監控、一定金額以上通貨交易申報、疑似洗錢或資恐交易申報、持續性員工訓練計畫、獨立稽核等各項防制洗錢及打擊資恐計畫應管控之面向。

4、辨識各類型之細部管控措施，並定義管控措施有效性等級（即訂定評等表）：可依已明確定義之評分標準或可採質化評等（如：強、滿意、待改善、欠佳等）或數值評分以進行評估。

評估管控環境及風險抵減措施時，考量的因素包括控管是否到位、控制措施是否有效。

就各類型管控措施之評分標準，當符合下列情形時，得評定為最完善之控管等級：

（1）完全遵循並實施相關政策及程序

（2）實施自動化的管控措施

（3）無重大查核或稽核缺失

5、發送問卷、自行查核或資料蒐集等方式請相關受評單位就各管控措施、依據執行與落實的程度評估自身管控之有效性。

6、依自評或資料蒐集結果計算各類管控措施之總分及評等或評級，並視需要請受評單位提供佐證或進行資料驗證，以及於必要時調整特定項目分數或評等。

7、銀行得考量自身業務性質，就國家風險評估或產業風險評估中得適用之管控措施項目或所辨識之高風險結果，納入銀行各自之管控作業、政策、或全面性洗錢及資恐風險評估作業。例如得參考國家風險評估結果中高洗錢威脅之犯罪，納入銀行的控管作業，並於銀行的風險評估作業中，評估管控的有效性：

（1）如執行客戶審查時，依據風險基礎方法，透過姓名檢核作業以辨識客戶是否涉及高洗錢威脅犯罪相關之負面消息。

（2）就高洗錢及資恐風險犯罪，依據主管機關所設立之預警指標，篩選異常交易帳戶。

（3）應對執行防制洗錢與打擊資恐相關人員進行持續性教育訓練，以反映當前的法規、業務需求及洗錢與資恐的發展趨勢，並使該等人員均能意識到與其作業相關的洗錢與資恐風險。

（三）評估剩餘風險

經各項評估結果，決定風險控制抵減後剩餘風險程度，依據評估方法論決定剩餘風險之總評等。評等得為低、中等、中高及高風險。

五、全面性洗錢及資恐風險評估作業後，建議依據控制落實情形及剩餘風險程度制定改善計畫並採取如下措施：

（一）風險胃納係指銀行依其經營策略及目標，願意接受的風險種類及程度。

確認剩餘風險等級是否符合風險胃納，如否，應依據風險基礎方法之原則訂定降低風險之改善計畫。

（二）即便剩餘風險等級已符合風險胃納，得就風險控制抵減措施未予遵循、效能不足或風險控制抵減措施本身不足情形者，制定改善計畫以進行強化。

（三）改善計畫可包括政策面計畫及執行面計畫，並視改善計畫之性質而考量納入整體防制洗錢及打擊資恐計畫中。

（四）應注意改善計畫不影響當次風險評估之結果，僅可能依據實施之結果影響下次評估結果。

（五）評估結果應依內部流程由負責單位與各部門高階管理人員進行充分溝通。

（六）防制洗錢及打擊資恐專責主管應於完成或更新風險評估報告時，向董（理）事會及高階管理人員陳報全面性洗錢及資恐風險評估之結果，各項資源之運用以及所定改善措施之優先順序。

董（理）事會及高階管理人員應瞭解其洗錢及資恐風險、控管措施或執行效能不足之情形、以及應採取之改善計畫，並確保各項資源之運用以及所定改善措施之優先順序與所辨識之風險相符。

外國銀行在臺分公司就本文件關於董(理)事會之相關事項，由其總公司授權人員負責。

（七）應於完成或更新風險評估報告時，將風險評估報告送金管會備查。