劉曉軒
執行副總經理
勤業眾信風險管理諮詢(股)公司

毛武揚
副理
勤業眾信風險管理諮詢(股)公司

金融犯罪防制系列 - 金融機構應如何強化貪腐賄賂之風險管理

勤業眾信風險管理諮詢 (股) 公司 / 劉曉軒執行副總經理、毛武揚副理

隨著 2019 年成績揭曉，台灣防制洗錢與打擊資恐於亞太防制洗錢組織 (Asia-Pacific Group on Money Laundering, APG) 第三輪相互評鑑中取得「一般追蹤」的佳績，證明台灣公私部門的上下齊心，已獲得國際認可；然而對於金融機構而言，相關的挑戰尚未結束，參酌國際間大型外商銀行的發展趨勢，「防制洗錢與打擊資恐專責單位」將逐漸蛻變為「金融犯罪防制中心」，亦即舉凡洗錢犯罪、稅務犯罪、詐欺、制裁武擴以及貪腐賄賂均落於其範疇，此即為本系列文章所強調之重點，而本篇文章則是闡述金融機構如何面對反貪腐反賄賂 (Anti-Bribery and Corruption, ABC) 之議題，儘管它是一個存在已久的議題與風險，然而如何協助金融機構在風險管理上能夠更加落實並展現效率是在 2020 年的重要課題。

金融業反貪腐反賄賂之挑戰

儘管貪腐與賄賂議題是古今中外常見之弊病，惟國際間重視程度已日益提高，例如：金融同業的盡職調查問卷 (Wolfsberg CBDDQ) 已納入 ABC 部分，作為金融機構整體內部控制評估的一環，並要求機構進行全面之貪腐與賄賂風險評估，了解機構之固有風險與剩餘風險。

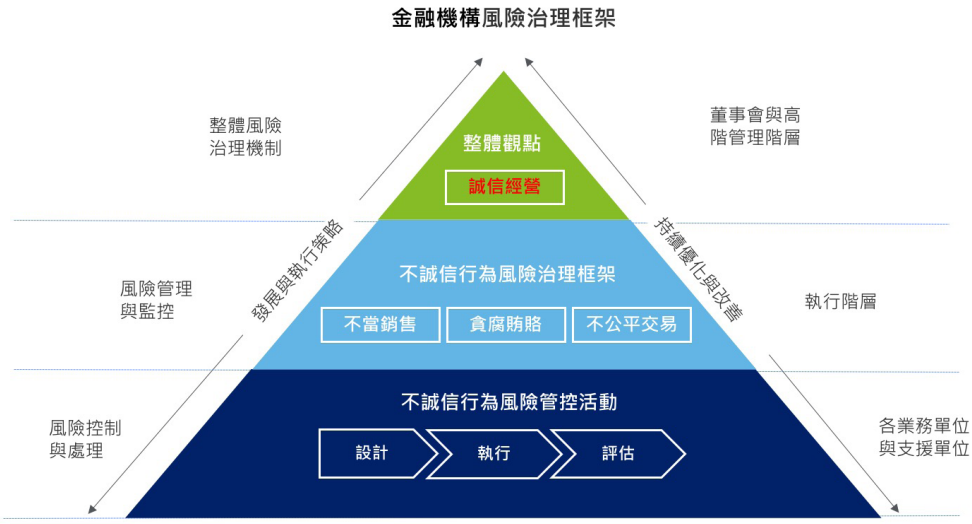
台灣近年亦已訂立相關法規，且規範對象不再僅限於公部門，例如：《上市上櫃公司誠信經營守則》，即明訂上市櫃公司應禁止一切不誠信之行為，並應進行風險評估，分析營業範圍內具較高不誠信行為風險之營業活動，包含行賄及收賄、提供非法政治獻金、不當慈善捐贈或贊助、提供或接受不合理禮物、款待或其他不正當利益、侵權行為、從事不公平競爭之行為與消費者保護等面向。

綜上所述，針對反貪腐反賄賂的觀點，國際標準與台灣法規要求均認為訂立相關政策與辦法僅是第一步，接下來如何要透過風險之辨識與評估，以風險為導向，擬定後續之管控措施，包含組織規劃、盡職調查及教育訓練等才是重點。

金融機構該如何因應內外之法規要求？

上述內外法規要求，不外乎要求金融機構進行「風險評估」，但對於金融機構而言風險評估絕不陌生，面對日益趨嚴之法令規範，包含：洗錢與資恐風險、法令遵循風險、資訊安全風險、網路犯罪風險等，金融機構均已建立一套嚴謹之風險評估與管理機制；惟未來面對接踵而至之風險議題，如：貪腐賄賂風險、詐欺風險、制裁風險等，倘若均以不同的方法論或風險管理框架進行風險評估，則不僅執行單位容易混淆，對於管理階層，亦將難以掌握其管理意涵。

有鑑於此，我們企圖建構統一的風險評估框架，面對非財務風險類型，以誠信經營之觀點出發，搭配不同的內容設計，讓評估方式得以貼合風險之本質以及業務之生命週期。



金融機構該如何執行貪腐賄賂風險評估？

金融機構在執行貪腐賄賂之風險評估執行步驟，與其他風險評估並無不同，主要係可分為以下五大步驟，以下將分敘各步驟之執行重點：

一、定義評估範圍

在具體辨識貪腐賄賂風險前，應掌握對應的產業流程或產品別、相關涉及部門以及相關的法令法規要求之後，再具體針對貪腐賄賂風險的本質進行盤點與辨識。言雖如此，惟金融機構部門龐多，組織分工精細，如評估對象多達數十個，將造成作業冗長進而失去效率，故建議以部門業務性質加以分類，將業務性質相近的部門進行綜合評估。以銀行業貪腐賄賂風險評估為例，建議可將受評對象初步分為業務單位、規劃單位與行政單位，主要係著眼於上述三類單位面臨之貪腐賄賂形式大相逕庭，故須加以區分。

二、評估固有風險

固有風險之評估係以金融機構各部門為單位，藉由分析該單位各項常見之貪腐賄賂手法發生之可能性與嚴重性，評估該單位之貪腐賄賂風險。而貪腐賄賂之固有風險應至少可分為六類：行賄與收賄、餽贈與招待、利益衝突、捐贈與贊助、政治獻金、交易特性。

上述風險分類應逐步展開更細部的風險指標，指標之選用應盡量以量化指標的概念蒐集數據，而非僅以詢問是否曾發生相關之風險事件，如此方能使風險評估更加細緻化，利於後續風險抵減計畫之研擬。例如：評估業務單位之行賄與收賄風險，可透過了解客戶之職行業或所屬國家，如屬於高貪腐賄賂風險之行業或國家，則較易發生貪腐賄賂之行為；評估業務單位之餽贈與招待風險，應可透過分析該公司 VIP 客戶之數量與獲利占比，了解機構潛在之餽贈與招待風險。

上述之指標屬於領先指標，透過相關數據之蒐集，機構得以了解其風險本質，並得以預測未來可能發生貪腐賄賂之部門與形式為何。反之，如果在固有風險階段，僅被動地了解過往的風險事件始末，作為風險評估的項目，則未來只要犯罪的手法有所改變，機構將無從偵測其潛在風險，導致風險評估失去風險偵測之作用。

三、評估管控有效性

金融機構針對管控措施的研擬，建議可搭配上述風險面向之分類，針對不同的風險本質，擬定不同的管控措施，同時須制訂共通的管控項目，例如：組織職掌與權責、吹哨者機制、獨立稽核審查等。此外，在設計管控活動時，可以「規劃」、「執行」、「評估」三階段擬定不同的管控點，並參酌國際組織之建議內容，如國際標準 ISO37001 等。

四、評估剩餘風險

由於係首次進行風險評估，在剩餘評估的部分，建議可以矩陣對應法進行，換言之，即為經過各項管控措施抵減後之風險即為剩餘風險，可透過矩陣對應法對應出各部門之剩餘風險等級。

五、發展風險抵減計畫

透過上述的剩餘風險評估，機構應可瞭解組織內高風險之業務為何，在本階段，即應針對高風險之業務進行針對性的管控強化，亦可參酌國際標準內容 ISO37001 擬定風險抵減計畫，此外，金融機構亦須多注意風險抵減的效果是否能夠讓貪腐與賄賂的剩餘風險回到金融機構可忍受的水準之內，才能確保其改善效度。

結語

金融機構進行風險評估之方式繁多，上述方法僅為眾多分析角度之一，其優點在於架構簡單明瞭，但整體風險評估活動之設計不僅可有效使各單位辨識出蘊藏之風險，並且得以主動偵測單位內部潛在的風險議題。「預防勝於治療」，這不僅是防疫的核心觀念，亦是風險評估的重要意涵。