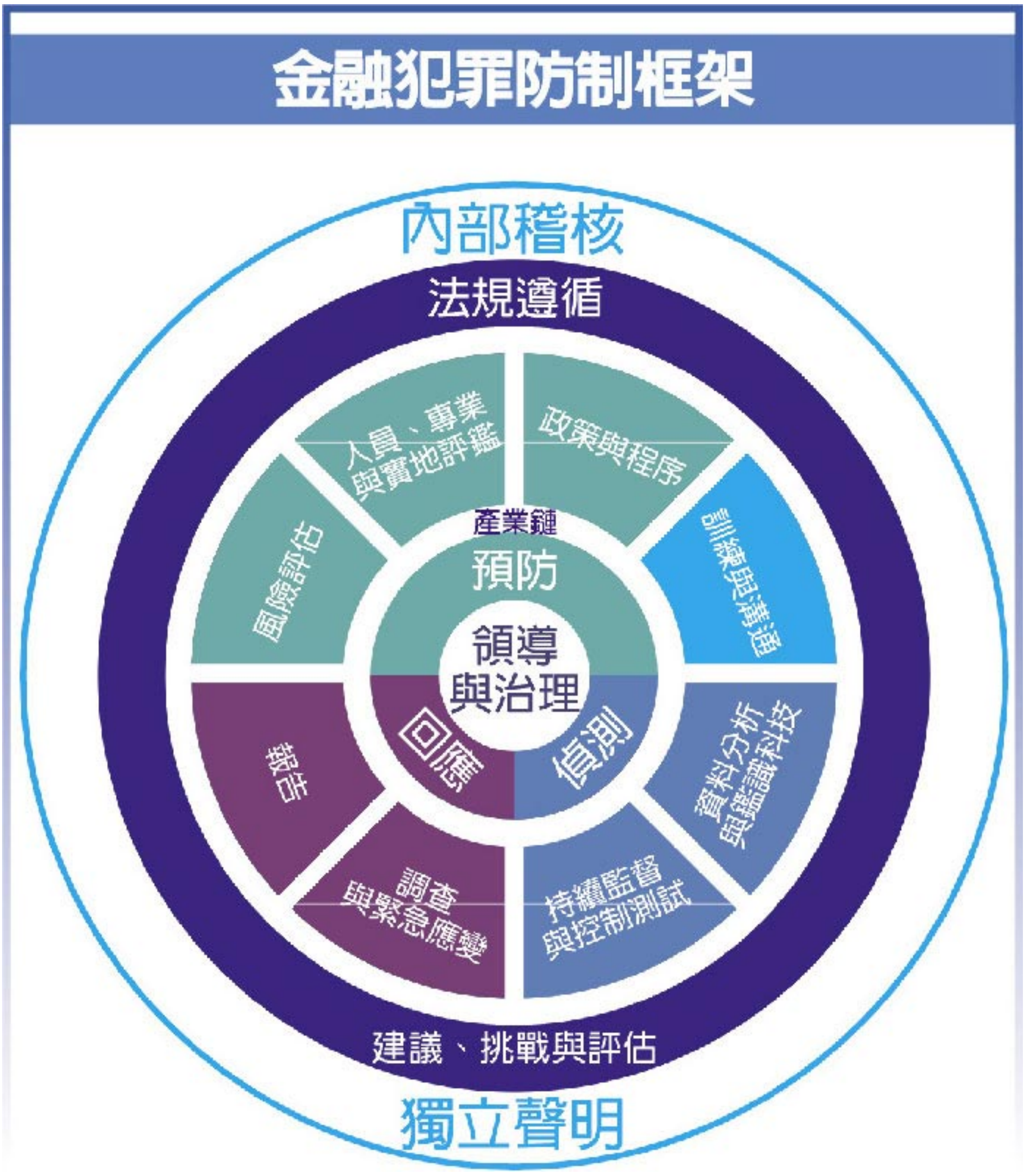
後巴拿馬文件時代... 金融犯罪與舞弊風險管理

04:10 2016/05/27 | 工商時報 | 朱成光



金融犯罪防制框架

內部控制制度與標準化管控程序

從最近新聞媒體中層出不窮的舞弊與不當行為事件，一再提醒我們：舞弊不是現在才存在，亦非特定產業才會存在舞弊風險；舞弊事件所帶來的潛在有形與無形損失金額，有急速攀升趨勢，影響與衝擊的產業，更是橫跨非金融產業，以及擁「金錢」於一身的金融機構。從舞弊風險預防角度以及風險管理的治本觀點來思考預防策略與方法前，必先了解舞弊形成的因素。

鑒於全球經濟景氣低迷，及環境因素刺激（Stimulus），例如：生活壓力或投機等因素，加上地球村經濟與網際網路普及的概念，金融機構面臨了比過去更多來自外部與內部的舞弊威脅，而這些威脅有可能是來自個人或團體組織，甚至涉及跨國組織或個人。無論是從作業風險管理（Operation Risk Management,ORM）或是反洗錢暨反資恐（Anti-Money Laundering and Counter Financing Terrors,AML-CFT）角度思考，舞弊威脅來源可能來自內部人員、內部人員勾串外部人員或是外部人員，例如：支持恐怖主義之人員。

後巴拿馬文件時代

的舞弊風險管理

巴拿馬文件事件的揭露，除提醒了世界各國政府對於境外公司（Offshore Banking Unit-OBU,OIU,ODU）之租稅與反避稅相關議題外，於反洗錢的法令遵循領域中，金融機構如何持續落實與遵循各國政府對於反洗錢相關要求。境外公司的存在，有著過去的歷史背景與需求，然而金融機構如何在現有經營環境的挑戰下，降低執行業務所衍生的潛在洗錢風險、法遵風險甚至於涉入金融犯罪的風險議題中，皆值得我們關注與思考。以巴拿馬文件披露的風險議題思考反洗錢法令遵循作業，這不僅是反洗錢作業中KYC（Know Your Customer）程序的要求，更需要金融機構於客戶實地評鑑（CDD,Customer Due

Diligence）的作業中投入更多的檢核資源，以落實風險管控的目標。巴拿馬文件的批露不只有衝擊金融機構的法規遵循或風險管理議題，對於非金融產業而言，採購及銷售的等交易中，如何進行交易對象實地評鑑與檢核，交易對手的透明程度，亦可能影響企業經營過程中存在虛假交易對象的風險。

金融科技

V.S.

金融犯罪

當前金融科技風潮席捲全球，當全球金融機構紛紛大舉投入與催生金融科技相關應用下，金融犯罪（Financial Crime）的風險已經悄悄大幅襲擊金融機構中。在金融科技應用的議題中，區塊鏈（Blockchain）、比特幣（Bitcoin）、P2P（PEER TO PEER）、網際網路（Internet）、行動式裝置與新型態交易模式，不僅僅影響金融產業過去的經營思維或型態，對於受高度監理的金融機構而言，其風險管理環境亦可能遭受極其快速的衝擊。這是因為，在前述金融科技的發展下，網路、資訊設備、移動式裝置、點對點交易、甚至於虛擬貨幣（比特幣，BTC）的流通下，從作業風險或是內部控制的角度而論，過去傳統風險管控機制已顯然不足以應付前述新興金融科技的應用。同時，該些新金融科技應用，從交易層面上，也極為容易產生資訊不對稱（亦可稱資訊差）的舞弊風險；何謂資訊不對稱的舞弊風險，簡單地說，就是實際交易其物流、金流與資訊流間，因交易頻率高、交易量大而經常性的存在差異時，風管或監督單位很難逐一比對與校驗，即可能給舞弊人員帶來舞弊的機會。此外，即便風管或監督單位發現疑似舞弊的可疑行為時，亦可能因為經常性存在差異而視為「理所當然」，如此一來，舞弊者即可能大膽遂行不當行為，而公司卻可能束手無策。

再者，當前金融機構可能面對的舞弊與不當行為，隨著科技應用日新月異，往往以資訊流或帳上交易資訊作為基礎，這已經涉及實際交易文件（實體的，書面的）可能與資訊系統平台（非實體的，資訊化的）間存在不一致之情形，更遑論交易數據量龐大到無法透過人工逐一檢視方式進行監督與管理。由此可知，目前金融機構在既有風險管理模式所著重之方向與金融科技之應用方向上正逐漸地產生落差，甚至存在資訊不對稱的風險。

舉例來說，倘若有內部或外部人員透過資訊系統弱點或是移動式裝置遂行不當行為時，金融機構是否有能力先「預防」、「偵測」與「回應」潛在舞弊或不當形為活動；當金融科技對於客戶資訊越來越保護（即越來越難以識別真正交易個體為何人），交易對象的真實性與識別性越加難以判斷，是否增加監管單位或風險管理單位的挑戰？金融機構與相關交易對象進行交易並提供服務，是否難以識別其背後的真正對象，以至於可能在不知情的情況下成為幫手？因此，伴隨金融科技所衍生的另外一項重大風險管理議題 - 金融犯罪油然而生。承前述，金融犯罪所涉及之領域廣泛且複雜：舞弊及不當行為領域、資訊科技（網際網路犯罪）領域，以及□融產品或服務之作業流程等三個議題。

金融犯罪

風險管理策略

風險管理從治理與文化做起。金融機構從管理當局推動公司治理文化，到各營運單位真正落實與尊重風險管控作為，透過預防、偵測與回應機制強化並落實金融機構中各產品及服務的內部控制設計與執行。舞弊風險管理區分成「預防」、「偵測」與「回應」等三大策略方向。因過去金融機構受高度監理，所有單位皆已設有內？控制制度與標準化管控程序，KPMG推薦金融機構從「偵測」出發。

舞弊偵測

由於金融機構業務特性，在舞弊偵測機制上，以關鍵風險指標（Key Risk Indicator）搭配鑑識資料分析技術（Forensic Data Analytics）為主，除分析過去歷史交易數據外，對於交易發生之持續性監控亦能發揮良好偵測效果。

何謂關鍵風險指標，簡單地說，透過檢視作業流程後，將作業流程中內部控制的偵測性控制點，進行分析與篩選，並透過資訊系統監控的規則（RULES）訂定、找尋出來後，透過數據資料分析工具，連接金融機構核心交易系統，以及時化或批次化之執行頻率進行交易分析，以達成持續性稽核與監控之目標，並找出潛在疑似不當行為交易後，進而評估是否為舞弊活動，亦或是內部控制缺失或弱點。

隨時代快速變遷，金融機構除改變思維，以金融科技之新思維進行經營轉型外，對於衍生的舞弊風險甚至於網路犯罪或金融犯罪等新議題，除透過鑑識科技之數據分析進行關鍵風險指標辨認、設定與持續監督等作為外，亦須思考相關法令遵循與風險管理於轉型期間之自我診斷、矯正及應變作為。（本文作者為安侯企業管理股份有限公司鑑識會計服務朱成光執行副總經理）

#金融科技 #科技

發表意見