

監理科技發展契機及風險摘譯

本公司國關室翻譯

- 壹、導言
- 貳、監理資料檢視
- 參、監理程序
- 肆、採用監理科技之風險及挑戰
- 伍、小結

壹、導言

監理機構自核發金融機構執照至法規執行，均需仰賴各項申報資料、內部流程、相關人力及其他資源輔助。開發中國家的監理機構因其職權、法規、專業知識及資源不足，挑戰更大。然不論何國之監理機構皆面臨程度不等之資料品質不佳及人工作業耗時之挑戰。故此，監理科技 (Supervisory Technology, 以下簡稱 SupTech) 可提供解決方案。

貳、監理資料檢視

監理機構目前使用之資料來源多取自金融機構申報之資料。該種申報方式由金融機構填具監理機構事前設計之相關格式表單，但因填報費時且不盡然正確、資料驗證繁瑣等因素而影響資料品質。同時表單間存在資料重複及資料不一致等問題，該問題可能源自人工資料輸入失誤、資訊系統設施不完備、金融機構內部分類方法與表單規範不一致等。

另監理機構也使用外部資料 (如公開資訊、媒體報導、其他主管機關之資料

本文摘錄自 Toronto Center “SupTech: Leveraging Technology for Better Supervision”

等)，此類資料多屬非結構化且為不同檔案格式（如 Word、HTML、PDF），儲存於許多不同個人或共享資料夾，亦妨礙資料之有效運用。隨著採行更具風險導向之監理方法，致申報義務總量及頻率激增，上揭問題阻礙有效監理，並造成金融機構負擔昂貴之法律遵循成本。

監理關鍵要素之一為監理報表分析，可作為總體及個體審慎監理、專案評估及其他監理目標（如洗錢防制、打擊資助恐怖組織及消費者保護等）之工具。許多先進國家監理機構採用複雜工具分析申報資料，然發展中國家之監理機構仍使用過時的分析工具，如 Excel 及人工方式擷取、合併等進行分析。

除監理報表，監理機構亦需分析結構化較低之資料，其格式及內容不盡相同。這可能包括外部結構化資料及非結構化資料，自網路下載之敘述性文件、消費者問卷調查，以及監理機構製作或儲存之文件。從此種非結構化資料中搜尋、發現、分類、分析及產生有用之監理資訊，仍是監理機構面臨之主要挑戰。

資料品質不佳，SupTech 工具便無實際價值。藉由 SupTech，監理機構得自傳統表單申報獲取資料，進階至自動化收集更細部之數據。

運用機器學習的 SupTech 可發現資料品質之問題，如資料缺口、不一致及錯誤，同時自動化整理資料、合併資料、驗證及確保資料品質。細部資料標準化需監理機構偕同資訊科技服務商及金融業者合作，如此可整合監理機構內各部門間或不同監理機構間之申報需求，從而降低其複雜度、提高透明度，長期而言降低成本。品質佳之細部資料可提高跨企業、跨時間之比較性，建置新的分析方法及降低彙總時驗證資料之負擔；亦可促使內部金融業者風險資料與監理資料之一致性。以下謹就部份國家運用 SupTech 使監理工作更具效率簡述：

- 一、奧地利中央銀行 (OeNB) 於 2015 年實施之申報系統採直接輸入資料方式 (input-based approach)，將高度微粒資料 (highly granular data)，即標準化基本方塊 (basic cube)，由銀行傳輸至 AuRep 資料庫。AuRep 係由銀行出資之公司，扮演銀行系統及奧地利央行系統之橋樑，為單一資料倉儲系統，由銀行共同負擔成本。奧地利央行不收集制式申報表單，惟將基本方塊內資料，轉換為所需之監理報告。此種申報微粒資料之方式使奧地利央行得在幾乎不影響金融機構下，自行改變申報格式，並創建

整合奧地利央行內各部門資料需求的單一模型。

- 二、菲律賓中央銀行為其銀行業試行一套應用程式介面，可讓銀行自動申報高度微粒及幾乎即時之資料。此介面提供如自動驗證、資料視覺化及客制化報告等功能。菲律賓央行亦希望藉此重新配置專門處理人工資料驗證之人力、改善資料分析及降低申報不合規之情形。
- 三、另一種為資料抓取模式 (data pull approach)。此模式係相關資料已存放於金融機構資料庫時，監理機構可依據事先訂定之規格，自金融業者系統抓取資料、將之標準化並轉換為所需之報表。盧安達央行便是在 2017 年實施此種模式。
- 四、新型態監理申報方式可使申報規範與金融機構的作業系統結合。藉由一貫化作業，自動產出監理報表，毋須人工判讀及介入。此種機器可讀或機器可執行之金融法規，需監理機構發布可在金融業者系統執行之程式碼形式法規。新加坡及英國之監理機構正研究此種申報方式。

鑑於分散式帳本技術確保資料高度安全及資料完整性，亦可控制資料彙整及移轉之成本，證券監理機構亦進行此技術研究，以期降低大量申報之複雜度及成本。歐洲央行指出，此種採用分散式帳本技術監理申報模式，可提供市場參與者透明、安全及可信賴之申報方式。

參、監理程序

SupTech 可數位化、自動化、優化或改變作業及行政流程，提高效率及標準化程度。優點包括改善績效（如縮短回應請求及申請時間）、降低歸檔成本、提高可用於新資料分析軟體之數位資料的可用性。其成果減輕人為判斷負擔，包括談判、關係管理及決策；同時亦可提高監理流程之透明度。

已開發國家監理機構多年來使用專門軟體管理各種流程（如發照之內部核准、年度計畫及專案管理）及製作檢查報告等數位文件。在監理眾多金融機構時，數位化尤其重要。為了監控非銀行金融機構中的洗錢與恐怖組織融資風險，巴西央行開發結合網路之監理系統，蒐集結構化及非結構化資料，與金融機構遠距互動，該系統並自動產生檢查報告及信件等文件。

肆、採用監理科技之風險及挑戰

採用 SupTech 存在風險與挑戰。演算法可能因其中偽陽性、偽陰性（誤報、漏報）及錯誤關聯性，降低風險導向監理方法論之有效性，並損害監理機構聲譽。機器深度學習等科技之複雜性及隱晦性可能導致監理機構喪失對自動化流程之控制，影響其信賴度及監理透明。另過度仰賴資料分析，可能削弱監理機構某些能力，如辨識可能無法在數據中顯示或量化衡量之問題，並導致監理機構對 SupTech 不能呈現之質化變數失去敏感度。

金融業者在使用類似科技時亦會面臨部份風險，如當資料藉由網路傳輸或由雲端業者等外包商處理時所產生之網路安全及第三方風險。與採用紙本之工具及程序相較，完全或部分轉換至數位資料及以演算法為基礎之流程將使監理機構面臨科技、電力、通訊或其他營運中斷時受更大影響。網路攻擊則是高度自動化環境中最嚴重威脅之一，其可能導致資料遺失及電腦遭扣押。

演算法模型存在加入及強化人為偏見之風險，此種風險是一種無法解釋機器學習結果之風險，特別是深度學習（如黑盒子問題），以及使用不切合監理機構需求之演算法的風險，或可能自初始時便存在瑕疵等風險。如果監理機構缺乏對 SupTech 解決方案之專業知識、經驗或理解，或缺乏明確之 SupTech 實行目標，則此類風險將加劇。

提供 SupTech 品質佳之數位資料（如建置機器學習應用程式），亦可能是項挑戰。演算法之訓練資料可能不完整，且即使僅使用標準化之監理報表，許多監理機構亦普遍面臨資料品質問題。此外，大數據通常可信度低、品質不佳，特別是社交媒體，易被第三者操縱。使用社交媒體亦可能涉及資料隱私議題。

採用 SupTech 另一項挑戰為金融機構人工作業依然存在。金融機構作業流程及文件數位化程度越高，越多數位資料可使用於 SupTech 方案。墨西哥退休金基金管理機構為建置即時異地數位監理，藉由法規規範，要求該產業改變紙本處理流程，如客戶自某個退休金管理單位移轉至另個退休金管理單位之表單。採用 SupTech 之監理機構可能需要評估是否因金融機構數位化程度低而面臨阻礙。

另與舊系統整合亦可能是項挑戰。舊系統與資料格式可能無法與 SupTech 相容，致使歷史資料難以與新資料一起被充分使用。監理機構可能也欠缺使用

SupTech 之儲存容量及電腦運算能力，如大數據分析。此外，金融機構舊系統、資料及組織孤島^(註 1)等問題，將可能使 SupTech 在改善監理申報上受阻。

SupTech 仍是發展中行業，無現成之解決方案可滿足所有監理需求。解決方案大多需結合內外部軟體開發。許多監理機構可能缺乏軟體工程師、足夠之技術、資料分析法及專業行業知識等處理大量微粒資料，以及建議、選擇、開發、實施及維護 SupTech 之能力亦不足。即使上述所提情況曾存在於某時點，然專業知識亦難以留存，特別是在機器學習這種對專業知識高需求之領域，缺乏專業知識亦將限制監理機構比較不同 SupTech 產品之能力。

即使上述所提問題皆不存在，然抵制變革、內部官僚、組織內缺乏合作協調等亦會妨礙 SupTech 之推行。員工抗拒來自可能擔心被機器取代，及不斷改變之使用方法與程序造成之不確定性。

伍、小結

SupTech 可協助強化人們判斷力、決策能力及緩解監理挑戰，亦可提高監理資料品質、即時性及相關性、數位化及自動化監理流程、擴大分析能力、協助監理機構監理新的金融服務、可擴大監理範圍及因應傳統商品與商業模式之挑戰。高端資料分析方法藉由額外資料及格式，延展細部申報資料，可發現過去未曾發現與審慎監理、市場監控及金融法規執行有關之資料樣態、關係及生態。藉由 SupTech，監理機構終可成為具前瞻性、資料為本及具即時性之監理者，免於耗時及流程導向之人工作業，SupTech 促進更有效之風險導向監理。

惟採行 SupTech 方案需改變思維方式、組織變革、軟硬體重大投資及在資料科學、軟體工程及機器學習等專門技術。總體而言，實行 SupTech 可能存在諸多挑戰，例如：

- 一、缺乏實行 SupTech 之明確目的及目標。
- 二、缺乏監理機構內部跨部門及各監理機構間協調，以利整合可由單一 SupTech 解決方案解決之監理需求。
- 三、提供客製化 SupTech 解決方案之侷限，無法滿足多種監理需求。
- 四、難以找到及並留存專業知識。

- 五、採購 SupTech 專案之預算不足或行政程序上之限制。
- 六、金融機構持續存在人工作業流程和文件。
- 七、難以將 SupTech 解決方案與舊系統及資料整合。
- 八、散落在監理機構及金融機構且無法有效運用之資料。

另使用 SupTech 攸關科技及資料之風險，此類風險可能影響監理機構之聲譽及有效執行。其中包括：

- 一、錯誤警示或設計不良之演算法導致錯誤結果之風險。
- 二、使用無法解釋其結果之晦澀機器學習工具。
- 三、過度依賴資料量化分析方法並忽視 SupTech 未識別之質化面之風險。
- 四、網路及資料安全風險增高。
- 五、雲端計算及演算法供應商等第三方風險增加。
- 六、作業風險增加（如電力或通訊中斷）。
- 七、SupTech 演算法納入及強化人為偏見之風險。
- 八、使用社交媒體等替代資料所涉及之資料隱私風險。
- 九、某些大數據類型（如社交媒體）之不可靠及低品質。
- 十、第三者操縱 SupTech 大數據之可能性（如金融機構企圖誤導監理機構之演算法）。

監理機構可擬訂 SupTech 投資及執行策略，以結合監理目標及方法，可包含下列面向：

- 一、清楚表達可經由 SupTech 強化之監理目標及政策。
- 二、SupTech 投資之優先領域。
- 三、尋求特定 SupTech 解決方案。
- 四、SupTech 解決方案之局限性。
- 五、以演算法轉化監理內容及政策選項之內部程序。
- 六、演算法管理及治理。
- 七、因應採行 SupTech 所需之基礎設施及組織安排，包括運算及儲存容量，以及資料管理與治理框架之整合。
- 八、監理機構所需之技能，以及獲取及留存專業知識之政策。

- 九、與供應商訂定契約之政策，尤其需取得原始碼的控制權。
- 十、健全之網路防衛計畫。
- 十一、有效作業風險管理架構。
- 十二、金融機構所需之投資或改革，以及監理機構需擬定使其接受採用 SupTech 之策略。

註釋

註 1：組織孤島 (organizational silos) 係指組織內部缺乏合作協調。