金融監督管理委員會出國報告

（出國類別：研究-參加訓練課程）

參加東南亞國家中央銀行研究訓練中心 (The SEACEN Centre) 「監管與監理之新興技術：人工智慧、法遵科技與監理科技」課程

服務機關：金融監督管理委員會檢查局
姓名職稱：賴稽核淑婷
派赴國家/地區：臺灣(參加於印尼峇里島舉行之線上課程)
出國期間：115年4月6日至4月9日
報告日期：115年7月6日

課程摘要

本課程由東南亞中央銀行研究訓練中心(SEACEN)與日本銀行共同主辦，並由印尼銀行承辦，於 2026 年 4 月 6 日至 9 日在印尼峇里島舉行，採實體與線上混合模式進行。課程主要探討人工智慧(AI)、法遵科技(RegTech)與監理科技(SupTech)在金融監理領域的應用與轉型，並透過案例分享、課堂互動及分組討論等方式強化學習效果。藉由參與本次課程，有助學員瞭解新興科技在現代監理生態系統中的角色，並掌握將相關技術整合至現行監理框架所需的技能。

本次課程為期 4 天，謹將課程重點摘述如下：

第一天的內容講授 RegTech 與 SupTech 的基本概念，並深入探討 AI 與機器學習(ML)在金融監管中的應用。課程透過分享菲律賓央行的專案實務與技術展示，引導學員初步瞭解科技如何重塑風險管理與合規流程，並分析自動化監測與即時監管帶來的效率提升。

第二天內容有關技術實踐與治理平衡，進一步討論 SupTech 專案的開發與專題研究。課程重點探討如何在創新與審慎監理間取得平衡，建立必要的治理防護機制，並針對利用科技與 AI 打擊金融犯罪(AML/CFT)進行深入討論，強化學員對金融安全韌性的認知。

第三天內容有關國際監理實務與案例應用，分享紐約州金融服務署的虛擬貨幣數據治理經驗，以及印度儲備銀行運用監理工具進行網路安全監管的實例。另進行分組活動，讓各國學員實作演練及分享實務經驗。

第四天則是數據倡議與跨國協作經驗分享，探討標準制定組織的數據倡議與日本銀行的數據採集經驗。課程亦分享香港金管局與西班牙銀行的應用案例，強調國際間在 SupTech 領域的協作與 AI 展示。最後透過課程回顧與交流，掌握金融科技監理的重要實務經驗。

目　錄

壹、課程緣起及目的

隨著科技的快速演進，金融產業正經歷深刻變革，為監理機關帶來了全新的風險與機遇。新興工具如人工智慧（AI）在推動創新之餘，亦可能引入新的脆弱性或放大既有風險；此外，未來如量子運算等技術突破，更可能對網路韌性產生具系統性影響之威脅。為了有效應對這些挑戰，監理人員必須深入理解驅動變革的技術背景及其風險意涵。

此同時，監理科技（SupTech）與法遵科技（RegTech）的發展也提供了顯著優勢，能實現自動化、即時監測並提升監理效率。因此，培育具備技術素養、能負責任且自信地將 AI 與其他工具應用於監理職能的專業人才，已成為當前金融監理領域之重要課題。

本課程參與學員來自汶萊、柬埔寨、印度、印尼、寮國、馬來西亞、尼泊爾、巴布亞紐幾內亞、菲律賓、斯里蘭卡、我國、越南、中國大陸、韓國、泰國、東帝汶及馬爾地夫等 17 個國家或地區共計 64 名代表參與。

課程內容旨在協助資深中央銀行與金融監理人員理解並運用正轉型中的監理框架與技術。透過本課程，學員將能深入理解 AI、RegTech 與 SupTech 在現代監理生態系統中所扮演的核心角色，並具備評估以技術驅動之合規監控、風險評估及監理分析解決方案之能力。同時，藉由分析全球中央銀行與監理機關成功導入新興技術之實務案例，學員將能有效識別數據治理、網路安全及監理情境下 AI 倫理等相關挑戰，進而培養出將新興技術整合至現行監理框架中之策略擬定能力。

貳、課程介紹

一、**課程時間**：115年4月6日至4月9日。

二、**課程內容**

日期	主題	主講人/任職機構
4月6日	法規科技與監理科技導論 Introduction to RegTech and SupTech	Mark McKenzie The SEACEN Centre
	人工智慧與機器學習在金融規範與監理上的應用 Artificial Intelligence and Machine Learning in Financial Regulation and Supervision	Ashutosh Jaiswal The SEACEN Centre
	菲律賓中央銀行監理科技/法遵科技之實務經驗-SAFr-QIT 專案 BSP Experience in SupTech / RegTech – SAFr-QIT Project	Christian Rick Soriano Bangko Sentral ng Pilipinas(BSP)
	法遵科技/監理科技成果展示 RegTech / SupTech Showcase	Amanah Ramadiah FNA / Universitas Indonesia
4月7日	菲律賓中央銀行監理科技/法遵科技之實務經驗-GabAI 專案 BSP Experience in SupTech / RegTech – GabAI Project	Christian Rick Soriano Bangko Sentral ng Pilipinas(BSP)
	監理科技專案開發 Developing SupTech Projects	Mark McKenzie The SEACEN Centre
	運用科技與人工智慧打擊金融犯罪、反洗錢與反資恐 Using Tech/AI to Combat Financial Crime/AML/CFT	Vacharakoon Jivakanont The SEACEN Centre

日期	主題	主講人/任職機構
4月8日	紐約州金融服務署的法遵科技與監理科技之經驗與實務案例 NYC DFS Experience/Case Studies in RegTech and SupTech	Trevor Collins New York State Department of Financial Services
	印度儲備銀行運用監理科技工具強化網路安全監理之實踐 RBI Supervisory Tools (including SupTech Tools) for Cyber Security Supervision	Pradeep Raj Singh Reserve Bank of India(RBI)
4月9日	標準制定機構數據倡議概述：以日本銀行開發證券融資數據蒐集與彙整之經驗為例 Overview of Recent Data Initiatives by Standard Setting Bodies including BOJ's Experience in Developing Securities Financing Data Collection and Aggregation	Shintaro Nakamura Bank of Japan(BOJ)
	香港金融管理局監理科技與法遵科技之實務案例 KMA Experience/Case Studies in SupTech and RegTech	Benny Li Hong Kong Monetary Authority(HKMA)
	中央銀行與各國監理機關在監理科技上的跨國多邊協作機制 Cross-Border Collaboration on SupTech among Central Banks and Supervisors	Nico Lauridsen European University Institute
	西班牙銀行 (BdE) 的監理科技專案與應用案例 BdE SupTech Project/Case Studies	• Nico Lauridsen European University Institute •Javier Tarancón Banco de España(BdE)

參、課程內容摘要

一、法遵科技與監理科技導論

(一)監理科技（SupTech）之定義與應用

1.監理科技之定義與理論定位

根據 Broeders & Prenio（2018）之學理定義，SupTech 係指「監理機關使用創新技術以支持監理工作」，核心功能在於協助監理機關將「申報」及「法規處理程序」予以數位化，從而轉為「預警式監控」。監理科技不能取代人類的監理判斷，由於模型與測試均存在固有限制，人類參與決策過程（Human-in-the-loop）係為必要。

2.監理科技之關鍵技術

近 10 至 15 年間，技術已從「胚胎階段」躍升至成熟應用，關鍵技術如下：

(1)大數據（Big Data）：處理海量、多樣且高頻之監理數據。

(2)機器人流程自動化（RPA, Robotic Process Automation）：自動化執行重複性行政作業，解放人力。

(3)人工智慧（AI）與機器學習（ML）：用於預測模型建構、異常行為偵測及系統性脆弱點識別。

(4)自然語言處理（NLP, Natural Language Processing）：用以分析非結構化文本數據，如董事會會議紀錄或監理報告，可大幅提升非結構化資訊之處理效率。例如：馬來西亞國家銀行（Bank Negara Malaysia, BNM）投入相當資源，運用自然語言處理（NLP）技術，系統性掃描並分析約 16,000 份銀行監理報告及董事會會議紀錄（Board Minutes），目標在於從海量非結構化文本中自動提取標準化語言模式與關鍵風險訊號，NLP 技術得以在短時間內跨越機構規模與語意障礙，將分散於各機構文件中之治理警訊予以結構化，大幅提升監理資訊之覆蓋廣度與分析深度。

(5)深度學習（Deep Learning）：用於更複雜之模式識別與預測。

(6)生物識別技術（Biometrics）：應用於客戶身分核驗（KYC）等合規場景。

3.監理科技之應用

(1)數據蒐集與處理：自動化蒐集大量且多樣化之數據，減少依賴易於出錯之人工輸入，提升數據完整性與一致性。

(2)數據分析與風險檢測：嵌入即時分析（Real-time analytics）與預測模型，用以偵測異常、詐欺行為、市場操縱趨勢或系統性脆弱點。如，機器學習模型可針對反洗錢（AML）場景中之可疑交易行為建立基準行為模式，一旦個別交易偏離統計常態，即自動觸發警示，供監理人員進行後續研判，有效取代傳統人工逐筆核閱之低效模式。

(3)監理程序自動化：將報告審查、互動式儀表板建置及案件管理等任務數位化，釋出人力從事更高層次之監理工作。

(二)法遵科技（RegTech）之定義與應用

1.法遵科技之定義

法遵科技係指金融機構應用先進技術，以「自動化與優化」監理風險管理、申報、監控及合規程序。

2.法遵科技之應用

(1)監理申報自動化：透過自動化技術進行數據蒐集、格式化並直接提交監理機關，大幅減少人工干預之錯誤率。

(2)即時風險監控：實現對反洗錢（AML）、認識客戶（KYC）、詐欺偵測及行為風險之持續監控。以詐欺偵測為例，ML 模型可即時比對每筆交易之交易地點與歷史行為，於毫秒間完成風險評分，效能遠超人工審核。

(3)監理情報：自動追蹤全球不斷演進之法規變動，迅速將更新內容整合至機構內部合規系統。

(4)動態合規：提供追蹤法規變更之解決方案，使機構得基於即時營運數據進行自動化評估，而非仰賴人工逐一比對。

(5)生態系統連接：透過 API 介接、機器可讀法規（Machine-readable regulations）及跨部門系統整合，增進監理機關與金融機構間之數據共享效率。

(三)法遵科技與監理科技之交集

1.二者底層技術相同

使用的底層技術（AI, ML, Cloud, Big Data）是完全相同的，銀行端與監理端其實是在使用同樣的工具達成不同的目的。

2.二者之連結點

法遵科技係金融機構端之法遵技術，監理科技係監理機關端之監督技術，其核心連接點在於「數據交換」，如：金融機構透過自動化接口向監理機關提交監理申報，或監理機關透過 API 直接從銀行系統獲取特定資訊。

3.監理機關應支持金融機構之數位轉型

監理機關不應僅關注自身監理科技之建置，亦必須積極支持被監理機構之數位轉型。若銀行之數據仍以傳統 Excel 格式存在，監理端之 AI 系統再強大，亦無法發揮作用。

(四)導入監理科技之挑戰與調整

1.技術同質化之系統性隱憂

若監理機關與大型商業銀行同時採用完全相同之 AI 技術、雲端平台與供應商，此一現象將構成系統性威脅，第一層為技術性風險，當所有機構依賴同一雲端服務或同一模型，一旦發生大規模技術故障，整個金融體系之監控機制將同步癱瘓；第二層為監理判斷萎縮風險，監理人員若長期過度依賴 AI 輸出之結論，而疏於培養自身之監理判斷，一旦模型出錯，人類將因判斷能力退化而無法及時識別並糾正錯誤，產生難以挽回之監理失靈。

2.數據治理之挑戰

現有數據與現代技術之「磨合期」，大量以舊有格式儲存之歷史數據，難以直接供給現代 AI 模型使用，數據清洗與格式轉換本身即構成相當之技術負擔，在推動監理科技專案前，監理機關與金融機構必須共同建立數據字典（Data Dictionary），此為整個技術生態之底層基礎設施。

3.監理人力之調整

技術應取代底層之行政勞動，而非削減監理人力，應將釋出之監理人力專注於治理品質查核、合規一致性評估及深層風險洞察之辨識。

二、人工智慧與機器學習在金融規範與監理上的應用

(一)人工智慧、機器學習、深度學習與監理認知基礎

1.技術層級的包含關係

(1)人工智慧（**Artificial Intelligence**，AI）：最外層，泛指所有智能機器領域。

(2)機器學習（**Machine Learing**，ML）：AI 之子集，聚焦於「從數據中學習的算法」。

(3)深度學習（**Deep Learning**，DL）：ML 之進一步子集，以模擬大腦結構之神經網絡（Neural Network）為核心，具備多層架構。

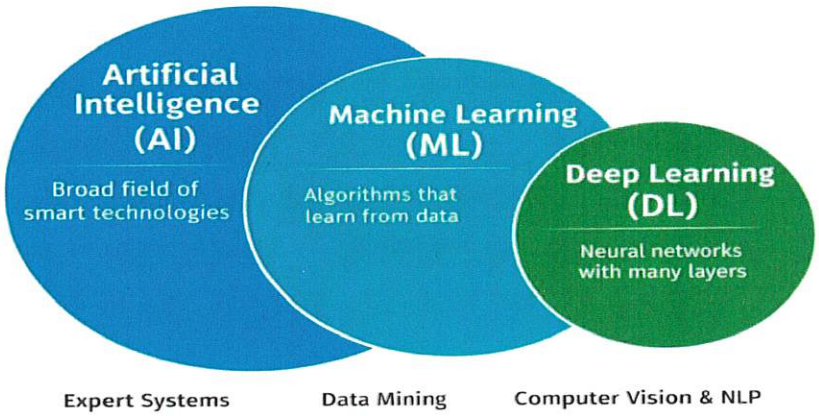


圖 一：AI、ML 及 DL 三者的關係。說明從人工智慧到機器學習，再到深度學習等三層技術的從屬關係。

2.監理機關應有之認知取向

監理機關應建立核心判斷能力，避免因供應商的商業推銷 AI 工具而被動接受技術採用，應持續保持批判性思考。

(二)機率論式模型（Probabilistic Model）

監理機關必須理解當前許多尖端模型並非「決定論式」，而是「機率論式」，兩者在監理框架設計上具有根本性差異，有關機率論說明如下：

1.定義：輸出結果基於機率分布，相同的提示詞再次輸入，可能得到不同答案，具有本質上的不確定性。

2.動態學習機制：此類模型（如大型語言模型 Large Language Model, LLM）會根據與用戶的互動模式持續學習與演進，依賴龐大數據中心不斷供給數據以維持運作。

3.數據漂移（Data Drift）問題：模型本身未必改變，但數據環境可能產生變化，若模型無法因應此種漂移，便會輸出偏差結果。

(三)AI 系統技術三大組成要素

包含數據（Data）、算法（Algorithm；邏輯涉及 ML/DL 架構）及輸出（Output），該項輸出分二類；一為連續型輸出，得出精確數值（如違約機率之具體數字）；二為類別型（Class）輸出，得出分類結果（如信用評分「通過/拒絕」決策）。

(四)機器學習之三大核心特徵

1.自動優化（Automated Optimisation）：在有限或無人為干預的條件下自動尋找最優解。

2.大數據模式識別：能在海量數據源中，識別人類肉眼無法察覺的規律。

3.非因果推論（Not Causal Inference）：此為極重要之監理警示。ML 不關心「為何 X 導致 Y」，它只告訴監理者：「根據海量歷史觀察，當此 10 個條件同時滿足到特定程度時，Y 便會發生。」。ML 雖可能具備高度預測能力，卻缺乏因果解釋能力，監理機關必須學習與此種不確定性共存。

(五)深度學習架構與黑盒問題

1.深度學習被稱為「黑盒」原因：人類根本無從解釋微調某一變數如何影響最終產出，此為當前監理實務之重大缺口。

2.深度學習架構主要為神經網絡結構：試以兩層隱藏層之典型架構為例，參數規模之數學推演，第一隱藏層產生 110 個參數，第二層同為 110 個，輸出層 11 個，合計兩層架構之系統估計 231 個變數。當層數與節點數增至數千乃至數百萬（如現代 LLM），人類根本無從解釋微調某一變數如何影響最終產出，此即深度學習被稱為「黑盒」之根本原因。

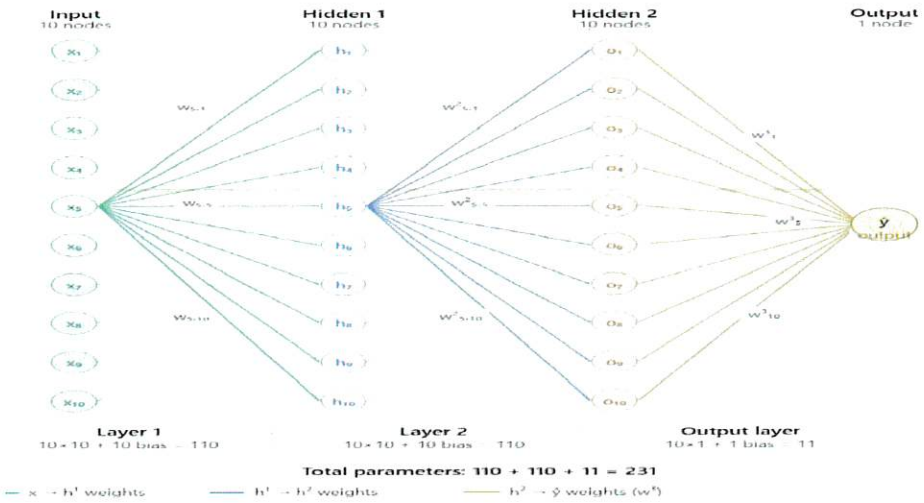


圖 二：深度學習架構與可解釋性。以精細的神經網絡連線圖，完整呈現 Input（10 節點）→Hidden 1（10 節點）→Hidden 2（10 節點）→Output（1 節點）的全連接架構，並在圖下方以公式標示各層參數數量（110+110+11=231），即便只是 2 層隱藏層就已有 231 個參數，一旦增至數千層，可解釋性幾乎為零。

(六)監控上的挑戰

1.黑盒下的盲區：監理機關無法監測 AI 的實際運作。這對所有系統性風險維度（流動性、關聯性等）都構成了最高等級的風險。AI 模型具有高度遞迴性（Recursive Nature），模型驗證結果可能迅速失效，因此監理機關必須建立持續驗證（Validation）及校準（Calibration）機制，形成「驗證－校準－再驗證－再校準」之循環治理模式，以確保模型持續維持有效性與可靠性。

2.模型同質化 (Model Homogeneity)：從整體金融體系角度言，若所有金融機構都採相同的算法來處理市場信號，當市場發生波動時，所有模型可能會同時下達相同的指令（如集體拋售某種證券），將瞬間爆發嚴重的流動性問題。

3.技術集中度風險：全球金融體系對 CrowdStrike、微軟、AWS 等少數技術供應商之高度依賴，構成不可替代性之巨大隱患；一旦供應商發生重大故障，將觸發全球連鎖反應。

(七)監理調適策略

1.AI 適用面：AI 適用於單一金融機構之合規檢核與反洗錢偵測，但目前絕對不建議將其作為整個金融體系決策或處置大型銀行倒閉等高度複雜情境之工具。

2.提升能力：監理機關建立自有 IT 基礎設施與分析能力，避免全盤依賴外包，方能實現實質有效之監督。

3.人才競爭痛點：目前美國數據科學家中位數年薪極高（約 12 萬美元起跳），央行與監理機關若無法提供具競爭力之薪資待遇，將難以吸引頂尖人才，不易具有理解與審查金融機構複雜模型之能力，形成監理能力之缺口。

4.問責框架之調整：將提供金融服務之技術公司納入問責框架，特別是對拒絕接受監理審計之大型科技業者應予強制規範。

三、菲律賓中央銀行監理科技/法遵科技之實務經驗-SAFr-QIT 專案

(一)SAFr-QIT 內容架構主要有三大核心支柱

1.財務數據：其 2026 年專案首推的核心內容。

(1)涵蓋內容：資產負債表(BS)、損益表(IS)以及選定的各類績效比率。

(2)核心特性：所有數據均自動化計算且具高度互動性，於介面上變動時間期間、產業類別或特定銀行名稱時，系統會瞬間自動重新計算並更新所有數據顯示。

2.非財務數據

(1)實體網絡：揭露銀行全菲律賓各地的分行數量與 ATM 數量。

(2)銀行基本資料：包含總行位置、聯繫資訊等基本資料。

(3)負責人員：不僅列出銀行的聯絡人員，也列出 BSP 內部負責分析該銀行報表提交情形的對口監理人員。

(4)地理分布脈絡：各分行分布及瞭解特定分行與周邊其他金融機構間的鄰近程度。

3.經營模式與風險指標：這是 SAFr-QIT 最具「智慧」的靈魂部分。

(1)重大活動：此被定義為銀行的經營模式，系統會識別在特定期間內被標記為「重大」的活動（如：某些時期銀行可能專注於某類交易活動或零售存款）。

(2)銀行同業間比較：運用進階的機器學習(ML)方法，採「階層式分群法(Hierarchical Clustering)」，依各銀行經營模式的相似性進行動態分群，而非僅看規模。

(3)固有風險：每項風險都存在固有風險，並非所有風險都能計算出來或能用量化數據體現，大多數風險只能透過質化資料來衡量，但仍將這類風險告知監理人員，並提供對銀行及其子公司機構整體性之評估。

(二) SAFr-QIT 核心功能

1.中央數位中心(Centralized Digital Hub)

SAFr-QIT 被正式定義為金融監理人員進行所有最初評估風險的中央數位中心。這意味著它打破了過去資訊散落的僵局，將所有必要的評估維度整合在一起，並確保所有監理人員具備標準化作業的起點與一致的風險視角。

2.從傳統到前瞻的遷移

透過從 CAMELS/ROCA 轉至 SAFr，監理方式變得更加前瞻，在 SAFr-QIT 中查看所有初始的固有風險(Inherent Risk)與財務資料，能更有效地據此評

估銀行風險管理的品質。

3.提供「一站式」服務

將財務與非財務數據、分析工具及監理指南等整合至單一且直觀的互動性儀表板中，監理官在分析數據時能同步查閱該項指標對應的監理標準。該設計能強力驅使決策一致性，確保每一項判斷有規章可循。

(三)導入 SAFr-QIT 實施案例

1.資訊與地理脈絡

(1)在深入分析財務數據或風險指標之前，先掌握銀行基本非財務資訊，包含銀行實體網絡、辦公室數量與 ATM 數量、銀行聯絡方式、地址、負責該機構的監理人員(AO)。系統不僅顯示特定銀行的網絡，亦能瞭解周邊共同運營的其他銀行。

(2)實例應用：模擬強烈颱風的情境：假設一場強烈颱風襲擊了保和島(Bohol)，透過 SAFr-QIT 的地圖即時監控，監理人員能立即辨識出該受災區域內有哪些銀行的分行受影響的情形，在財務指標產生變化前，監理人員就能預判哪些分行同時關閉、ATM 停機、員工失聯、電力或通訊中斷等，這種基於地理位置的判斷，提供營運與流動性壓力的早期訊號，讓監理人員在風險正式顯現於數據前，能先行介入。該項亦與 2024 年修訂巴塞爾核心原則(Revised Basel Core Principles)中，針對系統性風險與集中度風險，明確要求監理機關進行具前瞻性及風險性評估之原則一致。

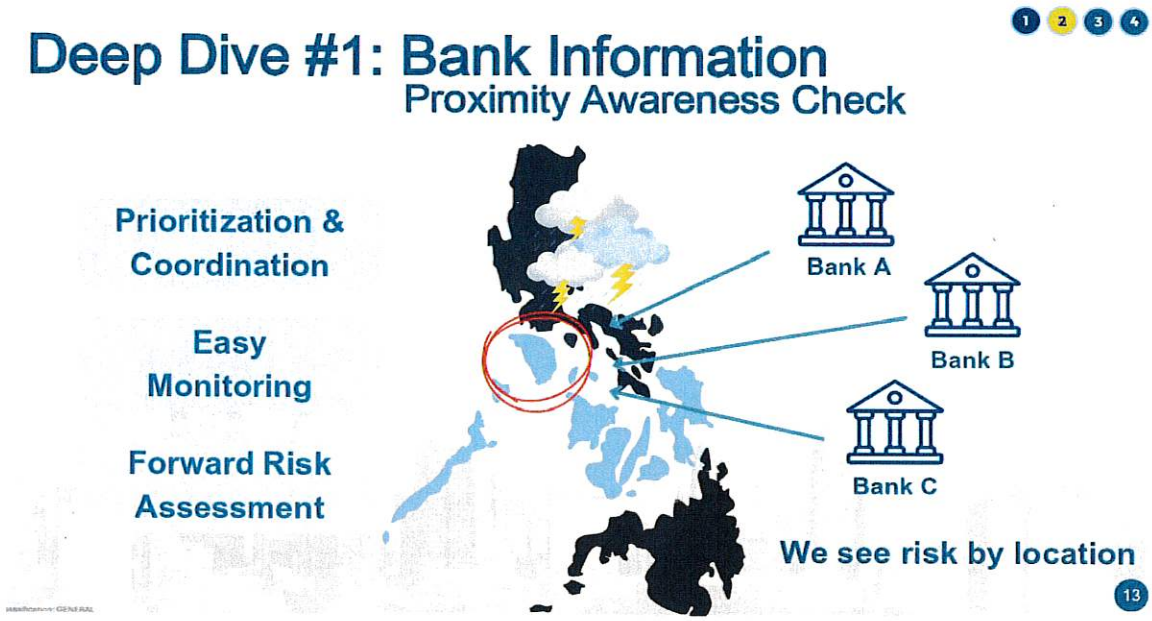


圖 三：地理鄰近感知檢查。一張菲律賓地圖，以紅色圓圈圈出颱風受災區域，當同一地區多家銀行同時暴露於外部衝擊（如颱風），監理優先順序與協調行動的必要性一目了然。

2.財務數據分析

(1)銀行與產業之比較，如：銀行的成長、槓桿或資金結構是否異於產業水平。

(2)趨勢圖：顯示餘額、比率隨時間的演變，識別趨勢風險，如：信用暴險持續上升、流動性緩衝下降、盈餘品質惡化等。

(3)地理集中度：利用地圖顯示資產負債表項目（如存款）的地區分布。識別銀行是否過度暴險於特定區域，增加區域性經濟衝擊或自然災害的脆弱性。

(4)季度變動訊號與變動幅度的告警機制：系統利用直觀的圖示標示相較於上一季的增減幅並以色彩編碼，如：綠色係微小或符合預期的變動、黃色係中度變動、橘色係顯著變動、紅色係大型或異常變動。

(5)實例應用：貸款或存款出現紅色警示（如劇增 50% 或 70%），雖不直接等於有問題，但該強力「早期信號」促使監理人員調查背後原因，是否基於策略擴張、市場環境變化，或新興的隱憂？

3.重大活動的識別

(1)多層次分析：系統利用資產負債表及相關量化數據，參照不同產業層級的門檻值，自動識別並標記銀行最實質的業務，如：交易(Trading)、信用卡(Credit Cards)、存款負債 (Deposits)或特定的子公司/業務部門，並以多層次分析方式，如：銀行層級係查看特定機構有哪些重大活動、產業層級係評估特定活動在該產業中的集中程度。

(2)關鍵效益：確保監理資源集中在銀行最重要的部分並在初始階段減少對手動計算或主觀判斷的依賴，促進識別跨機構重大活動的一致性。

4.經營模式的銀行同業分組

(1)SAFr-QIT 運用機器學習(ML)演算法，分析各銀行的經營模式組成與行為特徵，找出彼此間相似性，將其自動分類為不同的同業群組，如：零售導向型、相似資金組合型、消費金融為主等。

(2)運用機器學習的三種方式，如預測分析，當數據超出預測邊界時發出警示；歷史偏差檢測，基於標準差之變化；關聯帳戶分析，不只看單一帳項（如總存款），而是監測與其相關的其他會計項是否同步變動。

(3)監理價值：可掌握特定組別在該季度的表現，若某家銀行在分組中脫穎而出或異常落後，能有助識別係產業性趨勢或為個別機構的特有問題。

5 風險指標—監理風險訊號

(1)運用自然語言處理技術分析新聞與社交情緒，系統能自動將新聞情緒分類為流動性風險、信用風險或市場風險等類別，協助掌握市場對特定機構之觀感。

(2)涵蓋信用風險、市場風險、流動性風險、營運風險、市場行為風險、聲譽風險以及利率風險等資訊，整合量化及質化的資訊，作為評估的基礎。

(3)提供早期訊號，可引導監理機關的專注力與專業裁量，瞭解哪些領域需要優先更深入的實地檢查。

6.一頁式快速表達資訊：係「一頁式」的頁面，整合銀行最重大的活動、核心風險指標(如：信用風險、流動性風險、市場風險與利率風險的評等結果、機構的收益(Earnings)、資本(Capital)及流動性(Liquidity)的關鍵比率與排名(如CAR、LCR、NSFR 等比率)，可在詳細評估前，快速鎖定銀行最脆弱或變動最劇烈的領域。

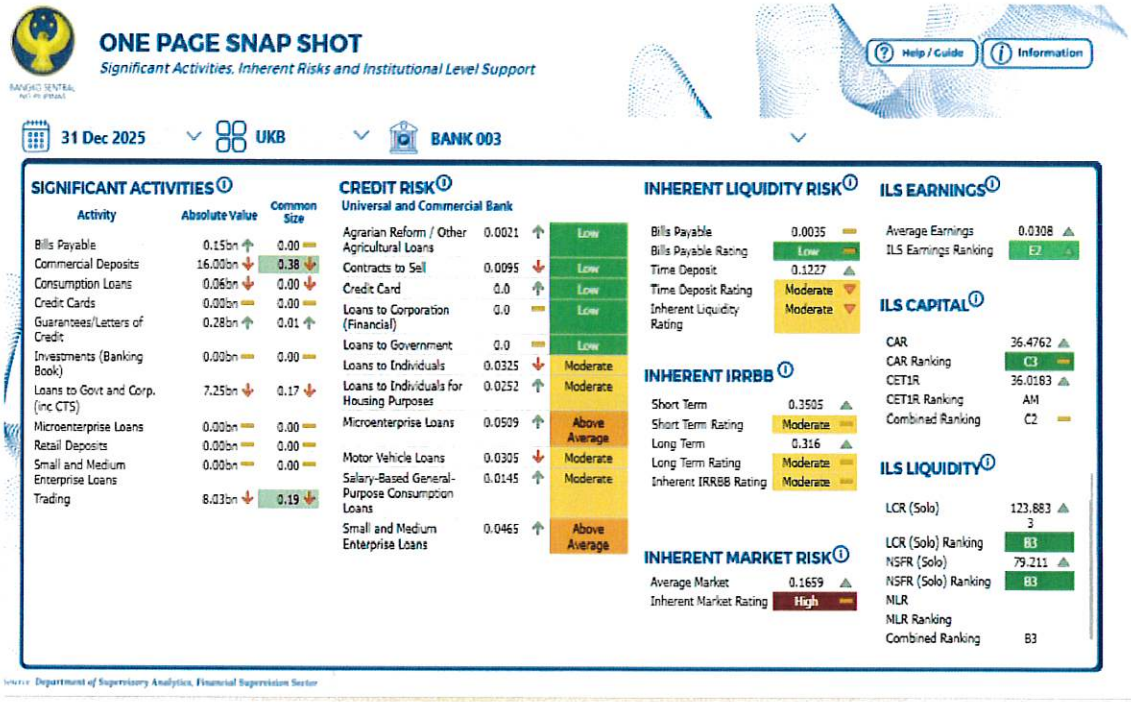


圖 四：一頁式快速表達。

7.架構優化與成本控管：為解決 1,000 多名人員之授權成本，BSP 將系統從本地伺服器遷移至 MS Fabric 雲端平台。僅開發人員需發布授權，其餘人員可透過安全加密連線存取最新數據，確保資安與行動便利性。

四、法遵科技(RegTech)/監理科技(SupTech)成果展示

全球截至 2025 年，已有 140 個國家、197 個監理機關完成監理科技部署，較 2022 年成長逾三倍。各機構反映之主要價值集中於三項：申報作業時間大幅節省、跨部門數據整合能力顯著提升，以及風險分析準確性的增強。重點實務案例如下：

(一)香港金融管理局（HKMA）：推動顆粒化數據之申報

目前亞太區監理機關蒐集交易層級之顆粒化數據，係 HKMA 之推動實務為最具代表性。其系統性蒐集企業貸款、銀行間貸款及金融機構間交易之原始交易明細之數據，並將該等數據應用於對個別銀行的風險評估、銀行間風險暴險監控及整體流動性分析等多元監理場景。監理機關不再仰賴金融機構彙整後之 KPI 數字，而是直接掌握最細顆粒度之原始交易紀錄，從而大幅提升風險識別的時效性與精準度。

(二)馬來西亞—國家詐騙應對中心（NSRC）模式

馬來西亞在央行支持下建立之國家詐騙應對中心（National Scam Response Centre，NSRC），係目前東南亞地區在詐騙防制協作上最具制度完整性之機制平台。NSRC 的設計核心在於「速度」，透過技術加速法院流程，使監理機關得以在正式司法判決作成前，先行對涉嫌詐騙之帳戶採取「暫時凍結」措施，有效防止詐騙資金在訴訟程序完成前遭提領流失。此一模式之啟示在於，技術工具與制度設計必須相互配合，方能產生實際防制效果。

(三)菲律賓—AFASA 法案之立法突破

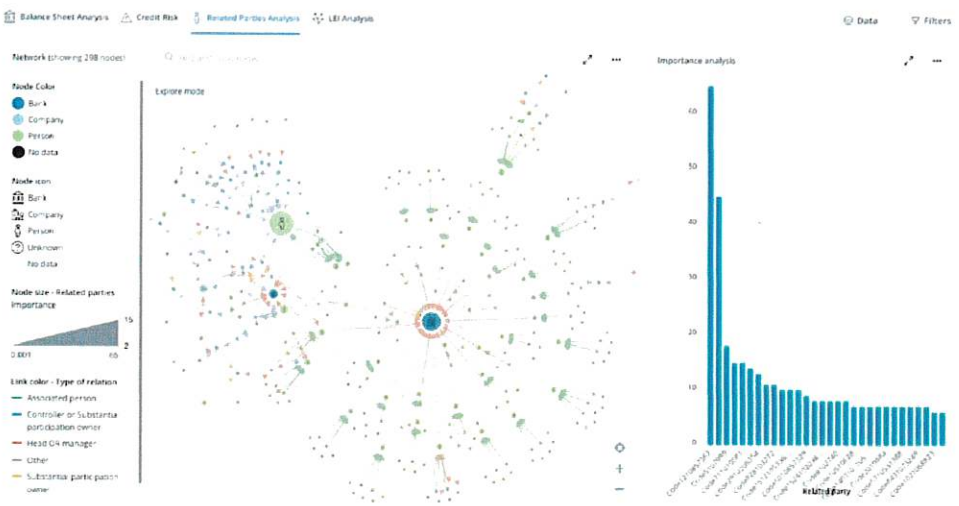
菲律賓新頒布之「金融詐騙帳戶法」（Account Financial Scamming Act，AFASA）提供了一項關鍵之立法示範。該法案明定，當案件被認定潛在涉及詐騙時，銀行保密法之適用將予排除，銀行得依法共享涉案帳戶資訊。AFASA 法案的意義，係為技術的有效運行提供不可或缺之法律基礎。

(四)實機展示(採合成數據計算，目前有央行採用)：

1.個別銀行之分析模組

最特別的是「關聯戶分析與關鍵人網絡圖譜」功能，系統整合各機構在不同申報資料中之股東、所有者與關鍵職位人員等資訊，建構完整之關係網絡圖，得以辨識在整體金融體系中具有高度重要性之「關鍵的利害關係人」（Key Person of Interest），防範隱藏之利益衝突或系統性集中風險。

此外，透過「法律實體識別碼」（Legal Entity Identifier, LEI，係將全球所有國家的企業統一格式計有 20 碼，可跨國比對，底層數據還綁定「關係鏈」），系統能追蹤跨國複雜控股結構，以演示中「哥倫比亞銀行控股公司」為例，系統得以揭示其透過北美子公司與阿布達比資產管理公司之跨境連結，使監理者能穿透複雜股權鏈條，掌握集團層級之整體風險圖像。



圖五：關聯戶分析。左側放射狀網絡圖是關聯戶分析，節點依顏色分為 Bank / Company / Person / Unknown，邊線代表不同關係類型（Associated Person / Controller / Head OR Manager 等）；右側為「Importance Analysis」降序長條圖，量化各關聯戶的重要性分數。此圖直觀呈現「關聯戶分析與關鍵人網絡圖譜」的運作邏輯。

2.整體金融體系與壓力測試模組

「重疊投資組合」（Overlapping Portfolios）之風險量化方法，如「波哥大銀行」與另一家銀行為例，兩者雖無直接借貸關係，但因均貸放予相同企業群，形成

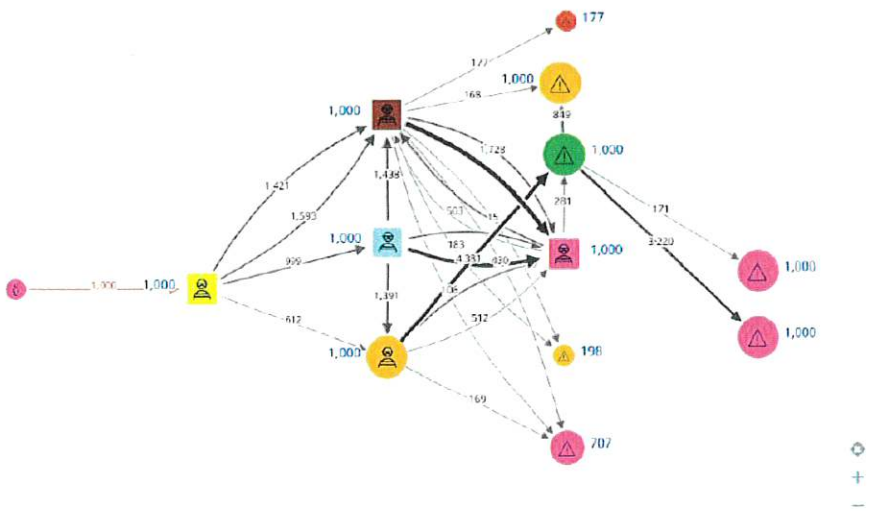
高度重疊之資產組合。當這些企業所處產業受衝擊時，兩家銀行會產生強烈的「間接連鎖反應」。

在壓力測試數值上，若 1 家銀行倒閉，系統即時計算結果顯示：若該銀行今日倒閉，將直接導致系統內 47%的支付遭到拒絕，此量化數據，使監理機關得以精準評估單一系統重要性機構失效，對整體金融體系流動性所造成之毀滅性連鎖影響。

3.詐騙防制與市場行為監理模組

在詐騙防制模組中，系統於受害者完成舉報後，自動生成多層次「資金軌跡」（Money Trails）。技術能自動識別第一層「人頭帳戶」（Mule Account），並持續追蹤資金流向第六層乃至更深之轉帳節點，協助相關銀行在詐騙者於 ATM 領現前，精準識別並攔截資金。

此外，系統設有「績效管理儀表板」（Performance Tab），使監理機關得以比較各銀行對詐騙案件之處理效能。若 A 銀行能在 1 小時內識別 70%之事件；而 B 銀行有 66%帳戶處於「待處理」狀態，監理人員可據此得知 B 銀行顯未履行應有之消費者保護義務。



圖六：資金流向多層網絡圖。多家銀行節點的資金流向圖，以不同顏色標示不同銀行、以箭頭標示資金流向、以節點大小呈現交易金額，呈現多層次資金軌跡自動追蹤的技術效果。

五、菲律賓中央銀行監理科技/法遵科技之實務經驗-GabAI 專案

專案於 2025 年 7 月正式啟動，與第三方供應商 Microsoft 協作，採最小可行性產品(MVP)模式，僅歷時三個月即完成初步部署與試點推廣。經開發專屬的 AI 虛擬助理 GabAI，旨在利用生成式 AI(Generative AI)技術，協助監理人員「更聰明、更快速」地處理資訊搜尋、法律檢索、摘要與公文寫作等日常任務。

(一)專案背景與面臨之痛點

1. **極度耗時之資訊檢索**：監理員常需在多個內部伺服器、外部網站及分散的法規指南中搜尋特定條文，導致作業流程碎片化。
2. **監理疏漏風險(Risk of Oversight)**：手動檢索易遺漏最新修訂之公告規範，引用過時資訊可能對監理決策與檢查報告造成致命性錯誤。
3. **重複性勞動與效率瓶頸**：不同監理單位常對相同法規詮釋提出重複詢問，造成內部溝通成本與人力資源之浪費。

(二)GabAI 核心功能模組與技術應用

GabAI 架構於 Azure 雲端環境，整合專有資料庫，提供四大核心模組以支援監理實務：

1. **法規與內部知識檢索(Regulations & Internal)**：整合各項法規手冊、公告、備忘錄以及「機密（Confidential）」及以下為限之部門命令，「極度機密（Secret）」等級文件則不在知識庫範疇之內。系統採智慧查詢規劃(Query Planning)，能根據問題自動導向正確之文件索引，並提供原始文件連結供查核。
2. **寫作支援模組(Speeches)**：系統內建 BSP 正副總裁之歷史致詞稿訓練資料，能模擬官方語氣，並採「大綱預覽、互動修改、正式生成」之流程協助撰寫演講大綱。
3. **文件摘要功能(Summary)**：支援 PDF 與 Word 格式之跨文件摘要，協助監理員快速提煉外部報告之核心內容。惟單一檔案受限於 10MB 以內，以確保處理效能。
4. **底層**技術：系統整合多項微軟雲端服務元件，其資料流處理程序如下：文件首先上傳至 SharePoint，再透過 Python 程式轉換並儲存於 Microsoft Blob Storage，其後由 Azure Doc Intelligence 負責分析文件並提取文本數據塊（Chunks），最終由 Azure AI Search 結合使用者提示詞與聊天紀錄，驅動大型語言模型（Large Language Model，LLM ）生成最終答案。系統程式碼全

數存放於 GitHub 進行版本控管，並符合 BSP 內部網路安全協議規範。

(三)治理框架與安全控制措施：

1. **數據安全性**：系統與 BSP 之 Active Directory 連結，僅限授權人員透過單一登入(SSO)存取。所有監理數據均儲存於菲律賓境內，符合國家數據主權要求。
2. **護欄機制(Guardrails)**：系統內建內容安全防護，自動過濾與監理任務無關之提問，並在開發過程使用合成數據(Synthetic Data)以保護真實客戶隱私。
3. **責任使用原則(Responsible Use)**：AI 僅為輔助工具，絕不取代監理員之最終專業判斷、所有 AI 輸出用於正式工作前，須由監理人員進行事實查核。使用者必須對 AI 生成內容所引發之行政決策負起完全之法律責任。
4. **AI 幻覺（Hallucination）風險之防範機制**：生成式 AI 之「幻覺」問題—即模型生成無法源依據之虛假內容—在監理環境中具有高度危險性，一旦監理員誤引 AI 捏造之法條或數據，將直接影響監理決策之合法性。GabAI 透過 RAG 架構從根本上壓制此風險：系統所有回傳內容均嚴格錨定於已載入之官方文件，大型語言模型（LLM）僅就檢索結果進行整合生成，而非憑空推斷。此外，系統強制要求每一則回答均附上原始文件連結，以利使用者逐一複核。

(四)GabAI 系統之技術侷限

1. **缺乏數學運算能力**：系統擅長於文字檢索與摘要，但無法執行數學計算（如合計或增長率計算），相關數據須人工覆核。
2. **時效性與提問策略**：AI 缺乏時間感理解，無法辨識何謂「最新」資訊，故提示詞(Prompt)必須明確包含年份與日期。此外，須儘量具體提及法規手冊名稱(如 MORB)以提升回傳精確度。
3. **圖表與非結構化數據限制**：系統目前無法解讀掃描圖片式 PDF 或複雜之視覺化圖形（如圓餅圖），對於複雜表格處理亦有困難。

六、監理科技專案開發

(一)數位轉型之時代背景與監理缺口

1. 2023 年 3 月美國矽谷銀行（Silicon Valley Bank, SVB）倒閉事件清楚揭示，現代數位金融環境下之流動性危機可在不到 24 小時內產生。SVB 於 2023 年 3 月 8 日宣布無法籌集資本後，當日即有約 60%之存款流出，翌日存款流失比率接近 100%，堪稱史上速度最快之銀行倒閉事件。

2.現行主要流動性指標，包括流動性覆蓋率（Liquidity Coverage Ratio, LCR）及淨穩定資金比率（Net Stable Funding Ratio, NSFR），均係以約 30 天為壓力情境下之流動性流失假設期間，屬月度或季度頻率之靜態衡量工具。對此類「小時」速度發展的危機，完全失去預警效用，爰韓國發展存款即時監控系統。

(二)韓國存款保險公司（Korea Deposit Insurance Corporation, KDIC）存款擠兌預警系統

1. KDIC 存款監測系統之技術架構

KDIC 該系統之核心設計理念在於：透過儲蓄銀行聯邦作為數據中介、建立 API 連結、實現每 20 分鐘更新一次之高頻監測，並以存款下降達預設門檻值作為自動觸發條件，同步通報監理機關與中央銀行。此一架構將危機通報時間由傳統之日報制度大幅壓縮，充分體現「即時監控」理念之制度落地。

2. 數據傳輸路徑

系統之數據傳輸採三層架構：第一層為各家儲蓄銀行，負責整合並傳送存款資訊；第二層為「韓國儲蓄銀行聯合會（Federation of Savings Banks；類似臺灣全國農業金庫）功能」，作為數據集中中介機構；第三層為 KDIC，透過應用程式介面（API, Application Programming Interface），獲取存款數據。此一設計將數據傳輸標準化，確保 KDIC 無需逐一對接各家銀行系統，有效降低整合成本。透過每 20 分鐘更新一次存款數據之高頻監測能力。相較於傳統日報或月報制度，此一機制將監

理反應由數日縮短至分鐘級別，為存款異常流動之早期偵測提供技術基礎。

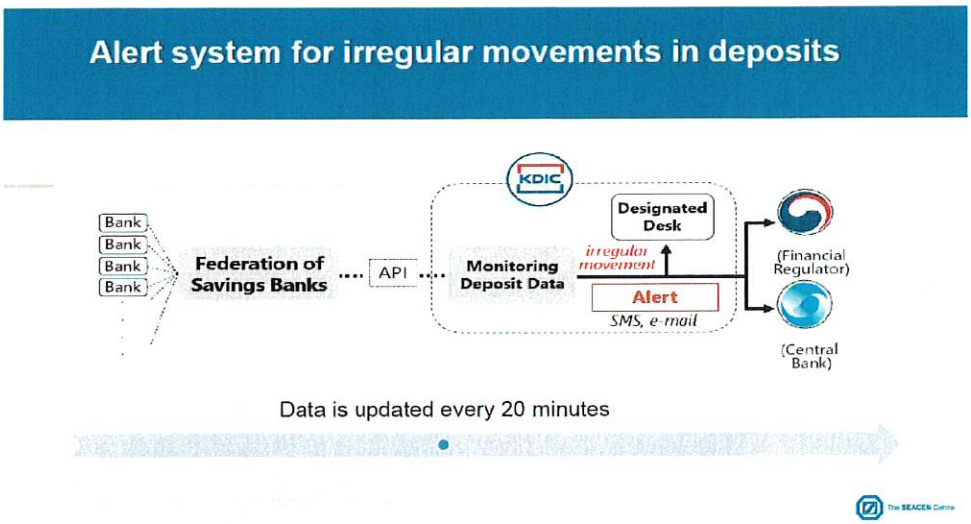


圖 七：存款異常流動警報系統。此流程圖呈現三層傳輸架構及從銀行端到監理端的自動告警路徑，資料每 20 分鐘更新一次。

3.異常偵測與自動化預警系統

系統設有明確之門檻值之觸發機制，當特定銀行之存款餘額在短時間內下降幅度達到預設某個百分比時，系統即自動判定為異常流動事件。一旦觸發，系統將透過簡訊或電子郵件，向指定管理台發出自動警報，全程無需人工判斷介入，確保通報時效。

4.跨機關同步通報架構

警報觸發後，系統將同步通報金融監理機關與中央銀行。其制度意涵在於：中央銀行若評估情況符合標準，得在危機萌芽之極早期階段介入，提供必要之緊急流動性支援，實現「監理預警」與「央行救援」之無縫銜接。

(三)發展監理科技之挑戰

1.數據治理

現行監理報送體系面臨之最根本技術痛點，在於「同一參數在不同機構間有不同定義（Same Parameter Reported Differently）」。此一問題導致數據在端對端整合過程中無法直接串接，須耗費大量行政資源進行人工清

洗與對帳，嚴重削弱監理決策之時效性與精確度。是以，建立統一之數據字典（Data Dictionary），確保全機關對相同參數採用一致定義，係推動監理科技轉型之前置重要工程。

2. AI 模型之可解釋性

鑑於 SupTech 系統日益深度整合 AI 與機器學習技術，監理機關在擴大應用規模前，必須確保以下治理框架之完備：其一，可解釋性（Explainability），AI 模型之決策邏輯須能向監理官及受監理機構清晰說明，不得作為「黑箱」；其二，模型風險管理（Model Risk Management），對演算法進行定期驗證，並確保跨報表之驗證邏輯（Interlinkages）相互一致；其三，人類監督（Human Oversight），人類對於自動化系統必須保有最終的控制權與責任。

3.動態反饋循環之持續義務

系統上線是建立動態反饋循環（Responsive Feedback Loop）之起點。監理機關必須持續依據市場演變調整預警門檻值與監控參數，並就誤報、重大異常與系統故障等不同警報類型，預先設計分級回應與職責分工機制，確保警報發出後有明確之問責路徑。

七、運用科技與人工智慧打擊金融犯罪、反洗錢與反資恐

(一)運用 AI 實務案例

1.泰國——監理技術應用之實驗場域

(1)人頭帳戶凍結政策之非預期後果：泰國央行初期授權銀行，凡帳戶符合特定「涉詐網絡特徵」即由系統自動凍結。然而，詐騙集團察覺此規則後，刻意向全國大量合法中小微型企業（SME）帳戶轉入極微小額資金，致使無數清白之合法商家帳戶因被系統誤判為詐騙網絡節點而遭集體凍結，引發社會抗議與行政混亂。泰國央行被迫於兩至三週內緊急修正凍結準則，加入交易頻率、單日交易次數及特定金額區間等多項判定條件，以取代原先過度僵化之單一關聯規則。

(2)監理數據轉型專案（Regulatory Data Transformation, RDT）之三階段推進：核心目標係將金融機構之報送數據從彙總型態的數據升級為顆粒化數據，儲存於標準化數據集市（Data Marts）中，以作為建構 AI 監理入口網站之數據基礎。然而，實務推動中遭遇銀行強烈抵制：各機構既有系統架構與央行要求之七個標準化數據模組架構，概念差異懸殊，重置成本高昂，多數銀行明確拒絕投入系統改造資源。最終，泰國央行採取分階段務實策略，依序推進信貸數據、支付數據及外匯與衍生性商品數據三階段，以漸進式路徑取代一步到位之理想藍圖。

(3)彩券日資金網絡分析實驗：每月公布彩券號碼後一小時內，針對全國資金流動進行即時網絡分析（Network Analysis），藉由視覺化圖形中異常龐大之資金節點（Big Node），成功識別出非法地下博弈或犯罪組織之資金轉移行為。此一技術現已被延伸應用於詐騙偵測場域，充分展現顆粒化數據結合 AI 視覺化分析之監理，可掌握完整之跨機構資金流向全貌。

2. 新加坡—— AI 預測性宣導與多部會協作典範

新加坡之監理實踐展現了將 AI 預測能力與國家級跨部門協作機制深度整合之先進模式。

(1)AI 行為預測與針對性詐騙宣導：新加坡當局運用 AI 模型預測社會行為模式，並據此主動部署防詐宣導，如當系統預測未來兩週將有大型 K-pop 演唱會時，AI 即預判將出現大量假門票詐騙，促使當局立即針對性發動宣導活動；此外，AI 亦能識別每年八至十月為退休金提領高峰季，研判此期間

投資詐騙風險將顯著攀升，從而提前於八、九月間精準投放防制性資訊，此「事前預測、主動干預」之模式，公眾宣導從被動回應轉向主動預防之重大典範。

(2)國家防詐中心之協作架構：新加坡以內政部（Ministry of Home Affairs）作為跨部門協調之「指揮者（Conductor）」，整合中央銀行、電信業者與各執法機關之資源，形成一體化之詐騙防制生態系。此架構之核心邏輯在於：詐騙涉及金融、電信、科技平台及執法等多個領域，唯有以具法律權威之國家級機構統籌協調，方能實現有效預防與追查。

(二)跨國監理碎片化與協作機制建立之迫切性

當前跨境詐騙之監理困境：「人頭帳戶在國家 A、騙局本身在國家 B、受害者在國家 C」，各國監理架構差異為詐騙集團創造可剝削之法律漏洞。因此，建立具法律效力之跨國數據共享協議、統一之詐騙事件通報標準，以及多邊監理協作機制，乃當前最為迫切之制度性建設工作。

八、紐約州金融服務署(NYC DFS)的法遵科技與監理科技之經驗與實務案例

(一)數據驅動監理之全套落地實踐—以虛擬貨幣為例

建構之監理科技體系，係目前全球虛擬資產監理領域中，自法規設計至技術實作均最為完整之範例之一，其應用場景如下：

1.代幣上架（Coin Listing，即將新的加密貨幣加入加密貨幣交易所的可交易清單中）監控儀表板

DFS 自 2015 年開始監理紐約虛擬貨幣業務，數據治理團隊維護一份代幣主表（Master Table），記錄各受監理機構所提供之虛擬貨幣產品、初始自我認證時間、是否在紐約提供服務，以及上架與下架日期，並上傳至 Snowflake 數據倉儲後對接 Tableau(係視覺化軟體，可查詢關聯式資料庫和電子試算表以及視覺化資料)，產製區塊鏈分布與代幣分布儀表板。監理官得透過儀表板懸停功能(即當滑鼠游標停在圖表元素上時會自動彈出詳細數據)，即時識別所有提供特定幣種服務之受監理機構；當比特幣價格出現顯著跌幅時，亦可迅速掌握受影響機構名單，為即時風險應對提供數據支撐。

2.資本充足率監控儀表板

DFS 依監理協議要求受監理機構每月申報資本數據，包含冷錢包託管資產、熱錢包託管資產、傳輸中資產及停業成本等四大因子之每日平均值與期末餘額，並設有尖峰日交易金額欄位，以反映交易高峰期之最大風險暴險。Tableau(係視覺化軟體)儀表板提供過去 12 個月之趨勢圖，監理官可藉由工具提示（Tooltip，即滑鼠游標懸停在某圖示不點擊時，系統彈出一小的懸浮視窗）即時拆解要求資本之四大組成，並觀察熱錢包是否出現異常波動。當資本比率低於 110%門檻時，系統觸發每日申報機制，受監理機構須連續至少 10 個日曆天提交日報，直至 DFS 判定風險解除為止，形成自動化之監理強化機制。

3.穩定幣監控儀表板

DFS 於 2022 年年中發布美元掛鉤穩定幣發行指引，要求受監理機構定期提交涵蓋供應端（Supply Table）及儲備端（Reserve Table）之詳細數據，包括各區塊鏈之總發行量、淨發行量、總流通量，以及儲備帳戶之銀行名稱、SWIFT 代碼、資產組成（含存款、國債、反向回購及貨幣市場基

金）。儀表板以鑄幣（Mints，綠色長條）與銷毀（Burns，紅色長條）視覺化供應動態，並以「緩衝區（The Buffer）」，即總儲備減總供應量，作為核心監控指標。一旦緩衝比率（Buffer Percentage）趨近於零，即代表穩定幣之 1:1 美元掛鉤面臨重大壓力，係監理官優先關注之預警信號。

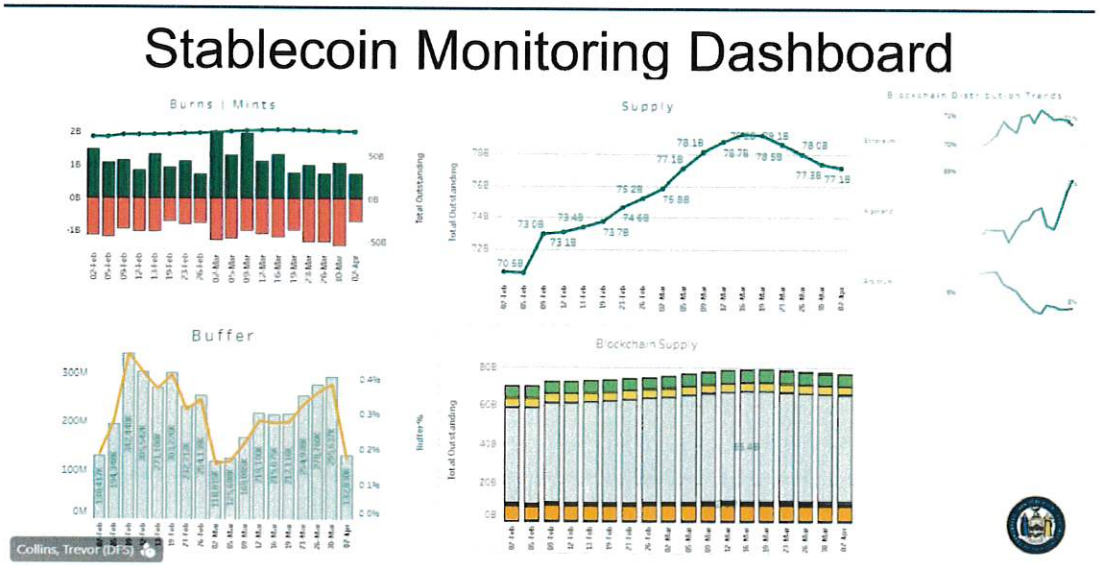


圖 八：穩定幣監控儀表板。(左上角為「Burns / Mints」綠紅雙色長條圖，直接以顏色區分鑄幣與銷毀量；左下角為「Buffer」折線區域圖，以區域填色呈現緩衝區（總儲備減總供應量）隨時間之變動趨勢，並可觀察是否趨近於零；中間另有「Supply」走勢圖。此種「顏色＋面積」的視覺設計，能讓監理官一眼掌握緩衝區是否逼近警戒線)。

4.大額虛擬貨幣交易報告（VCTR）儀表板

(1)依 NYDFS 發布的（法規代號：23 NYCRR Part 200）中的《第 200.15 條：反洗錢計畫，對於幣對幣交易單日累計逾 10,000 美元者須觸發申報。DFS 已完成 VCTR 申報 API 之建置，數據流轉路徑為：虛擬貨幣實體（API）→Oracle 資料庫→SQL Server 數據倉儲→Tableau 儀表板。最終產出 Excel 試算表與 Tableau 儀表板。

(2)儀表板呈現交易筆數與美元交易量之月增率趨勢，並依鏈上（On-chain）存取款、鏈下（Off-chain）帳本交易及客戶對客戶（P2P）交易分類監控。當圖表出現異常高峰時，監理官於定期會議中直接向機構詢問原因，形成數據導向之主動監理對話。此外，儀表板亦揭示全美地理分布，課程演示數據顯示，交易量與筆數最高者為加利福尼亞州，反映 DFS 之監理視野已超越紐約州轄區本身。

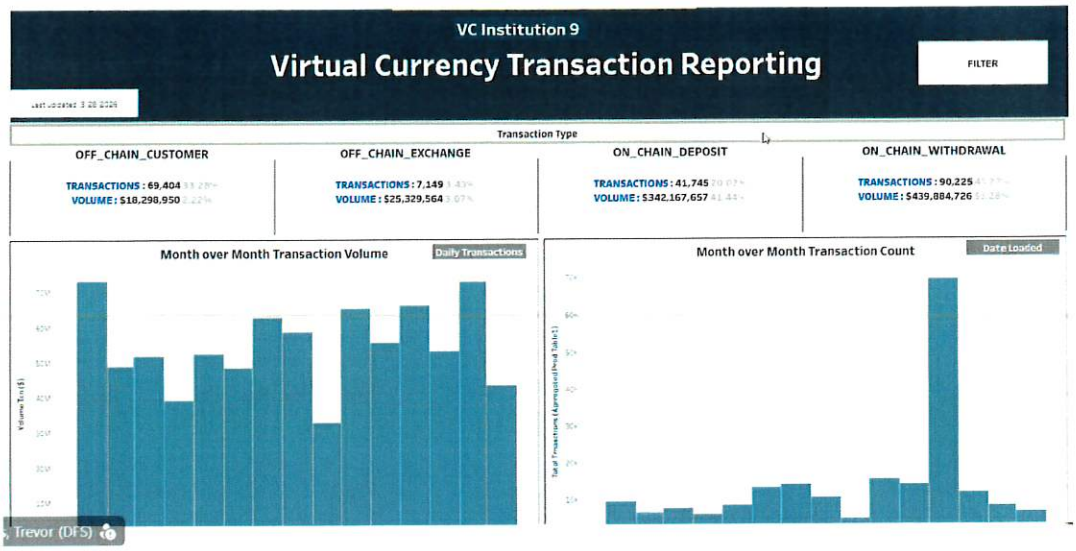


圖 九：交易筆數與美元交易量之月增率趨勢之儀表板

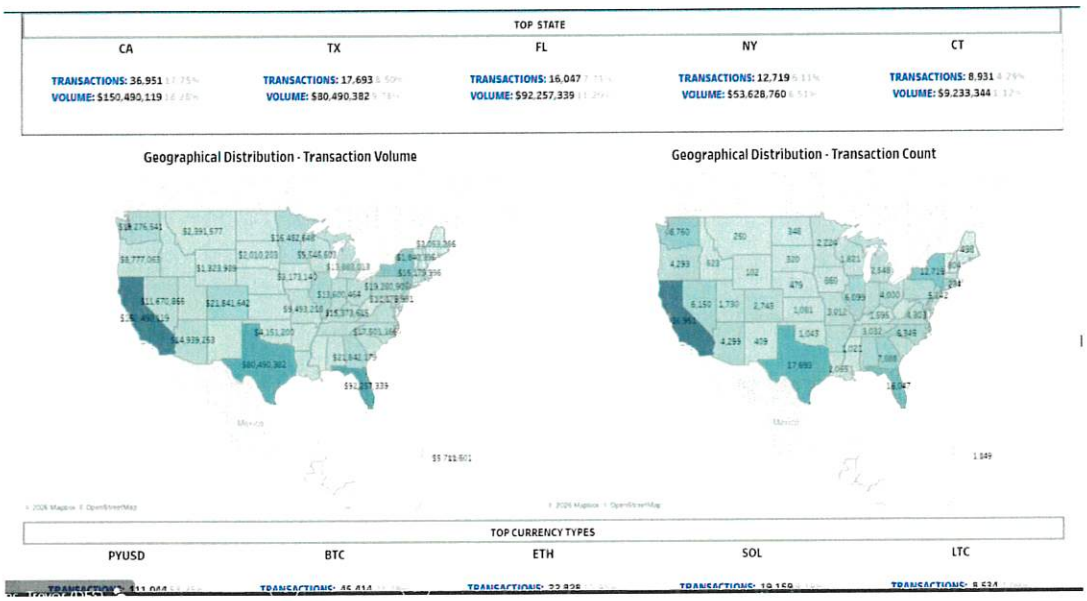


圖 十：地理分布儀表板(以美國地圖色塊呈現各州交易量與交易筆數的「地理分布熱力圖」，並列出 Top State 排行（含加州 CA 數值最高）

(二)新興市場監理機關之實務建議

就斯里蘭卡詢問有關新興市場如何建構虛擬資產監理框架，其建議如下：

1.以資本充足率框架為最優先基石，設定機構必須維持之最低資本門檻，並將市場波動情境納入考量。

2.建立自動化預警機制，確保資本低於特定門檻時系統能即時發出警示。

3.將反洗錢（AML）計畫與客戶識別（KYC）審查列為申請准入之核心審查標準，要求新申請人於申請階段即須證明具備完善之 AML 政策與執行安排。

(三)虛擬貨幣市場波動之系統性風險控管

1. 壓力測試方法論

DFS 針對少數獲准將比特幣計入監理資本之機構，採用過去數月之價格波動歷史數據建立情境模型，模擬比特幣下跌特定百分比時，機構實際資本何時跌破法定要求資本之臨界點。透過雙重控制手段，限制虛擬貨幣計入監理資本之上限比例，並要求維持最低現金持有量，已在制度層面預先降低市場極端波動引發連鎖之系統性風險。

2.迷因幣（Meme Coins，係基於網路的爆紅梗圖、搞笑影片、時事話題等而誕生的加密貨幣其價格取決於社群熱度）之監理態度

對美國監理機關言，該類虛擬幣缺乏基本面支撐，持高度保留態度，認定為危險異常且須提高警覺防範發生問題。

九、印度儲備銀行運用監理科技工具強化網路安全監理之實踐

(一)有關網路安全之監理模型與平台

1.關鍵風險指標（KRI）模型：量化評分機制

(1)數據採集規模與分類：RBI 定期透過 DAKSH 門戶蒐集每家銀行 160 個網路安全相關細部數據點，如：資料庫已修補 vs.未修補比例、存取關鍵伺服器時是否規避特權帳號管理系統之越權行為、已回報但尚未處理之漏洞數量等多個維度資訊。

(2)模型技術架構：採用 Java 與 Python 等多種程式語言開發，內建數學公式以計算各項風險比率，並將 160 個數據點分別映射至「風險指標組（Risk Indicator Group）」。

(3)單一評分與決策連結：模型最終計算出每家銀行在特定時間點之單一網路安全風險評分。監理機關透過視覺化之蜘蛛圖（Spider Chart）直觀呈現各機構在 ATM 安全、委外管理、身分識別管理、數據安全等逾 20 個子領域之強弱分布；並結合季度趨勢分析。此一評分結果直接作為決定「該機構近期是否須進行現場查核」之優先排序依據，實現資源之精準投放。

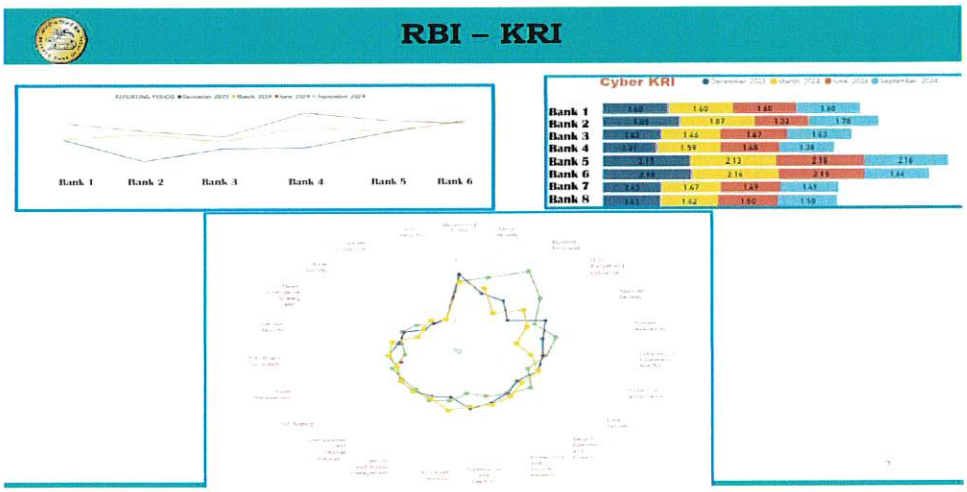


圖 十一：關鍵風險指標（KRI）模型。左上為各銀行跨季度 KRI 折線趨勢圖，右上為各銀行 Cyber KRI 各季橫條比較圖，折線圖與橫條圖係跨機構、跨時期的風險比較。下方為多維度蜘蛛圖（Spider Chart），以超過 20 個安全子領域（ATM Security、Network Security 等）呈現單一機構之風險輪廓。可瞬間辨識一機構的「弱點集中區」。

2.微觀數據分析（MDA）平台：AI 輔助非結構化文件深度分析

(1)AI 處理非結構化文件之具體應用案例：MDA 之主要分析對象包括受監管機構之董事會 IT 策略委員會會議紀錄、資訊安全委員會議程，以及標準作業程序（SOP）等文件。AI 工具可自動閱讀數百頁之會議紀錄，識別哪些重要議題已獲充分討論，哪些議題雖被排入議程卻遭反覆略過（Agenda Skipping）。若某一關鍵議題連續多次於會議中被以「讓我們進入下一個議題」一語帶過，此本身即構成重大之監理發現（Supervisory Finding），顯示管理層對該議題之重視程度不足，反映出深層之治理漏洞。

(2)KRI 與 MDA 之交叉關聯分析之案例：若 KRI 評分顯示某機構之「IT 策略指標」分數持續下滑，監理官可旋即調用 MDA 分析該機構過去兩年之委員會會議紀錄，進一步查明究竟係因相關委員會根本未如期召開，抑或會議雖已召開但採購議案始終未獲核定預算所致。此種「量化預警啟動、質性文件確認」之雙軌方法論，可產出極為精準之針對性監理意見（Targeted Opinion）。

(二)運用 AI 監理之實務與案例

1. RBI 網路安全 SupTech 工具生態系之實務部署

鑑於單一工具難以涵蓋網路安全監理之全部面向，RBI 爰在 DAKSH 主幹平台之外，另行建置一套環繞主幹之立體工具生態系，各工具分別針對不同攻擊向量與監理痛點提供精準之問題解答。

(1)網路釣魚模擬演練（Phishing Simulation Exercise）：電子郵件釣魚攻擊迄今仍為金融機構遭受網路入侵之最主要初始攻擊媒介之一。RBI 爰開發網路釣魚模擬演練工具，可同時對最多 5,000 個受監管機構同步發起模擬釣魚攻擊，量測各機構之電子郵件安全防護成熟度。具體評核面向包含三項：其一，受測機構能否有效偵測並封鎖偽冒 RBI 網域之「仿冒網域（Look-alike Domain）」來信；其二，電子郵件網域型訊息驗證、網域金鑰識別郵件及寄件者政策之設定合規情形；其三，員工對於含有惡意附件或可疑連結之釣魚郵件之識別及回報能力。此工具使監理機關得以在完全不需事先知會受監管機構之情況下，以「真實世界攻擊情境」為準繩，對全體機構之電子郵件防禦能力進行客觀、一致之橫向比較評估。

(2)網路偵察工具（Cyber Reconnaissance）：為一被動式外部攻擊面掃描工具，無需與受測機構之內部系統進行任何互動，即可從外部攻擊者之視角全面盤

點各機構之數位風險暴露程度。監理機關將其偵察結果與機構自行委託之漏洞評估比對，此工具可揭穿機構「書面合規」情形，確保監理機關評估所依據之技術有充分可信度。依該國經驗，評等為 D 或 F 之銀行遭受勒索軟體攻擊的機率，高達評等為 A 之銀行的 7.3 倍，充分佐證 KRI 風險評分與現實威脅暴露程度之強烈相關性。

(3) Cyber Edge（Cyber Range）實戰演練平台：此為 RBI 目前在主動量測網路韌性方面最具前瞻性之工具。Cyber Edge 係一完整模擬真實銀行 IT 生產環境之封閉式演練平台，平台可容納 10 至 20 個金融機構同步參與，由 RBI 內部之技術團隊扮演「紅隊（Red Team）」主動發起攻擊，受測機構之 IT 與資安人員則作為「藍隊（Blue Team）」進行防禦並進行綜合評分，亦評估高層管理人員面對大規模網路攻擊時之危機處理與治理決策之能力。

2. RBI 近年推動之三項生態系統層級（Ecosystem-level）之國家監理防禦措施

(1).bank.in 專屬網域強制遷移：要求所有受監理銀行將其官方網站遷移至.bank.in 受管制頂層網域，透過行政手段從源頭消滅網路釣魚詐騙中大量使用之偽冒銀行網站。

(2)簡訊標頭綁定（SMS-Header Binding）：以區塊鏈技術為底層骨幹，在電信層對金融機構發送予客戶之商業簡訊進行發送方身分驗證，從電信網路層級系統性攔截偽冒金融機構之詐騙簡訊，使攻擊者無法輕易偽造合法金融機構之發訊標頭。

(3)1600 系列客服專號統一機制：要求金融機構對外撥出之交易相關客戶服務電話統一採用 1600 開頭號碼，便於客戶即時辨識來電之合法性，降低電話語音詐騙得逞之機率。

(三)風險控管

1. 網路事件通報時效之黃金時限設計

RBI 要求受監管機構於識別重大網路事件後 2 至 6 小時內完成初步通報，此「黃金通報時限」之設計邏輯，在於即便機構在事件發生初期尚無法全面掌握原因，監理機關亦須在最短時間內獲悉潛在之系統性衝擊，以便啟動必要之跨業協調與防範措施。爰此，RBI 要求所有委外服務合約（Outsourcing Contracts）之服務等級協議（Service Level Agreement，SLA）中，強制納入

供應商在發生安全事件時對委託機構之通報義務條款，確保通報責任鏈自受監管機構向下延伸至其整個第三方服務供應鏈。

2. 供應商集中度風險之系統性管理

鑑於金融機構高度依賴少數主要資通訊（ICT）服務供應商，一旦關鍵供應商發生技術故障或遭受攻擊，其連鎖效應可能同時癱瘓多家金融機構，形成不可忽視之系統性崩潰的風險（Systemic Failure Risk）。爰此，RBI 建立「網路地圖（Cyber Mapping）」框架，每兩年系統性盤點一次受監管機構與 ICT 服務供應商之依賴關係，識別整個金融體系中具有「單點失效（Single Point of Failure）」特性之關鍵技術節點，並據以訂定集中度上限與備援要求。

十、標準制定機構數據倡議概述：以日本銀行開發證券融資數據蒐集與彙整之經驗為例

(一)日本銀行依金融穩定委員會標準蒐集證券融資交易數據

1.政策起源與目標

鑑於 2008 年金融危機揭示證券融資交易（Securities Financing Transactions, SFTs）資料掌握不足之問題，G20 指示金融穩定委員會（FSB）建立全球數據標準，涵蓋附買回協議(以有價證券作為擔保之短期融資機制，為金融機構及政府取得流動性之重要來源)、證券借貸(將持有證券出借予市場參與者進行放空交易，並收取擔保品)與保證金貸款(由主要經紀商向避險基金或投資人提供槓桿融資)。其核心目標在於透過數據標準化與彙整，提升數據品質、共享機制及跨境監測能力，方能及早辨識潛在風險並維護金融體系穩定。

2.日本推動數據監理成功之策略

(1)機關職能深度互補：日本金融廳(JFSA)依法擁有要求金融機構報送資料之法定權限，日本銀行(BOJ)則具備較強之技術能力及研究資源，由日本銀行投入 500 萬美元研負責建置數據蒐集平台，維護資訊系統及進行監理分析。雙方透過人員借調制度深化合作，形成法律監理能力與技術分析能力之互補架構，有效提升監理數據治理效能。

(2)市場特性與漸進式策略：利用日本 Repo 市場高度集中之特性（前 50 大銀行及證券商已占整體市場交易量超過 95%）爰當時規劃聚焦有限家數之重要機構，提升數據蒐集效率與覆蓋率，採行「從小處著手(Start Small)」策略。透過長達兩年的定期對話，將數據項與國際標準完全對齊，日本為 23 個會員轄區中唯一達成 FSB「綠燈」評等之國家。

3.日本推動數據監理成功之作法

(1)建立密切溝通機制：制度建置初期連續兩年每月召開協調會議，並透過大量說明會與問答交流，協助業者理解申報要求及技術規格。

(2)落實標準化定義：將所有資料欄位、格式及交易定義與 FSB 國際標準完全接軌，確保跨國資料具可比性。

(3)採取分階段推動策略：優先建立業者報送習慣，再逐步提升資料品質與細緻程度，避免一次性要求過高造成執行困難。

(4)日本共通數據平台建置經驗：日本銀行將共通數據平台視為監理現代化的重要基礎建設。其核心概念係建立統一的資料交換與管理架構，使各金融監理機關能共享相同資料來源，避免金融機構重複申報及監理機關重複蒐集。透過共通平台機制，監理機關可直接取得標準化且具高顆粒度之監理數據，並結合法人機構識別碼等國際標準進行跨機關與跨國資料串接，

該國數據可直接納入 FSB 全球資料庫，作為國際監理分析基礎，強化國際接軌，提升金融風險監測能力及國際監理合作效率。

(5)直接蒐集底層交易資料並自行計算 12 項早期預警風險指標（Early Warning Indicators），包含部位暴險、槓桿程度、融資來源、保證金準備、流動性、展期風險、集中度、互連性、敏感度、擁擠度及潛在損失等面向，透過提升資料顆粒度與報送頻率，以有效辨識高槓桿部位與潛在系統性風險，並提升監理機關掌握國際資本流動及風險傳染之能力。

(二)G20 框架下的監理現代化

1.監理現代化之核心理念

(1)由定期報送轉向持續監測，直接蒐集交易層級數據。

(2)由人工處理轉向自動化分析，提升監理效率與資料品質。

(3)由事後查核轉向事前預警，透過風險指標及異常偵測機制提前發現潛在風險。

(4)由機關分散管理轉向跨機關共享，建立共通數據平台與標準化資料架構。

2.人工智慧(AI)於監理科技（SupTech）之應用

(1)異常交易偵測：運用機器學習模型分析大量交易資料，自動辨識異常交易行為及潛在風險事件。

(2)早期預警系統：透過槓桿、流動性、集中度及保證金等風險指標，建立即時監控機制。

(3)跨境風險分析：整合多轄區數據來源，辨識跨境金融活動及風險路徑。

(4)監理報表自動化：利用 AI 進行資料整理、驗證及報告生成，減少人工作業負擔。

(5)政策決策支援：透過情境分析及風險模擬，協助主管機關評估政策措施可能產生之影響。

3.AI 導入監理之治理挑戰

AI 雖可大幅提升監理效率，但仍須兼顧資料品質、模型風險及治理要求。監理機關於導入 AI 時，應建立透明且可解釋之治理架構，確保模型輸出具備可驗證性與可追溯性，並建立適當的人工作業覆核機制，避免過度依賴自動化決策。

此外，監理機關亦須持續強化資料治理能力、培育數據分析及 AI 專業人才，並透過跨機關合作及國際標準接軌，逐步建構具韌性之智慧監理體系。

十一、香港金融管理局監理科技與法遵科技之實務案例

(一)數據集中與處理平台

1. Supervision 360（S360）平台

係一端對端數位監理平台，定位為「一站式銀行資訊門戶」，作為 HKMA 內部之單一資訊來源，該平台提供受監理機構關鍵資訊與指標之整體概況，大幅提升工作流程與管理效率。

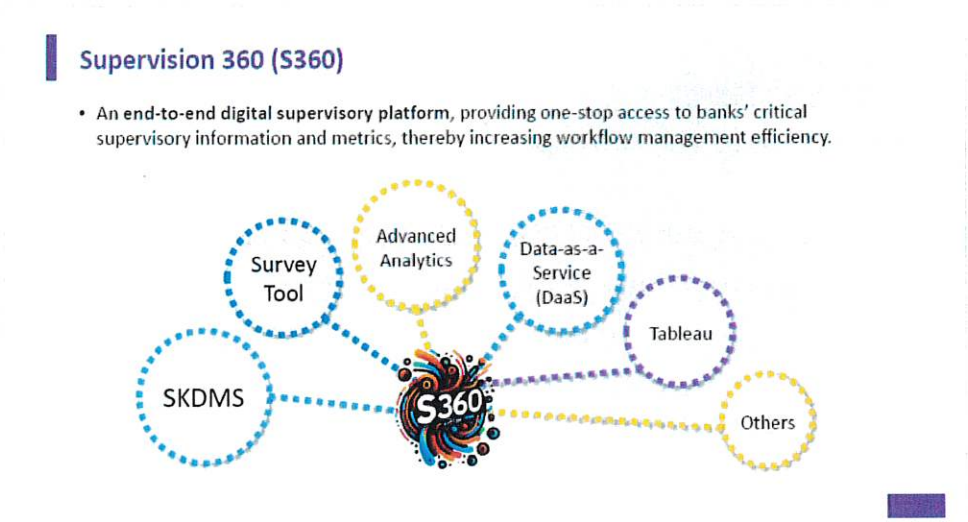


圖 十二：S360 概況

2.智能知識管理系統（SKDMS）

該系統集中儲存跨部門之監理資訊，同時處理結構化資料（如銀行申報表／Banking Returns）與非結構化資料（如董事會會議紀錄、內部審計報告），並具備文件標籤（Tagging）與全文檢索功能，解決過去文件分散且難以搜尋的痛點。

(二)自動化與行為監控工具

1.機器人流程自動化 (RPA)

模擬人類點擊、輸入、複製貼上等動作，自動處理高重複性且具備規則邏輯的任務，如數據提取、填表、報表生成及系統監控等，降低人工負擔。

2.語音轉文字(Speech-to-Text)

利用 AI 轉錄多語音（如廣東話、普通話、英語）銷售錄音轉為文本，並結合 NLP 情緒分析與關鍵字識別。實例：抽查複雜金融產品銷售行為，確認銷售人

員是否依規提供足夠的風險免責聲明，以及評估客戶是否理解產品。

3.自動化調查工具 (Survey Tool)

建立 Web 版平台，簡化 HKMA 發布特定調查需求及蒐集銀行回覆之作業流程。

(三)前瞻性分析技術

1.新聞掃描工具(AMI)

利用自然語言處理（NLP）及大型語言模型（LLM）監控社群媒體與新聞，進行情緒分析。它能主動發出警報，及時識別負面事件或系統性危機（如大規模系統故障、詐騙案），針對新聞與社群媒體進行橫向掃描（Horizon scanning），識別潛在風險並發送主動告警。

2.網絡分析（Network Analytics）

可視化借款人與技術供應商間的關聯，識別銀行體系之集中度風險與系統性威脅。

3.資產質量預測

建立機器學習模型分析細粒度數據，識別信用風險之早期預警訊號。

(四)以上技術的後續維護與功能增強的方式

主要係透過與專業技術公司合作，利用市場上成熟且先進的技術實現監理工具的數位化，尚非完全依賴 HKMA 內部的技術開發人力。

十二、各國監理機關在監理科技上的跨國多邊協作機制

(一) SupTech 之生命週期：從概念到部署

1.技術從研發到實際應用之三階段生命週期

(1)概念驗證（Proof of Concept, PoC）：此為最初步之技術可行性驗證階段，規模通常極小，目的在於確認特定技術方案能否解決預設之監理業務問題。

(2)運作原型（Working Prototype, WP）：係將 PoC 擴展為可供業務端實際測試之雛型模型。此階段面臨的核心挑戰為「規模化」（Scaling Up）。

(3)正式部署（Deployed, DP）：指技術工具完整整合進組織日常工作流程，並達到大規模實際應用之狀態。

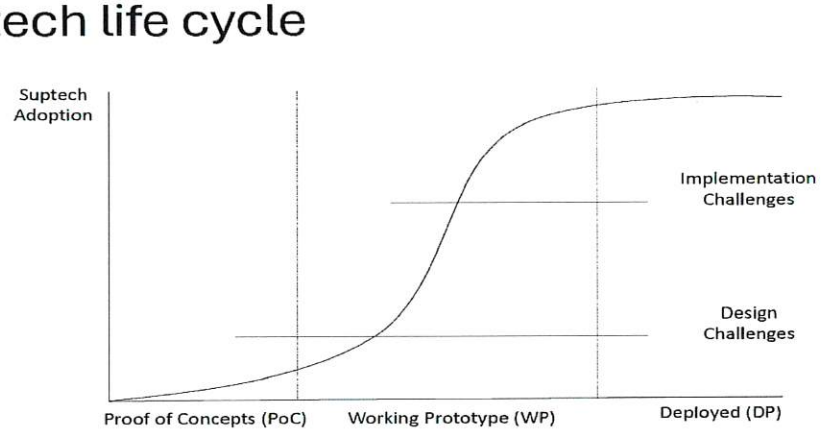


圖 十三：監理科技的生命週期。橫軸為 PoC→WP→Deployed 三階段，縱軸為 Suptech Adoption 程度，並用兩條水平線標示「Design Challenges」與「Implementation Challenges」兩大挑戰發生的時間點與相對位置。

2.該生命週期衍生兩大關鍵挑戰

(1)設計階段挑戰（Design Challenges），發生於 PoC 與 WP 之間，包括應用案例優先順序之決策、資源投入之分配，以及確保技術方案與真實業務問題之間具備高度「契合度」（Good Fit）。

(2)實施階段挑戰（Implementation Challenges），發生於 WP 轉向正式部署之過程，此為最困難之環節，涉及與既有舊系統之對接整合、雲端部署之合規性、

持續更新維護機制、模型生命週期管理（Model Lifecycle Management），以及專案整體之治理結構建立。

(二)各國監理運用 AI 實務與案例

1. 全球 SupTech 部署現狀之實證調查

佛羅倫斯銀行與金融學院（FBF）及劍橋大學合作，對全球 97 個國家 112 家金融監理機關進行之大規模調查（Gambacorta et al., 2025），共涵蓋 104 個 SupTech 使用案例，調查結果發現：絕大多數受訪機關之「正式部署」（Deployed）數量趨近於零，多數 SupTech 工具仍停滯於概念驗證（PoC）或運作原型（Working Prototype）階段。該數據顯示，全球監理機關普遍陷入「PoC 陷阱」，雖持續投入研發資源，卻在技術轉化為實際監理產能之關鍵環節遭遇嚴重瓶頸，且此現象無論在成熟市場或新興市場均廣泛存在。

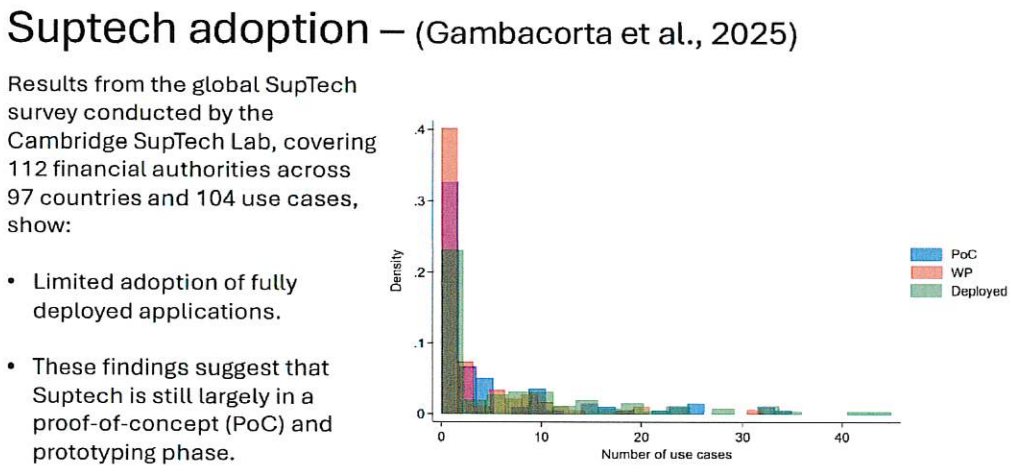


圖 十四：監理科技部屬情況。一張三色重疊直方圖，橫軸為使用案例數量、縱軸為密度，可見三色分布皆高度集中於左側 0 附近，紅色（WP）峰值最高且最靠近 0，綠色（Deployed）分布明顯較為扁平且趨近於 0，亦即正式部署數量趨近於零、多數停留於 PoC/WP 階段。

2. 荷蘭中央銀行氣候風險「數位孿生」（Digital Twin）專案

(1)採開源協作模式(Open Source Collaboration，係去中心化、高度透明的群眾參與開發模式)：評估洪水（Flooding）及森林火災（Wildfire）等極端氣候事件對其房貸資產組合之影響，屬氣候相關金融風險（Climate-Related Financial Risk）之 SupTech 應用。

(2)該技術實現方式具有高度可複製性：在資料來源方面，衛星地理數據（如房屋坐標、地形高程資料）與來自「信用登記處」（Credit Register）之私有敏感信用資料。在資料保護方面，敏感信用資料於程式碼中設有明確之隔離標記，確保對外共享時絕不外洩。在共享範疇方面，雖機密數據不對外流通，惟其完整之技術管線（Pipelines）架構與資料處理邏輯均完整公開，大幅降低他國監理機關複製開發之門檻，提供全球可直接援引之「架構藍圖」。

3. 歐洲央行（ECB）在單一監理機制（Single Supervisory Mechanism, SSM）架構下建立「虛擬實驗室」（Virtual Lab）

此係一共享監理科技環境之典範，此平台整合 Power BI(Microsoft 開發的數據分析與資料視覺化平台)以及不同規格的 OpenAI 基礎設施，系統根據資料的機密程度提供不同的運算能力，虛擬實驗室設有專門的程式碼庫，平台設有專屬之程式碼庫供所有 SSM 成員機關查閱，並建立「公共化標記」（Public Tag），凡經標記為「Public」之專案，所有參與 SSM 之成員國之中央銀行均可直接調用其開發邏輯，實質上形成歐洲監理科技之區域性共享生態系。

十三、西班牙銀行 (BdE) 的監理科技專案與應用案例

(一)金融監理運用 AI 背景說明

1.西班牙銀行推動監理科技之核心願景

突破過往「等待銀行申報、事後被動回應」之傳統監理模式，轉型為「主動偵測、數據驅動決策」之現代監理架構。該願景之落實須有高階管理層之支持與確保資源分配與策略目標之一致性，爰高階決策者有接受 AI 觀念的教育訓練，以具備足夠技術視野，有效引領組織轉型。另其設立數據長（Chief Data Officer, CDO）建構完善的數據架構，以確保數據品質、數據治理與數據流通之規範化。

2.監理機關必須掌握開源模型之能力

先就「專有雲端模型（如 OpenAI API）」與「本地部署開源模型（On-premise Open Source Models，如 Llama、DeepSeek 系列）」，評估二者在監理上所須能力之差異。鑑於 AI 領域之地緣政治風險日益顯著，監理機關必須掌握在自有基礎設施上運行開源模型之能力，以確保監理數據之主權安全不受制於單一商業供應商，爰選擇「本地部署開源模型」。

3.西班牙銀行「開源模型」來自歐洲央行「虛擬實驗室」雲端平台

歐洲央行單一監管機制（SingleSupervisory Mechanism, SSM）體系建立「虛擬實驗室」雲端平台，邀請來自歐洲各國監理主管機關技術人員密集協作開發，採全面開源（Open-source）原則，所有程式碼與開發成果均供所有參與機構自由使用，以期形成歐洲監理社群共同的技術資產。西班牙銀行即利用該平台之開源模型建立監理系統。

(二)西班牙銀行運用 AI 之實務案例

本課程以該行概念驗證（PoC）應用案例為主軸，各案例均以解決真實監理痛點為出發點，分述如下：

1. 案例一：「貸款失火了」（This Loan is on Fire）—氣候實體風險評估工具

(1)鑑於氣候變遷衍生之實體風險（Physical Risk）對銀行資產負債表之潛在衝擊日益受到國際監理機關重視，此案例係建立一套量化評估框架，模擬森林野火與洪水等極端氣候事件對西班牙銀行體系房貸資產組合之財務影響。

(2)多源數據整合架構：將四個類別之異質性數據加以整合，包含如下：

A.氣候類：野火數據取自 NASA 衛星圖像，洪水水位高度數據取自歐盟哥白尼計畫（Copernicus）。

B.房地產類：取自西班牙地籍局（Catastro）之精確建築物地理坐標及物理特徵（樓層數、用途類別）。

C.信用類：以西班牙信用登記局（Cirbe）數據為基礎，透過「隨機位置分配」技術生成合成數據（Synthetic Data），將貸款合約與真實地理坐標進行匹配，構建銀行資產組合之「數位孿生（Digital Twin）」模型。

D.損害估算類：應用歐盟聯合研究中心（Joint Research Centre, JRC）之損害函數（Damage Functions），依據災害強度（水深或火災半徑）計算建築物資產價值之減損比率。

(3)關鍵監理指標產出：模型產出三項核心監理指標：風險暴險（Exposure at Risk）（受災區域內之總貸款餘額）、貸款成數（LTV）上升幅度（因抵押品價值下跌所致）以及違約損失率（LGD）估算值，使監理人員得以即時回答諸如「若瓦倫西亞發生特定規模洪水，特定銀行之資本充足率將受多大衝擊」等精確監理問題。此外，以去年當地真實洪水與野火事件進行回溯測試（Backtesting），驗證模型預估損失之準確性，並確立後續研究方向——探討保險覆蓋率是否足以緩解上述損失，以評估銀行整體韌性，該案例係由荷蘭央行（DNB）與 BIS 創新中心（BIS Innovation Hub）協同開發。

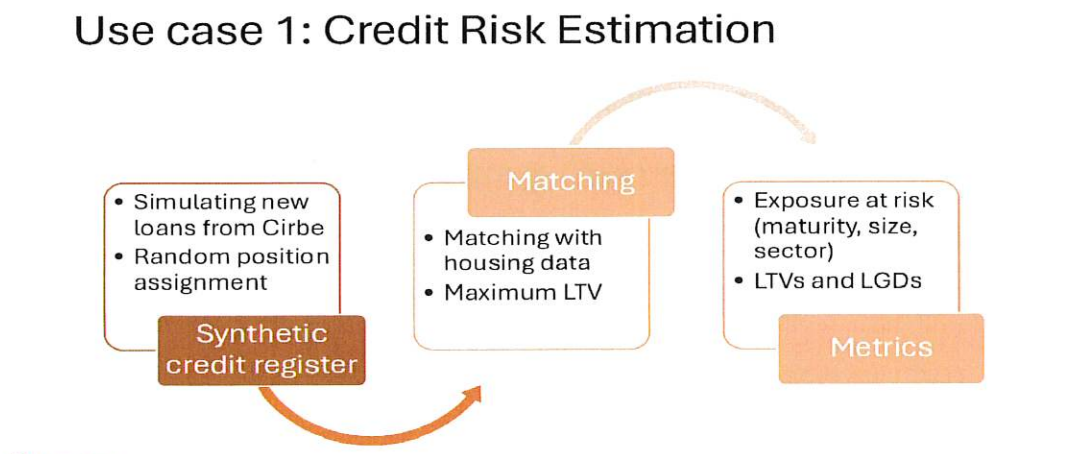


圖 十五：信用風險估算流程圖。左方「合成信用登記」方框（包含「模擬新增貸款」與「隨機位置分配」）→中間「匹配」方框（包含「與房屋數據匹配」與「最高 LTV」）→右方「指標」方框（包含「風險暴險與「LTV 及 LGD」），上方另有一條弧形回饋箭頭，顯示三個節點間之循環關係。

2.應用案例二：銀行系統停機獨立監測系統(Subito)

(1)現狀痛點：現行監理實務下，監理機關對於銀行系統停機事件之掌握，主要仰賴銀行依規定進行手動申報。然依歐盟《數位營運韌性法案》（Digital Operational Resilience Act, DORA）之規定，重大事件雖須於 4 小時內完成通報，但對於「非關鍵性停機」或「小規模系統故障」，銀行仍可能選擇延遲申報或不予申報，形成監理資訊之盲區。Subito（義大利文，意為「立即」）工具之開發目的，即在建立一套不依賴銀行自願申報之獨立偵測機制（Independent Detection Mechanism）。

(2)運用的技術：

A.技術架構：系統每小時透過 Google Trends API（serpapi）掃描所有歐洲央行單一監管機制（SSM）成員國，持續監控各受監理銀行之名稱搜尋熱度。當搜尋量出現異常尖峰時，系統即擷取相關搜尋詞彙，投入大型語言模型（LLM）進行語意分析，以區辨該尖峰係源於「APP 無法登入」、「支付系統故障」等真實停機事件，抑或係「行銷廣告活動」等無關雜訊。LLM 最終將非結構化趨勢數據轉化為結構化 JSON 格式輸出，包含三項欄位：受監理實體名稱（entity）、停機判斷（downtime: true/false）及信賴度分數（confidence）。

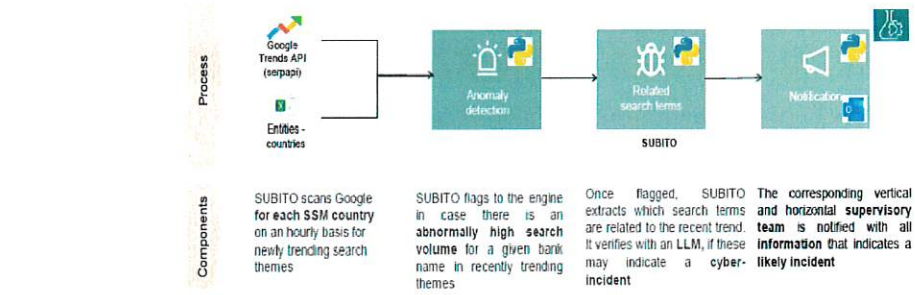


圖 十六：SUBITO 的自動化運作邏輯。橫向呈現四個處理步驟，上方標示「流程」，下方標示「元件」，並以四欄文字詳細說明各步驟的技術細節，清楚呈現從數據輸入到自動警報的完整自動化鏈條。

B.銀行可用性偵測器（Bank Availability Detector, BAD）儀表板：系統整合視覺化儀表板，提供詞雲圖（顯示與停機最相關之關鍵字，如「APP error」、「down」）及 24 小時趨勢走勢圖，並設有自動警報機制——當信賴度超過預設門檻時，即自動通知負責該銀行之監理機關，大幅縮短監理機關掌握異常事件之反應時間。

3.**案例三：「草堆中的數據」—報表導航與數據檢核**

(1)現況痛點：金融監理的數據（如銀行向監理單位申報的風險與資本狀況的報表）包含數以萬計的銀行申報數且複雜，惟對新進人員難以精確定位特定數據之法規依據、定義及其申報報表之欄位，因數據結構複雜，亦經常收到銀行申報端詢問有關特定法律定義如何對應申報報表之欄位。

(2)技術機制：開發一個 AI 聊天機器人，讓監理人員能透過自然語言提問（如：

「哪一個欄位包含第一類資本？」)，並採混合檢索模式(Hybrid Retrieval)與三層提示詞框架，包含系統提示(定義機器人的角色限制)、用戶提示(精確捕捉用戶的問題結構)及內容提示(從數據庫中動態提取最相關的欄位定義與法規背景)，系統自動定位數據路徑，運用語義相似性搜尋(即系統將用戶的查詢轉化向量座標，再至其向量資料庫進行「座標比對」)，將用戶的查詢尋找最接近的相關文檔或欄位的描述，精確回報報表路徑。

肆、心得與建議

一、心得

(一)全球監理趨勢由「事後被動回應」轉向「主動數據驅動」，強調蒐集交易層級顆粒化數據

現今採顆粒化數據者，如：韓國存款保險公司（KDIC）建立存款擠兌預警系統，實現每 20 分鐘更新一次資訊，大幅縮短監理反應時間。日本銀行（BOJ）蒐集證券融資交易（SFTs）資料，資料欄位與國際標準（如 FSB）接軌，提升數據品質及跨境監測能力。香港金管局（HKMA）透過蒐集細顆粒度的原始交易明細，直接掌握流動性風險與銀行間暴險。

然而，實務推動上仍面臨諸多挑戰，如泰國央行在推動顆粒化數據轉型時，曾因銀行端重置成本高昂而遭遇抵制，最終採分階段實施。目前各國運用 AI 前，均將建立統一的數據字典、強化數據治理架構，視為推動監理科技轉型之前置重要工程。

(二)妥善評估委外開發與自主開發模型之優劣，建立相應之風險防範機制

各國經驗顯示，委託專業廠商協助開發（如菲律賓 GabAI 與微軟協作、紐約 DFS 運用 Tableau 與 Oracle 體系）固然能加速導入進程，惟建議於委外合作時應特別注意：其一，數據主權與機密性風險，應確保所有資料儲存於境內，並透過單一登入及存取控制限制授權範圍。其二，監理機關於採購專業廠商之 AI 服務時，技術同質化與集中度風險與「黑盒問題」不容忽視，若所有金融機構均採用相同的 AI 算法或雲端供應商（如 Microsoft、AWS），一旦發生技術故障或市場波動，將觸發全球連鎖反應，應保留可移轉、可替換之系統設計彈性，以確保在地緣政治風險升高時，不受制於單一商業供應商。其三，應於合約中明定服務等級協議，要求供應商於發生安全事件時負通報義務。

至於自主開發路線，可參考西班牙銀行，積極掌握開源模型(Open Source Models)之本地部署能力，投入研究自有基礎設施運行開源模型，惟須留意內部技術人力與算力資源之長期投入成本，須有相應之專業團隊支撐。

上述無論採何種模式，均應建立「驗證－校準」之循環治理機制。監理科技不能取代人類的監理判斷，必須維持「人在迴圈內」(Human-in-the-loop)。，確保最終核決權與法律責任由真人主管承擔，以防範生成式 AI 之模型幻覺風險。

(三)善用 AI 承擔重複性作業，將釋出人力移往專注於高價值之深度分析工作

AI 可取代重複性任務（如資料提取、基礎計算、報表初步檢核、申報文件格式比對），並將該釋出之監理人力，移轉至查核、合規一致性評估、深層風險辨識等高價值任務，確保技術導入確實提升監理深度。

二、建議

(一)優先深化數據治理，參考國際經驗適時導入系統

本會業於 113 年 6 月委託聯徵中心建置「銀行監理資料數位申報暨分析系統」，採分階段循序導入，現已完成授信及信用卡業務試報作業，並刻正研議整合投資與衍生性金融商品申報資料，同步建置交易層級顆粒化數據。對照國際監理科技實務，AI 工具效能之發揮，根本取決於底層數據之顆粒度與標準化程度，爰建議於現階段優先落實數據標準化基礎工程：統一各機構間相同參數之定義，明確規範欄位定義與格式、合理值域及勾稽邏輯，並將監理比率分子、分母所對應之申報欄位明確文件化，確保未來自動化計算結果之一致性與可稽核性。俟數據基礎穩固後，未來於規劃「地理資訊系統(GIS)導入及應用(如氣候實體風險分析)」時，可參考課程中西班牙銀行、荷蘭央行與 BIS 創新中心偕同開發氣候實體風險評估工具之經驗，將氣象、擔保品房地座標等多源數據整合，估算極端氣候事件對房貸資產組合之影響。另可參考菲律賓 SAFr-QIT 經驗，整合銀行各財務數據與風險指標等資訊集中顯示於一頁面之儀表板，利於快速掌握銀行重要風險與概況。

(二)利用本會「大數據智能應用平台」智能搜尋功能，提升申報報表相關資訊檢索效率

鑑於銀行須申報之報表欄位數量龐大且結構複雜，建議參考西班牙銀行「草堆中的數據」案例，利用現行本會「**大數據智能應用平台」智能搜尋功能**，將各張申報報表、填報說明、欄位定義、常見問答及相關申報規範等整合為單一知識庫，以自然語言提問，系統運用語意相似性搜尋，回報相關資訊路徑，以提升檢索效率。

(三)強化國際交流，引進金融監理運用 AI 之前瞻實務

建議積極參與 SEACEN、國際清算銀行（BIS）等國際組織討論監理科技實務及開源工具之相關課程或研討會議，此為效益高之國際實務經驗之取得管道，可作為未來將 AI 運用於金融監理之重要參據。參與國際技術交流時，建議亦可指派具備資料科學或資訊技術背景之人員出席，不宜侷限於政策背景人員，俾能在 AI 模型架構與技術規格之實質討論中，提出具可行性之技術建議，有效將國際前瞻經驗轉化為本會可執行之監理科技方案。

(四)強化跨領域 AI 監理人才培育，建立長期穩定之人才供給機制

人才為 AI 監理工作能否成功之基石，建議前瞻性規劃跨領域專家團隊之培育，使傳統金融檢查人員學習 AI 模型原理與風險意涵，同時延攬資料科學人才加入監理陣容，或與學術研究機構建立常態性合作管道，增強監理人員對 AI 技術之認知與實務經驗，並應注意央行與監理機構若無法提供具競爭力之薪資待遇，將難以吸引人才，會導致監理機關不易具備理解與審查金融機構複雜模型的能力。

此外，參考美國、英國、新加坡及香港之實務經驗均顯示，金融監理之科技轉型須有高階管理層之策略支持，且對高階管理層有科技治理策略相關之培訓，方能確保資源配置與轉型目標一致，建議參酌課程中西班牙銀行經驗，規劃聚焦於生成式 AI 戰略走向、跨部門協作及監理科技長遠治理架構之高階培訓，確保決策層具備足夠技術視野，引領組織轉型。

參考資料

1.Mark McKenzie (2026/4/6), "Introduction to RegTech and SupTech".

2.Ashutosh Jaiswal (2026/4/6), "AI and ML in Supervision and Regulation".

3.Christian Rick Soriano (2026/4/6), "BSP's Suptech/RegTech Experience – Project 1".

4.Amanah Ramadiah (2026/4/6), "RegTech/SupTech Showcase".

5.Christian Rick Soriano (2026/4/7), "BSP's Suptech/RegTech Experience – Project 2".

6.Mark McKenzie (2026/4/7), "Suptech Project Development".

7.Vacharakoon Jivakanont (2026/4/7), "Leveraging Technology and AI to Combat Financial Crime, AML/CFT".

8.Trevor Collins (2026/4/8), "NYC DFS' RegTech and SupTech Experience and Use Cases".

9.Pradeep Raj Singh (2026/4/8), "RBI's Supervisory tools (including suptech tools) deployed by RBI for cyber security supervision".

10.Shintaro Nakamura (2026/4/9), "An overview of recent data initiatives by standard-setting bodies, including the Bank of Japan's experience of developing securities financing data collection and aggregation".

11.Benny Li (2026/4/9), "HKMA's SupTech/RegTech Experience and Use Cases".

12.Nico Lauridsen (2026/4/9), "Central banks and regulators authorities' collaboration on SupTech".

13.Nico Lauridsen & Javier Tarancón (2026/4/9), "Bank of Spain's SupTech project/ SupTech use cases including AI and demos".