



數位金融實務規範工作圈 第一季報告

20250522



玉山金控 E.SUN FHC

數位金融實務規範工作圈 – 使命及目標



使命 建立安心、普惠、共好、有共識的金融環境

目標 專注於跨銀行多元資料整合與應用，以及金融科技基礎建設的發展。
我們將優先建立制度並進行專案實證，期望達到兩年有感。

範疇

- 產出金融科技應用的實務指南（尤其是在跨銀行的資料整合），帶領業界共同合作編寫實務案例。
- 協助建立金融科技基礎建設的各項標準（目前以AI及雲端為主），並整合其他工作圈的工作項目。



目前目標

- A. 建立「金融無塵室」雛形，以「警示帳戶聯防」為第一個任務，以進行跨銀行的防詐任務。
- B. 建立「可程式化的 AI 治理制度」，參考國外範例並建立國內標準，廣邀金融同業參與討論並建立共識。

2025 Q1 進度總覽



- A. 金融無塵室
 - 3 月底第一階段結案報告
 - 0506 開始實驗室關閉工作
 - 4 -5 月底第二階段啟動
 - 0430 防詐實驗室成立與開始招募
 - 0531 專案成員招募結束
- B. 可程式化的 AI 治理
 - 至 5底 完成第四次大會
 - 7 月在銀行公會完成研究報告 (預計)
 - 12 月運用合適的工具與規範實作範例 (預計)



A. 金融無塵室



整體計畫時程



— 已完成 — 進行中 - - - 規劃中



▶ 警示帳戶聯防案

與工作圈 1 & 4 整合

階段一：
聯防案 PoC

跨金流資訊網 PoC (3 月底
完成、4 月底發表)

→ 玉山、中信、郵局

階段二：
跨業防詐

跨業防詐籌備

跨業實證

落地規劃

▶ 完善制度與環境

跨機構資料探勘與
服務模式

精進第一階段架構安全

金融無塵室專案現階段



第一階段 (實證)

2024.08 - 2025.03



實證案 1：同業聯防機制

整合三家金流資料，評估整合分析加上即時電文通知機制可以“額外”阻攔多少詐騙金額與戶數

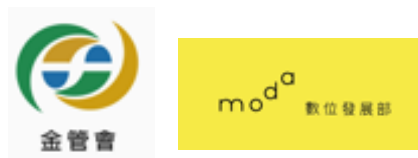
實證案 2：金融無塵室

建立資料匯流實驗制度與環境，作為後續各種防詐機制的驗證環境。此案也作為金融業在雲端運用的相關實務案例。

第二階段—防詐實驗室(擴大實證+應用)

2025.04 ~

小範圍
擴大金融業加入



擴大實證：邀請更多單位參與

- 擴大聯防單位
- 使用“金流圖”以攔阻多對多金融詐欺行為，需要持續進行計算效能優化與 AI 導入

小規模上線

- 前導行庫優先透過 API 服務，即時示警異常帳戶，縮短 165 通報單一行庫至其他行庫管制之時間
- 以財金公司為主建立金流Hub，規劃同業聯防機制系統建置方案

同業
聯防



跨業
聯防

全面聯防

- 建置同業聯防系統
- 延伸範疇至跨業聯防。如：金融x電信、金融x電商

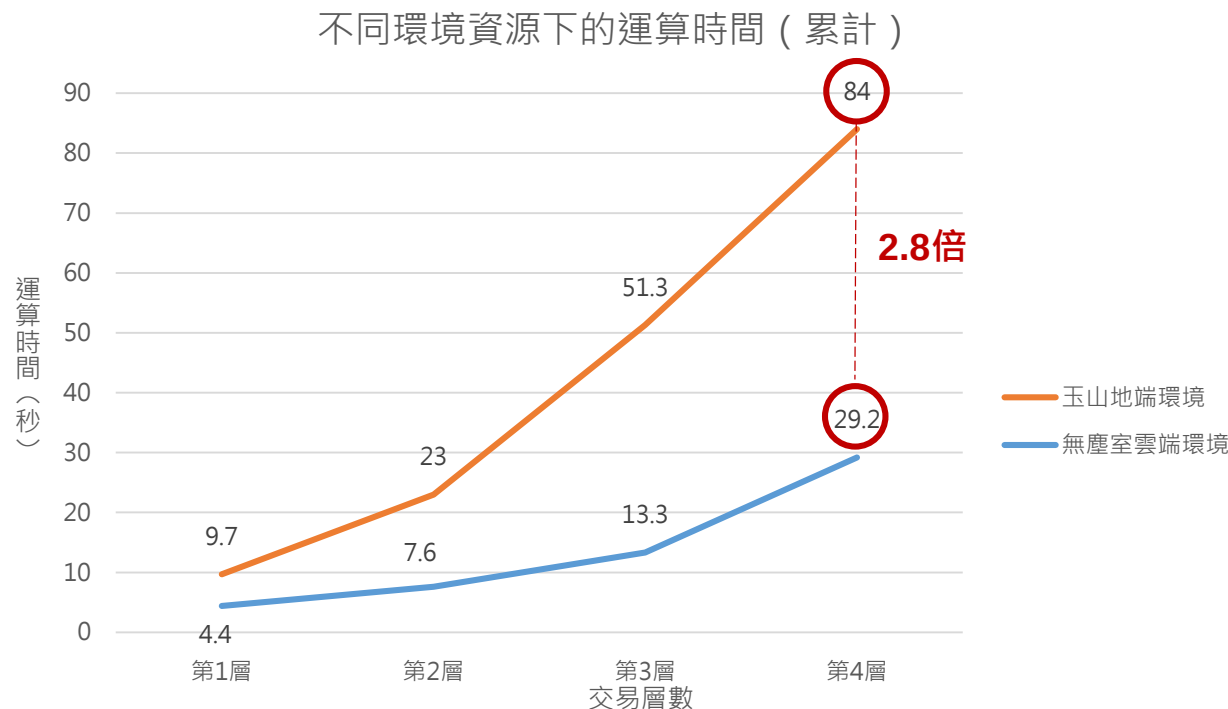
追蹤成效、持續優化

由於此案成效不僅只是民眾詐騙是否下降，還有後續機制的更新與 AI 導入的需求。

合作優勢 – 共同探索技術、跨業資源整合



玉山地端 x 無塵室雲端 運算時間



1 隨著向外查詢的層數增加，單筆所需查找的時間顯著提升。

2 若要能即時回饋前端查詢，相應硬體和演算法皆須做優化處理。

分析背景

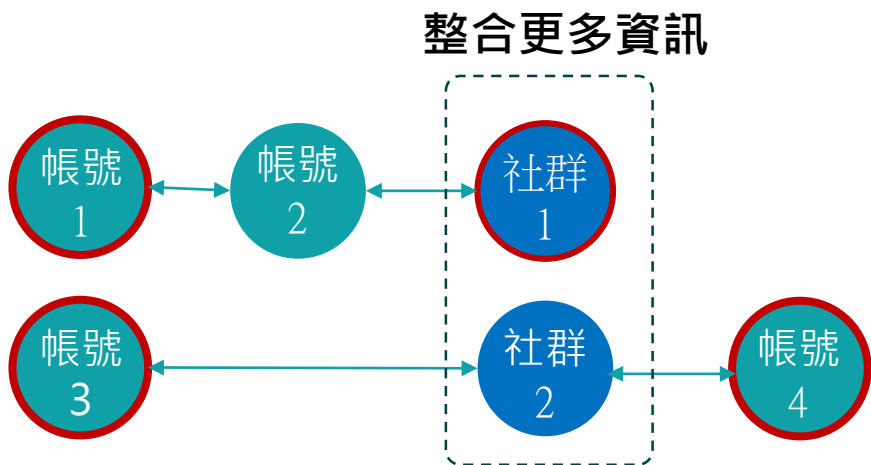
- 以2024/4/1 – 4/30 玉山警示帳戶 402 戶節點出發
- 玉山環境資源 - CPU : 8 Core ; memory : 128 GB ; DB : EDB (PostgreSQL enterprise)
- 雲端環境資源 - CPU : 4 vCPU, 2 Core ; memory : 16GB ; DW : BigQuery

金融無塵室第二階段 - 防詐實驗室方向



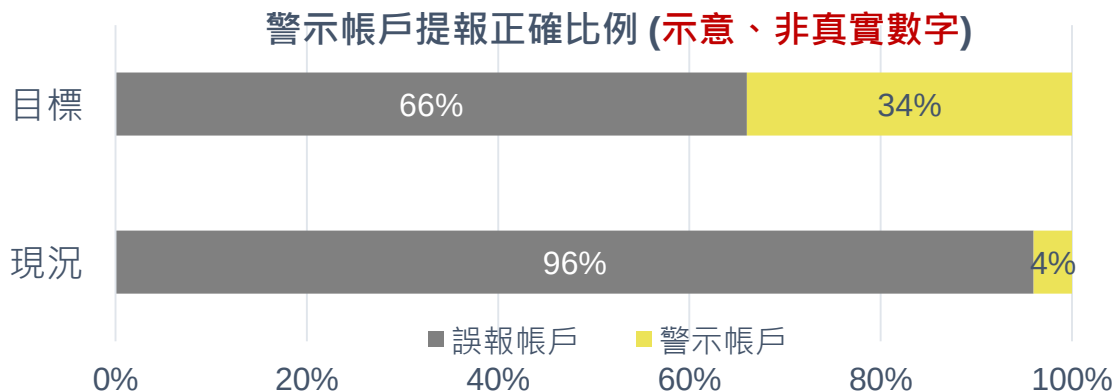
1. 找出更多潛在被害人

結合**多元跨業**資訊，捕捉更多**潛在**被害人



2. 提升警示精準度

更好的演算法與硬體架構，迅速且精準抓取警示戶

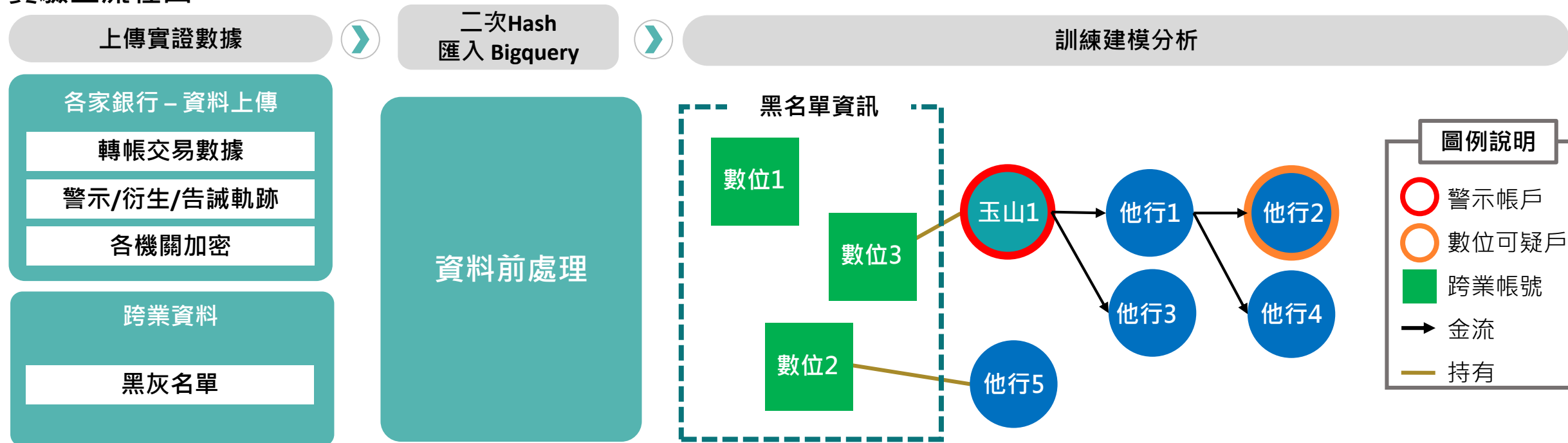


1. 整合通聯、社群、跨業資料，找更多潛在被害人
2. 加快演算法速度，更快捉出有問題的人
3. 持續調校，讓誤報更少、抓得更準

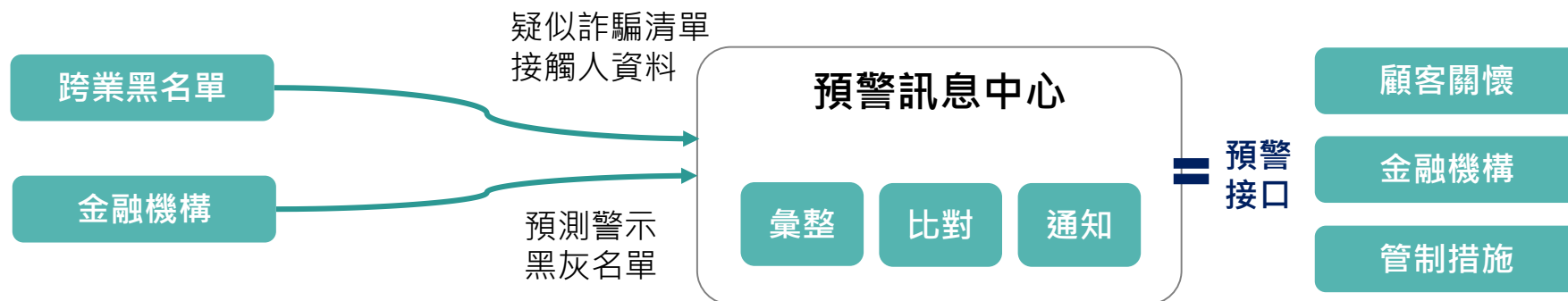
跨業防詐優勢 – 研發與應用



實驗室流程圖



預警機制 (Pre-alert Mechanism)



跨業防詐計劃里程碑



— 時程規劃 —

計畫籌備期
3月-4月底

環境準備
5月-6月底

6月雲端實驗室精進完成

分析期
7月-10月

資料上傳及實證
10月成果發表

落地推動
11月~

跨業防詐專案規劃

2025.04	2025.05	2025.06	2025.07	2025.08	2025.09	2025.10
---------	---------	---------	---------	---------	---------	---------

1. 精進無塵室
2. 參與方簽訂 MoU
3. 第二階段規劃
4. 設備準備

1. 資料規格確認
2. 資料加密&上傳

研發階段

跨業資料

- 提供跨業資料使用上的專家經驗，將可提供的數位資訊加密上傳

無塵室環境精進

- 設計者：玉山
- 準備實體實驗室及雲端開發環境精進，加強資安防護及易用性

模型研究與即時關懷

- 將金流資料加密後上傳，研究期間共同分析建模精進模型
- 討論即時關懷機制

跨業防詐協作聯絡人與場地資訊



智金處 林鉦育 資深副總工程師
ntuaha-13240@esunbank.com



智金處 廖子慧 副總工程師
jcaliao-13701@esunbank.com



智金處 蘇麟雯 副主任工程師
sualice-21979@esunbank.com

實體實驗室地點

digiblock C 數位創新基地（臺北市大同區承德路三段287號）

使用時間

預計 2025.04-2025.10 (兩季)

使用空間說明

1. 一樓有設門禁控管
2. 開放空間：處理分機敏資訊作業，15人位置
3. 會議室空間：處理機敏資料、進入雲端實驗室環境等，8-10人位置，有配置門鎖

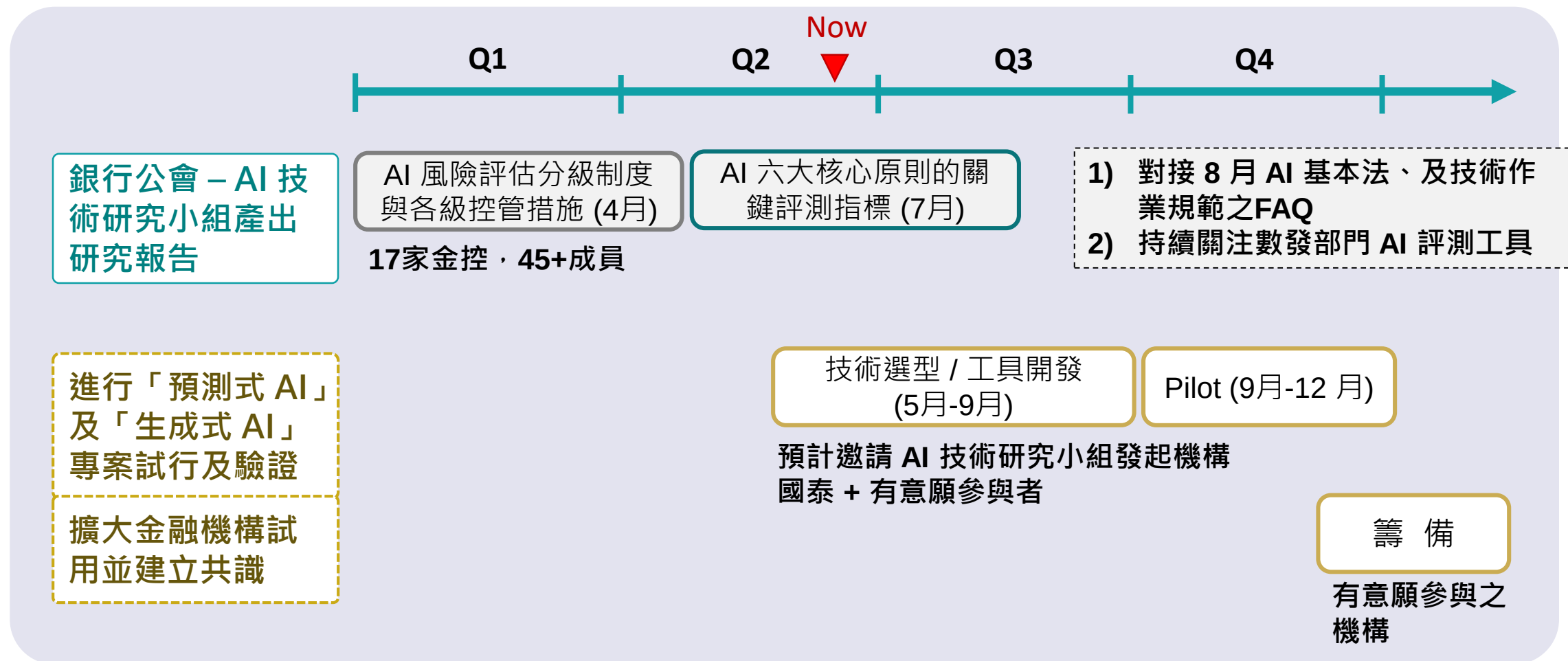


B. 可程式化的 AI 治理

整體計畫時程



— 已完成 — 進行中 - - - 規劃中



編制與進行方式



- 銀行公會金控業務委員會金融科技創新發展組轄下 - AI 技術研究小組

- 小組成員：共計 16 家金融機構，45+ 位成員

發起機構 - 國泰金控、玉山銀行、中國信託銀行、

參與機構 - 凱基金控、臺灣銀行、台新銀行、第一金控、第一銀行、新光金控、兆豐銀行、王道銀行
、富邦金控、合作金庫、永豐銀行、華南金控、土地銀行

- 推動方式：

以讀書會分享形式舉辦，事前依照 AI 成熟度將各家機構區分三組。當月由主責之發起機構帶大家導讀
與分享相關研究，研究主軸：

(1) AI 風險評估分級制度與各級控管措施

(2) AI 六大核心原則的關鍵評測指標

各階段具體產出(1/2)



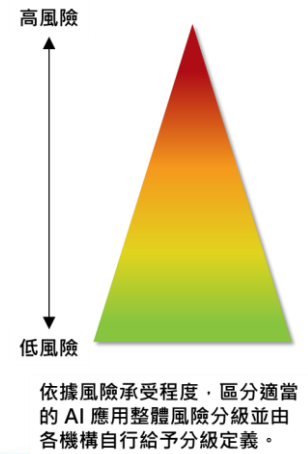
1

2月 研究國外重要規範與實務做法

研究對象	研究素材/機構	收斂台灣可借鏡發展項目
新加坡	1. MDDI(數位發展及新聞部) 2. CSA (網路安全局) 3. 金融管理局(MAS)	1. 制定執行指南：訂定治理架構、管理措施(包含指引表、風險分級之管制措施) 2. 發展檢測工具：由新加坡政府補助成立的非營利組織發展的AI檢測工具。發展可操作可執行達到可程式化的管理指標 3. 應用自評作業：新加坡政府機關提出治理架構後企業則依業務應用，自評執行狀況
香港	個人資料隱私公署(PCPD)	1. 區分為「自建模型」、「自第三方取得AI解決方案」(包含不限於生成式AI) 2. 隱含的風險分級(I類)概念、不可接受AI應用由組織自行決定 3. 提供不同規範情境建議的流程與實作案例，並對應至“現行適用法規”
歐盟	EU AI Act	1. 補充並定義GPAI：通用人工智慧被廣泛運用於各場景並可以與下游系統或應用程式整合 2. 風險為導向的管理方法：正面表列不可接受風險，方向以禁止侵害基本人權出發 3. 補充鼓勵創新措施：AI監理沙盒應建立在國家層級、對中小企業或新窗公司可優先進入沙盒、使用訓練計畫等資源，並協助回覆對AI Act法案之疑問

2

3月 風險分級方法論



交叉分析法

依據各評估面向分別作適當的判斷，求出AI 應用案件的風險等級。

影響對象		內部營運		外部用戶	
對客戶權益或企業之影響性		小	大	小	大
AI決策程度	AI直接判斷	中低	中	中低	高
	人機協作判斷	低	中低	低	中

內部營運大：提供監理規範、產品訂價、准駁決策參考
外部用戶大：提供金融商品交易、准駁、決策

條件矩陣法

依據自定義條件，任一觸及即屬高風險，並以兩軸線交集切分三個等級。

AI服務應用場景影響程度		AI模型固有風險	
高風險應用場景	非高風險應用場景	低風險	高風險
M	H	L	M

AI模型固有風險：自主決策程度、產出不確定性程度
AI服務應用場景影響程度：對客戶、公司營運、員工權益

評分法

依據各評估因子給定分數，訂定整體風險總分所對應的風險分級

X軸(問責性)	權重	有無	評分
AI應用程度	2	0	0
模型可解釋程度	3	1	3
總評分			3

Y軸(客戶面)	權重	有無	評分
使用個資	3	1	3
影響顧客權益	2	0	0
服務對象(內/外)	1	1	1
總評分			4

各階段具體產出(2/2)

3-4月 分級制度對應控制措施建議



生命週期
① 系統規劃與設計
② 資料蒐集及輸入
③ 模型建立及驗證
④ 系統佈署及監控



AI 指引核心原則	控制措施 (可視機構內部措施增減)	風險評級			建議實施細項	建議 二道防線單位
		高	中	低		
透明性與可解釋性	1. 模型版本控制、模型檢視更新計畫				既有AI模型如有重大變更(版本)更新，需重新進行AI服務應用的上線程序；或如採用 CI/CD 流程或其他標準作業流程，後續則依 CI/CD 流程或其他標準作業流程辦理。	
	2. 模型選擇說明				與版號。	
	3. 可解釋性指標：SHA dependence Plots					
	4. 網站揭露、說明模型如何應用於服務				如屬對外使用的AI服務應用，提案單位需說明是否提供淺白扼要的方式揭露。	法遵、法務
	5. 消費者溝通管道(含意見提出請求申覆或提供替代方案)				如屬對外使用的AI服務應用，提案單位需說明是否提供替代方案(如真人服務)；或官網等對外通路設有意見回饋專區、使用告知聲明等內容。	法遵、法務
	6. 數據源評估及應用目標定義				評估有效數據源，並明確定義應用衡量目標，以提高模型的透明性及可解釋性	

原則與對應控制措施

4-5月 (下一場會議產出)各控制措施對應指標



數據合流翻乾坤，百行同心護錢財

智慧財產權聲明

本資料各項內容之各項權利及智慧財產權（包括但不限於著作權、專利權、商標權等）均屬玉山金融控股股份有限公司及其子公司（以下簡稱「玉山金控」）所有。除非獲得玉山金控事前書面同意外，均不得擅自以任何形式複製、重製、修改、發行、上傳、張貼、傳送、散佈、公開傳播、販售或其他非法使用本資料。除非有明確表示，本資料之提供並無明示或暗示授權貴方任何著作權、專利權、商標權、商業機密或任何其他智慧財產權。

Intellectual Property Rights

The rights and the intellectual property rights (including but not limited to the copyrights, patents and trademarks, and etc.) of the Material belongs to E.SUN Financial Holding Co., Ltd. and its subsidiaries (hereinafter referred to as "E.SUN"). Any copy, reproduction, modification, upload, post, distribution, transmission, sale or illegal usage of the Material in any way shall be strictly prohibited without the prior written permission of E.SUN. Except as expressly provided herein, E.SUN does not, in providing this Material, grant any express or implied right to you under any patents, copyrights, trademarks, trade secret or any other intellectual property rights.