



數位金融實務規範工作圈 第二季報告

20250821



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 年度進度總覽



Q1



Q2



Q3-Q4



工作事項

A. 金融無塵室

- 4 月底第一階段結案報告
- 4 月底第二階段啟動
 - 0430 防詐實驗室成立

A. 金融無塵室

- [防詐金流履歷] 處理無塵室相關行政
- [跨業聯防防詐] 資料規格討論
- [跨業聯防防詐] 實驗室規格調整

A. 金融無塵室

- [防詐金流履歷] 完成環境準備
- [跨業聯防防詐] 完成分析

B. 可程式化的 AI 治理 至 4/30 完成第三次討論

B. 在AI技術研究小組持續進行AI 治理讀書會

B. 可程式化的 AI 治理

- 7 月完成讀書會報告
- 8 月籌備專案與規劃實證工作
- 9 月開始 (預估)
- 12 月分享金融 AI 治理實務案例 (進行中)

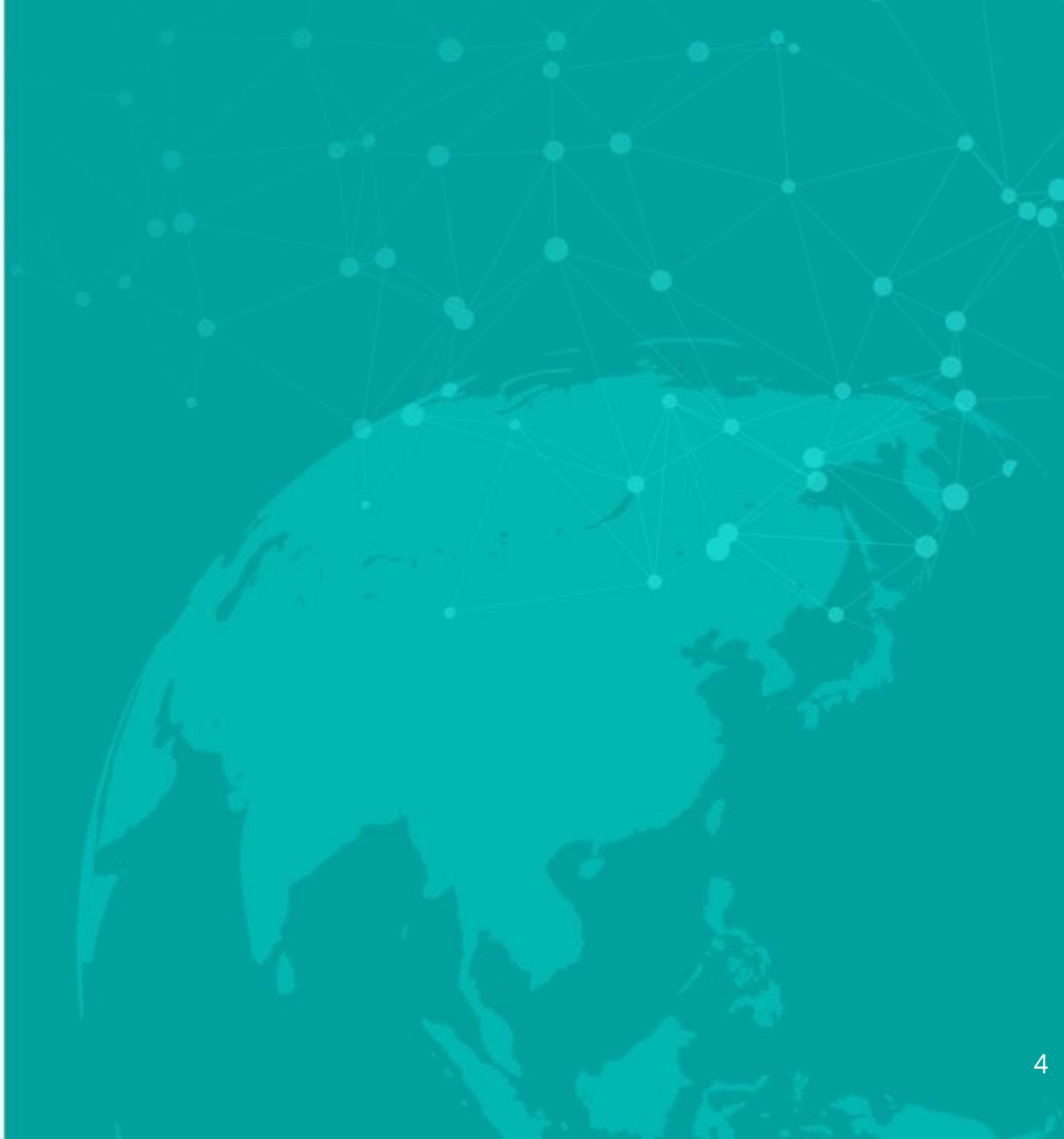


2025 Q2 進度總覽

- A. 金融無塵室
 - 6 月招募作業 (已完成)
 - 7 月實驗室環境建置與資料規格確認 (已完成)
 - 8 月資料上傳與進駐分析
- B. 可程式化的 AI 治理
 - 7 月在銀行公會完成報告 (已完成)
 - 8月籌備下一階段可程式化的AI治理落地實作



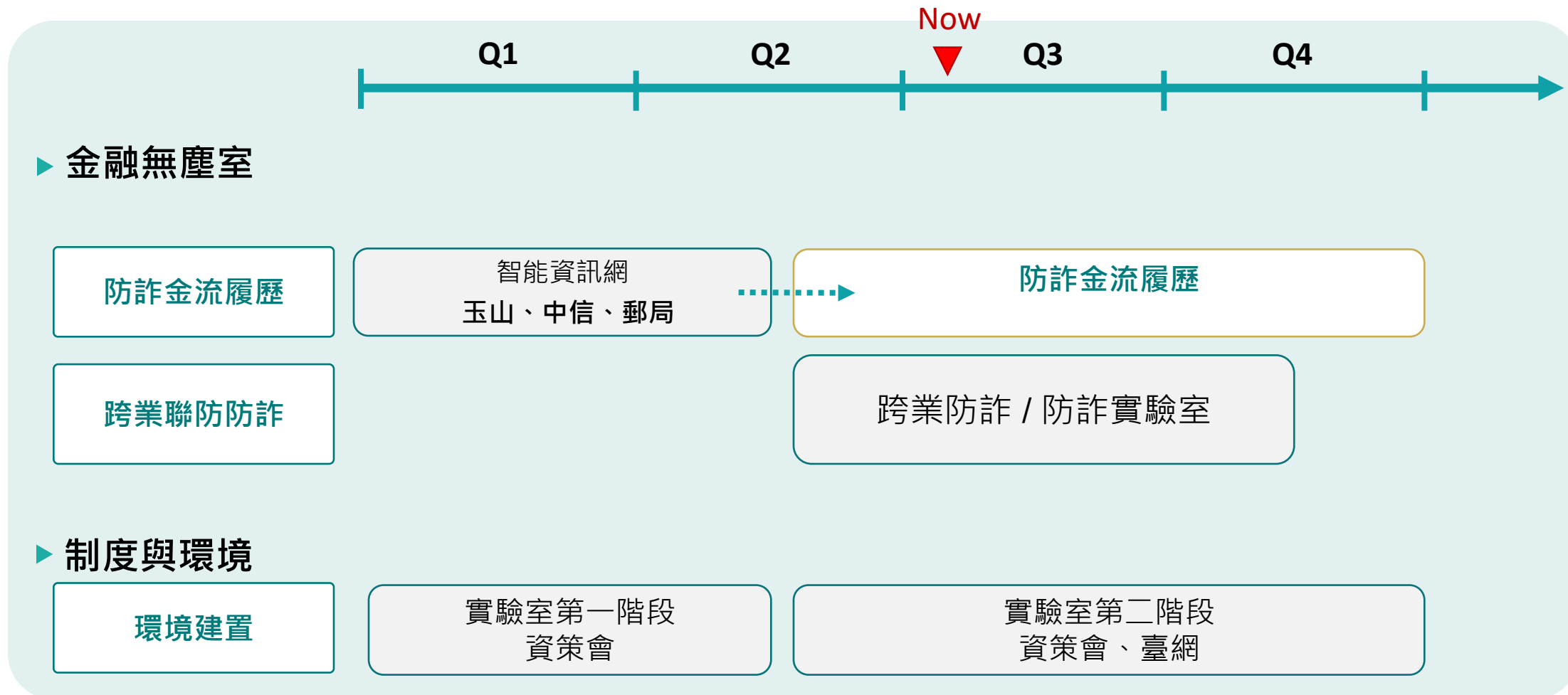
A. 金融無塵室



金融無塵室第二階段 – 跨業聯防時程



參與專案成員：參考不同專案的成員資訊



跨業聯防參與成員-R&R



金融監督管理委員會
Financial Supervisory Commission R.O.C. (Taiwan)



財金資訊股份有限公司
FINANCIAL INFORMATION SERVICE CO., LTD.



資料提供

- 資料上傳無塵室，參與專案進度與成果分享

Gogolook



應援科技



第一銀行



台新銀行

分析方

- 在防詐實驗室中通過金融無塵室進行資料分析
- 討論研究狀況，一起推進研究進度，成果報告



應援科技



第一銀行



台新銀行

支援體系

Google



- 無塵室技術顧問
- 協助構想無塵室

- 無塵室架構設計
- 無塵室建置
- 無塵室教學

TWCA
臺灣網路認證

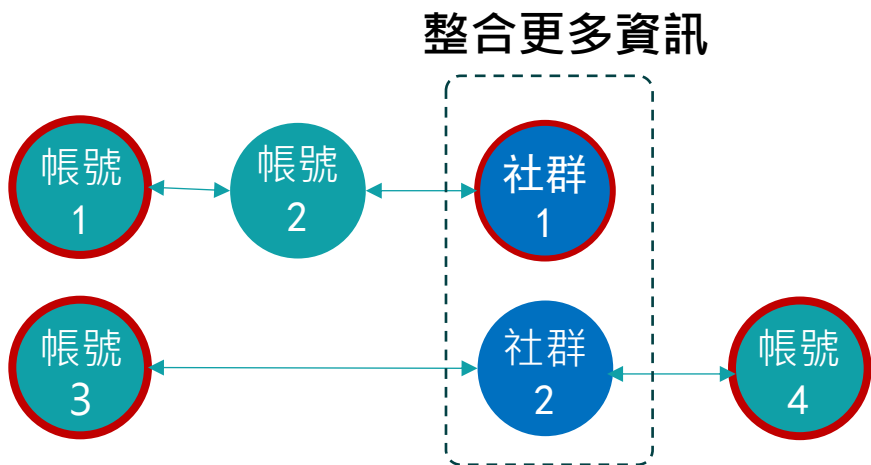
- 防詐實驗室第三方管理
- 防詐實驗室及無塵室安全監管
- 無塵室管理者

金融無塵室第二階段 - 跨業防詐 / 防詐實驗室



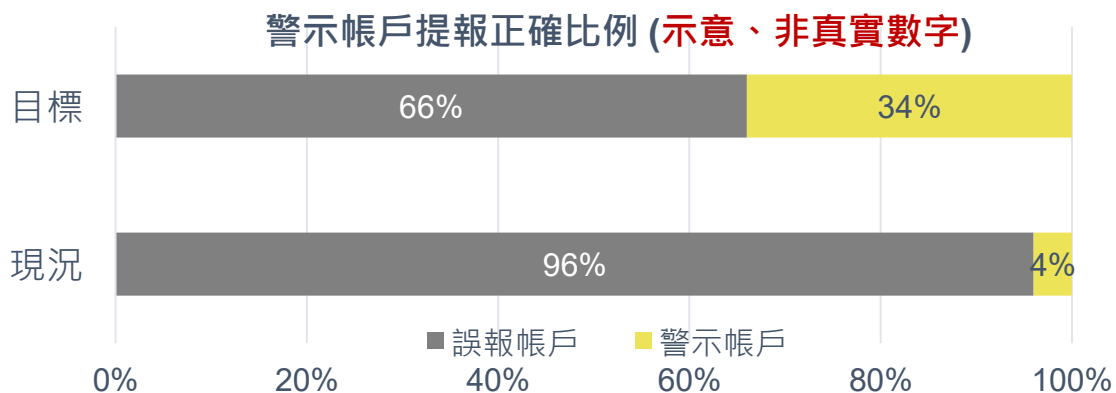
1. 找出更多潛在被害人

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

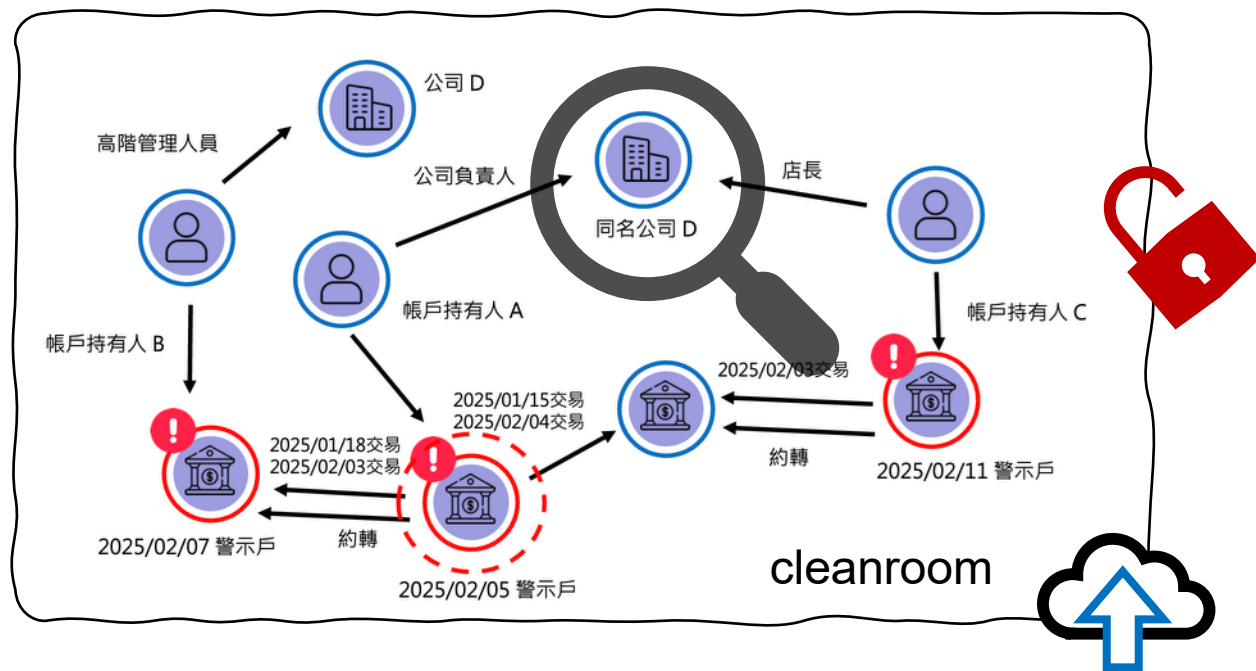


1. 整合通聯、社群、跨業資料，找更多潛在被害人
2. 加快演算法速度，更快捉出有問題的人
3. 持續調校，讓誤報更少、抓得更準

跨業聯防目標設定



公私協力，運用資料在防詐實驗室的框架下集結力量，打造安心的金融環境



三個月內達成以下成果

跨業尋規防詐害，
鎖定潛在警示早；
模型補強成效在，
運算加速跑更快。



電信 D



銀行 A



政府 B



加密貨幣 G

金融無塵室分階段計畫 (相關部會：金管會、數發部)



成果報告

二階進行中

第一階段 (完成)

2024.08 - 2025.05



財金資訊股份有限公司
FINANCIAL INFORMATION SERVICE CO., LTD.



金融無塵室設計與建置

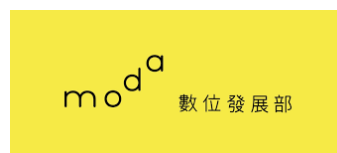
- 建立資料匯流實驗制度與環境，作為後續各種防詐機制的驗證環境。此案也作為金融業在雲端運用的相關實務案例。
- 請資策會運作實驗室、Google 協助相關資安與環境

智能資訊網實驗

整合三家銀行(玉山、中信、郵局)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

第二階段 (擴大+落地)

2025.05 - 2026.03



財金資訊股份有限公司
FINANCIAL INFORMATION SERVICE CO., LTD.

金融無塵室 2.0 (防詐實驗室)

- 擴大聯防單位。如：金融x電信、金融x虛擬貨幣
- 由於此案需要考慮“金流圖”以攔阻多對多金融詐欺行為，因此需持續在實驗室進行研究計算效能優化與 AI 導入的形式 (需雲端、算力、經費支持)

防詐機制落地規劃與應用

- 以財金公司設立金融阻詐聯防平台，部署同業聯防機制系統建置
- 增加台網 (TWCA) 成為可運作實驗室單位

第三階段 (AI 研發基礎建設)

2026.03 - 2026.12

產業
標準



智慧
共構

金融無塵室 3.0 (跨業合作平台)

- 延伸專案範疇至非防詐領域
- 推動更多單位、機構運用此無塵室框架，連結資料發展新產業、新業務

金融智創研發區

- 將金融無塵室兩階段推行成果，成為未來跨業合作的案例，作為國內 AI 發展或 AI 新創產業可以引用的案例。

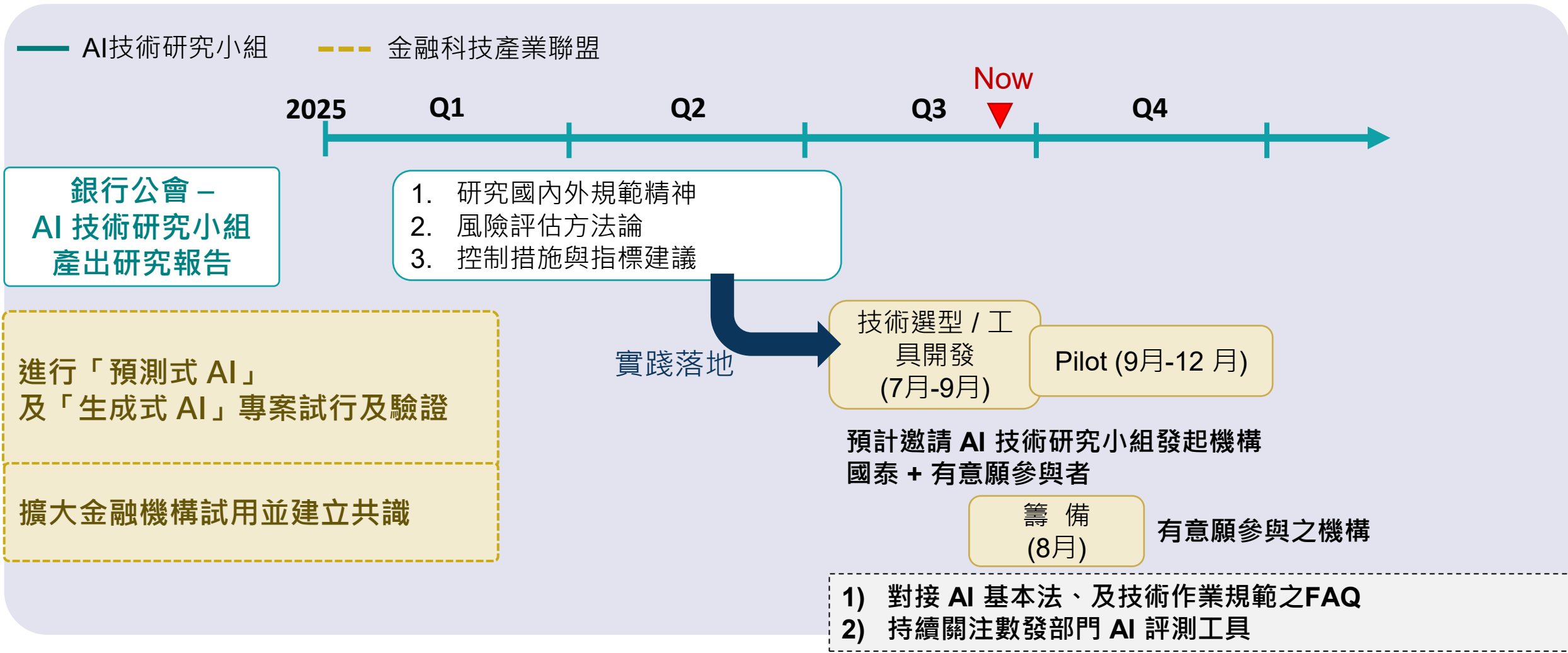


B. 可程式化的 AI 治理

可程式化的 AI 治理 -時程



從理解精神走向落地實踐：實作可程式化AI的相關方法論和工具，確保金融機構在運用AI技術時能依循標準作業



AI 技術研究小組(讀書會) - 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

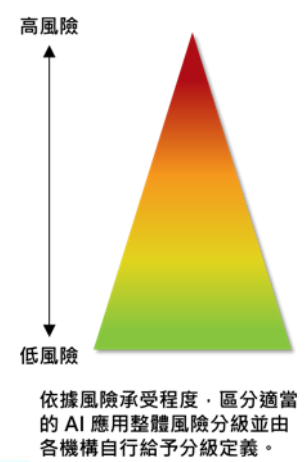
讀書會各階段具體產出(1/3)



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(/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	M	H
		L	M
		低風險	高風險

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)			
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)			
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		

讀書會各階段具體產出(2/3)



3 4月 分級制度對應控制措施建議



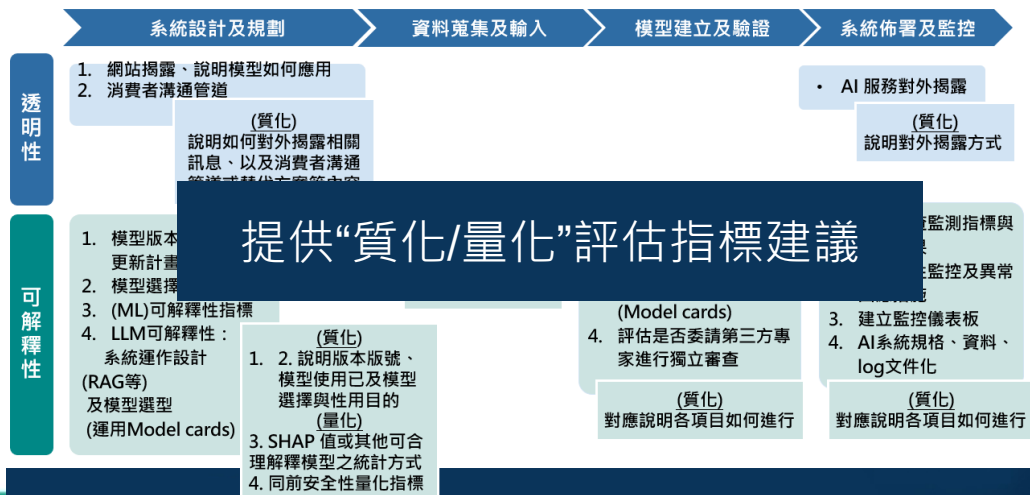
生命週期
① 系統規劃與設計
② 資料蒐集及輸入
③ 模型建立及驗證
④ 系統佈署及監控



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				提案單位需說明模型類型、模型邏輯與版號。	
	3. 可解釋性					
	4. 網站用於服務				是否提供淺白扼要的	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 各控制措施對應指標

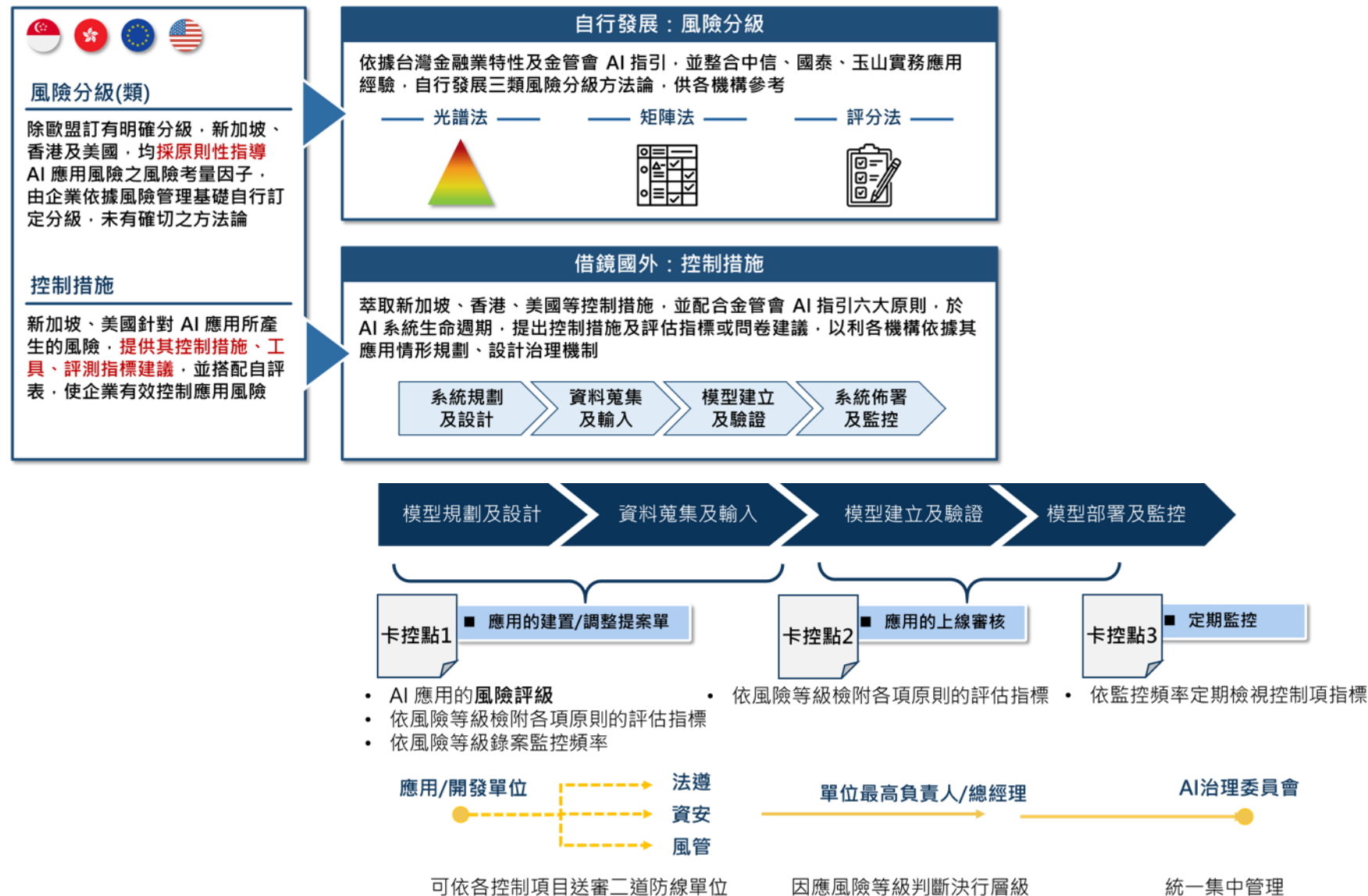


讀書會各階段具體產出(3/3)



5

7月 最終報告



AI 創新加速前行，治理更需同步到位



監理趨勢

- 金管會已於 2024 年 6 月正式發布「金融業運用人工智慧(AI)指引」，並預計將逐步完善 AI 基本法。
- 從監管單位釋出相關內容可見高度重視在導入 AI 時的風險控管、消費者保護與資訊安全

產業現況

根據金管會公布金融業應用人工智慧(AI)調查結果，已有超過百家金融機構在不同業務中導入 AI，應用範圍涵蓋智能客服、風險管理到廣告行銷等，但治理仍在建構中

核心痛點

目前的 AI 指引多為「原則性」規範，例如公平性、問責性、透明度與可解釋性。這些原則立意良善，但在實務上缺乏客觀、量化的評估標準，導致：

- **合規舉證困難**：如何向主管機關「證明」合乎原則的軌跡
- **內部管理不一**：不同團隊、不同專案對「透明度」的解讀可能完全不同。

可程式化的 AI 治理 – 落地規劃與建議參與角色



Aug.
籌備

Sep.
招募與前置作業

Oct.
Pilot 與工具選型

Nov.
開發與實做
Pilot 報告解讀

Dec.
治理框架釋出

建議參與角色

資料科學家 / AI 工程師 驗證實務 業務與技術可行性

1. 實作組織 pilot 模型資訊卡 (Model Card)
2. 評估指標實用性
3. 分享「治理痛點」

風控 / 法遵 / 資安人員 建立指標對應規範解讀性

1. 校準合歸對照文件
2. 量化指標來實踐指引原則的可解讀性

兼顧創新與風控，提升企業核心競爭力



對齊監管期望

具體落實金管會 AI 指引要求，為即將到來的 AI 法規做好準備，有效降低合規風險

加速業務創新

建立可靠的 AI 風險護欄，讓業務單位更安心、更快速地推動 AI 應用，搶佔市場先機

強化風險管理

將 AI 模型風險納入機構風險管理體系，實現標準化、自動化的監控與預警

建立內部標準

打造全機構一致的 AI 治理語言與標準，提升跨部門協作效率

提升客戶信任

透過可證明的公平與透明機制，贏得客戶與合作夥伴的信賴





聯盟聯絡窗口

可聯絡聯盟、專案各種事宜



玉山工作圈主要窗口

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



玉山工作圈主要窗口

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

可聯絡專案相關事宜



金融無塵室 - PM

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



可程式化的 AI 治理 - PM

智金處 林仙琪 主任工程師
kikilin-10281@esunbank.com



感謝聆聽

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.

數位金融實務規範 – 目標 A：金融無塵室



建立「金融無塵室」，讓未來各種跨機構合作案，均能確保金融資料應用的安全和合規性。

- **安全控管**

所有進出人員、裝置和分析環境都會受到嚴格控管，以符合資訊安全標準。

- **可靠環境**

安全而封閉的實體和數位環境，讓不同機構的資料可以進行整合與分析。

- **創新支持**

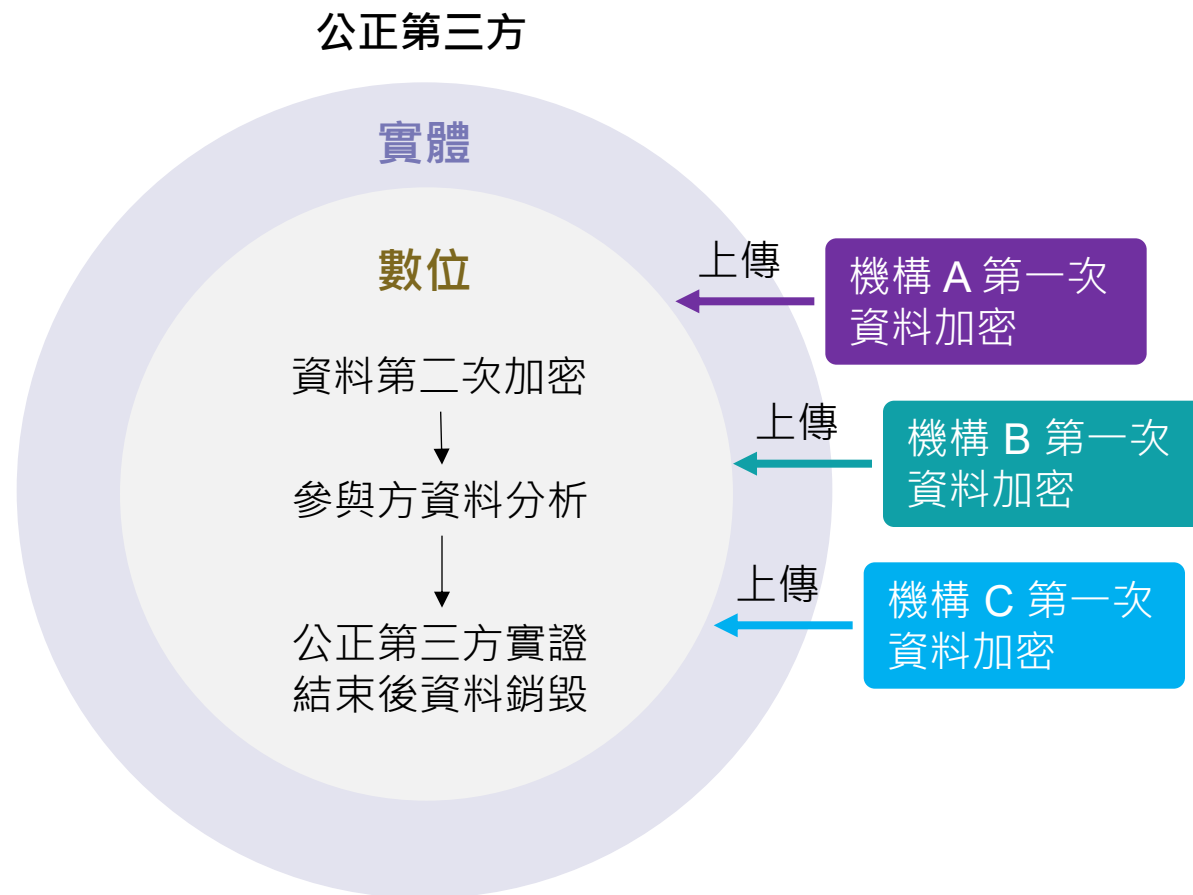
透過此平台，將能快速進行金融創新的實證，以加速新技術的發展和應用。

- **數據安全**

所有資料在使用前均進行雙盲加密，並由公正第三方管理，確保所有資料均受到嚴格的控管。

- **靈活設置**

此系統具有快速佈署與擴充的能力，並有完善的資料銷毀流程。



數位金融實務規範 – 目標 B：可程式化的 AI 治理



根據金管會的六大指引，整合銀行公會針對 AI 治理的研究報告，提供對應實務指南，以建立適用於台灣金融機構的可程式化 AI 治理框架。

管理 框架

1. 方法論與工具實作

實作可程式化 AI 的相關方法論和工具，確保金融機構在運用 AI 技術時能依循標準作業。

2. 檢測資料集

建立檢測資料集，幫助金融機構評估和驗證其 AI 應用的相關指標。

3. 監測與控制

制定監測指標，針對 AI 的運作進行觀察，確保符合規範與標準。

4. 風險管理

實施過程中，建立相應的風險控制措施，以降低潛在的 AI 風險。

參考資料：Veritas Initiative by MAS
to deal with AI's principles of FEAT
(fairness, ethics, accountability, transparency)

風險	開發期	上線前	維運期	行動
高	觀測指標			控制措施
中				
低				