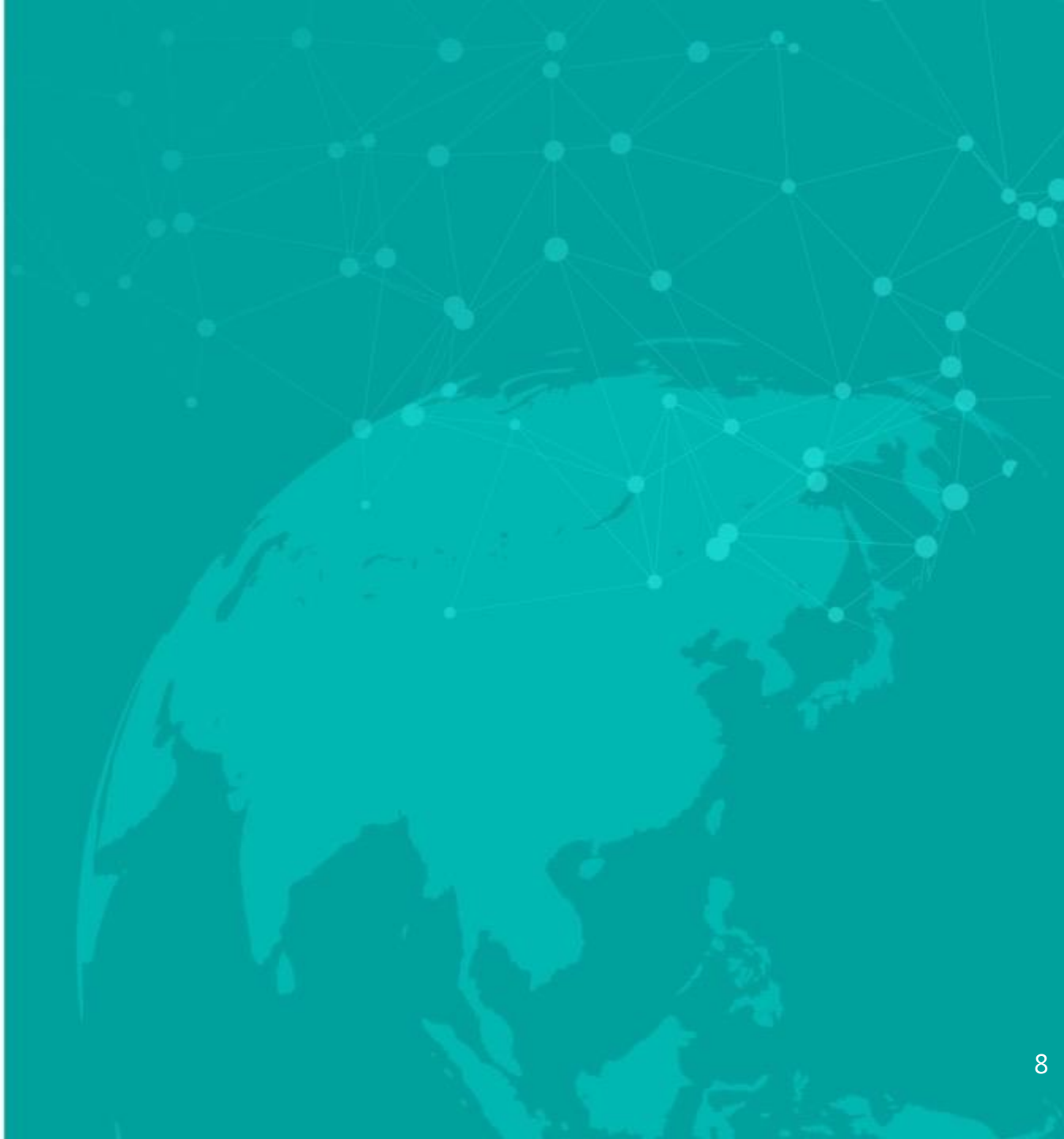




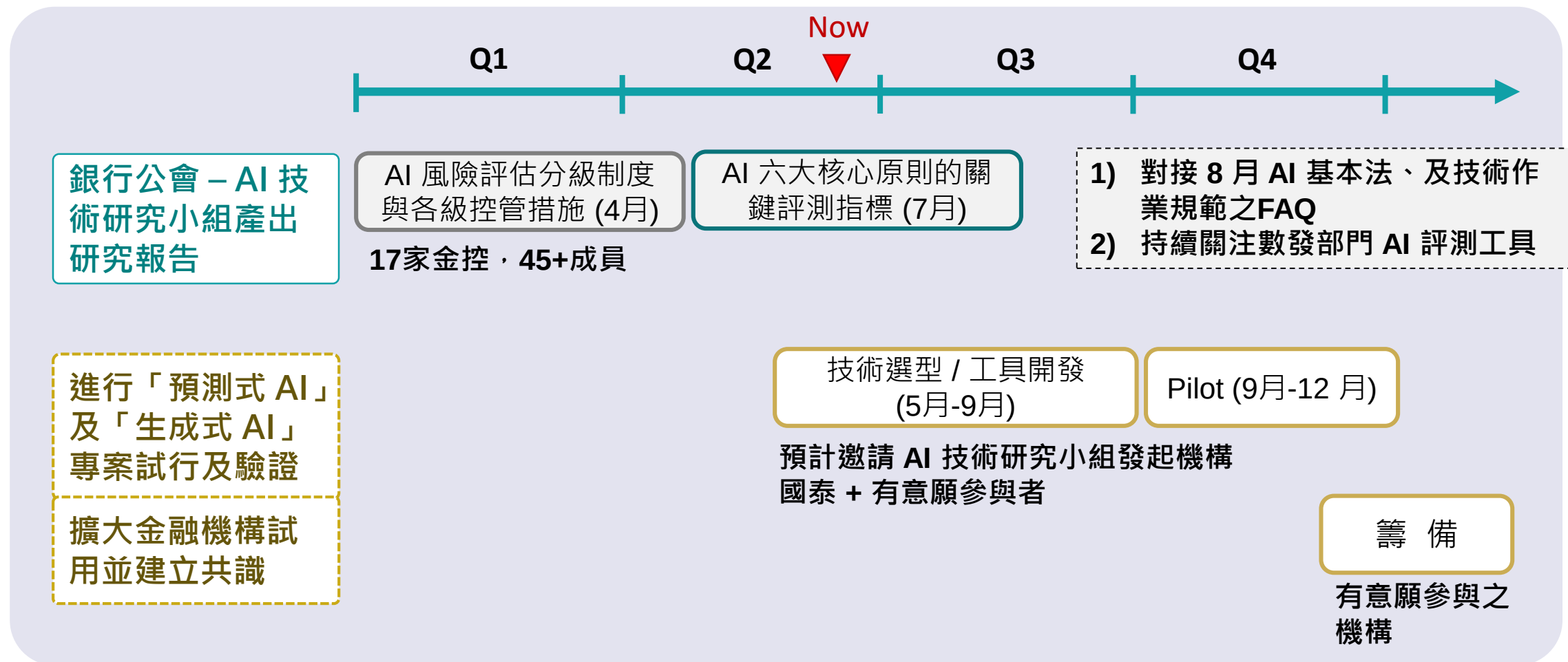
B. 可程式化的 AI 治理



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

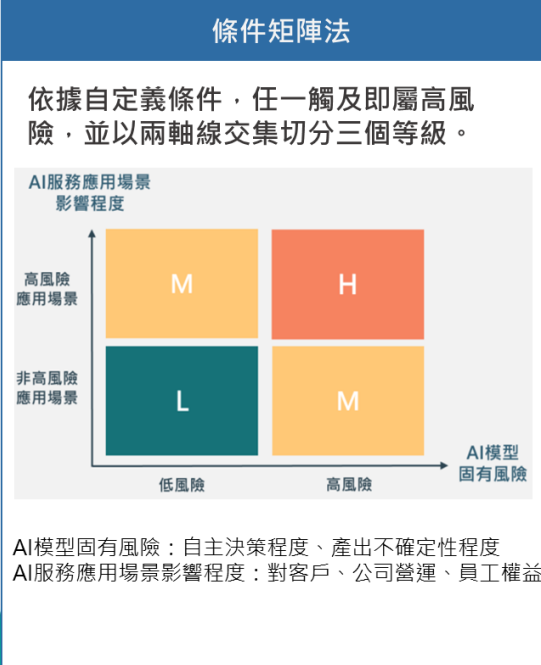
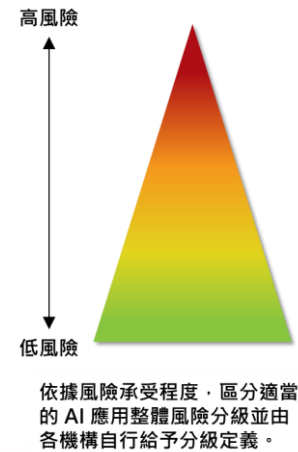
各階段具體產出(1/2)



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



各階段具體產出(2/2)

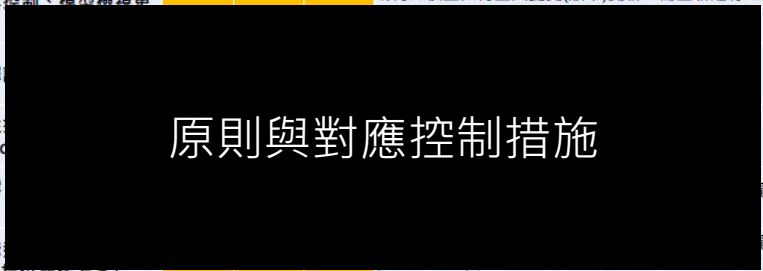
3-4月 分級制度對應控制措施建議



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服務應用的上新計畫，後續則依	
	2. 模型選擇					
	3. 可解釋性 depend					
	4. 網站揭露 用於服務				提供淺白扼要的	法遵、法務
	5. 消費者溝 請求申覆或提供替代方案)				提供替代方案 、使用告知聲	法遵、法務
	6. 數據源評估及應用目標定義				明等內容。 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	



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.