工作圈主題：數位金融產業標準的建立與科技治理

玉山金控在數位金融產業標準的工作圈中擔任召集人，目標是根據其在金融科技領域的豐富經驗，建立數位金融的實務案例與指南，並協助制定相關規範，以引導金融科技的發展。此工作特別聚焦於人工智慧（AI）、雲端技術以及多元資料的應用。

第一任期主要規劃

1. **金融無塵室：**

   此無塵室的主要目的是提供一個安全的跨機構資料分析環境，同時建立資料整合應用的新模式。後續也針對防詐議題，推動常設型防詐實驗室，讓相關專家與資料有一個穩定可長時間探索與研發的環境。金融無塵室類似於半導體晶圓廠的無塵室，僅允許授權人員進入，並對進入的物品進行檢查，以確保資訊安全。在無塵室內使用的所有資料都會經過雙重加密，並由第三方進行管理與保護。金融機構可以在此環境中進行數據分析和 AI 建模，而所有處理的資料在達成使用目的後將被安全銷毀，以確保資料只進不出。

2. **可程式化的 AI 治理：**

   我們將建立一套能夠用 AI 管理 AI 的機制。根據金管會所發布的「金融業運用人工智慧(AI)指引」原則，我們將設立 AI 模型的監控指標，並設計監控機制與管理制度，運用程式或高可解釋性的 AI 來協助監管各種 AI 應用。可程式化的 AI 治理將針對六大指引設計一套客觀評估機制，以檢測 AI 應用的表現。例如，若要評估貸款模型的公平性，我們可以透過自動化的公平性檢查機制，利用預先設計好的客觀指標和自動化評估流程，確認不同群體（如不同年齡或國籍）在貸款核准率上的差異，從而檢視是否存在歧視現象。

FAQ

1. 什麼是金融無塵室，主要的特色為何？有什麼突破性的做法？

- 金融無塵室的主要功能是提供一個安全、封閉的數位及實體環境，使不同機構能夠整合、研究和運用資料。傳統上，各機構獨自管理資料，缺乏共同分析的環境，這使得即便在有適當目的需要跨機構協作的情況下，相關分析仍難以進行。例如，在防詐騙方面，當金流從 A 行庫轉移至 B 行庫時，由於無法整合跨機構的資料，金流追蹤可能出現斷點，使得洗錢防制和詐騙交易監測變得困難。

  透過金融無塵室，能夠將多家機構的資料安全整合進行分析，突破了過去的限制，強化了科技防詐的能力。未來，若各金融機構間有適合進行跨機構資料整合分析的主題，金融無塵室都將成為理想的實證平台。

2. 金融無塵室如何確保資料的安全性與顧客隱私？

- 金融資料涉及顧客的金流與隱私，運用上必須是個資法範疇下可使用的特定目的，且必須禁止資料未經合理授權的傳送。高水平的資料安全性意味著資料必須具備機密性、完整性和可用性。只有優先加強資料安全，才能在保障顧客隱私的前提下進行有效的數據分析。

  具體執行方法如下：各機構首先對資料進行加密，然後由公正的第三方進行二次加密，以實現雙盲加密機制。這種機制確保參與的任何一方都無法單方面查看明碼資料，這些資料將在第三方的管理下安全存放，以確保其安全性。此外，分析的實體環境將實施嚴格的人員與設備管控，因此資料無法被攜出，進一步增強安全措施。

3. 可程式化的 AI 治理為什麼對金融機構來說很重要？

- AI 治理的監理成本與完整性是落實 AI 治理的關鍵因素，因此提升治理的效率與全面性將成為金融機構關注的重點。可程式化的 AI 治理旨在透過客觀指標，針對金管會所發布的「金融業運用人工智慧(AI)指引」中六大原則項目進行評估，並以易於編程的評估機制展示 AI 模型在問責性、公平性、隱私性、安全性、透明度和永續發展等方面的表現。這將引導 AI 模型不斷完善各項評分指標，從而增強服務的安全性和穩定性。