保險業運用人工智慧系統自律規範問答集

金融監督管理委員會民國 115 年 2 月 2 日金管保綜字第 1140438097 號函修正後洽悉

問題	答覆
問題 1 **就本自律規範第三條適用範圍，若作業過程中有人工介入或干預之情形產生時，是否仍適用該自律規範？**	**【答覆】** 是。參照「金融業運用人工智慧（AI）指引」總則章第三節風險評估考量、第一章核心原則一「建立治理及問責機制」與第二章第四節「以人為本及人類可控原則之落實方式」之說明內容，本題所稱「人工介入或干預」係指於運用 AI 系統過程中，涉及人員參與及監督之機制。金融機構對所使用之 AI 系統應負相應責任，建立全面且有效之風險管理與問責機制，並依個別使用情境採取風險為本之評估與資源配置。又前揭指引並未因有人為介入即排除其適用，故凡於作業流程中使用 AI 系統者（無論為全自動、半自動或輔助決策），均屬本自律規範之適用範圍；惟管理強度仍應視風險程度及使用情境，採取相稱之管理措施。
問題 2 **第三條所稱對營運有重大影響者：** **所指之營運重大影響可參考「保險業作業委託他人處理內部作業制度及程序辦法」（下稱辦法）第四條第五項之重大性定義，自行評估。** **辦法所稱之重大性，係指下列情形之一：** **(1) 委外作業如無法提供服務或有資訊安全疑慮，對保險業之業務營運有重大影響者。** **(2) 委外作業涉及客戶資料安全事件，對保險業或客戶權益有重大影響者。** **(3) 其他委外作業對保險業或客戶權益有重大影響者。** **上述是否可進行具體定義、案例列示闡述說明？**	**【答覆】** 本自律規範第三條所稱之「對營運有重大影響者」，係指人工智慧系統產出之影響程度符合「保險業作業委託他人處理內部作業制度及程序辦法」第 4 條第 5 項之重大性定義者；其判斷範圍同時包含已發生之事件與經合理認定足以致生重大影響之風險情境。提供以下案例供業者評估： 案例： (1) 保險業運用 AI 系統辦理核保作業或進行核保決策，因 AI 系統有產生錯誤或偏差資訊之可能，導致短期內發生大量異常核保，影響保險業內部營運，經保險業評估對其業務營運有重大影響，即屬「對營運有重大影響者」。 (2) 保險業運用 AI 系統辦理理賠作業或進行理賠決策，因 AI 系統有產生錯誤或偏差資訊之可能，導致短期內發生大量異常理賠，影響眾多客戶權益及公司信譽，經保險業評估對其業務營運有重大影響，即屬「對營運有重大影響者」。 (3) 保險業運用 AI 系統進行投資決策或協助產出投資建議，因 AI 有產生誤導或虛構資訊之可能，導致保險業內部損失及投資利益時，經保險業評估對其業務營

問題	答覆
	運有重大影響，即屬「對營運有重大影響者」。
問題 3 **第五條所定人工智慧作業委託第三方業者辦理之規範一節：第二項所指「宜要求第三方業者提供相關資訊」範圍為何？**	**【答覆】** 保險業委託第三方業者導入 AI 系統時，宜要求該業者提供例如系統/資訊規格、資安認證、系統資訊安全防護措施、資料保護措施、可移交之 AI 系統數據資產等相關資訊，以供保險業評估決定欲委託之第三方業者。
問題 4 **第六條所稱「其他法律規範與相關資訊使用規定」，請舉例具體包括哪些相關規範？**	**【答覆】** 舉例包括： (1) 保險業核心法規及自律規範：如《保險法》、保險業辦理資訊安全防護自律規範》、《金融消費者保護法》、《保險業招攬及核保理賠辦法》等。 (2) 作業委託相關：如《保險業作業委託他人處理內部作業制度及程序辦法》、《保險業作業委外使用雲端服務自律規範》等。 (3) 消費者保護相關：如《消費者保護法》、《公平交易法》等。 (4) 洗錢防制相關：如《洗錢防制法》、《資恐防制法》、《金融機構防制洗錢辦法》等。 (5) 反歧視相關法規：如《就業服務法》、《性別平等工作法》、《身心障礙者權益保障法》、《老人福利法》等。 惟各項 AI 應用場景之業務、資料與運作模式不一，適用法規亦異。上述僅為示例，非屬窮舉；各會員公司應依實際情境，自行評估並審慎檢視現行法令、行政命令及主管機關指引，確保符合法規要求。
問題 5 **第七條所稱「落實辦理人才培育，提供適當之培訓資源」，具體執行方式？**	**【答覆】** 本條所稱之「適當培訓資源」，包括保險業自行規劃並辦理之內部教育訓練（如委託第三方業者導入 AI 系統，得請其提供必要之教育訓練與後續支援）或由主管機關、金融研訓院、壽（產）險公會等外部機構開設之 AI 相關課程，以供保險業內部負責 AI 系統之部門、團隊及相關人員作為培訓之用。
問題 6 **第八條若保險業自行運用市場既有之**	**【答覆】** 本題所稱「自行開發」之認定，參酌金管會「金融業運用

問題	答覆
AI 演算法（如機器學習模型 Scikit-learn、XGBoost、Random Forest、SVM 等；深度學習模型 CNN、RNN；大語言模型如 LLaMa、GPT、Gemini、Claude 等）及相關函式庫進行 AI 模型之資料處理、訓練微調、調整推論階段參數或進行檢索增強生成（RAG）相關優化調整者，是否屬於自行開發之範疇？	人工智慧（AI）指引」之意旨，除金融機構獨立開發外，亦包括與其他機構共同或聯合開發 AI 系統，以及以市場上既有之開源 AI 模型為基礎，進一步自行訓練、微調、調整推論參數或進行檢索增強生成（RAG）等相關優化調整完成之 AI 系統。 無論使用開源或閉源 AI 模型（如 GPT、Gemini、Claude 或其他第三方業者提供之模型，以 API 或服務提供者），若保險業者進一步實質開發，建置為 AI 系統，主導控制 AI 運作參數、AI 關鍵功能及版本變更等事項，對 AI 系統具開發主導控制權者，屬「自行開發」，應適用本自律規範第八條之規定。 若委由第三方業者提供成品辦理 AI 系統，保險業者僅執行基本設定或串接者，非屬「自行開發」。 若僅使用一般性 AI 訂閱服務供個人作業，未與保險業者內部系統進行串接者，非屬保險業運用「AI 系統」之範疇，亦非屬「自行開發」。
問題 7 **第九條及第十五條保險業運用生成式 AI 時，是否可依循金管會金融業運用人工智慧（AI）指引之 AI 系統生命週期包含系統規畫及設計、資料蒐集及輸入、模型建立及驗證系統部署及監控四階段，分別進行闡述並檢附相關資料，以確保可說明其運作模式及如何做出回應，使其具備可解釋性？**	**【答覆】** 是。參照金管會「金融業運用人工智慧（AI）指引」之生命週期框架，屬通用架構，涵蓋各類 AI 系統的風險與治理要求，生成式 AI 亦適用；惟其運作原理之特性，直接解釋模型本身具技術限制，得以該模型所屬之 AI 系統為主體，依循生命週期框架各階段進行闡述並檢附相關資料，以說明 AI 系統之運作模式及如何作出回應，使其具備可解釋性。
問題 8 **第十三條針對模型韌性（resilience）之定義，是否依循金管會金融業運用人工智慧（AI）指引之定義：係指 AI 模型能適當地處理未在預期內的資料輸入或於信心水準過低時拒絕做出預測；以利保險業者選擇並評估模型之依據？**	**【答覆】** 是。可參照金管會「金融業運用人工智慧（AI）指引」之韌性定義。