出國報告(出國類別：開會)

參加日本公益財團法人亞洲人壽保險振興中心 2024 年秋季研討會「風險管理」(OLIS 2024 Autumn)出國報告

服務機關：金融監督管理委員會保險局

姓名職稱：董珏安專員

簡禎科員

派赴國家/地區：日本東京

出國期間：113 年 10 月 23 至 113 年 10 月 30 日

報告日期：114 年 1 月 16 日

摘要

本次日本公益財團法人亞洲人壽保險振興中心於 113 年 10 月 23 日至 29 日舉辦秋季研討會(OLIS 2024 Autumn)，聚焦「保險公司風險管理」，旨在探討保險業於當前市場環境中所面臨的風險挑戰及應對策略，並提供國際間專業交流平台，以促進風險管理知識的深化與實務經驗的共享。

會議內容涵蓋六大核心議題：投資風險管理、作業風險管理、企業風險管理、資訊科技（IT）風險管理、核保風險管理及內部稽核。首先，會議強調投資風險管理的重要性，在當前全球經濟不確定性高漲的情況下，保險公司需建構穩健的投資風險評估機制，以維持資產的穩定性與流動性。其次，作業風險管理著重於強化業務流程控管，強調透過制度化的風險預警機制，有效降低人為錯誤及作業風險，提升整體運營效率。企業風險管理則致力於全方位整合風險管理策略，通過系統性辨識及評估各項潛在風險，建立跨部門協作機制，提升整體風險抵禦能力。此外，IT 風險管理聚焦於資訊安全與系統穩定性，保險公司面臨的網路攻擊及資安風險日益增加，必須建立完善的防護機制及即時監控體系，以確保資訊系統安全運作並保障客戶資料安全。核保風險管理對保險公司的經營穩健性與長期盈利能力具有深遠影響，在商品設計及核保時須綜合考量風險胃納、保險市場趨勢、經濟環境變化、客戶需求等，並應定期進行風險監控及制定事後措施。最後公司應建立獨立且全面的稽核機制，達到風險早期預防與確保公司經營符合相關法令規定的目標。

本次研討會突顯出風險管理於保險業永續發展中的關鍵地位，尤其在全球風險環境快速變遷的背景下，日本保險業的整體風險管理機制值得借鏡。其對企業風險管理（ERM）的嚴謹導入、對 IT 風險的高效控管以及稽核機制的落實，皆展現了高度的前瞻性與成熟度。未來我國保險業可參考其經驗，針對風險管理架構進行強化與優化，進一步提升保險業的風險抵禦能力，並為產業的長期穩健發展奠定堅實基礎。

目錄

第一章　會議背景及目的

第一節　會議背景

日本公益財團法人亞洲人壽保險振興中心（Oriental Life Insurance Cultural Development Center，以下簡稱 OLICD Center）成立於 1967 年，是專為促進亞洲地區人壽保險業發展而設立的重要機構。該中心由協榮人壽保險公司（現為直布羅陀人壽保險公司）時任社長川井三郎博士（Dr. Saburo Kawai）提議並捐資成立。OLICD Center 設立目的在於促進亞洲國家對人壽保險知識的深入了解，並透過培養專業人才，加強國際間的交流合作，推動亞洲人壽保險事業的穩健成長。

OLICD Center 每年定期舉辦春季與秋季的「亞洲人壽保險研討會」（Oriental Life Insurance Seminar，以下簡稱 OLIS），每次為期一週，吸引了來自亞洲各國的保險監理官及保險業界中高層管理人員參加。截至目前，OLIS 的參與人數已超過 5,200 人，成為亞洲保險業界重要的國際交流平台。

第二節　會議目的

OLIS 2024 秋季研討會於 113 年 10 月 24 日至 10 月 29 日在日本東京舉行。本次研討會共邀請來自 13 個國家的 38 位代表參加，包括柬埔寨、中國、印尼、韓國、馬來西亞、蒙古、尼泊爾、巴基斯坦、菲律賓、臺灣、泰國、烏茲別克及越南。本次活動以「保險公司風險管理」為主題，深入探討保險業在多變環境中所面臨的挑戰，主要議題涵蓋投資風險管理、作業風險管理、企業風險管理、資訊科技風險管理、核保風險管理及內部稽核等，並安排各國與會代表進行簡報交流。

本次會議透過專家演講和案例分析，探討保險業面臨之風險挑戰及應對策略，提升參與者對於關鍵風險管理領域的理解與應用能力。透過國際經驗分享，協助參與者掌握最新風險管理趨勢，進一步建構完善的風險預防與治理架構，強化保險企業的穩健經營及風險應對能力。

第二章　會議過程及內容重點

第一節　會議議程及進行方式

本次會議邀請日本保德信控股公司(Prudential Holdings of Japan, Inc.)及直布羅陀人壽保險公司(The Gibraltar Life Insurance Co., Ltd.)之相關部門成員擔任講師，會議進行方式係由講師先行分享各議題內容，於各議題分享完畢後，給予足夠時間讓各國與會代表發言及討論，並於四天議程中安排各國與會代表進行簡報，分享各國近年來保險業營運變化。本次會議議程整理如下表：

日期	議題/講師
10 月 24 日	**投資風險管理 Investment Risk Management at Life Insurance Companies** 廣富弘樹先生 (Mr. Hiroki Fukudomi) 直布羅陀人壽保險公司 (The Gibraltar Life Insurance Co., Ltd.) 風險管理部門經理
	作業風險管理 Operational Risk Management 小松崎正大先生 (Mr. Masahiro Komatsuzaki) 日本保德信控股公司 (Prudential Holdings of Japan, Inc.) 作業風險管理部門主管
10 月 25 日	**日本的人壽保險企業風險管理 Life Insurer's ERM in Japan** 上村信康博士 (Dr. Nobuyasu Uemura) 福岡大學 (Fukuoka University) 商學院教授
10 月 28 日	**資訊科技風險管理 IT Risk** 齋藤浩一先生 (Mr. Koichi Saito) 日本保德信人壽保險公司(The Prudential Life Insurance Company, Ltd.)

	商業資訊安全主管
	核保風險管理 Underwriting Risk Management 藤林昭宏先生 (Mr. Akihiro Fujibayashi) 直布羅陀人壽保險公司 (The Gibraltar Life Insurance Co., Ltd.) 簽證精算師
10 月 29 日	**內部稽核 Internal Audit** 高橋望女士 (Ms. Nozomi Takahashi)及劉珊美女士 (Ms. Sammi Liu) 保德信金融公司日本代表處 (Prudential Financial Inc., Japan Representative Office) 資深稽核經理

第二節　會議內容重點

本次會議主題為風險管理(Risk Management)，會議內容包括投資風險管理、作業風險管理、企業風險管理、資訊科技風險管理、核保風險管理、內部稽核等議題，就該等議題之會議內容重點分別整理摘要如下：

壹、投資風險管理(Investment Risk management at Life Insurance Companies)

一、投資風險管理概述：

投資風險管理是壽險公司穩健經營的核心環節，其主要目的是確保資金運用的效率與安全，並確保長期保險責任的履行。隨著市場環境日益複雜，投資風險管理需要更精準的策略和多層面的執行機制。壽險公司投資應遵循以下四大原則：

(一) 獲利性原則：壽險公司需透過長期穩定的投資，達到一定的資金運用收益率，從而滿足投保人和股東的期望。為此，保險公司應積極尋找全球化的投資機會，並合理分散於股票、債券、不動產等多元資產類別，以降低單一市場風險。

(二) 安全性原則：壽險公司的投資操作應以嚴謹的風險控制為基礎，例如利用衍生性商品對沖市場波動風險，實施有效的資產負債管理，並保持投資組合的多樣性。特別是在配置高風險資產時，需建立全面的預警與監控機制。

(三) 流動性原則：壽險公司需預測未來現金需求，靈活調整資金配置，以確保資金在保險給付、解約金支付等情況下的充裕性。常見措施包括持有現金、短期金融工具及其他具備高流動性的資產。

(四) 公共利益原則：作為承擔重大社會責任的產業，壽險公司應將資金運用與社會發展結合。例如，採取 ESG（環境保護、社會責任、公司治理）投資策略，並積極響應聯合國永續發展目標（SDGs），在實現財務回報的同時創造社會和環境效益。

二、日本保險業的資產管理挑戰：

預計 114 年起日本的清償能力指標將從目前的 SMR（邊際清償能力比率）評估方式，轉為 ESR（經濟清償能力比率）評估。SMR 側重於帳面價值的資產與負債衡量，而 ESR 則引入市場價值法（Market Value Approach），根據金融市場的動態進行評估。此一轉變將要求保險公司具備更高的資產負債匹配能力及動態調整策略，以應對市場波動對資本穩健性的影響。

SMR 的計算較為簡單，其公式主要基於帳面價值計算資本適足率，側重於靜態評估，且不完全考慮市場波動的影響，因此可能低估或高估資本的實際風險，且 SMR 的風險權重設置較為固定，對於市場的反應能力有限。相較之下，ESR 更能反映資產與負債的實際經濟價值及風險，其計算方法採用市場價值法，將資產與負債按市場價格進行動態評估，並整合壽險公司未來現金流的預測和隨機情境測試。ESR 相較 SMR 更具靈活性，同時對數據分析能力、資本模型的精確度以及模型驗證有更高的要求。

ESR 並引入經濟資本的概念，要求壽險公司根據風險暴露情況計算所需的資本，並對不同類型的風險（如市場風險、信用風險、作業風險）進行量化。ESR 的導入旨在提升保險公司的風險管理水準及整體透明度，促進市場的穩健發展，並更有效地保護保戶權益。

三、投資風險管理：

隨著金融市場環境的不斷變化及競爭的日益激烈，公司面臨的投資風險越來越多樣化且複雜。透過資產負債管理（Asset-Liability Management, ALM）與企業風險管理（Enterprise Risk Management, ERM）來強化投資決策和風險管理策略，不僅能有效降低不確定性，亦能提升公司的整體競爭力。ALM 注重資產與負債的動態匹配，實現穩健性與收益性的平衡；ERM 則著眼於全面風險管理，旨在整合內部資源與策略，以實現可持續的價值創造。以下分別說明其主要應用方式：

(一) 資產負債管理（ALM）：ALM 是一種將資產與負債進行匹配與整合的管理方式，目的是在不同經濟條件下維持公司的財務穩健性與收益性。常見的 ALM 策略如下：

1. 匹配型（Matching Type）：

   透過確保資產與負債在期限結構與現金流量上的一致性，可以有效降低利率風險及流動性風險。當公司承擔長期負債時，若能適當配置期限相符的長期資產，將有助於減少期間錯配所可能引發的風險，進一步提升資產負債管理的穩健性。

2. 平衡型（Balance Type）：

   以維持資產與負債間的穩定平衡為核心目標，該策略根據市場環境的變化適時調整資產配置比例，在可接受的風險範圍內追求更高的投資回報。此類型策略特別適用於具有較高風險承受能力的公司，重點在於靈活應對市場波動，同時兼顧收益提升與資產負債動態管理的需求。

3. 剩餘型（Surplus Type）：

   剩餘型資產負債管理策略旨在針對超出負債需求的資金進行有效運用，採取穩健且多元化的資產配置方式，以達成資產價值的長期增長。此策略強調精準掌控剩餘資金的配置與運作，透過細緻的風險管理與投資績效提升，實現資本運用效率的最大化，同時有效控制潛在風險。

(二) 企業風險管理（ERM）：企業風險管理是一種以整體視角來識別、評估、應對及監控風險的管理框架，旨在協助企業在風險與收益之間取得平衡，並為股東創造長期價值。具體做法如下：

1. 提升公司經營能力：透過 ERM 的落實，企業能顯著改善經營表現，具體體現在以下幾個方面：

(1) 獲利能力：ERM 可協助企業識別最有效的資金配置策略，減少資源浪費，從而提升投資收益並增強盈利能力。

(2) 清償能力： 透過精準的風險量化與有效的資本管理，確保保險業的清償能力（Solvency）要求，以滿足監管要求並保障保戶的權益。

(3) 效率：ERM 強調內部流程優化與資源整合，減少因管理疏失導致的損耗，提升運營效率，增強企業競爭力。

2. 全面識別與分析風險：對內部及外部各類可能影響企業目標達成的風險進行系統性分析，確保風險因素被精確辨識與量化，為後續決策提供數據支持。

3. 制定策略與控制機制：根據風險評估結果，設計符合企業目標的策略，並建立相應的風險控制機制，以最大化資源運用效益，同時將風險控制在可接受範圍內，確保企業運營的穩健性與可持續性。

四、投資風險種類：

企業在進行投資活動時，可能面臨來自多層面的風險。清楚識別與分類這些風險，能協助企業設計更加精準的風險管理策略，以提升投資效益並降低潛在損失。以下針對三大主要風險類型進行說明：

(一) 市場風險（Market Risk）：市場風險指因市場價格波動（如利率、匯率、股票價格或商品價格變化）導致的潛在損失。這類風險往往受到外部環境因素影響，例如經濟衰退、政策調整或地緣政治事件等，具有難以完全規避的特性。然而，企業可採取對沖策略，例如利用期貨、期權或遠期合約等衍生性金融工具，來減少市場波動所帶來的損失。

(二) 信用風險（Credit Risk）：信用風險是指交易對手或借款方未能履行其合約義務，可能導致企業遭受損失的風險，例如債券違約或貸款無法按期償還。為

有效降低此類風險，企業可引入信用評級系統，強化事前審查機制，或透過擔保措施、分散投資組合等方式，提升整體風險抵禦能力。

(三) 流動性風險（Liquidity Risk）：流動性風險指當企業需要資金時，因市場流動性不足而無法迅速將資產變現，或被迫以折價出售資產所帶來的損失。為應對這類風險，企業應保持足夠的現金儲備，同時增加對高流動性資產（如短期政府債券或貨幣市場工具）的配置，以確保資金調度的靈活性與穩定性。

五、風險衡量方法：

在投資風險管理的實務中，準確衡量風險是制定有效管理策略的核心基礎。透過適當的量化工具，企業得以具體掌握風險的特性與程度，進而設計針對性應對方案。其中，VaR 值法與壓力測試法為目前被廣泛應用且具高度實務價值的兩種風險衡量方法，具體說明如下：

(一) VaR 值法（Value at Risk, VaR）：VaR 值法是一種以統計模型為基礎的風險衡量工具，主要用於估算在特定信賴水準（如 95%或 99%）及一定時間範圍內，投資組合可能遭受的最大潛在損失。此方法對於穩定市場條件下的日常風險監控與管理，提供了清晰的量化參考。然而，VaR 值法的假設通常基於資產收益呈現常態分佈，因此在極端市場情境（例如金融危機）下，可能低估尾部風險。為補足此侷限，條件尾端期望值（Conditional Tail Expectation, CTE）被引入作為輔助工具，聚焦於尾部風險的損失評估。CTE 能協助管理者進一步了解極端情境下的風險分佈，為資本配置與應變策略的制定提供更全面的依據。

(二) 壓力測試法（Stress Testing）：壓力測試法是一種模擬極端市場條件下，投資組合可能表現的風險評估技術。相較於 VaR 值法，壓力測試不依賴於特定的統計分佈假設，而是根據假設性或歷史性的市場事件進行情境分析。此方法可模擬如經濟衰退、大規模政策變動、地緣政治衝突及自然災害等情境對

投資組合的潛在影響。壓力測試通常結合歷史數據分析與假設情境建模，既反映過去重大市場危機的實際影響，又考量假設性極端事件的潛在風險，以便於企業評估「最壞情況」下的財務影響程度。透過壓力測試，企業能針對可能出現的極端情境提前制定緊急應變計畫，例如提高資本緩衝、調整資產配置策略或強化流動性管理能力。

貳、作業風險管理(Operational Risk Management)

一、作業風險概述：

作業風險是指因內部流程、系統、人員或外部事件的缺陷或失誤，可能導致公司面臨財務損失或聲譽損害的風險類型。與財務風險和市場風險不同，作業風險涵蓋了非金融性的內外部事件，例如系統故障、人為錯誤、法律合規問題及自然災害等。作業風險的管理對於維持公司經營的穩定性和可持續發展至關重要。有效的作業風險管理需要構建專門的組織和架構，確保責任明確、流程清晰，並能動態應對風險挑戰。具體包括：

(一) 風險管理部門設置：設立專門的風險管理部門，負責制定政策、推動執行並監控風險管理計劃。

(二) 分層管理架構：在組織內部形成自上而下的管理體系，包括董事會、高層管理層及基層操作部門，各層次分工明確。

(三) 培訓與意識提升：對全員進行定期培訓，提升員工對作業風險的識別與應對能力。

二、作業風險管理的基本策略：

作業風險管理的基本框架應包括以下關鍵要素：

(一) 實施作業風險管理：確保組織內部建立一致的風險管理流程和政策，包括制定策略、分配責任及配置資源，形成有效的風險管理體系。

(二) 識別公司作業相關風險：通過全面檢視業務流程及內外部環境，發現可能影響業務目標的風險因素，如技術風險、操作失誤或法律合規問題。

(三) 分析與評估風險：採用量化與質化分析方法，評估風險發生的概率及其潛在影響，並確定管理的優先順序。

(四) 應對風險：針對已識別的風險規劃具體應對措施，如流程優化、內控加強或技術支持，以減少風險發生的可能性和影響範圍。

(五) 控制與監控風險：建立實時監控機制，通過關鍵風險指標（KRIs）及數據分析，監測風險狀況，並對異常情況及時採取行動。

三、作業風險失敗案例：

作業風險失敗案例的分析有助於機構了解過去失誤的根本原因，並制定針對性的預防措施。以下為講者分享之案例：

(一) 2005 年日本某證券公司：因輸入錯誤，將 610,000 股的一家公司股票以每股 1 日元出售，而非以 610,000 日元賣出 1 股。此次操作失誤導致超過 4 億美元的損失。

(二) 2011 年日本某銀行：由於夜間批量處理系統中斷，導致 ATM 和帳戶轉帳功能無法正常運行，損失高達 8,000 萬美元。

(三) 2014 年日本某銀行分包商：該分包商非法製造虛假銀行卡和信用卡，並利用客戶信息進行資金提取，最終損失達數十萬美元。

四、監管措施之演進：

監管措施在作業風險管理中扮演關鍵角色，確保金融機構的運作符合國際標準並減少潛在風險。

(一) 巴塞爾銀行監管委員會（BCBS）：

1998 年：提出「銀行內部控制系統框架」及「作業風險管理」概念。

2003 年：引入「管理與監督作業風險的實務」。

2010 年：將「先進計量法」引入資本充足率的計算中。

(二) 日本金融廳（Financial Services Agency, FSA）：

2007 年：針對日本的作業風險數據進行調查。

2010 年：舉辦研討會探討「作業風險進展—數據場景共享的重要性」。

(三) 國際保險監督官協會（IAIS）：

2011 年：引入《保險核心原則》（ICP）。強調保險公司應識別並解決所有可預見及相關的重大風險，包括承保風險、作業風險、流動性風險等。

作業風險雖然不可完全消除，但通過建立健全的風險管理架構與流程，可以有效降低其對保險公司營運穩定性與可持續發展的威脅。同時，借鑒過去的失敗案例與教訓，不僅可以協助公司在日常營運中避免類似問題，還能提供制定針對性風險因應策略的寶貴指引。此外，遵循國際監管標準，亦有助於公司確保其落實風險管理。以系統化、動態化和前瞻性的方式持續改進，並全面應對當前和未來的挑戰，才能為企業長期發展奠定穩固基礎。

叁、日本企業風險管理(Life Insurer’s ERM in Japan)：

一、日本壽險市場概況：

日本壽險市場主要以傳統型產品為主，這些產品在銷售時便已確定未來的現金流，因此其收益結構在一定程度上受到市場環境的影響。自 1990 年代以來，儘管主要壽險公司逐漸轉向銷售保障型產品，但大量的責任準備金仍集中於終身

壽險及長年期年金保單。對於銷售高利率儲蓄型產品的壽險公司而言，長期的低利率環境進一步加劇了經營挑戰。這種經濟局勢成為壽險公司生存與發展的關鍵。

日本壽險市場的產品結構自 1980 年代以來呈現多元化趨勢，過去以生死合險為主的局面逐漸被多樣化的產品所取代。然而，2000 年前後的低利率環境對市場造成了重大衝擊，導致日本七家中型壽險公司破產，這些公司的資產總額超過行業總資產的 10%，突顯了以日圓計價的長年期儲蓄型保單在低利率環境中的脆弱性。破產的原因包括外部與內部多重因素。外部因素如泡沫經濟破滅導致利率下降、股票與土地價格大幅下跌；內部因素則與商業模式及管理層能力不足相關，此外，過度銷售高利率儲蓄型產品也加劇了壽險公司的財務壓力。

日本壽險市場的集中度相對較低，主要壽險公司僅約佔市場保費收入的 50%，其中包含兩家上市公司及三家相互保險公司；非壽險市場的集中度則較高，由三大集團主導。

壽險業面臨的主要業務風險涉及多個層面，包括死亡率及罹病率遠高於預期的風險、壽險責任準備金的低估、資產負債管理失當，以及解約率快速上升的挑戰。壽險公司普遍持有大量的證券與不動產，並向企業及個人提供貸款，但低利率環境不僅對清償能力構成負面影響，也使得提供以日圓計價的長期儲蓄型產品更加困難。

二、從傳統風險管理到企業風險管理（ERM）

傳統的風險管理主要目的是避免和減少損失，其覆蓋範圍集中在特定風險，並由風險管理部門或專責單位負責。這種管理模式基於對不同風險類型的識別，並在需求時採取相應的應對措施。

相較之下，企業風險管理（ERM）採取了更為全面且整合的方式。ERM 的目標是在維持財務穩健的基礎上，實現企業價值的可持續增長。其涵蓋範圍不僅限於已知風險，還包括新興風險，並且不局限於單一部門，而是由整個公司層面進

行風險管理活動。ERM 強調以整合且一致的方式看待所有風險，並將風險管理與業務策略緊密結合。

三、風險管理中的關鍵挑戰與失敗

風險管理失敗不僅僅表現在企業遭受損失，還可能體現在未能合理承擔應有風險的情況。例如，企業在具備專業能力與足夠資本的條件下，仍選擇過度保守的策略，也是一種失敗的風險管理方式。因此，成功的風險管理應當在利潤、資本與風險之間實現平衡，從而提升企業價值。

在 ERM 框架下，風險管理團隊的角色至關重要。團隊需負責制定風險政策，明確企業應承擔的風險，並確保風險控制措施與公司的風險偏好相符。這種綜合性的管理方法要求風險管理不僅僅是某個部門的職責，而是整個組織的集體責任，並需要在清晰的政策與流程指引下執行。

四、清償能力監管發展

日本在 1995 年《保險業法》修訂後，保險市場的自由化進程顯著加速。壽險公司與非壽險公司得以通過子公司進入彼此的市場，並推動了產品的多樣化與費率的自由化。然而，自由化帶來的競爭壓力也對保險公司的財務穩健性提出了更高的要求。在此背景下，監管機構強調壽險公司需適當累積責任準備金，並保持足夠的償付能力邊際比率（SMR）。SMR 作為早期糾正措施的核心指標，其計算公式如下：

$$\text{Solvency Margin Ratio (\%)} = \frac{\text{Solvency Margin}}{\frac{1}{2}\text{Risk Amount}} \times 100$$

日本金融廳（FSA）已計畫於 2025 年全面引入以經濟價值為基礎的監管框架（即 ESR），旨在進一步強化自律管理與風險控制能力。另自 2015 年起，FSA 已要求壽險公司提交保險業自我風險及清償能力評估（ORSA）報告，進一步提升風險透明度與管理能力。

肆、資訊科技風險管理(IT Risk)：

一、人工智能(Artificial Intelligence, AI)：

生成式人工智能(生成式 AI, Generative AI)係一種能透過學習數據及資料，生成新內容的人工智能。相較於傳統人工智能(Conventional AI)主要係自動化執行指定的動作，生成式 AI 則可生成各種全新內容，包括文字、圖像、影片和音訊等，因此生成式 AI 與其他 AI 有著顯著不同。生成式 AI 讓沒有專業知識的一般人都能相對輕鬆地創作內容，故隨著生成式 AI 進一步發展與普及，預計生產力將會有顯著的提升。

根據麥肯錫(McKinsey)的調查，2024 年約有 72%的企業採用 AI，且約有 65%的企業採用生成式 AI。此外，日本總務省的調查顯示，各國企業使用生成式 AI 的普及性有很大的差異，例如在美國有 85%的企業使用 AI，而日本僅有 47%的企業採用 AI。

二、人工智能在保險業之應用：

(一) 理賠管理：透過 AI 的自然語言處理技術(natural language processing, NLP)，從大量客戶及理賠資料中提取有價值的資訊，從而協助理賠人員根據更充分的資訊進行決策。

(二) 客戶服務：使用 AI 聊天機器人，可以減少客服人員的回應時間，從而提升客服品質。

(三) 詐欺檢測及預防：透過機器學習和人工智能演算法，分析非結構化和半結構化數據，如理賠備忘錄 (claims memos)可檢測並分析潛在的不當行為。

(四) 優化核保程序：透過結合機器學習模型及深度學習模型，核保作業所需時間可減少至幾秒鐘。

(五) 預測客戶流失率：透過人工智能和機器學習演算法，保險公司可預測客戶是否有可能解約，並採取相應措施。

三、人工智能風險管理框架(AI Risk Management Framework, AI RMF)：

雖然運用 AI 技術可以提高作業效率及品質，但仍須注意可能的資料外洩、版權、安全性、隱私性等問題，因此 2023 年 1 月美國國家標準與技術研究所(NIST)發布了 AI RMF 1.0，協助公司開發、導入及使用可信賴的人工智能。AI RMF 分為兩個部分：

(一) 第一部分為 Foundational Information，主要闡述組織如何框定與 AI 相關的風險及可信賴 AI 系統的特徵：

1. AI 風險管理之困難：

(1) 風險衡量(Risk Measurement)：AI 風險不只來自第三方資料或軟體，也可能與如何使用這些資料及軟體有關，但目前衡量風險及可信度的方法還不成熟，同時 AI 系統的不透明性也增加了風險衡量的難度。

(2) 風險優先級(Risk Prioritization)：風險不可能完全消除，因此建立風險管理文化十分重要，應根據風險等級及影響，評估資源分配。

(3) 組織整合(Organizational Integration)：企業風險管理(ERM)策略與流程中應加入 AI 風險管理，並應同時考量其他 IT 風險，如網絡安全、隱私、軟體開發及運行常見的風險等。

2. 可信賴 AI 系統的 7 種特徵分別為有效且可靠(valid and reliable)、安全性(safe)、資安與韌性(secure and resilient)、系統運作機制可解釋性與產出結果可詮譯性(explainable and interpretable)、個資隱私保護(privacy-enhanced)、公平性—偏見管理(fair-with harmful bias managed)及可歸責與資訊透明度(accountable and transparent)。

(二) 第二部分為 Core and Profiles，說明實務上如何應對 AI 系統的風險，並提出人工智能風險管理框架核心(AI RMF Core)。該框架核心包括以下 4 個功能，各功能有項目(Category)及子項目(Sub-category)：

1. 治理(Govern)：應制定並可落實之人工智能風險相關的政策、流程和規範，建立責任架構，以確保相關團隊和個人能確實執行以下 3 個功能，並培養組織人工智能風險文化。

2. 映射(Map)：進行人工智能系統的分類與目標設定，理解其功能、預期效益與成本，並辨識風險，包括第三方軟體與數據。

3. 衡量(Measure)：辨識並使用適當的方法與指標，包括使用前述可信度特徵進行評估，並建立機制持續追蹤人工智能風險的變化。

4. 管理(Manage)：對人工智慧風險進行排序、回應及管理。

四、常見之資訊安全問題：

(一) 勒索軟體(Ransomware)：

除了資料加密外，近年來許多勒索軟體攻擊係以公開其所竊取之資料勒索受害公司。根據 Veeam 統計，遭到勒索軟體攻擊之資料中，僅有 57%成功恢復。另外，受害公司約有 11%未支付贖金即成功恢復資料，54%在支付贖金後成功恢復資料，但有 27%即使支付贖金仍無法恢復資料。有關保險的部分，支付贖金的公司中，有 67%係透過資安保險支付，但有 22%即使購買了資安保險，仍選擇自行支付贖金。

根據 SOPHOS 統計，2024 年平均恢復成本創新高，達到 273 萬美元，且受到勒索軟體攻擊後所需恢復時間顯著增加，其中約 34%需要超過一個月才能恢復。

據統計約有三分之一的資料外洩案件與勒索軟體或其他勒索手法有關，其中具代表性的案例是 2023 年 5 月發生之 MOVEit 檔案傳輸平台案，根據 EMSI SOFT 統計，共有 2,773 家公司及 95,788,491 人受到該事件影響。

(二) 美國網路安全暨基礎設施安全局(CISA) 已知遭駭漏洞（KEV）之修補情形：

根據 2024 年 Verizon 之資料外洩調查報告(2024 Data Breach Investigations Report)，在 CISA 已知遭駭漏洞中，有 50%的漏洞在公布後 55 天內完成修補，通常在漏洞公布 30 天後開始進行大規模修補程序，然而在漏洞公布一年後，仍有 8%的漏洞仍未被修補。

(三) 網路釣魚(Phishing)：

根據 2024 年 Verizon 之資料外洩調查報告，使用者從點開網路釣魚信到完成資料輸入通常不到 1 分鐘。另外，從釣魚信測試發現，大約有 20%使用者（包括 11%點開釣魚信的使用者）能成功辨識並通報，因此仍需持續增強使用者對網路釣魚之防範意識。

(四) 憑證盜竊攻擊(Exploiting of stolen credentials)：

過去十年所發生的資料外洩事件中，約有三分之一被證實與憑證盜竊攻擊有關，其中許多針對網頁應用程式的攻擊已證實與撞庫攻擊(credential stuffing)有關，即用過去從其他資料外洩事件取得之帳號及密碼，至其他網站嘗試登入，而非使用暴力破解攻擊(brute force)。

五、MITRE 攻擊性策略、技術和常識(ATT&CK; Adversarial Tactics, Techniques & Common Knowledge)：

(一) 網路攻擊(Cyberattacks)之目的：

1. 財務動機(Financially-motivated)：網路攻擊成本很低卻可以帶來巨大利潤，根據 Verizon 統計，超過 90%的資料外洩攻擊與財務動機有關。

2. 商業信息(Business Intelligence)：該類網路攻擊利用如網路釣魚等技術盜取用戶資料，滲透入商業網絡或取得機密商業信息。

3. 國家支持之攻擊(State-sponsored Attacks)：由國家雇傭之駭客進行。

4. 駭客行動主義(Hacktivism)：駭客行動主義者(hacktivists)透過攻擊政府或大型組織試圖引起人們對政治議題、網路相關法規、審查制度等之關注。

5. 個人原因(Personal Reasons)：通常是現任或前員工，因對公司不滿，而竊取並出售機密數據以獲取利益或損害公司。

6. 白帽駭客/道德駭客(White Hat Hacker)：有些駭客係為使組織加强其安全防禦而進行善意的駭客行為，但仍可能造成商業系統損害。

(二) 攻擊性策略、技術和常識(MITRE ATT&CK)：

MITRE ATT&CK 是一個針對已知網路犯罪行為進行建模、檢測、預防及應對網路安全威脅之可普遍取得並持續更新的資料庫，其有 4 個主要組成成分：(1)策略(Tactics)，描述網路攻擊者(advisory)行動目的及原因、(2)技術(Techniques)，描述網路攻擊者如何通過行動達到策略目標、(3)子技術(Sub-techniques)，針對攻擊行為的更具體及細節描述、(4)程序(Procedures)，說明網路攻擊者實際使用的工具、技術、子技術等。

(三) 技術之應用：

1. 網路釣魚：網路釣魚屬於網路攻擊者偵察(Reconnaissance)之策略，用以收集目標之資訊。除了欺騙目標在假冒網站上輸入 ID 或密碼外，亦可能利用社交工程技術(social engineering technologies)，假冒成需要目標提供信息的可信人物。因應措施包括使用寄件者原則架構(Sender Policy Framework, SPF)等電子郵件技術來防止僞冒，及訓練使用者使其能辨識網路釣魚等。

2. 有效帳戶 (Valid Accounts)：網路攻擊者使用已遭入侵的有效帳戶進入目標系統，從而可以做到初始存取、進入 VPN、網路設備等。攻擊者常透過前員工的帳戶入侵系統，因此因應措施包括使用多因子驗證(MFA)、定期檢核帳戶並停用或刪除不必要的帳戶等。

3. 濫用公開存取的應用程式 (Exploit Public-Facing Application)：網路攻擊者利用主機或系統的弱點進入網路，如程序錯誤、配置錯誤(configuration errors)或系統軟體臨時缺陷。因應措施包括網路分區隔離 (Network Segmentation)、使用 Web 應用程式防火牆 (WAF) 、最小化服務帳戶的權限、將軟體更新至最新版本、定期進行漏洞測試等。

4. 加密數據 (Data Encrypted)：網路攻擊者可能加密目標系統上的數據，影響系統和網路可用性。通常勒索軟體會加密一般用戶文件，而部分勒索軟體能在網路中擴散。因應措施包括使用行為監控端點安全工具(behavior detection-type endpoint security tools)、備份數據等。

伍、核保風險管理(Underwriting Risk Management)

一、核保風險(Underwriting Risk)：

(一) 核保風險：係指保險公司因經濟情況改變（如利率、匯率等波動），或保險事故發生率（如死亡率、罹病率、解約率等）與訂定保費時的預測不符，而可能遭受損失的風險。因壽險通常為常年期契約，保險公司於契約訂定後難以因損失率增加而調整保費或保障內容，因此核保風險將對保險公司營運造成長期的影響，且較難以控制及調整相關風險。

(二) 風險胃納(Risk Appetite)：保險是承受風險的產業，有風險才會有報酬，因此風險管理並非要避免風險，而是選擇性承受風險。

二、風險選擇(Risk Selection)：

核保風險選擇之目的係為拒絕高風險者之投保申請，並根據風險等級訂定保險費率。核保風險選擇之步驟為（1）面談、詢問及觀察、（2）聲明及體檢、（3）核保、（4）合約確認及（5）繳交保費評估。核保風險選擇主要評估事項包括被保險人之年齡、健康狀況、是否有高風險之習慣、繳交保費之來源等，風險選擇方法則依被保險人的年齡、保險金額、保障範圍等決定。核保風險選擇需在盡可能同意承保及拒絕高風險者之投保申請以維護保戶間之公平性及防止民眾濫用保險間，依公司之風險胃納取得平衡。

三、保險商品規劃(Product Planning)：

規劃保險商品需瞭解公司能承受之風險、思考客戶需求、公司的風險胃納、銷售通路類型、保險事故發生頻率及單次賠付金額等。

(一) 保險給付條件(Payment Conditions)：若保險給付條件為生存或死亡，理賠判斷相對單純，但若為醫療險，給付條件較為複雜。若採用公共系統標準(Public system standards)，雖然保險給付條件明確，但會受到公共保險系統影響，給付條件非保險公司可自行控制或預期；若採用保險公司自定標準，給付條件將由保險契約條款約定，較具有彈性，且保險公司較可以控制給付條件。

(二) 保險銷售通路及市場：公司可依銷售通路之特性設計適合的保險商品種類及保障範圍，或選擇符合公司銷售策略之通路：

1. 保險業務員：主要係透過個人關係接觸客群，進行面對面銷售，會更清楚保戶之健康狀況。

2. 保險代理人：不同的保險代理人差異較大，亦以面對面銷售為主。

3. 銀行保險：以面對面銷售為主，主要客群為高齡及高資產客戶。

4. 網路銷售：以年輕族群為主，且客戶多偏好自己研究及選擇保險商品。

(三) 保險期間：

1. 終身險：客戶通常偏好購買終身險，因可獲得終身保障，且保費固定不變，但通常保費較高且核保流程較為複雜。保險公司銷售終身險有助於降低保戶到期不續保之風險，惟一旦開始銷售就較難調整保費計算基礎(premium calculation basis)。

2. 定期險：客戶若選擇投保可續保之定期險，初期保費相對較低，且可在續保時重新評估調整保障範圍，然而隨著年齡增加，保費亦會提高，且高齡時公司不一定會同意續保。保險公司銷售定期險可在續保時調整保費計算基礎，然而易有逆選擇之風險，即體況較差之保戶更可能續保。

(四) 被保險人年齡範圍：須綜合評估客戶需求、銷售通路及市場上同類型商品，以符合公司之風險承擔能力，同時避免出現逆選擇等問題。

(五) 設計特殊的保險商品：

1. 解約價值減少型(Surrender Value Reduction Type)：在保費計算時納入預期解約率，以提供低解約價值或無解約價值的保險商品。透過降低解約價值，可降低保費，亦有助於減少保戶解約。

2. 初期給付金額減少型(Initial Benefit Suppression Type)：透過限制保單初期階段給付金額以減少風險選擇(risk selection)，且可稍微放寬核保標準要、被保險人投保此類保單可避免繁瑣的體檢，銷售通路可簡化作業流程，而保險公司可減少相關成本。

3. 放寬核保標準型(Relaxed Underwriting Standards Type)：為放寬核保標準、減少部分應揭露事項、同意承保有健康問題客戶之保單。然而因承保高風險保戶，保費較高，故可能透過提供小額死亡及醫療保障之保險商品，降低保費，以提供更多體況較差之民眾保險保障。

四、保單訂價(Pricing)

(一) 收集數據資料：

	公開資料(Public Data)	內部資料(In-house Data)
優點	有大量資料，較為可靠。	較符合保險商品內容及條件。
缺點	可能不完全適用保險商品內容及條件，且不一定會持續更新資料，或可能變更資料定義等。	資料量有限，且就新商品，公司可能無法取得相關資料。

保險公司亦會使用人身保險標準生命表(Life Insurance Standard Life Table)作為計算保單準備金之基礎。

(二) 獲利能力檢查：在設定保險費率後，需定期評估該商品之獲利能力。獲利能力之評估主要透過參考類似商品之經驗及未來市場預測等，估計銷售量與保單分布、死亡率、罹病率、解約率、營運費用及投資收益率等。通常使用內部報酬率(IRR)、利潤率(Profit Margin)及新業務價值(Value of New Business, VoNB)作為獲利能力指標，並搭配敏感度分析(Sensitivity Analysis)。

五、定期監控(Monitoring)與事後措施(Post-event Measures)

(一) 定期監控(Monitoring)：透過短期監控（6 個月至 1 年），瞭解實際保單銷售量及保單分布是否符合商品設計時之假設，及長期監控（3 年、5 年、10 年……），定期比較實際之死亡率、罹病率、解約率、等是否偏離商品訂價時之假設。

(二) 事後措施(Post-event Measures)：若經定期監控發現實際情況與設計保單時之預期有較大的偏差，必須採取事後行動，但可採取的措施有限，主要包括：調整佣金、更改承保標準、修改保費率（在日本需要其監理機關 Financial Services Agency (FSA)之同意）、停止銷售該保單、多累積負債準備金等。

(三) 未來利潤分析(Future Profit Analysis)：係用以驗證保險商品準備金之適足性，確保未來準備金能夠持續累積而不需認列損失。

六、未來可能面臨之核保風險管理挑戰及機遇

(一) 醫療技術與診斷技術的進步：將導致未來可能之保險給付金額提高，但亦可能產生新保險商品之機會。

(二) 人口高齡化：對高齡保險商品之需求增加，但保險公司沒有過去的承保及理賠經驗。

(三) 基因資料(Genetic information)：可能造成新的資訊不對稱及逆選擇等問題，部分國家已禁止使用基因檢測資料等作為核保標準。

(四) 資料科學(data science)：優化現有死亡率估計等。

(五) 人工智能：自動化及優化核保流程。

(六) 全球性事件：未來若再發生類似新冠疫情之事件，保險公司應如何因應。

陸、內部稽核(Internal Audit)

一、內部稽核(Internal Audit)：

(一) 三道防線模型(Three Lines Model)：有助於公司建立其組織架構及作業流程，以達到其營運目標、強化公司治理及風險管理。國際內部稽核協會（Institute of Internal Auditors, IIA）提出之三道防線模型如下：

1. 公司治理層(Governing Body)：監督公司運作，並對利害關係人負責。
2. 管理階層(Management)：第一道防線提供客戶商品及服務並管理風險，包含各業務單位等，而第二道防線則負責在風險相關事務上提供專業知識、支援、監控及挑戰，包含風險管理、法遵等單位。
3. 內部稽核：負責獨立且客觀地確認及建議公司所有與達成公司營運目標有關之事項，為第三道防線，亦為此部分課程之主題。

(二) 內部稽核：內部稽核應透過系統化且具紀律性之方法，評估並改進風險管理、內部控制及公司治理流程之有效性。內部稽核部門應依據 IIA 之標準運作，所有內部稽核人員均應了解並遵守 IIA 倫理守則。內部稽核應採用以風險為基礎的稽核方法論(risk-based audit methodology)，定義可評估單位，衡量相關風險，並在制定稽核計畫時著重於高風險及監理要求之領域。根據 IIA 全球指引，有效的內部稽核需有詳細規劃，並能靈活應對快速變化的風險，且內部稽核的優先事項應符合公司目標。

二、動態稽核計劃(Dynamic Audit Planning)：

(一) 動態稽核計劃概念：動態稽核計劃應能靈活應對各種變化，因此需確保稽核計劃與不斷演變的組織目標及風險概況(Risk Profile)一致。應加強稽核計劃之敏捷性、彈性和應對能力，以利處理新興風險、優先事項及其他內外部因素之變動，需使內部稽核單位能應對各種不確定之情況。

(二) 動態稽核計劃流程：每年內部稽核部門應正式向稽核委員會提交年度稽核計劃，其流程包括：辨識內部及外部風險、執行整體風險評估、制定以高風險為重點之稽核計劃、設定稽核目標並確定稽核項目類型(audit project type)。

(三) 風險評估：

1. 自上而下的風險評估(Top-down risk assessment)：自上而下的風險評估從整個組織開始分析，包括組織結構、策略計劃及風險偏好。內部稽核執行相關活動，以識別總體環境、產業及整個公司範圍內目前或潛在的風險，並制定適當的稽核策略。

2. 自下而上的風險評估(Bottom-up risk assessment)：從運營層面（個別業務單位或部門內部）進行風險管理，內部稽核負責評估與各單位相關的風險，並根據評估結果決定各單位之風險等級，以便安排稽核頻率。

三、控制環境框架(Control Environment Framework)：

控制環境框架係用於評估影響整個組織風險管理的員工行為。內部稽核針對高風險領域，聚焦於以下 4 大支柱透過員工訪談與相關資料審查進行評估。

(一) 氛圍及文化(Tone & Climate)：瞭解領導階層傳遞的訊息與公司價值一致性。

(二) 風險管理(Risk Management)：瞭解員工對風險管理流程的認知程度。

(三) 人員風險(People Risk)：領導監督力度、績效目標指定流程、人力資源分配與人才發展等。

(四) 公司治理(Governance)：評估組織架構及公司治理框架的有效性、明確定義人員角色及職責等。

第三章　會議心得及建議

本次 OLIS 秋季研討會以「風險管理」為主題，邀請來自業界與學界的多位專家參與授課，內容涵蓋投資風險管理、作業風險管理、企業風險管理、IT 風險管理、核保風險管理及內部稽核等主題，深入探討保險公司如何在快速變化的市場環境中強化風險管理，並分享日本保險業在相關領域的經驗與實踐，讓與會者能夠全面理解現代保險業面臨的風險挑戰及應對策略。

現代保險業面臨的風險環境日益複雜且多變，涵蓋經濟、技術、法規及市場等多方面的挑戰。有效的風險管理已成為保險公司穩健運營及長期發展的基石，透過全面的評估、預測與控制機制，能夠提升企業抵抗風險的能力及競爭優勢。由本次研討會可深刻感受到，要達到確保保險公司落實風險管理之目標，除了主管機關訂定相關法規，要求保險公司落實法令遵循，更重要的是保險公司本身應注重公司治理與形塑風險管理文化。風險管理文化可使全體員工在日常決策中主動考量相關風險因素，從而有效預防和降低潛在損失。隨著科技、醫療等不斷進步，在快速變化的環境下，唯有透過健全的公司治理架構、整個組織全體參與的風險管理文化及持續優化的控管機制，才能更快速靈活的應對各種風險及挑戰，落實風險管理，使保險公司長期穩健經營。

投資風險是保險公司面臨的重要議題之一。在當前全球經濟不確定性高漲的情況下，保險公司需要具備穩健的資產配置能力，通過多元化的投資組合降低風險。同時，動態風險評估和數據分析工具的應用，可以幫助企業在市場波動中保持資產的穩定性和流動性。此外，作業風險的管理也尤其重要。透過完善的內部控制系統與風險預警機制，可以有效減少人為錯誤和流程漏洞，提升營運效率並降低潛在損失。企業風險管理（ERM）的全面導入，對保險業的整體風險控管具有深遠意義。通過跨部門協作和整合性風險評估機制，企業能夠系統性地識別和管理各類風險，從而提升應對複雜挑戰的能力。在當代保險業

的風險管理中，資訊科技（IT）風險逐漸成為一個不容忽視的議題。數位化浪潮下，保險公司日益依賴資訊科技與數據資料，然而隨之而來的網路攻擊及資料外洩等風險卻持續增加。為此，建立全面的資訊安全防護體系及即時監控機制，對於確保業務穩定性及客戶信任至關重要。此外，核保風險管理直接影響保險公司的長期盈利能力與穩健性，因此在核保過程中，綜合考量市場趨勢、經濟環境、客戶需求及風險胃納，並定期監控相關風險。同時，內部稽核作為風險控制的重要環節，強調獨立性與全面性，以達到控制風險與確保公司經營符合相關法令規定的目標。

臺灣保險業的 ERM 制度已推行多年，ERM 框架已具備較高成熟度。根據我國產、壽險公會修訂之「保險業風險管理實務守則」（ERM 守則），多數保險公司已建立包含風險辨識、風險衡量、風險回應、風險監控等的風險管理架構，依風險特性與其風險胃納，訂定並定期檢視風險限額，並定期監控及落實執行限額超限之處理。在公司風險管理組織架構部分，保險業應設置隸屬董事會之風險管理委員會，負責擬訂風險管理政策、架構、組織功能、管理標準，協助與監督各部門進行風險管理活動，並定期向董事會提出報告。保險業應同時透過「由上到下」和「由下往上」兩個處理面向執行 ERM，及建立有效之橫向溝通管道，並透過內部教育訓練、績效管理等確保全體員工充分瞭解及遵循風險管理之相關規定，且金管會已要求保險業將 ERM 守則「應」執行原則訂定於內部控制制度，落實風險管理。又本次研討會發現，日本有部分保險業在實踐 ERM 時，善於結合科技技術及工具，進行動態風險評估，如導入儀表板(dashboard)，整合公司各種風險評估資料及結果，並透過視覺化圖表及燈號等，使風險管理部門及內部稽核部門能夠更快速清楚地瞭解公司營運情況、應重點關注面向及新興風險等，台灣保險業者或可參考日本做法運用新興科技工具，例如使用大數據搜集市場資料，或運用 AI 分析公司財務業務資料，協助分析及辨識公司風險，使三道防線相關人員更快速有效地監控及掌握風險，並做出回

應，並使經營階層依據業務及風管單位之反饋資訊，整合評估精進公司風險管理政策及程序，以深化公司風險管理文化。

附錄　活動照片