出國報告（出國類別：開會）

參加富國銀行
「亞太區域銀行全球支付研討會」
報告

服務機關：臺灣銀行 國際部
姓名職稱：施惠娟 高級襄理
派赴國家/地區：韓國首爾
出國期間：112年8月22日-25日
報告日期：112年10月18日

摘　要

本行通匯行富國銀行(Wells Fargo Bank,N.A.)於2023年8月22日至24日，在韓國首爾舉辦「亞太區域銀行全球支付研討會」(APAC Regional Banking Conference)，邀請50多位來自亞洲地區包括韓國、日本、臺灣、香港、新加坡、越南等國之銀行資深主管參加。

本次「亞太區域銀行全球支付研討會」之主題為全球支付，旨在與亞太區域金融同業交流並分享實務經驗與探討現今與未來的金融產業主題，包括全球經濟概況、全球支付之未來、金融犯罪與風險管理、網路安全與詐欺風險管理策略、新興科技與數位創新及 SWIFT 最新資訊。重點議題如下：

一、 ISO 20022遷移：SWIFT 組織採用 ISO 20022的背景、理由及重要性。

二、 金融犯罪與新出現的威脅：介紹洗錢前置犯罪—Pig Butchering Scam。

三、 有關 SWIFT Customer Security Programme (CSP) 客戶安全計畫框架。

四、 AI 與數位化之影響：探討 AI 的應用與負責任的使用(responsible AI)及風險管理的重要性。

目　　次

壹、 目的

富國銀行(Wells Fargo Bank NA)與本行於1953年4月建立通匯關係，亦為本行重要的存同行，雙方業務往來密切。依據2023年7月版"THE BANKER"雜誌公佈之全球千大銀行排名，該行位居美國第4名,全球第8名，為全球系統重要性銀行之一。

為踐履「Together We’ll go far」理念，富國銀行自2006年起主辦贊助「全球支付諮詢小組」(Global Payments Advisory Group，簡稱 GPAG)，主要邀集國際重要的通匯金融機構聚集及討論影響金融產業的最新議題。除了定期舉行電話會議分享與討論外，並在加州舊金山每年舉行年度會議。此外，也主辦了 APAC、EMEA 和美洲地區的年度區域活動，多年來已有85個國家的600多家銀行、1,800多名參與者參與 GPAG。

本次的「亞太區域銀行全球支付研討會」(APAC Regional Banking Conference)為富國銀行 GPAG 主辦的 APAC 年度區域活動，藉由與亞太區域金融同業交流並分享實務經驗及探討現今與未來的金融產業主題，對本行瞭解金融產業的發展趨勢及建立銀行同業的溝通網絡有相當助益。

貳、 過程

本次「亞太區域銀行全球支付研討會」之主題為全球支付，主題包括全球經濟概況、全球支付之未來、金融犯罪與風險管理、網路安全與詐欺風險管理策略、新興科技與數位創新及 SWIFT 最新資訊，歸納摘述如下：

一、 ISO 20022遷移

(一)、 背景：

銀行與市場支付基礎設施使用 SWIFT(Society for Worldwide Interbank Financial Telecommunication，環球銀行金融電信協會) MT 標準格式傳遞金融訊息已40餘年。然而，基於上世紀70年代網路傳輸成本和計算處理能力構建的 MT 跨境支付標準格式，已無法滿足當今現代化的開放支付標準需求。

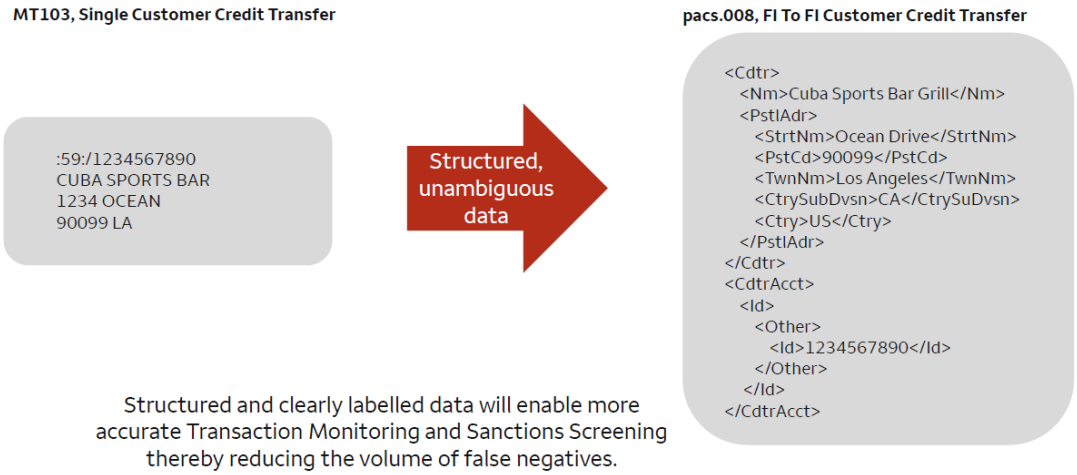
面對日益嚴峻的國際形勢和監管的期望、客戶對端到端(end-to-end)支付解決方案的需求及新興企業涉足金融領域的激烈競爭，金融服務業著手開展一項多年期計劃，採用開放標準的 ISO 20022協議，期能建立一個新的基礎來克服 MT 訊息的限制，並提供創新的平台。

ISO 20022即「金融界通用報文方案」，是2004年由國際標準化組織制定並發佈的國際標準。它是金融業與 IT 技術高度結合的產物，採用可擴展標記語言（XML）技術為基礎，實現使用者之間通過單一標準與金融機構系統的「無縫」對接和跨產業協同運作的理想。採用 ISO20022標準將大幅提升匯款電文的標準化程度，為支付行業帶來創新和效率。

(二)、 業界需要 ISO 20022的理由：

1. 法令遵循及防制洗錢的自動化：
   （1） 資料要素得到更好的定義，誤判的情形可能會減少。
   （2） 相關主體資料高度結構化，因此資訊請求(Requests for Information,RFI)可能減少。
   （3） 由於所有主體都有明確的角色，因此可以提高流程的自動化和交易的透明度。

（4） 例示：MT103 和 pacs.008 的對照範例



(資料來源：富國銀行研討會簡報)

MT103電文地址資訊欄位，是以 free-text 的形式來表示，而 ISO 20022 的 pacs.008，會將地址再區分成街道、大樓、城鎮等不同 tag，讓地址資料更結構化，也有利後續的資料運用。

2. 改善客戶體驗：

（1） 透過結構化的匯款資料，提昇受益人偵察的自動化。

（2） 提高現金流的可見性。

（3） 減少異常及調查處理，並提高自動化處理效率。

3. 提供支付內容、支持新的業務流程：

現代業務流程的實際情況已經超出了傳統 MT 訊息的能力，而 XML 可延展性的標籤語言使其訊息更具彈性，可以改善過去 MT 規格之訊息欄位固定、訊息內容不易擴充的問題。

新的 MX 訊息可以承載更多的資訊，有利於交易雙方確認交易內容及過程。一些法規遵循的資訊，也可以附加上去，達到防制洗錢等監管目的。另一方面 ISO 20022也支援非拉丁語系字元，例如中文字元、阿拉伯文字元等。

4. 創建生態系統連結：

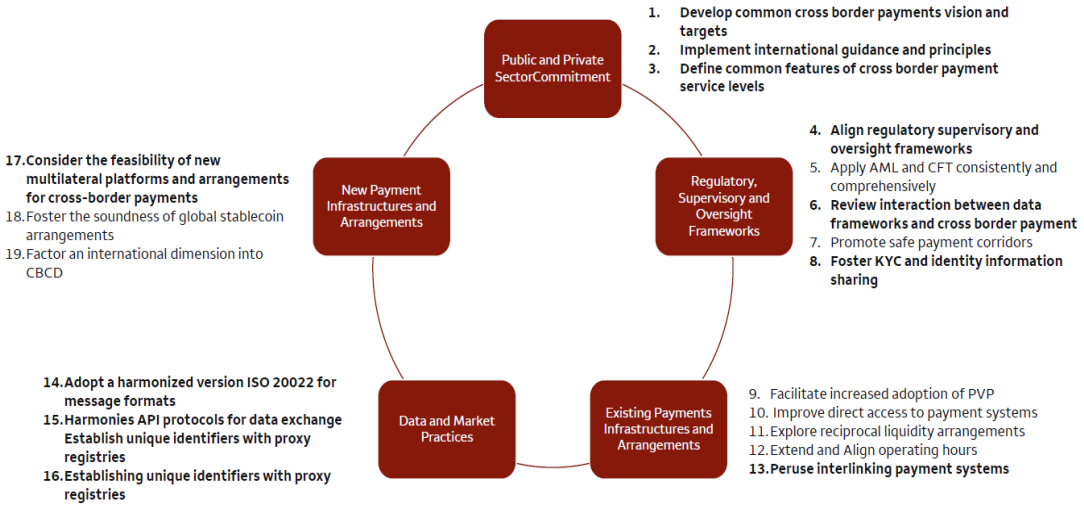
（1） 將不同的支付工具整合為一種共同的標準格式，減少摩擦。

（2） 為開發人員提供基於訊息和 API 解決方案的一致語法。

（3） 靈活支持新實例的使用(例如：付款請求、電子商務)。

(三)、 ISO 20022的重要性：

ISO 20022 不僅引起了支付系統運營者和銀行的興趣，也引起了監管機構的關注。近年來G20金融穩定委員會 (Financial Stability Board, FSB) 透過國際清算銀行下的支付暨市場基礎設施委員會(Committee on Payments and Market Infrastructures ,CPMI) 發起的一項計劃，為改善當前的跨境支付制定了藍圖(如下圖)。



跨境支付改善計劃藍圖 (資料來源：富國銀行研討會簡報)

在已經確定的19個措施方向中，其中11 個工作流程一致提到了對 ISO 20022 通用支付資料標準的需求。由此可見 ISO 20022雖然不是支付領域所有問題的解決方案，但卻是未來解決方案的重要基礎。

(四)、 ISO 20022格式的轉換時程：

採用 ISO 20022是一個長期計劃，建議可以考慮分階段進行，並隨著時間推移逐步轉換施行：

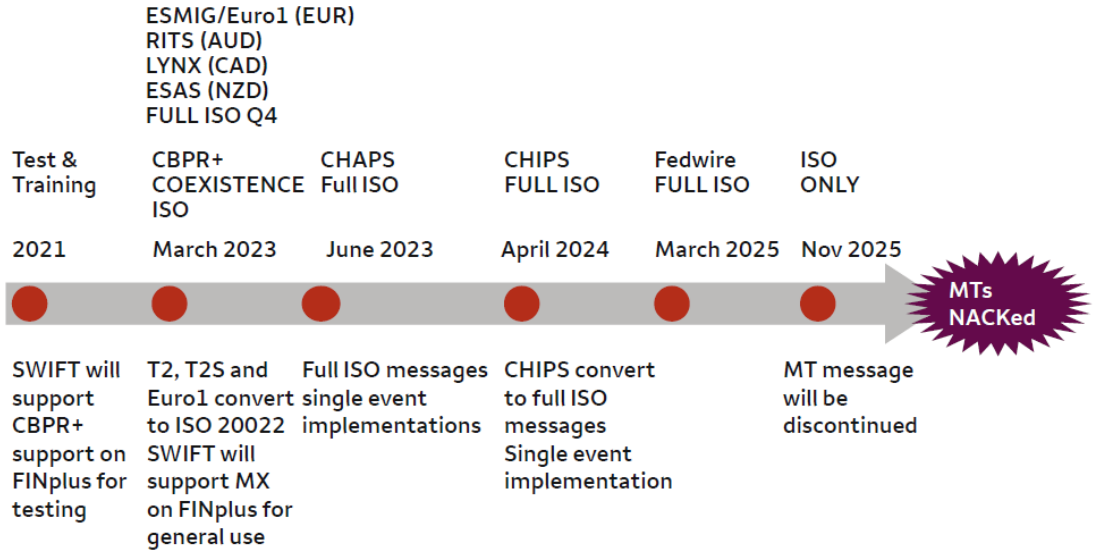
第一階段：升級電文介面以接收 MX 電文，並使用內嵌電文轉換器。

第二階段：以類同格式(like for like)生成 MX。

第三階段：升級渠道捕捉新要素、支持豐富的地址格式。

第四階段：採用 MX 報告(reporting)及調查(investigation)訊息。

SWIFT 採用 ISO 20022標準之 MX 格式電文於2023年3月20日開始上線運行，各金融機構於是日後須能接收 MX 格式電文，而在2025年11月全面採用(接收及發送)MX 格式電文之前，為 MT 與 MX 格式電文並存(coexistence)的過渡時期。

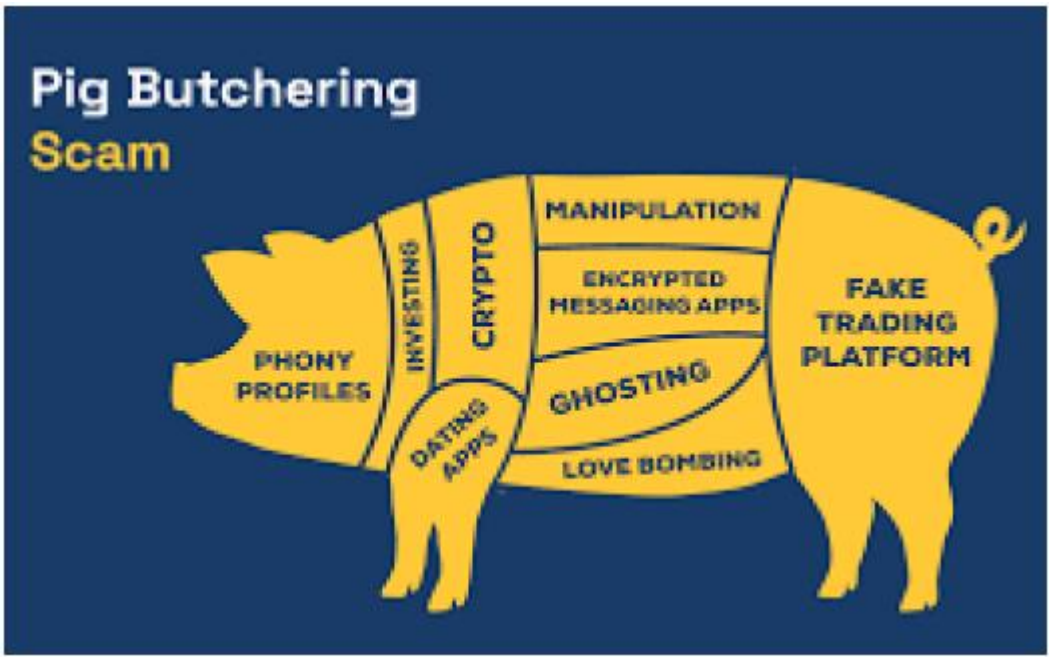


ISO 20022遷移時程表（資料來源：富國銀行研討會簡報）

(五)、 ISO 20022轉換過程中的學習經驗

1. 反覆測試：除了需要與 SWIFT 及市場支付基礎設施進行測試外，與客戶進行測試也是重要的一環，將有助於瞭解基本的 pacs.電文類型之外的內容與交流。
2. 制裁(Sanction)掃描系統和團隊能否達到更高的要求？
3. 預測最壞的情況：即預計收到被截斷(“+”)的付款電文數量，是否建立了可以支持處理更多數量的解決方法，並模擬各種電文狀況？
4. 對於付款資訊截斷、資料丟失的市場慣例及相關的服務水平協議(SLA)是否完全了解？

二、 金融犯罪與新出現的威脅－Pig Butchering Scam



(資料來源：富國銀行研討會簡報)

Pig Butchering Scam(又名 Sha Zhu Pan，殺豬盤)2019年起源於中國，詐騙者通常用愛情和財富(投資獲利)的承諾來哄騙受害者，之後再拿走受騙者所有的錢並切斷聯繫，是一種日益猖獗的金融詐騙型態。

(一)、 Pig Butchering Scam 的特點：

1. 騙局有條不紊、針對性強、而且有耐心—Pig Butchering Scam 的名字反映了受騙者的帳戶在被“宰殺”之前逐漸“變胖”。
2. 詐騙者通常由電話詐騙者、網站設計者和錢騾(Money Mules)所共同組成，並以組織型式進行運作。其中錢騾(Money Mules，俗稱“車手”)在詐騙案件中扮演中間人的角色，主要任務是協助清洗電子犯罪非法所得。錢騾通常是利用現有或新開的銀行帳戶，透過第三方付款供應商的轉帳服務將資金轉移至另一個詐騙主謀者控制下的帳戶(處置和多層化階段)。儘管詐騙主謀者可能從事前置犯罪，但並未直接參與洗錢，藉此避免被逮捕和起訴。因此越來越多的個人犯罪分子和組織犯罪集團選擇利用錢騾來進行洗錢，以匯集和轉移非法資金。
3. 通常針對年輕且受過良好教育的個人，以浪漫的、柏拉圖式的或專業的型

式手法，與受騙者建立關係並贏得信任，然後巧妙地引導受騙者進行加密貨幣投資。

4. 受騙者被大量引導從合法的加密貨幣交易所購買加密貨幣，然後再將加密貨幣轉移到詐騙者所控制的虛假加密投資平台、銀行帳戶或空殼公司。
5. 受騙者持續被鼓勵進行更多的投資，甚至貸款或從退休計劃中取出錢來繼續投資。

(二)、 值得關注的趨勢：

1. 詐騙建立於”關係”之上(relationship-based)，通常造成更大的損失。
2. 詐騙是由有組織的犯罪集團控制，這些詐騙中心通常位於東南亞（例如：緬甸、寮國、柬埔寨和泰國）。
3. 詐騙者通常是強迫勞動或人口販賣的受害者。

(三)、 殺豬騙局的警示訊號(Red Flags)

1. 對金融機構而言：
   - 年齡通常在 40 歲以下、沒有金融或投資背景的個人，代表新創的投資企業開設企業帳戶。
   - 從未有提供相應商業服務的個人，收取超過 1,000 美元的整數存款。
   - 個人的存款金額短時間內增加至數萬美元。
   - 當日轉出與潛在受害者資金相對應的金額，以便將帳戶每日的餘額保持在接近於零。
   - 受騙者以整數形式從其帳戶中轉移資金(例如：1,000美元)。
   - 被販運者在移居海外之前可能會清空並關閉其帳戶。
2. 對受騙者而言：
   - 收到來自陌生人的隨機簡訊或電子郵件，並與受騙者進行頻繁的虛擬(文字)交談。
   - 對方似乎了解受騙者的興趣及上線狀態、讀懂受騙者的想法並能猜出心思。
   - 對方拒絕透過電話交談，因為他可能實際不會說受騙者使用的語言，並且正在使用自動翻譯功能。

- 如果受騙者提出太多問題，或是要求拍照或視訊通話，對方可能會威脅停止交談。
- 談話內容很快地集中在可以獲得高獲利的投資上，且大多數在受騙者談論投資的時候，對方的談話內容充滿調情及讚美。
- 投資機會聽起來好到令人難以置信。

(四)、 建議的控制措施和風險緩解措施

1. 對於為投資企業開立帳戶的新客戶進行加強審查。
2. 對於高風險司法管轄區的業務關係及交易加強盡職調查。
3. 制定政策防止受騙者資金進一步移動，以便在進行調查時凍結涉嫌詐騙的帳戶。
4. 建立程序審查涉嫌詐騙的帳戶所有者(例如：取得證明文件如發票、投資證明或資金轉入的錢包地址等)。
5. 聯繫對外交易的接收方，以提高其詐騙意識，並確認轉帳目的是合法的。
6. 實施行為分析技術，檢測並報告與正常客戶行為的偏差。
7. 採用區塊鏈分析、機器學習工具和警示訊息產生軟體來監控交易。
8. 對員工進行定期教育訓練，以提高對殺豬騙局相關的可疑活動及警示訊號的辨識。
9. 與執法機構密切合作，協助調查和追回被詐騙的資金。

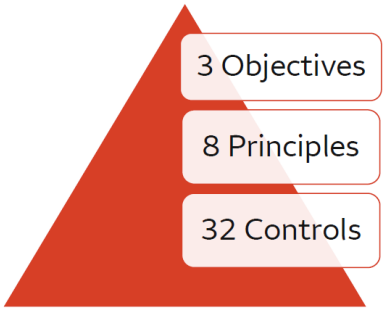
三、 SWIFT 客戶安全計畫(CSP)

SWIFT 於1973年5月成立，協會總部位在比利時，比利時國家銀行(National Bank of Belgium)、美國聯邦準備系統(U.S. Federal Reserve System)、英格蘭銀行(Bank of England)、歐洲央行(European Central Bank)、日本銀行(Bank of Japan)都是重要成員。

SWIFT 的主要功能是為全球的銀行及其他金融機構、企業提供安全的金融訊息傳輸服務，可說是跨境金流的重要支柱。SWIFT 客戶安全計畫(Customer Security Programme, CSP)於2016 年建立，期望透過一系列必要性及建議性的安全控制措施、社群的資訊共享機制及強化相關工具的安全性，以預防及偵測

詐騙活動，SWIFT 用戶必須在每年12月31日之前向 SWIFT 的 KYC 網站提交評估報告。

CSP 的安全控制框架係以防護資訊環境(Secure Your Environment)、限制存取(Know and Limit Access)及偵測與應變(Detect and Respond) 作為三大安全強化目標，再依據各項目標之重點強化領域，發展出8 項安全原則，再分別列出32項對應之安全控制措施。



CSP 安全控制框架 (資料來源：富國銀行研討會簡報)

(一)、 防護資訊環境(Secure Your Environment)：

1. 限制網際網路存取
2. 區隔關鍵系統與一般的 IT 環境
3. 減少攻擊面與漏洞
4. 保護實體環境

(二)、 限制存取(Know and Limit Access)：

1. 預防憑證遭到破解
2. 管理身分與區隔帳戶權限

(三)、 偵測與應變(Detect and Respond)：

1. 偵測系統或交易紀錄之異常活動
2. 事件因應與資訊分享計畫

四、 AI 與數位化的影響

研討會的最後，由該行舊金山的 Ms. Cleane Sakaguti(Head of

Innovation Data Products & Insights)線上分享當前銀行業面臨的重要議題－AI 與數位化的影響。

Cleane Sakaguti 自2008年起在巴西的銀行服務時，即開始著手研究 AI 和機器學習領域，經驗相當豐富，其主要的工作是充分利用內部和外部數據來提昇富國銀行的產品及服務，並且利用新技術來推出新產品。

以下是摘錄 Cleane Sakaguti 分享內容的重點：

(一)、 生成式 AI (generated AI)的出現

生成式 AI (generated AI)可以依照輸入的簡單提示((prompt)創建新內容，包括文字解釋、語音、圖像和模擬影片等。主要是因生成式 AI 背後的大型語言模型接受大量的聲音、圖像等數據訓練。當接收到輸入的提示時，這些模型即將該指示與數百萬筆現有的數據進行比較，並給(輸)出接近需求的結果。而促成生成式 AI 成型的要素有三：

1. 大量的可用數據(data)：AI 不是新事物，AI 的概念在1950年即由圖靈(Turing)測試過了，但當時的問題是沒有像現在有這樣多的可用數據。
2. 基礎設施(infrastructure)的投資：OpenAI 消耗了整個網路約45TB 文本數據來訓練其龐大的語言模型，諸如 Microsoft、Google、Salesforce、Amazon 等對硬體等基礎設施的投資使其成為可能。
3. 大型語言模型被 OpenAI 公開：因為是向所有人公開，所以世界各地的開發人員或企業家們無需從頭開始創建，現在大家可以使用預訓練模型(pre-trained models)，並且根據需要進行修改和微調，提高了這些模型的可用性。

(二)、 與第三方供應商合作發展

當富國銀行思考應用生成式 AI 和大型語言模型以及所有這些新技術時，評估與 Microsoft、Google、Salesforce、Amazon 等第三方供應商合作將會更有意義，因為這些供應商投入大量資金於基礎設施，以確保擁有正確的技術。而銀行只須在受保護的高度複雜環境中利用大型語言模型，確保負責任地進行操作，而無須投資大量資金如圖形處理器(GPU)等基礎設施。

(三)、 AI 的應用

可用以提高效率、降低成本、降低風險並提升客戶體驗，分為以下2方面來說：

1. 自動化(automation)：

使用 AI 來取代手動重複性任務，如：處理大量文件的重複性流程、搜尋異常、總結提供或顯示出感興趣的內容，並透過分類(classification)來實現。舉例來說當在分類一大批數據，客戶打電話來說他們感興趣的內容時，該如何進行分類，以便將通話內容整合並對應到正確的工作人員？

又如一名服務中心工作人員正在與客戶進行對話，當客戶詢問特定的產品時，工作人員必須手動查閱許多產品手冊、程序、流程等。當 AI 應用於訊息檢索(information retrieval)時，即能獲取工作人員所談論的內容，並告訴工作人員應向客戶提供的相關訊息，此即以自動化流程方式，檢索訊息並提供給客戶。

2. 總結(summarization)：

在工作人員與客戶對話的同時，將語音轉換為文字內容的技術已經存在很長時間了。但現在需要確保的是，工作人員只須專注在與客戶的對話上，當對話結束時，模型能夠總結所討論的主題，而不須工作人員逐個將對話進行整理。

需要進一步了解的是，從法規的角度來看，需要記錄哪些必要的訊息？需要將哪些訊息發送給客戶，使之了解所需的產品？以及如何確保追蹤客戶面臨問題的解決方案等。

(四)、 負責任的人工智慧(responsible AI)

隨著開始探索生成式人工智慧，持續探討、評估和減輕與這項新技術相關的風險，以防止對客戶和企業造成損害是至關重要的。以下8項核心原則指導在整個 AI 生命週期中負責任使用 AI 的方法，也是富國銀行在交付的所有模型中所遵循的原則：

1. 公平性(Fairness)：設計多元觀點的 AI 模型，減輕歧視及偏見。
2. 可解釋性(Explainability)：模型必須能夠被清楚地解釋，讓人理解操作、輸出的含義和其侷限性。

3. 負責性(Accountability)：建立對整個 AI 生命週期的監督機制。
4. 安全性(Security)：減輕潛在的網路威脅和弱點，以確保 AI 系統安全性。
5. 隱私(Privacy)：遵守資料隱私法規和確保客戶資料的安全。
6. 安全性(Safety)：避免對人類生命、財產及環境安全造成衝擊。
7. 數據完整性(Data Integrity)：數據的質量、治理及豐富度，以建立對數據的信任。
8. 可靠性(Reliability)：AI 系統以所需的準確度和一致性的水準執行，確保輸出的結果值得信賴。

(五)、 生成式 AI 的風險與管理

1. 生成內容的管理：考慮內容生成時，可能是交付所需時間最長的領域，因為它伴隨了巨大的責任。監管機構現在正在試圖找出如何正確監管這個領域，主要關切在於向顧問、銀行家提供訊息時，如何確保最終提供的是正確的訊息，而且不會涉及操縱市場等。
2. 數據的安全性：生成式AI 通常使用神經網絡，可以大規模在現有數據集上進行訓練，以創建新的數據或物件，如文件內容、提案、營銷優惠等等。這包括來自不同人的輸入數據、不同數據來源的數據。當在以數據訓練時，基本上是複製和使用該數據，並用於其他用途。須確保大型語言模型可用，並保護用於訓練模型時提供的數據不會離開公司的雲端或系統結構。
3. 員工濫用的問題：在於員工使用模型生成的輸出內容，不經驗證就將輸出結果提供給客戶。舉例來說，幾個月前，紐約的一名律師在法庭上利用 ChatGPT 準備了一個案子，但卻被法官拒絕，因為提供的所有訊息都是錯誤的，這歸因於允許模型被創建(造)的幅度。使用者必須要確保無論輸出結果是什麼，都仍然能夠證明其正確性。而生成的結果不準確，一可能是使用的數據不是自己的。二是在未驗證背景的情況下創建事物。三是在未經適當驗證的情況下呈現結果。此即在整個識別使用案例、捕捉數據、使用模型、驗證模型的整個過程中需要有適當治理的重要性，而呈現在客戶面前的內容，也必須非常清晰並經過驗證，這同時也是保護公司聲譽及保

護客戶數據的方法。

4. 惡意使用者的風險：生成式 AI 具有強大的創造力，惡意使用者可能會利用生成式 AI 來生成假新聞、假廣告等，以欺騙或獲利。此外，生成式 AI 還可能帶來了網路安全風險，網路犯罪分子可以使用這項技術來創建更真實和複雜的釣魚騙局或憑證，以入侵系統。因此必須做好識別惡意行為者的準備，並開始制定控制措施以防止這些風險。

參、 心得及建議

本次參加研討會，深感 AI 與數位化之影響是金融產業現在及未來必須關注的焦點，以下是個人之淺見：

數位化浪潮勢必對銀行業的勞動力帶來衝擊，數位化轉型的關鍵在於將 AI 納入並優化現有的流程，在 AI 的幫助下更有效率地處理複雜的任務，以釋出人力和時間來解決更具挑戰性的問題，從而提高整體生產力。未來人力發展須從單純的作業處理朝向人力加值的方向提升，善用科技來提高效率、減少作業風險。

領導者本身不須是創新者，但應該要瞭解 AI 等數位化技術與趨勢，並具有能夠賦予團隊創意、進行創新的思維方式；員工則需要學習運用和掌握新技能，積極參與數位化和自動化的變革，並意識到作業團隊仍然不可或缺，但需要透過科技方法提升自我價值，以實現人機協同合作的目標。

最後，在開始探索生成式人工智慧這項技術的同時，我們須謹記並實踐負責任的人工智慧(responsible AI)核心原則—公平性(Fairness)、可解釋性(Explainabililty)、負責性(Accountability)、安全性(Security)、隱私(Privacy)、安全性(Safety)、數據完整性(Data Integrity)及可靠性(Reliability)，持續探討、評估和減輕相關的風險，以防止對客戶和企業造成損害。