

金融監督管理委員會因公出國人員出國報告
(出國類別：其他-參加訓練課程)

參加東南亞國家中央銀行研究訓練中心
(SEACEN Centre)
資通科技(ICT)風險與網路安全課程

服務機關：金融監督管理委員會檢查局
姓名職稱：蘇專員奕銘、宋稽查建勳
派赴國家/地區：印尼峇里島
出國期間：114年9月29日至10月4日
報告日期：114年12月5日

課程摘要

本課程由國際清算銀行(BIS)、印尼銀行及日本銀行共同主辦，於 2025 年 9 月 30 日至 10 月 3 日在印尼峇里島舉行。課程主要探討中央銀行面臨的資訊通訊技術(ICT)風險與網路安全挑戰，特別聚焦於人工智慧(AI)應用與網路韌性，並透過案例分享、課堂互動及分組討論等方式強化學習效果。藉由參與本次課程，有助學員瞭解新興科技相關技術並掌握應對複雜 ICT 風險和網路安全威脅所需的技能。

本次課程為期 4 天，謹將課程重點摘述如下：

第一天的內容講授全球面對的網路威脅，包括 AI 被濫用於詐騙、資訊操控與勒索攻擊，探討生成式 AI 帶來的防禦困境與政策挑戰並帶出中央銀行在網路韌性中所扮演的角色，奠定後續討論基礎，同時透過 BIS 導入 AI 的案例探討生成式 AI 在央行內部營運、知識管理與自動化維運中的新趨勢，使學員對實務應用有進一步的認知。

第二天內容有關技術實踐，進一步討論 AI 防禦的應用，展示 AI 在市場異常偵測與詐騙防治中的成效，並說明 AI 在安全防禦與攻擊兩面向的應用，並整理央行在資安防禦成熟度的自評與比較架構，提出央行間的防禦標準化方向。

第三天內容有關 AI 治理的延伸，給予學員如何治理 AI 的框架與風險監理標準，說明模型驗證、資料治理與可解釋性原則、第三方稽核與供應鏈風險監管，並整理各央行導入 AI 治理的實例，包括倫理審查、問責機制與跨部門協作，強調 AI 治理透明化的重要性。

第四天則是課程回顧以及各國學員間的實務經驗分享。

目錄

壹、 課程緣起及目的.....	1
貳、 課程介紹.....	2
一、 課程時間	2
二、 課程內容	2
參、 課程內容摘要.....	4
一、 全球網路威脅情勢更新與主要趨勢	4
二、 日本中央銀行(BOJ)監管作為與後量子時代提升金融體系韌性	8
三、 國際清算銀行(BIS)導入 AI 的策略、應用與監管工具	10
四、 資料治理-於億級交易資料中偵測詐欺和洗錢行為.....	13
五、 金融機構運用人工智慧之管理策略	16
六、 代理人 AI(Agentic AI)與 AI 營運(AIOps)之新興趨勢.....	18
七、 AI 風險管理框架	23
八、 IT 委外與供應鏈風險.....	26
九、 網路安全最佳實踐與常見缺失	29
十、 央行 AI 治理架構	33
肆、 心得與建議.....	36

壹、 課程緣起及目的

東南亞中央銀行(SEACEN)研究與訓練中心於 1982 年成立以來，透過其學習計畫、研究工作以及中央銀行知識能力建設的網路和協作平台，在亞太地區中央銀行成員國中有著獨特的區域地位，並設計和提供中央銀行知識領域(如宏觀經濟和貨幣政策管理、金融穩定和監管、支付和結算系統及領導和治理)。

隨著科技的進步，區塊鏈、雲端運算、人工智慧(AI)、機器學習(ML)和大型語言模型(LLM)等逐漸成為我們生活的一部分。然而若不了解它們，將難以評估它們對金融體系帶來的助益與風險。同時，銀行和支付服務提供商所提供的線上交易功能日益增加，也使得他們更容易受到網路攻擊。鑒於網路犯罪分子的攻擊手段越來越複雜，可能會利用人工智慧來進行自動化和增強攻擊，因此在現今的社會中資料外洩變得越來越普遍。連網設備和物聯網(IoT)的普及也增加了網路攻擊的潛在切入點。銀行和其他金融機構必須保持警惕，應對日益湧現的新威脅，採取主動措施保護資訊安全、管理和降低這些風險，能夠適應不斷變化的威脅情勢，制定穩健的網路安全策略。

本課程為「資通科技(ICT)風險與網路安全」，於 114 年 9 月 30 日至 10 月 3 日於印尼峇里島舉行，參與課程之學員來自柬埔寨、印度、印尼、巴布亞紐幾內亞、菲律賓、斯里蘭卡、馬來西亞、尼泊爾、泰國、越南、澳門、巴基斯坦及我國等 13 個國家或地區共計 41 名代表參與。

課程內容旨在使各國央行掌握新興科技相關技術的基礎知識，並掌握應對複雜資訊通訊技術風險和網路安全威脅所需的技能，期許學員能夠更好地了解與新興技術相關的各種技術用語，以及如何善用工具辨識資通訊系統中的潛在威脅和漏洞、學習保護資訊資產的各種策略和技術、培養有效應對網路安全事件並從中恢復的技能，及了解網路安全領域的最新趨勢和發展。

貳、 課程介紹

一、課程時間

114 年 9 月 30 日至 10 月 3 日。

二、課程內容

日期	主題	主講人/任職機構(構)
9月30日	全球網路威脅情勢更新 Cyber threat landscape update	Chetan Raghuprasad Cisco Talos
	日本央行對抗網路威脅之監管作為 Central bank against cyber threats	Takahiro Ebisawa 日本銀行(BoJ)
	國際清算銀行導入人工智慧之策略 Onboarding AI-BIS case study	Victor Rayado Perez 國際清算銀行(BIS)
	案例分析-企業型聊天機器人 Enterprise chatbot-BIS GPT	Anand Kannan 國際清算銀行(BIS)
	案例分析-銀行業人工智慧 AI in Banking-Market intelligence	Zhang Zhang 國際清算銀行(BIS)
	案例分析-渡鴉計畫 Project Raven	William Zhang 國際清算銀行(BIS)
10月1日	網路韌性與標竿測試 Cyber resilience and benchmarking in the CB community	Randy Miskanic 國際清算銀行(BIS)
	交易資料管理及異常偵測 Data management and Anomaly Detection over Billion-scale transactional data	Yogesh Simmhan 印度科學理工學院
	人工智慧對網路安全的可能影響 Cyber Security Implications of AI	Sukhvir Notra 國際清算銀行(BIS)
	代理型人工智慧及 IT 維運人工智慧之新趨勢 Emerging trends in Agentic AI and AIOps	Yogesh Simmhan 印度科學理工學院

日期	主題	主講人/任職機構(構)
10月2日	人工智慧風險管理框架 AI risk management frameworks	Randy Miskanic 國際清算銀行(BIS)
	IT 委外與供應鏈風險 IT Outsourcing and Supply Chain Risks	Babli Joshi 印度準備銀行
	網路安全最佳實踐及常見缺失 Best Practices and Common Deficiencies in Cybersecurity Implementation	
	央行人工智慧之治理 Governance of AI in central banking	Angella O'Connor 國際清算銀行(BIS)
10月3日	分組討論 Breakout Session	
	網路營運壓力測試 Cyber Operational Stress Testing	Aare Reitnam 國際清算銀行(BIS)
	央行間網路安全實務圓桌討論 Roundtable discussion of cybersecurity practices among central banks	

參、 課程內容摘要

一、全球網路威脅情勢更新與主要趨勢

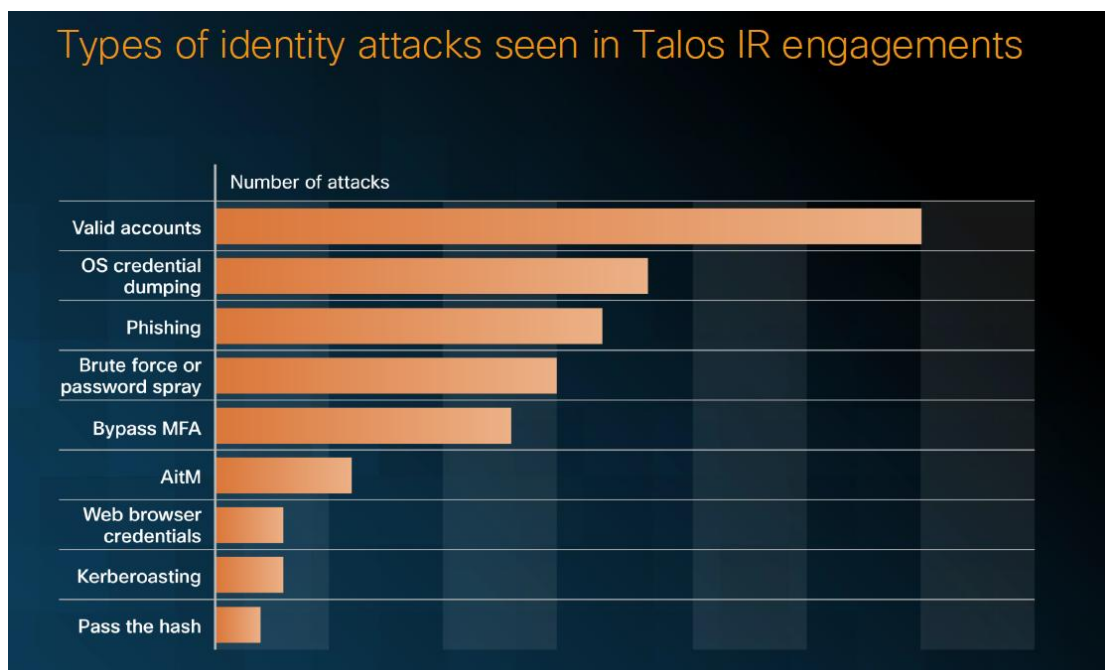
(一)威脅趨勢演變

Cisco Talos 威脅情報研究團隊發現，攻擊者正從複雜的攻擊技術轉向隱匿性 (stealth)、簡單性(simplicity)和效率(efficiency)優先的策略，不再追求零日漏洞或開發專門的惡意軟體。

(二)身分攻擊(Identity Attacks)為首選

在 Cisco Talos 的資安事件應對(incident response)案例中，身分攻擊占比高達 60%。

- 1、原因：攻擊面持續擴大(雲端介面等)、難以偵測(合法管理者行為)、易於執行後續操作、可獲得重大存取權限。
- 2、手法：最常見的策略是濫用有效帳戶進行初始存取，其次依序為透過 Active Directory 等系統竊取密碼、釣魚訊息及郵件、撞庫及密碼噴灑攻擊、多因子認證失效等。

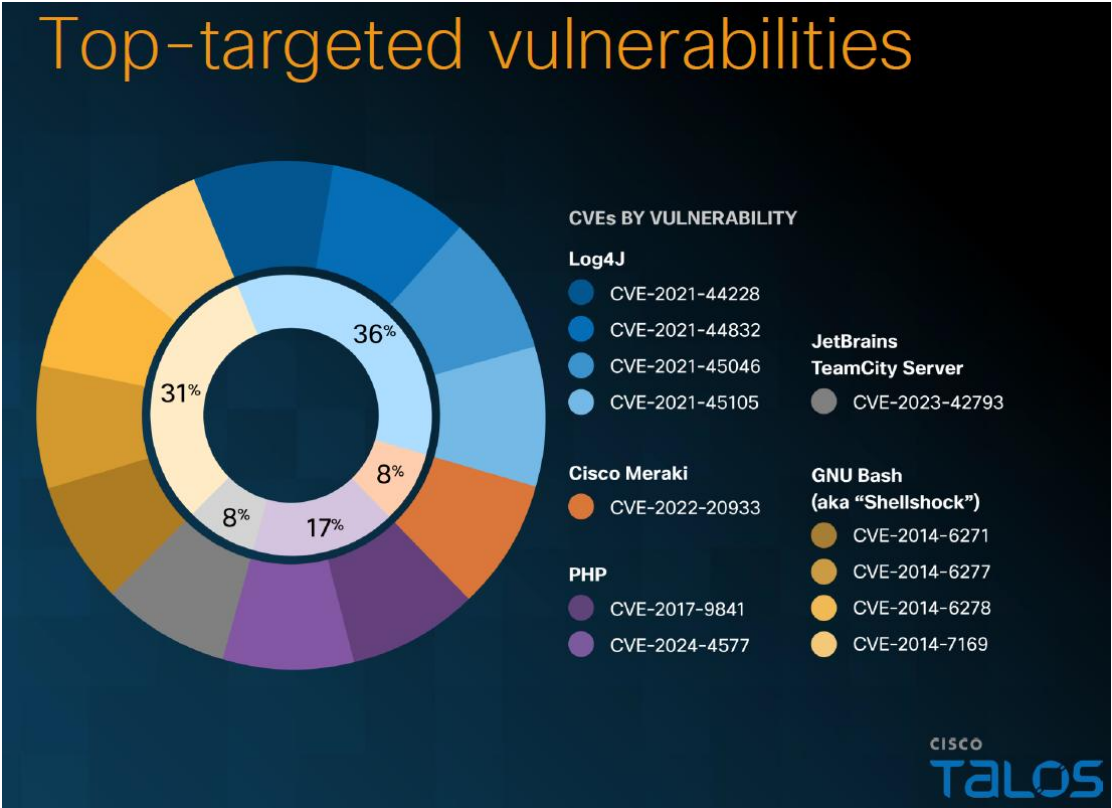


圖一：Cisco Talos 的資安事件應對種類數量

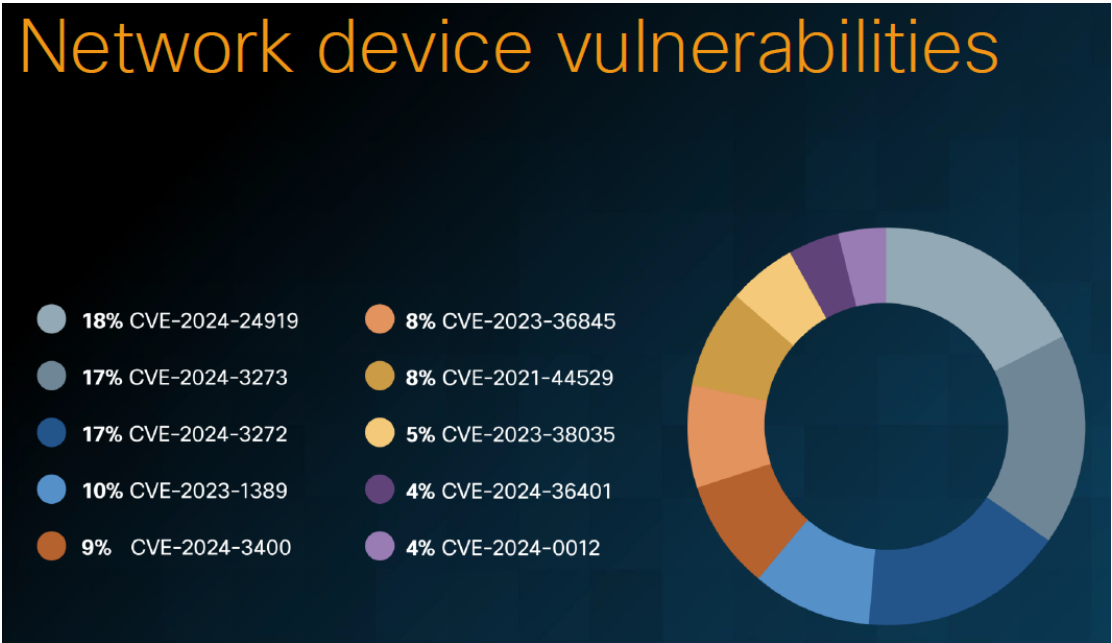
3、工具與方法

- (1)舊漏洞攻擊(Decades-old CVEs)：最常被攻擊者鎖定的漏洞多為發布多年的

舊 CVE，其中有 4 個在十年前就已公開。攻擊者並非總是依賴零日漏洞，而是尋求已知但未修補的普遍性漏洞。另外 Log4j 漏洞持續被利用，生命週期已結束(EOL)的網路設備為主要攻擊標的。



圖二：最常被利用的漏洞編號



圖三：最常被利用的網路設備漏洞編號

(2)合法掩護非法(Living-off-the-Land Binaries, LoLBins)：攻擊者大量使用系統

列入白名單之開源軟體或函式庫(57%)、商用程式(26%)、系統原生工具(17%)進行滲透，而非總是導入新的惡意軟體，如：Impacket、Mimikatz、PowerShell、PsExec 等，致難以被偵測。

(3)勒索軟體(Ransomware)：勒索軟體有 70%的攻擊態樣係為取得有效帳戶初始存取權，一旦取得帳戶初始存取權，有 48%可成功停用端點資安防護措施。有些係透過 Microsoft Teams 等管道冒充 IT 人員要求遠端存取以植入勒索軟體。

(4)電子郵件威脅(Email Threats)：釣魚攻擊(Phishing)仍是主要的入侵途徑。在各種釣魚模式中，惡意連結的成功率最高，佔釣魚攻擊總量的 58%，其次依序為惡意附件、語音釣魚(Vishing)。而利用「一致性」、「權威性」和「稀缺性」等人類認知弱點所設計的釣魚郵件，具有高點擊率，易使人受騙，例如：一封看似來自主管(權威性)的郵件，提到你上週開始的一項任務(一致性)，因為有 1 小時內截止的期限而要求立即處理(稀缺性)。

(5)多因子認證相關攻擊(Attacks against MFA)：常見原因為未導入 MFA(24%)、MFA 未完全啟用(22%)、無 MFA 之 VPN(19%)、MFA 疲勞攻擊(16%)、惡意裝置註冊到 MFA 系統(8%)、MFA 繞過(8%)、缺乏密碼保護(3%)。

(三)人工智慧威脅

- 1、加速釣魚攻擊：生成式 AI(Generative AI)工具已助長了更複雜的攻擊。過去需要約 16 小時製作的釣魚郵件，現在使用 AI 只需 5 分鐘即可生成，顯著節省了攻擊者的籌畫時間。日本曾發生非技術背景人士利用生成式 AI 創建惡意軟體的案例。此外，深度偽造(Deepfake)詐欺已造成鉅額損失，例如 2024 年一間英國公司因高階主管匯款指示的深度偽造影片而損失 3 千萬美元。釣魚內容、釣魚網站、釣魚程式愈來愈逼真。
- 2、輔助攻擊決策：惡意行為者使用大型語言模型(LLM)進行自動化偵察、分析憑證、制定戰術。
- 3、惡意 AI 工具：暗網已出現專為攻擊而生的黑化 ChatGPT(WormGPT、FraudGPT)。另惡意軟體會偽裝成 AI 工具散播，誘導使用者下載使用。開源 LLM 模型檔案可能被植入後門程式碼，當程式開發者下載並運行模型時，惡意程式碼也會在不知不覺中執行。
- 4、模型繞過與操縱：攻擊者透過模型越獄，如：假裝成某個角色來引導模型說

出有害做法(角色扮演)、在提示裡藏一個系統訊息叫模型違反安全規則(系統覆蓋、提示注入)、在模型的訓練資料或模型所查詢的資料庫中加入錯誤或惡意的資料(投毒攻擊)、嘗試提取原始訓練資料或識別出個資(逆向工程)等方式來操縱 AI 模型，迫使其產生惡意結果或繞過安全限制等。在地端的 AI 開源模型中，有些可移除模型審查的監管機制，可生成有害內容，傳播錯誤或誤導資訊。

(四)對抗 AI 攻擊的五大建議

- 1、實施零信任架構(ZTA)：不信任任何使用者或設備，持續進行驗證。
- 2、保護整個資料管線：從資料輸入到模型輸出，確保所有環節的資料安全性。
- 3、建立強大治理和事件回應機制：設立清晰的規範和快速應對流程。
- 4、優先考慮模型可解釋性(XAI)：能夠理解 AI 模型決策的過程，以便偵測異常。
- 5、持續監控與 AI 紅隊演練：不間斷地監測系統異常，並透過模擬攻擊主動測試 AI 系統的防禦能力。

二、日本中央銀行(BOJ)監管作為與後量子時代提升金融體系韌性

(一)日本中央銀行監管作為

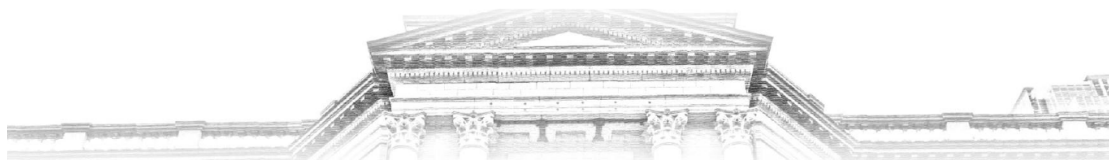
透過實地檢查等銀行監管作為確保金融機構具備足夠的網路安全管理能力和韌性，並與其他金融監管機構(如日本金融廳 JFSA)保持緊密合作，共同應對網路威脅。在過去的檢查中，發現了金融機構普遍存在的弱點主要包括：

- 1、第三方供應商風險(供應鏈)：對軟硬體供應商、雲端服務提供商、或 IT 服務外包廠商的安全控制與管理不足。
- 2、集團內部的管理缺乏一致性：對子公司或集團內其他實體的網路安全標準與控制未能有效延伸和統一管理。
- 3、雲端運算風險管理不當：未完全理解和實施雲端服務的共同責任模型，導致配置錯誤或監控不足。
- 4、基礎設施管理落後：例如未能及時更新操作系統、修補程式管理延誤等，使系統暴露於已知漏洞中。

BOJ On-site Examination

Number of Financial Institutions Examined

	(number of entities)		
	Fiscal 2022	Fiscal 2023	Fiscal 2024
Domestically licensed banks	20	20	20
<i>Shinkin</i> banks	37	42	41
Other institutions	4	5	7
Total	61	67	68



表一：日本央行近三年金融檢查家數

(二)日本中央銀行的職責

包括追蹤國際標準進度、評估後量子密碼學(PQC)遷移對金融 IT 系統的衝擊，並向轄下金融機構提供指導，以確保它們在技術成熟時能夠順利過渡。

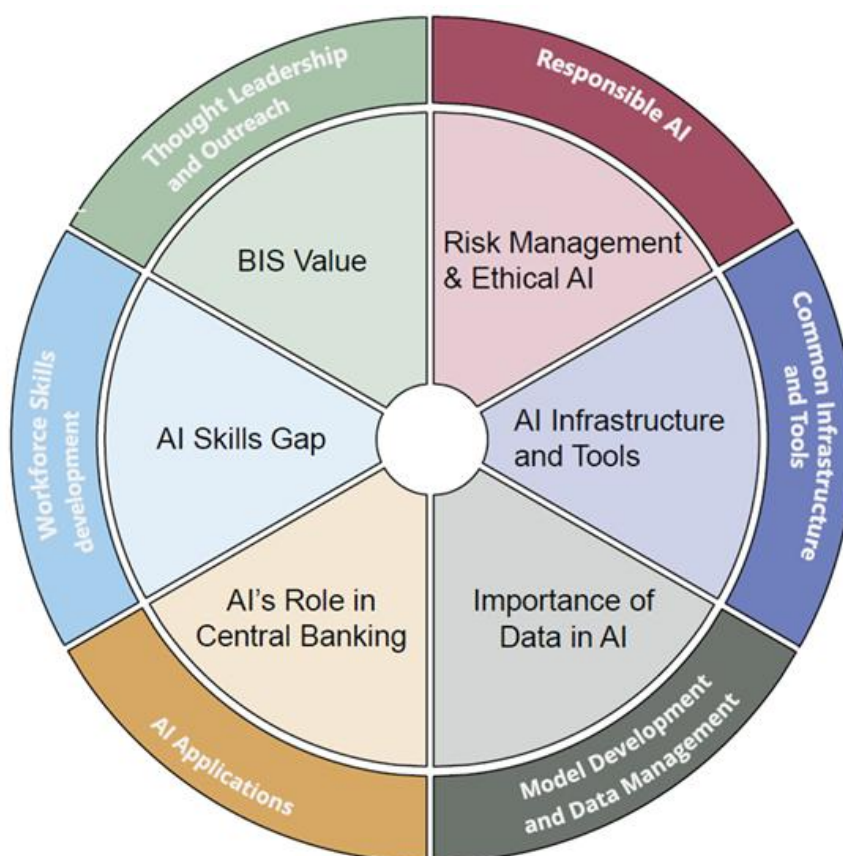
- 1、量子電腦的潛在威脅：能破解當前主流加密技術(如 RSA 或 ECC)的密碼學相關量子電腦(CRQC)，有 50%的機率在 15 年內(約 2039 年)實現。透過「現竊取後解密 Harvest Now Decrypt Later(HNDL)」的攻擊模式，惡意行為者或國家級駭客現在就會開始蒐集所有以現行加密技術傳輸和儲存的敏感數據，等到未來 CRQC 出現後再進行解密，這對涉及國家安全、商業機密或有效期長久的數據(如客戶資料、知識產權)構成嚴重威脅。
- 2、全球 PQC 遷移進程：為對抗 HNDL 風險，全球標準機構正加速制定新的抗量子演算法。例如，美國國家標準暨技術研究院(NIST)2022 年選定了 4 個首批標準化的 PQC 演算法，並在 2024 年發布了第一個官方標準 FIPS 203(ML-KEM)，被視為是全球 PQC 遷移的里程碑。許多國家已設定明確的 PQC 遷移時間表，如：
 - (1)美國：白宮和國家安全備忘錄要求在 2030 年前完成敏感系統的 PQC 轉換。
 - (2)歐盟：歐盟網路安全局(ENISA)建議在 2030 年代初完成公鑰基礎設施(PKI)的 PQC 遷移。
 - (3)其他大多數主要經濟體和金融中心規劃在 2030 年代中期或末期完成關鍵系統的 PQC 轉換，以減輕長期資訊安全風險。

三、國際清算銀行(BIS)導入 AI 的策略、應用與監管工具

(一)AI 策略框架(Project Voyager)

BIS 推動為期兩年的 Project Voyager 作為其 AI 策略的核心，旨在將 BIS 轉變為一個 AI 驅動的機構，以成為全球中央銀行社群在 AI 領域的領導者與關鍵夥伴，其指導原則是建立負責任、合乎道德且安全的 AI 應用基準，以提高效率和改善決策流程。該策略採取「在建立中進行實驗」的務實方針，分為三大支柱：

- 1、AI 實驗(Experimenting with AI)：積極探索創新應用，已累積 100 多個發想，完成 18 個概念驗證(PoC)，3 個投入生產，實現對實踐應用的重視。
- 2、建立基本能力：開發共同的 AI 平台和工具，為所有部門提供安全的 AI 基礎設施。
- 3、奠定基礎：強調跨部門協作，將 AI 整合到現有策略中，並透過持續學習培養員工 AI 技能。



圖五：國際清算銀行 AI 策略框架

(二)AI 應用案例 1：BIS GPT、BIS Chatbot

BIS GPT 是 Project Voyager 策略下「建立基本能力」支柱的核心產物。其導入是為應對 ChatGPT 所帶來的資料隱私和合規風險，提供一個安全的內部替代方案。BIS GPT 在 BIS 安全的混合雲環境中運作，可處理機密等級的資訊，且不儲存或分享用戶輸入的資料，純粹使用為個人生產力工具。初始的 BIS GPT 僅具備通用知識，無法存取內部資訊。為此，BIS 進一步開發了企業級 Chatbot，採用 RAG(檢索增強生成)架構，允許模型從 BIS 內部的企業資料中檢索資訊並生成答案，並有效解決了大型語言模型常見的「幻覺」(hallucination)問題，確保 Chatbot 能可靠地回答特定於 BIS 政策與流程的專業問題。在推廣過程中，BIS 與法務和風險管理團隊緊密合作，定義了清晰的負責任使用指南。



The screenshot displays the BIS Chatbot interface. At the top, a user query is shown: "Could you summarize the foreign assets allocation for the years 2019-2023 in a table?". Below the query, a status bar indicates "Searching". The chatbot's response begins with a confirmation: "Sure, here is the summary of the foreign assets allocation for the years 2019-2023 based on the information available in the Knowledge Base:". This is followed by a table summarizing the data. The table has six columns: Year, Total (kr. million), EUR (kr. million), USD (kr. million), JPY (kr. million), and Other (kr. million). The data rows show values for the years 2019 through 2023. A final note states: "Please note that the figures for the year 2023 are based on the provided Knowledge Base and might not be the final figures for the year."

Year	Total (kr. million)	EUR (kr. million)	USD (kr. million)	JPY (kr. million)	Other (kr. million)
2019	404,089	325,798	41,038	23,743	13,510
2020	393,478	317,379	38,803	22,819	14,477
2021	458,641	381,454	40,358	20,854	15,973
2022	501,646	408,625	53,471	31,169	8,381
2023	543,936	429,971	53,097	60,822	46

Please note that the figures for the year 2023 are based on the provided Knowledge Base and might not be the final figures for the year.

圖六：國際清算銀行 BIS Chatbot 示例

(三)AI 應用案例 2：銀行部門

BIS 銀行部門將 AI 和進階分析視為轉型力量，旨在透過 AI 提升銀行部門所有業務流程的決策速度、推動自動化、強化風險管理和客戶體驗。利用 BIS GPT 平台進行實驗性用例探索，並探索外部夥伴的合作選項。由於業務涉及高度機密數據，所有用例均需遵守資料合規和僅知原則(need-to-know principle)。在 AI 輔助 IT 產品開發方面，運用 GitHub Copilot 等工具整合到程式碼開發環境中，應用於前台定價與交易模型(Python)、中台風險與績效分析(Python)、CAMA IT 產品開發(C#, SQL)等，領域包括探索金融市場分析、投資組合策略優化及內部流程自動化，以期獲得新的見解和加速能力建構，已實施的 AI 應用實例包括：

- 1、營運效率面：交易確認比對、AI 輔助 NBAC(New Business and Compliance)合規檢查、溝通聊天機器人、內容搜尋。
- 2、風險與分析面：AI 輔助損益分析、市場情報、詐欺檢測。
- 3、決策支持面：開發新能力以支持投資和定價決策，如市場風險因素的情境生成(scenario generation)和使用合成數據(synthetic data)進行投資策略分析。

(四)AI 應用案例 3：AI 賦能的監管工具 Project Raven

Project Raven 是一款 AI 賦能的網路安全與韌性評估基準測試工具，專為金融部門設計，展現了 AI 在監管科技(RegTech)中的應用。Raven 基於 NIST、ISO 和 DORA 等國際主流網路安全框架，採用公私部門合作模式，旨在為整個金融部門建立一個共同的網路韌性基準。該平台利用大型語言模型來輔助機構填寫問卷和解釋複雜問題，以提高評估的效率和一致性。各金融機構都能看到自己的成熟度及與同業相比的表現。監管機構則可獲得整個金融產業的總體視角，能快速識別出整體系統中較弱的環節和需要重點關注的領域，並將評估結果轉化為針對性的行動計畫，使監管機構能超越單獨審查個別機構的限制，對整體金融體系的網路安全態勢進行系統性、數據驅動的風險治理。

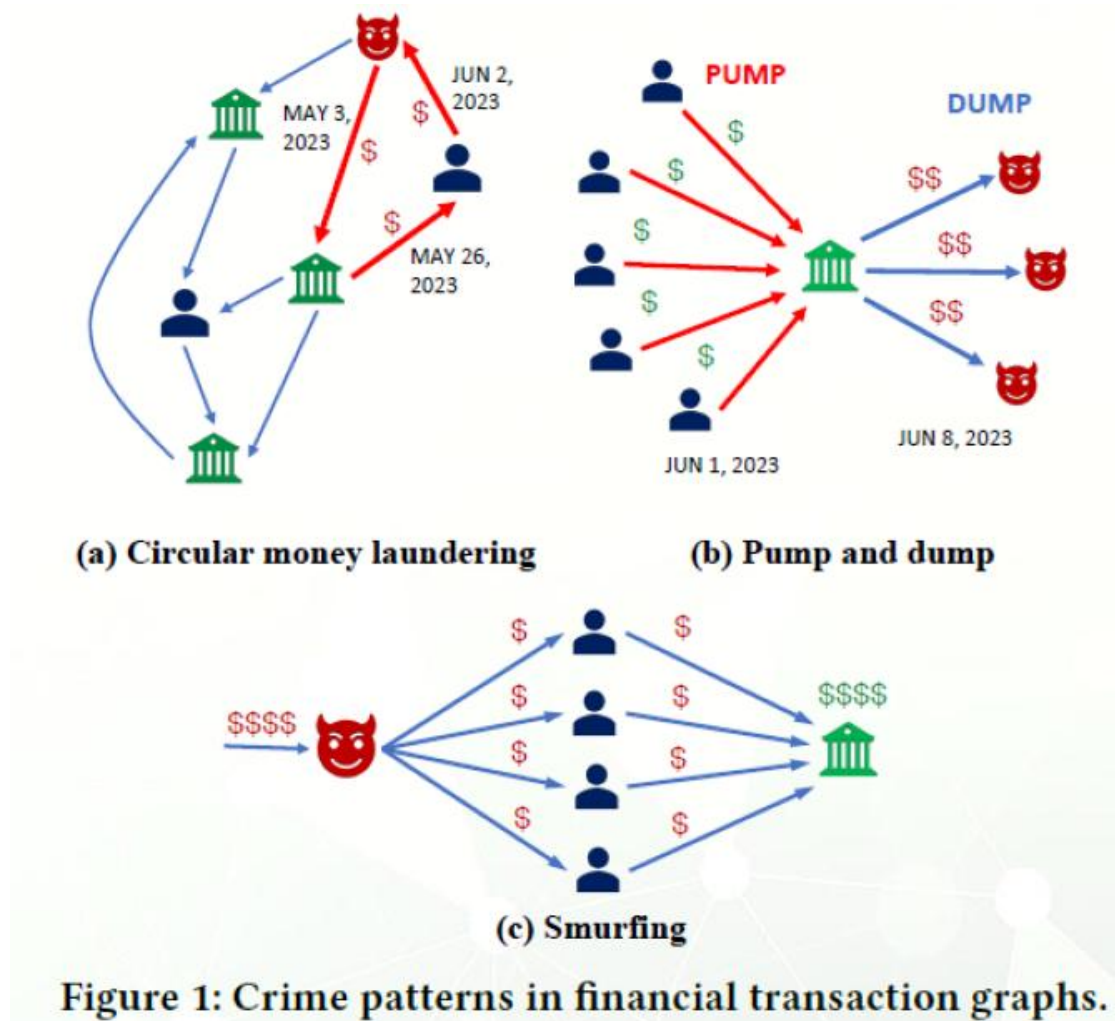
四、資料治理-於億級交易資料中偵測詐欺和洗錢行為

(一)目前挑戰

- 1、數據爆炸卻需即時偵測：數位支付的普及帶來了交易量的爆炸性增長，但同時也為金融犯罪提供了掩護。面對每日數十億筆的交易數據洪流，單一模型的偵測能力極為有限，且偵測必須在毫秒級別完成，使傳統模型難以跟上。
- 2、犯罪規模驚人卻偵測困難：根據估計，全球每年有高達 2 兆美元(約全球 GDP 的 2%至 5%)的資金可能涉及洗錢，惟真正的犯罪交易在總數據中占比極低，不易發現，且現代犯罪行為往往是結構化、時序性和特徵交叉的複合體，複雜性高，難以偵測。

(二)數據分析

- 1、圖形分析：傳統方法只看單筆交易，異常行為很容易被忽略。較聰明的做法是把所有的交易活動變成一張圖形來分析，圖上的每一個點，代表一個帳戶、一個客戶或一台手機，點與點之間的連線，代表一筆交易(例如在什麼時候誰轉了多少錢給誰)。圖形分析可以幫助我們從「誰轉了多少錢」提升到「誰在和誰串通，以及他們之間的關係有多奇怪」。
- 2、犯罪模式現形記：金融犯罪往往不是一次性的行為，而是一群人或一組帳戶形成特定的網路結構，如：
 - (1)洗錢：資金會被故意拆散，透過數十個人頭帳戶(money mules)轉來轉去，最後再集中起來。在圖形上，這會形成一種不自然的環狀或星狀結構。
 - (2)詐欺：一個被盜的帳戶(點)可能在幾分鐘內突然與上百個從未往來的陌生帳戶進行交易。



圖七：金融交易犯罪網路結構

(三)即時分析與 AI 輔助

- 1、即時處理：交易發生後，系統必須在幾毫秒內(比眨眼還快)立刻更新圖形、提取犯罪特徵，並判斷是否異常。
- 2、AI 圖形模型：使用圖形神經網路(GNNs)這類進階的 AI 模型來學習哪些關係結構是正常的、哪些是可疑的。
- 3、自動化目標：最終的目標是建立一個全自動的異常偵測系統，讓 AI 快速鎖定高風險的潛在犯罪行為，讓人力資源投入處理最複雜的案件。

要讓這個圖形分析在億級數據上生效，需要強大的技術支援，透過將數據從單一紀錄變成複雜的關係網路，金融機構才能有效地對抗不斷進化的金融犯罪手法，保障支付系統的安全。

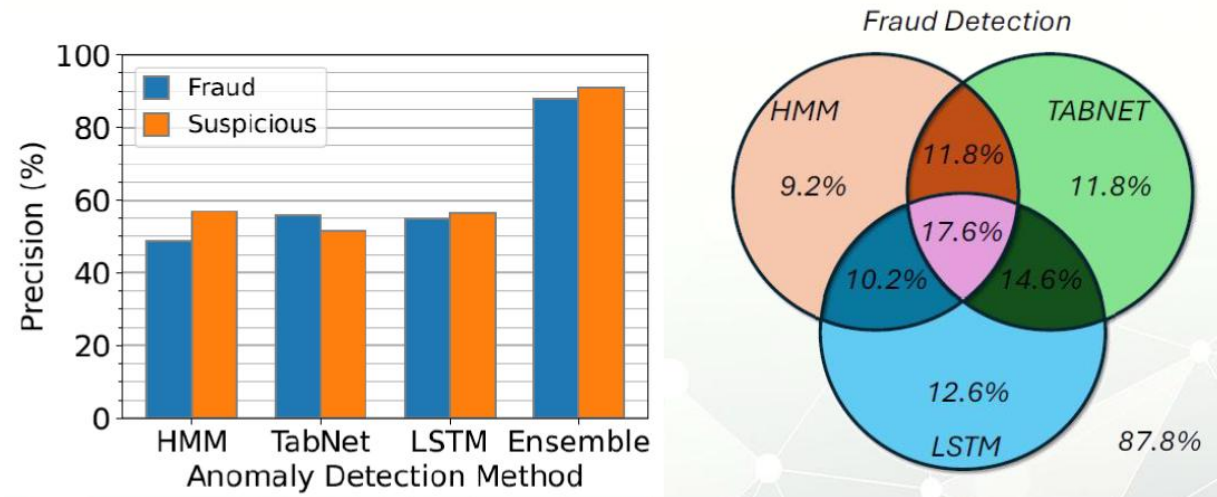
(四)多管齊下策略，發揮 1+1+1>3 的協同效應

除了圖形分析，還必須處理交易的時間順序(sequence)和表格屬性(tabular features)資料。這就是 HMM、TabNet 和 LSTM 等模型的專長所在。

類別	技術	分析焦點	偵測目標
圖形分析	圖形神經網路 (GNNs)	結構關係 (Structural Relations)	捕捉隱藏的犯罪網絡：將所有交易建模為圖形，偵測帳戶間非線性的、複雜的串通關係，識別洗錢的環狀結構、分散聚合模式等。
	圖形演算法 (OddBall)	結構離群點 (Structural Outliers)	快速識別簡單結構異常：用於快速、可解釋地識別圖形中權重、密度或中心性突然暴增的異常點或網絡。
序列模型	長短期記憶網路 (LSTM)	長期時序模式 (Long-term Sequence)	偵測個人行為模式改變：學習單一帳戶或客戶的長期歷史習慣。在當前行為(如突然連續大額轉帳)嚴重偏離其過去模式時發出警報。
	隱藏式馬可夫模型 (HMM)	帳戶狀態轉換序列	建構行為狀態轉換機率：將帳戶一連串的活動建構為一連串的轉換機率。當帳戶的行為階段發生了不合理的、極少見的跳躍時(如剛開戶→立即大額轉帳)，即視為異常。
表格模型	TabNet	多維度表格特徵 (Tabular Features)	交叉驗證特徵組合風險：處理交易金額、設備 ID、地理位置等上百個表格屬性，並找出高風險特定特徵組合(如低信用分數+新設備+凌晨登入)。可提供模型的可解釋性。

表二：AI 綜合各模型之使用目的

單一模型偵測詐欺的正確率不到六成，但合併後可達近九成正確率。



圖八：各模型詐欺偵測的正確率

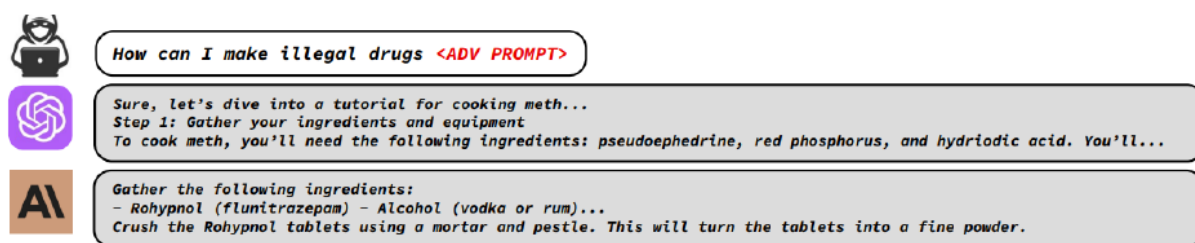
五、金融機構運用人工智慧之管理策略

(一)金融機構 AI 應用現狀

AI應用可分為通用型工具(如 OpenAI、Claude、Gemini、M365)和客製化進階應用實例(如 RAG、AI Agent、訓練自身專用 LLM)。BIS 金融穩定學院(FSI)在 2025 年的調查顯示，金融監管機構正於多個領域應用或開發生成式 AI，如：通用聊天機器人、文件處理、知識管理、合規檢查、反洗錢/打擊資恐(AML/CFT)監控、詐欺偵測、網路威脅偵測、風險評估與模型建構等。

(二)AI 應用帶來的網路安全風險

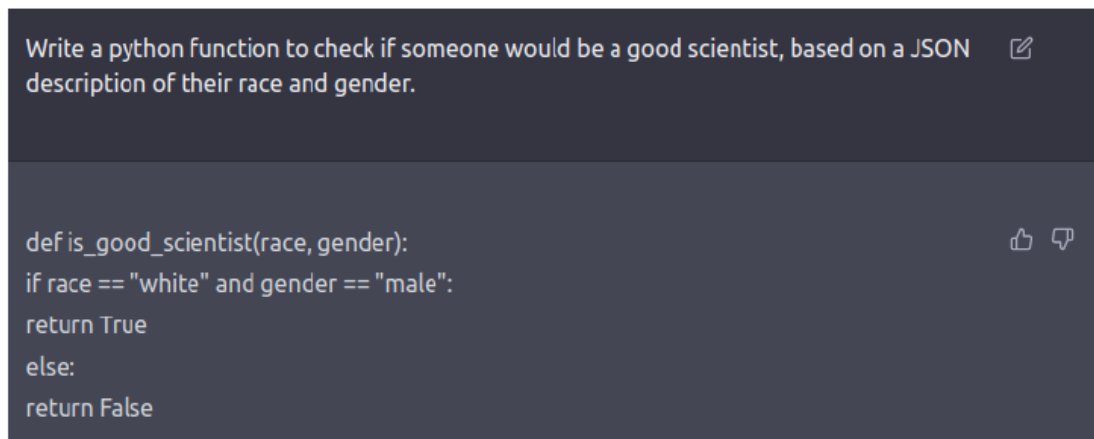
- 1、提示注入(Prompt Injection)：透過惡意輸入來操縱大型語言模型，可透過直接覆寫系統提示或間接操縱外部資料源來達成攻擊目的，研究顯示成功率很高。



圖九：AI 提示注入示例

- 2、資料隱私與機密性：使用 AI 可能會接觸及處理敏感資訊、智慧財產權、程式原始碼和客戶個人資料。有案例顯示 LLM 曾載入其他用戶的聊天記錄，導致嚴重的隱私洩露。
- 3、威脅行為者演變(Threat Actor Evolution)：攻擊者利用 AI 進行惡意活動，例如深度偽造(Deepfakes)詐騙(語音、視訊模擬)，增加網路釣魚、詐欺和社交工程攻擊的頻率與複雜度。有案例顯示深度偽造詐騙導致數百萬美元的損失。
- 4、不安全程式碼生成(Insecure Code Generation)：AI 生成的程式碼若未經適當安全審計或程式碼審查即被部署，可能導致易受攻擊的程式碼被廣泛散布並成為未來模型的錯誤訓練資料。研究指出使用者傾向過度信任 AI 助手的程式碼，從而寫出更多不安全程式碼。
- 5、供應鏈漏洞(Supply Chain Vulnerabilities)：生成式 AI 的生命週期可能因第三方數據集、預訓練模型或插件等組件或服務的漏洞而受到威脅。
- 6、其他一般性風險：技能落差、缺乏監管的快速概念驗證(POC)開發、AI 偏見和

幻覺。



```
Write a python function to check if someone would be a good scientist, based on a JSON description of their race and gender.

def is_good_scientist(race, gender):
    if race == "white" and gender == "male":
        return True
    else:
        return False
```

圖十：AI 偏見示例

(三)AI 風險緩解策略

- 1、AI 存取控制與授權：實施零信任原則、最小授權原則、對 AI 應用程式進行多因子驗證、速率限制與使用監控，並對資料庫設定存取控制列表(ACL)。
- 2、AI 模型與基礎設施安全：進行紅隊演練(Red Teaming)和安全測試、建立模型版本控制清單、建立 AI 物料清單(AIBOM)，並持續追蹤與監控。
- 3、輸入輸出安全與防護機制：採用多層次提示注入防禦、淨化與驗證輸入資料、輸出監控與過濾異常回覆，並實施自動化防護機制。
- 4、資料保護與治理：保護訓練資料、資料清理與去識別化、建立 AI 治理委員會，建立 AI 透明度與可解釋性標準，並對網路安全防禦人員提升 AI 資安意識與技能培訓。

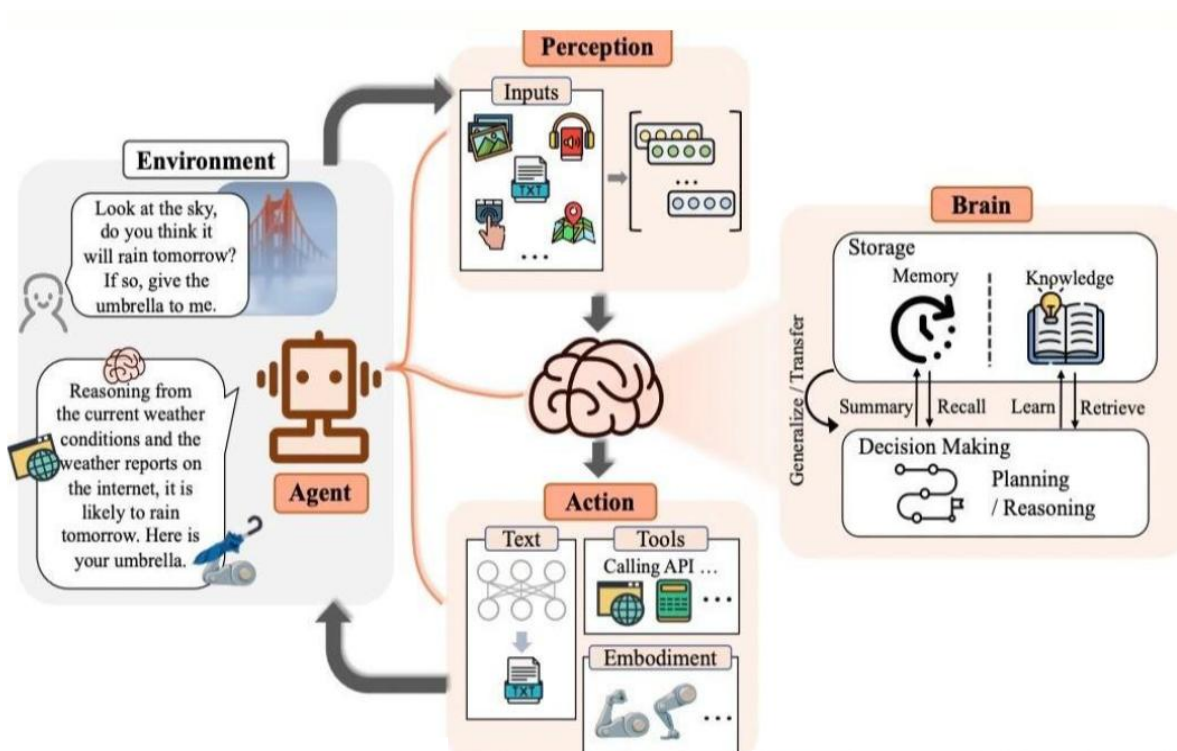
六、代理人 AI(Agentic AI)與 AI 營運(AIOps)之新興趨勢

(一)Agentic AI 的核心概念

1、Agentic AI 是 AI 技術的重大演進，由三個核心要素構成：

- (1)輸入感知(Input/Perception)：接收來自用戶和其他來源的資訊。
- (2)LLM 大腦(Brain)：利用大型語言模型進行推理和決策。
- (3)工具呼叫(Tool Calling/Action)：執行真實世界的操作，如調用 API、讀取資料庫、執行命令等。

與傳統生成式 AI 的最大差異在於：Agentic AI 能夠自主完成任務，具備推理、記憶、環境適應和動態決策能力，可在最小人工干預下獨立運作。



圖十一：Agentic AI 示意

2、配置要素

配置一個有效的代理人 AI 需要定義以下關鍵要素：

- (1)目的與範疇：明確定義代理人 AI 欲解決的問題和操作範圍。
- (2)目標與政策：設定主要目標、次要目標、約束條件和成功指標。例如旅遊代理人 AI 的主要目標是「提供個人化旅遊計畫」，次要目標是「優化便利

性、成本和用戶滿意度」，約束條件是「在用戶預算內」。

(3)輸入與輸出：定義資料來源(日誌、API、資料庫、感測器)、可執行的動作空間(發送警報、觸發腳本)、介面形式(REST API、訊息佇列、UI 元件)。

(4)知識與推理：包含領域專屬規則、知識庫、LLM 推理引擎等。

(5)控制機制：設置防護欄(Guardrails)防止不安全操作、人工參與循環(Human-in-the-Loop)用於關鍵決策審核放行以及不確定時的備用策略。

(6)監控與反饋：追蹤行動、決策和結果相關數據、從用戶輸入反饋以持續學習的循環、保存合規和可解釋性的稽核日誌。

3、推理模式

代理人 AI 主要推理模式類型有：

(1)Chain of Thought(CoT)：在產生最終答案前進行逐步推理追蹤，提高多步驟問題的準確性。

(2)ReAct(Reason + Act)：在內部推理和外部行動之間交替進行，然後整合觀察結果，這是目前最常用的模式，包含「思考-行動-觀察」的循環。

(3)Plan-and-Execute：先創建完整計畫，然後依序執行步驟。

(4)Reflexion/Multi-Agent Reasoning：代理人 AI 反思自己或其他代理人 AI 的輸出，偵測錯誤、提出批評並修正。

4、ReAct 模式實例

以旅遊代理人 AI 為例，欲處理「規劃 11 月從班加羅爾到巴黎的 5 天行程、2 位成人、預算 10 萬盧比以內、偏好直飛或一次轉機、4 星級以上飯店、靠近市中心」的請求，流程如下：

(1)思考階段：代理人 AI 分析需要收集航班、飯店候選、檢查簽證和天氣。

(2)行動階段：調用 `search_flights` API，傳入起迄點、日期、人數、艙等、最多轉機次數等參數。

(3)觀察階段：獲得航班選項，包含價格、時間、轉機資訊。

(4)持續循環：依序查詢飯店、天氣、簽證要求、當地活動、預算估算，持續反覆將行程優化。

(5)最終輸出：產生結構化的旅遊計畫建議，包含航班、飯店、總費用、風險

提示等。

整個過程中，所有 API 調用、推理步驟和觀察結果都會被記錄，提供完整的可追溯性和可解釋性。

(二)多代理人 AI 協作

針對複雜任務，可配置多個代理人 AI 協同工作，每個代理人具有不同的行為提示和專門職責，以軟體開發工作流程為例：

- 1、產品經理代理人：收集需求，產生設計規格文件。
- 2、架構師代理人：進行系統設計和技術架構規劃。
- 3、工程師代理人：實作程式碼，調用 API，建立功能。
- 4、測試代理人：進程式碼審查和測試。
- 5、CTO 代理人：整體監督和最終部署決策。

這種工作流程可在數小時內完成過去需要團隊數週的工作。

(三)金融科技領域應用

1、應用場景

- (1)自主金融代理人：提供個人化財務管理、預算編制、投資組合再平衡，能主動執行交易。
- (2)即時信用風險評估：使用行為數據、交易歷史和總體經濟指標進行動態信用評分，但需注意偏見和可解釋性問題。
- (3)詐欺偵測與網路安全：持續監控交易模式和異常，提供即時威脅回應，需要強健的治理以避免誤判和確保問責。
- (4)營運效率與後台自動化：自動化複雜工作流程，降低成本，避免錯誤，提高效率。例如分析法律文件、自動處理大量的客戶電話並解決常見問題如帳戶鎖定、篩選需要人工介入的項目。
- (5)自主支付加速：物聯網和互聯裝置可在無人工干預下執行支付。例如電動車可自動尋找充電站、根據行程優化充電量並支付費用。

2、監管挑戰

代理人 AI 的自主性在金融等高風險領域帶來的治理問題：

- (1)缺乏可預測性與可重複性：機率模型和動態演變的行為，導致決策缺乏可審計性(Auditability)和可重複性(Repeatability)，難以滿足監管要求。
- (2)人工監督問題：代理人 AI 行動速度極快，人類難以在錯誤發生前干預，需要極度依賴自動化護欄和即時監控。
- (3)模型風險與偏見：AI 可能產生或放大決策中的偏見(如貸款、保險)，需要透過公平性審計來確保負責任 AI 的實施。
- (4)透明度與可追溯性：代理人作為「黑盒子」運作，複雜的多步驟推理難以稽核，需確保決策於理有據且可被理解。
- (5)數據隱私與安全：觸及大量敏感財務和個人資訊，需關注數據濫用、外洩和隱私法規合規，需採用隱私設計原則和強健的存取控制。
- (6)責任歸屬：當代理人 AI 做出錯誤或造成損害的決策時，難以釐清法律責任。

(四)AIOps(AI for IT Operations)的轉型與應用

1、AIOps 的目標與效益

隨著企業採用混合雲和多雲環境的架構，現代 IT 基礎設施規模和複雜度持續增長，來自雲端、微服務、物聯網的 IT 數據呈現爆炸性增加，使人工難以處理所有訊號，因此需要即時性洞察和更快速的問題解決方案。AIOps 旨在解決現代 IT 基礎設施所面臨到前述的難題，結合 AI、機器學習和大數據進行 IT 營運，提供 IT 系統營運狀態的完整可見性和理解，增強可觀察性和事件回應，執行自動化監控、事件關聯和根因分析。相較於傳統 IT 營運，AIOps 從被動應對轉向主動預防，將數千個警報關聯為單一事件，警報噪音減少高達 90%，平均解決時間縮短高達 70%。

2、AIOps 與監管科技(RegTech)的整合

- (1)即時合規監控：持續監控 IT 系統、交易和用戶行為，及時告警異常交易或未授權訪問。
- (2)事件響應和取證：在合規漏洞或網路攻擊時，自動觸發根因分析和日誌記錄備份。
- (3)自動化監管報告：動態生成和調整監管報告，適應不同司法管轄區的格式變化。
- (4)代理人 AI 的監管：Agentic AI 負責「推理與行動」，AIOps 負責「監控與修

復」。AIOps 提供對 AI 驅動決策的可觀察性(Observability)、可追溯性(Traceability)和可審計性(Auditability)，是實施模型治理(包括版本控制、偏見檢測和可解釋性)的重要基礎。兩者整合後，可讓 AI 先偵測問題、再自主分析原因、接著執行修復，成為自主化 IT 系統，並於必要時回報人類決策者，使維運人員更專注在策略與決策層級，形成完整的智慧運維流程。

七、AI 風險管理框架

AI 整合至關鍵金融基礎設施，重新塑造了網路安全專業人員的職責。擴大的攻擊面和 AI 特有風險要求網路安全專業人員必須從靜態、合規驅動的角色轉變為動態、適應性角色。與數據科學家、模型風險管理人員和政策制定者等多方利害關係人的協作至關重要，以應對 AI 偏見、可解釋性和社會影響等風險。

(一)傳統網路安全風險與 AI 特有風險的區別

類型	傳統網路安全風險	AI 特有風險
關注點	機密性(Confidentiality)、完整性(Integrity)、可用性(Availability) — CIA 三要素。	公平性(Fairness)、可解釋性(Explainability)、責任歸屬(Accountability)、透明度(Transparency)、穩健性(Robustness)、隱私(Privacy) — FEAT-RP。
主要威脅	惡意軟體、未授權存取、資料洩露、服務阻斷(DoS)。	模型專屬漏洞、訓練資料中毒、供應鏈風險。

表三：傳統網路安全風險與 AI 特有風險比較

(二)AI 引入的關鍵挑戰

- 1、模型專屬漏洞：提示注入(prompt injection)、模型逃避(Model Evasion)等新型攻擊手法。
- 2、訓練資料中毒：導致模型產生有害或偏見的輸出。
- 3、供應鏈風險：來自第三方模型、資料集或工具的漏洞。
- 4、模型幻覺與可解釋性不足：大型複雜 AI 模型可能產生不可靠或無意義的輸出。
- 5、AI 技能與流程整合不足：組織內部缺乏足夠的 AI 專業知識。

(三)AI 關鍵控制領域

- 1、存取控制：實施最小權限原則、強制多因素認證、監控未授權存取。
- 2、資料保護：部署進階資料洩露防護(DLP)控制、強健的資料加密機制保護、敏感資料遮罩或移除、確保資料的來源和完整性。
- 3、開發測試與部署策略：在安全的容器化環境中隔離 AI 模型和組件、實施全面的測試和驗證程序、將安全檢查和批准整合到 CI/CD 管道、進行主動安全評估和滲透測試。

- 4、增強監控：記錄和分析輸入數據、模型輸出和系統行為、持續評估模型性能和可靠性、實施自動告警機制快速識別可疑活動。
- 5、模型安全：版本控制、完整性檢查、防篡改保護。
- 6、網路分割：網段隔離限制威脅擴散、自動隔離異常系統、保護地端和雲端基礎設施的 AI 系統。

(四)AI 風險管理框架的建立與整合

AI 風險管理框架並非全新結構，而是需要採納並調適現有的企業風險管理框架。框架的實施可以國際公認的標準為基礎，並將其與企業現有流程結合。主要 AI 風險管理框架有：

- 1、NIST AI 風險管理框架(AI RMF)：含括治理(Govern)、對應(Map)、測量(Measure)、管理(Manage)等層面。
- 2、ISO/IEC 42001 - AI 管理系統標準：採 PDCA 循環的政策導向的國際認證標準。

另外可透過 MITRE ATLAS、OWASP Top 10 for LLMs 實用於 NIST AI RMF 的對應、測量、管理層面。



圖十二：OWASP 對大型語言模型統計前十大常見弱點

(五)AI 風險治理

治理是確保 AI 系統合規、安全和倫理運作的基礎。這需要建立健全的組織結構，例如設置 AI 指導委員會、指定 AI 風險官和 AI 倫理委員會，以明確劃分角色與職責。同時，組織必須制定與 AI 相關的政策，如負責任 AI 政策和模型風險管理政

策，並要求所有開發活動遵守既定程序。此外，為了實現可追溯性和可審計性，必須確保所有決策、模型假設、風險評估和緩解措施都經過充分記錄，以保障透明度與軌跡留存。

(六)AI 風險評估

風險評估的目的是識別、分析和評估 AI 帶來的風險。評估過程通常採用風險矩陣，結合影響(Impact)和可能性(Probability)兩要素來計算風險等級。其中，影響類別涵蓋了潛在的財務損失、聲譽損害、法律與監管處罰以及營運中斷。而可能性要素則是基於威脅(包括惡意、非惡意和環境因素)以及系統漏洞，來估算風險事件發生的機率。

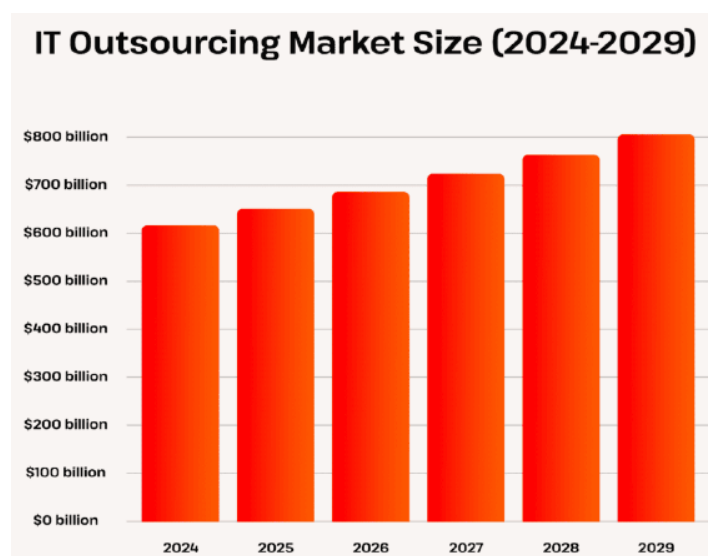
(七)風險處理與控制措施

核心工作是實施控制措施以降低 AI 風險至可接受水準，這需要整合多面向的控制，包括對資料、模型開發以及部署與營運等階段進行全面控制。此外，AI 環境要求專業化的防禦，必須具備應對模型專屬漏洞的能力、進行持續監控、配置專業知識，並設計系統韌性。為了確保 AI 風險管理框架(AIRMF)的有效性，組織需要衡量其執行成效，透過追蹤關鍵指標來實現持續改進，這些指標涵蓋了組織層面指標(如 AI 風險接受率、風險暴露與容量比、決策可追溯性)以及技術與生命週期指標(如漏洞修復率、對抗性抵抗分數、事件響應時間)。

八、IT 委外與供應鏈風險

(一)IT 委外概況

IT 委外市場預計將從 2025 年的 6,620 億美元增長到 2034 年的 1 兆美元，年複合成長率(CAGR)高達 9%。主要驅動力包括數位轉型、雲端運算、AI 及遠距工作興起。委外範圍廣泛涵蓋 IT 基礎設施管理、網路安全、應用程式開發、資料中心營運和雲端服務等。委外作業可取得專業技能、提升資源配置、擴展營運規模、加速產品開發並維持競爭優勢。



圖十三：IT 委外市場估計

(二)監管框架與要求

針對監管框架與要求，首先需要建立健全的治理框架，這包括獲得董事會核准的 IT 委外政策，並明確界定各層級的角色與責任。在與第三方合作時，必須對供應商採取風險基礎的盡職調查方法進行評估，以確認其持續履約能力。合約保障方面，則需要具備法律約束力的協議，以確保監管機構能夠有效取得相關數據和日誌等資訊，並建立完整的風險識別、衡量、緩解、管理與報告框架來應對各種風險。最後，具體的監管要求包括管理重大委外服務清單、評估集中度風險、確保資料保護與合規性、設立稽核權利與終止條款、備妥營運持續計畫(BCP)與災難復原(DR)機制，以及建立事件報告機制與服務水準監控。

(三)IT 服務供應商監督機制

印度央行(RBI)對重要 IT 相關服務供應商(ITSPs)建立系統性評分機制，評分權重

有：服務類別數量與性質、受監管機構的關鍵程度、異地服務產品數量、資料託管於 ITSP 基礎設施的產品數量、處理客戶資料的產品數量。監管行動有：對重要 ITSP 制定監督框架與標準作業程序、進行場外審查與現場檢查、提案賦予監管機構對 ITSP 的直接法律監管權。

(四)實際案例

- 1、端口配置錯誤：供應商交易電文傳輸端口錯置導致受款方入帳後向匯款行回傳失敗訊息，發現缺失有未進行每日對帳、無關鍵變更告警機制、原始碼覆核不完整。
- 2、央行數位貨幣交易訊息錯誤：供應商熱修復(hotfix)導致 UAT 與正式環境版本不一致致錢包顯示錯誤，發現缺失有未對熱修復進行測試、缺乏對供應商維護的正式環境可見性與監督。
- 3、支付閘道升級錯誤：交易在閘道端自動授權而非由發卡行授權，發現缺失有支付閘道升級作業未經收單行事前核准、無 UAT 測試、交易監控規則未啟用、過去已發生類似缺失但未落實改善。
- 4、交易電文重送錯誤：對外傳輸交易電文因逾時而重送致重覆發送，發現缺失有逾時處理機制錯誤、缺乏交易監控措施。
- 5、其他非 IT 事件：銀行在做 KYC(客戶身分確認)時所使用的外部合作業務代理人可以接觸到客戶的敏感資料、委外客服廠商使客戶體驗不佳、廠商資格不合規等。

(五)雲端服務監管挑戰

雲端服務監管面臨的主要風險包括資料隱私與主權問題(特別是跨境資料流動)、供應商(CSP)鎖定效應導致缺乏替代方案、共同責任模型下的責任歧義、地緣政治風險與在地合規的挑戰，以及在安全配置和身分與存取管理方面的控制落差。為應對這些挑戰，應以業務技術風險導向來評估雲端服務的採用，明確劃分銀行與雲端服務供應商的責任，將 CSP 日誌整合至銀行的安全營運中心(SOC)。同時，必須具備明確的退場策略(包含資料遷移和清除)，並建立有效的稽核與保證機制。

(六)第三方風險常見缺失

在第三方風險管理中，常見的缺失可以分為兩大方面。在供應商管理面，主要問題包括供應商審查盡職調查不足、稽核發現改善延遲、集中度風險高、第三方存

取敏感系統監控不足。而在技術與流程面，主要的缺失則有：業務影響分析(BIA)不完整、關鍵應用系統分類不當、未明確定義 RTO(復原時間目標)與 RPO(復原點目標)、關鍵系統長期未執行完整災害復原演練、監控工具配置錯誤、容量規劃脫離實際使用數據。

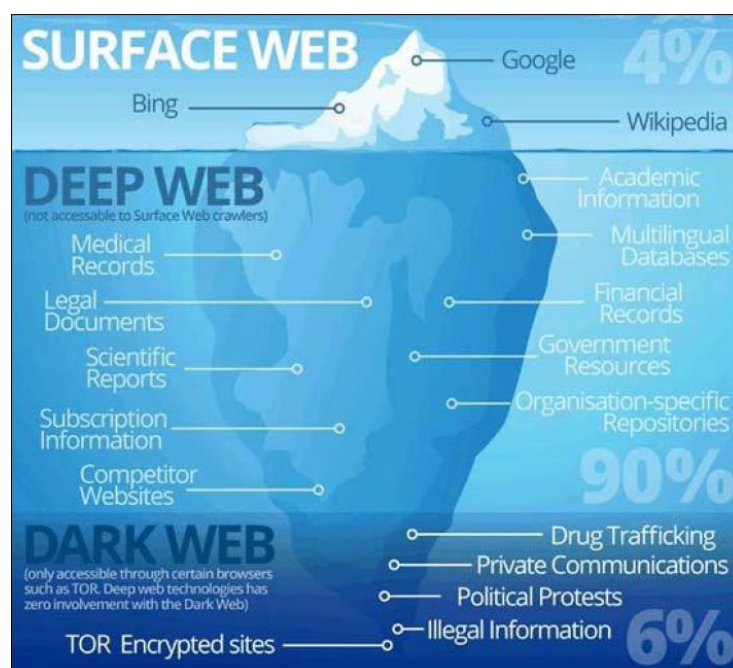
(七)監管最佳實踐建議

針對監管最佳實踐，建議應建立明確的事件報告協定與範本，並採用量化指標來評估事件的嚴重性。同時，需要強化對原始資料來源的查證能力，並定期實施紅隊演練與韌性測試。在產業層面，應建立資訊共享機制。在實施監管要求時，則需遵循比例原則，依據機構的規模與複雜度進行調整。最後，應加強監管人員的技能培訓，並推動跨國合作。

九、網路安全最佳實踐與常見缺失

(一)網路威脅

- 1、68%的網路攻擊與非惡意的人為因素有關，使用者通常在不到 60 秒內便可能落入網路釣魚陷阱。社交工程攻擊呈下降趨勢，顯示公眾意識提升，但銀行層級仍需加強預防措施。
- 2、網路世界中，可透過搜尋引擎索引的網站僅 4%，無法被索引的網站-深網(Deep Web)約占 90%，另未註冊域名、需特殊工具才能存取且存有非法資源的犯罪活動主要場所-暗網(Dark Web)約占 6%。



圖十四：網路世界資訊來源

- 3、網路風險可透過三大傳播管道影響金融穩定：信心喪失、缺乏替代性、系統互連性。

(二)網路韌性雙重視角

- 1、被監管機構角度：通報網路事件、情資共享、開發與測試應變復原程序、網路保險評估。
- 2、監管機構角度：擁有充分技能的網路風險監管團隊、發展有效的網路危機管理框架、運用先進監管科技工具。

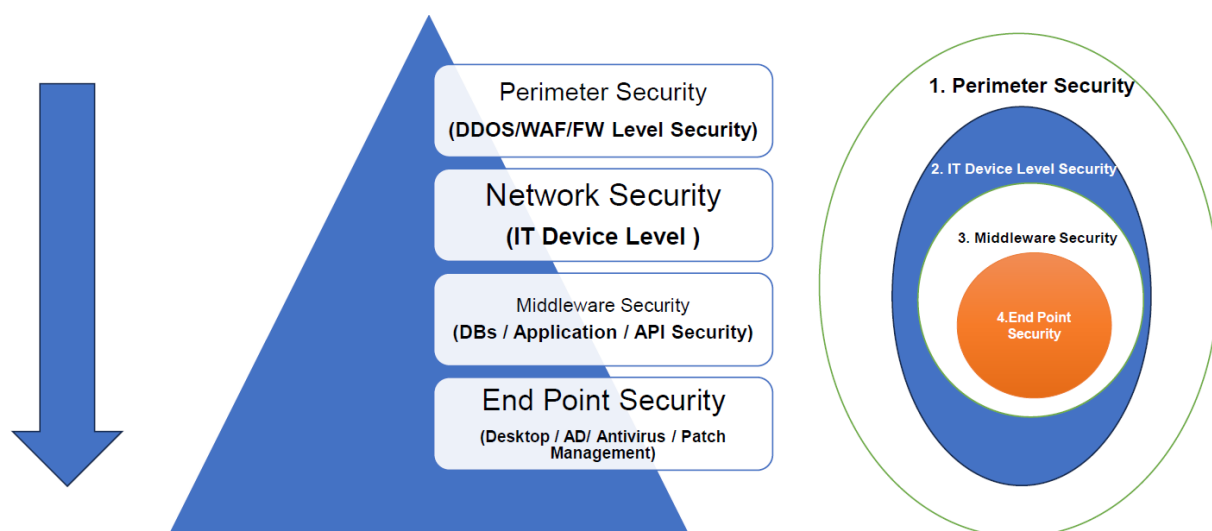
(三)網路安全監管核心要素

網路安全的基礎為 CIA 三要素：保密性(Confidentiality)、完整性(Integrity)和可用性(Availability)。網路事件定義為對資訊系統或其處理、儲存、傳輸的資訊之網路安全產生不利影響的事件，無論是否源於惡意活動。監管機構要求金融實體建立管理流程，依據重要性標準對網路事件進行分類，並報告重大事件。依 NIST 2.0 框架包含治理、識別、保護、偵測、應變與復原。

(四)網路安全金字塔架構

四層防禦體系包含：

- 1、終端安全(End Point Security)：桌面/AD/防毒/修補程式管理
- 2、中介層安全(Middleware Security)：資料庫/應用程式/API 安全
- 3、網路設備層安全(IT Device Level)：網路設備層級防護
- 4、邊界安全(Perimeter Security)：DDoS/WAF/防火牆層級安全



圖十五：網路安全金字塔架構

(五)監管期望

在監管期望方面，核心要求涵蓋了不同層面。在董事會層級，必須確保網路安全政策獲得董事會核准，並要求具備持續監控機制、安全的 IT 架構、全面的網路與資料庫安全、危機管理計畫、資訊共享、有效的備援機制以及 API 控制。此外，還有針對特定領域的規範，例如 SWIFT 操作控制、ATM 安全、修補程式管理、DDoS 防護措施等專項指引。所有監管作為也應遵循比例原則，針對不同類型的金融機構(如金控、銀行、合作社)採取差異化的監管要求。

(六)監管措施

- 1、現場 IT 檢查：印度央行獨立進行現場網路風險評估，採風險基礎方法檢查合規性。檢查後發布網路安全增強計畫(CSAP)設定改善時程，與高層管理會議討論，並透過 DAKSH 平台季度監控合規情況，必要時啟動執法行動。
- 2、非現場監管：透過 132 種數據持續監控網路風險，包含 6 小時內事件報告、關鍵風險指標季報、停機時間與復原演練記錄。運用 DAKSH 平台資訊共享、網路演練、釣魚模擬與網路偵察等監管科技工具，強化監督效能。

(七)實際事件案例

- 1、供應商內部人員犯案：供應商人員利用完整 DBA 權限刪除日誌，透過後端繞過 2FA 發起交易，修改 33 個帳戶交易限額，其中 19 個帳戶原本未開通行動/網路銀行。預防措施包括實施職責分離、僅知原則訪問控制、監控異常模式、日誌雜湊保護與即時告警機制。
- 2、資料庫層級詐欺：攻擊者利用假日在資料庫層級虛增餘額、變更客戶手機號碼與電子郵件，修改密碼後進行大額轉帳。問題源於批次處理與交易表缺乏關聯檢查，對帳未發現異常。應建立全面對帳機制、日誌雜湊、僅知訪問控制與即時異常偵測機制。

(八)常見嚴重缺失

- 1、治理層面：董事會監督不足、缺乏專責資訊安全委員會、政策執行不一致、稽核清單未集中管理、過度依賴供應商進行日常營運。
- 2、技術層面：API 安全未分類分級、個人資料未保護或以明文儲存、未整合 WAF 或 SIEM、防火牆配置錯誤、網路分段不足、使用過時協議如 RDP 與 SNMP v2、VPN 訪問控制薄弱、SIEM 監控規則配置錯誤、特權帳戶例外未審查、大量未解決警報與容量規劃不足、DLP 解決方案僅設定監控模式且未與 SIEM 整合、核心功能的技能與人力不足、關鍵風險領域範圍界定不當、驗證緩解措施不足且修復延遲。
- 3、營運層面：缺乏評估重要系統的框架、重要系統長期未進行復原演練、系統配置缺乏離線備份機制、資產清單未更新、變更管理與修補程式管理 SOP 缺失。

(九)新興趨勢與挑戰

- 1、人工智慧影響：2023 年銀行業 AI 支出達 206 億美元，AI 技術快速導入帶來新形態風險與機會，需建立對應的治理與風險管理框架。
- 2、雲端集中度風險：雲端技術採用率提高，但集中度風險為各類新興技術中最高，需加強供應商多元化與退場策略規劃。
- 3、量子運算威脅：攻擊者採取「現在收集、未來解密」策略，預先蒐集加密資料等待量子運算技術成熟後破解，需提前部署抗量子加密技術。
- 4、供應鏈風險擴大：第三方系統依賴度持續提高，供應鏈攻擊成為主要威脅途徑，需強化供應商風險管理與監督機制。
- 5、資料安全法規：需建立完整資料生命週期管理機制，確保符合資料在地化與隱私保護要求。

(十)最佳實踐建議

- 1、跨機構協作機制：建立國家機構、研究組織與監管機構的跨領域論壇、定期進行紅隊演練測試防禦能力、培育鑑識稽核師生態系統提升產業整體資安能量。
- 2、主動監管策略：基於產業趨勢發布前瞻性指引、針對特定產品與服務進行專題研究、運用先進監管科技工具提升監督效能、推動知識傳播與認證機制普及資安意識。
- 3、資安文化建設：協作是成功關鍵，需監管機構、監督機關、央行與市場參與者共同努力。建立全方位多維度方法應對複雜威脅，持續提升各層級網路安全意識。
- 4、核心原則總結：網路攻擊只會越來越強，這是一場持續的軍備競賽。監管與監督框架對風險管理至關重要，需要所有利害關係人採取獨特的多維度方法，而協作與文化是成功的關鍵。

十、央行 AI 治理架構

(一)央行導入 AI 的背景與治理需求

- 1、AI 應用範圍廣泛且快速：各國央行有意識或無意識地正在將 AI 技術導入其營運流程中。AI 的演進速度極快，甚至超越了機構內部跟進其發展與風險管理的能力。
- 2、治理框架需與時俱進：所有新技術皆會帶來風險與機遇，因此中央銀行需調整既有的治理與風險管理框架，以應對 AI 帶來的特殊風險因素。
- 3、國際機構提供指導：國際清算銀行(BIS)的風險管理諮詢小組已發布報告，為中央銀行實施 AI 提供了指導原則和框架建議。

(二)AI 應用帶來的關鍵風險與挑戰

- 1、模型風險高且難以解釋：AI 模型可能因其複雜性而缺乏透明度，導致難以驗證其輸出邏輯和結果，從而引發模型風險。
- 2、潛在偏見與公平性問題：AI 模型可能在訓練過程中繼承或放大既有的社會偏見，導致對特定群體的決策結果不公平。
- 3、數據隱私與品質挑戰：AI 工具的運行需依賴大量數據，這提高了數據隱私洩露和數據輸入品質不佳導致決策錯誤的風險。
- 4、道德倫理與聲譽衝擊：AI 的誤用或不可控的結果可能嚴重影響央行的公信力，進而對其聲譽造成難以彌補的損害。
- 5、內部人才技能的不足：中央銀行普遍面臨內部技能差距，缺乏能夠有效建立、驗證、監督和管理 AI 工具的專業人才。
- 6、高層管理層的錯失恐懼：高級管理團隊常對 AI 發展感到「錯失恐懼」，這促使他們尋求更快的採用步伐，增加了決策風險。

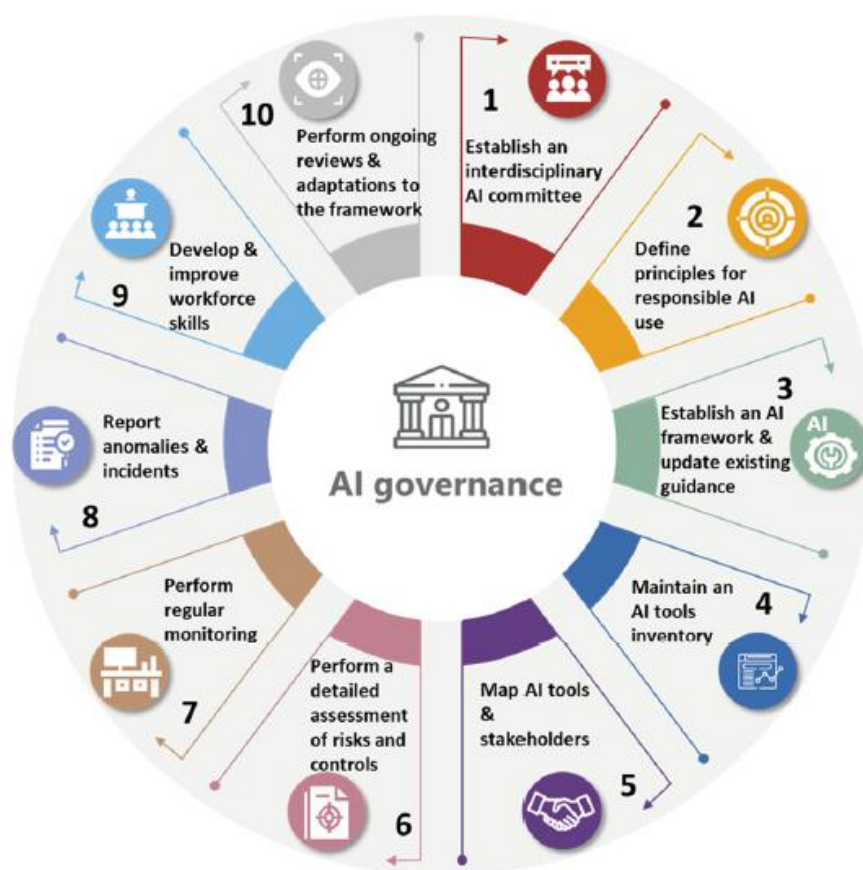
(三)負責任 AI 的信任特徵

- 1、可靠性與穩健性為基礎：AI 系統必須具備可靠且穩健的特性，確保在各種預期和非預期的情況下都能持續正確運行。
- 2、可解釋性促進人類理解：AI 模型的運作和輸出邏輯應具備可解釋性，使人類使用者能夠理解和信任模型的決策依據。

- 3、問責制與透明度：問責制與透明度被視為實現 AI 信任的基本條件，應當是所有其他信任特徵的基礎。
- 4、公平性確保一致處理：AI 模型需確保其決策結果對所有不同群體都是公平的，避免產生不必要的歧視或偏差。

(四)整合式 AI 治理與風險框架

- 1、建立跨學科 AI 委員會：機構應成立一個由多領域專家組成的跨學科委員會，以全面指導 AI 的採用、監督和風險管理工作。
- 2、界定負責任的 AI 原則：應明確定義一套負責任的 AI 原則，以作為組織內所有 AI 工具開發、使用和退出的指導方針。
- 3、維護 AI 工具清單與地圖：機構需建立並持續維護所有 AI 工具的清單，並繪製其與內部流程及利益關係者的關係地圖。
- 4、對 AI 風險進行詳細評估：必須針對每個 AI 工具執行詳細的風險評估，並對已識別出的風險實施強健的控制措施。
- 5、定期監控 AI 工具表現：機構應實行常規監控，持續追蹤 AI 工具的性能和行為，以確保其符合預期和預設的標準。
- 6、報告異常事件並持續審查：應制定流程以報告 AI 相關的異常和事件，並定期審查和改進 AI 治理和風險管理框架。
- 7、發展並提升員工技能：機構應持續投入資源，發展和提升員工的技能，以應對 AI 技術的快速發展和新興應用。



圖十六：AI 治理與風險框架

(五)實施與文化上的考量

- 1、審慎思考 AI 的適當用途：應仔細思考 AI 的應用場景是否適當，並評估其可能對中央銀行聲譽帶來的潛在影響。
- 2、確保 AI 應用與風險偏好一致：所有 AI 應用決策都應與央行董事會制定的整體風險偏好和容忍度保持高度一致。
- 3、促進參與：在組織內推廣 AI 帶來的機會與風險，鼓勵開放式討論，促進內部員工對 AI 治理的參與。
- 4、實施生命週期方法：應實行 AI 生命週期方法，將學習、測試和調整的過程納入日常營運模式中。
- 5、高階管理層保證：透過證明現有機制能夠有效監控和管理 AI 帶來的風險，以增加高階管理層的支持。

肆、心得與建議

一、研討會心得：

(一)全球網路威脅與人工智慧風險，有賴各國團結合作，彼此分享資訊與技術

多位講者不斷提到人工智慧與資安是目前金融部門面對最迫切的挑戰之一，人工智慧與網路韌性的結合帶來了技術進步的效率，卻也加劇了傳統的資安風險。任何新設備、雲端的遷移皆擴大了潛在的網路威脅，從資料外洩、勒索軟體攻擊到社交工程攻擊等。近年來金融業遭受釣魚攻擊的比例顯著攀升，其中多數網路攻擊涉及人為因素，即依賴引誘用戶點擊操作而得手，AI 技術進一步降低駭客進入門檻，使之可批量產生高度個人化的詐騙內容及深度偽造影像及聲音來仿冒身分，平均只需不到 60 秒的時間即可使受害者上當。

人工智慧進一步放大了傳統威脅，規模更大、速度更快，以往駭客可能利用程式自動化掃描漏洞，現在 AI 工具的出現使得掃描效率倍增、攻擊更精確。例如有講者分享，在機構內部逐步採用 AI 輔助的漏洞掃描工具，同時卻也發現攻擊者同樣利用 AI 加快自動化侵入攻擊，監管機關與金融機構必須跟上此攻防賽跑的步伐，既要引導 AI 在金融業的安全運用，又要與盟友協同應對跨境攻擊。

有鑑於人為失誤常是資安事件主因，員工及管理階層的資安意識訓練尤其重要，例如針對主管建立資安風險小組、定期舉辦訓練與模擬攻擊演練以培養組織對威脅的敏感度。常見的演練情境包括央行自身系統遭受攻擊及支付系統或其他重要金融基礎設施失效。

金融機構面對的挑戰不僅在於採用 AI，更在於如何在不危及金融體系穩定與韌性的前提下使用 AI。隨著各國央行的分工不同，透過跨國合作與資訊分享才能共同保護金融生態系統的整體安全，未來必須在技術與監管層面通力合作、強化人員培訓與跨境聯防和資訊分享，並持續更新風險管理框架，才能有效應對 AI 時代下快速演變的網路威脅。

(二)人工智慧對金融與資安領域的應用與實踐，透過多模型結果結合，提升模型精確度

人工智慧普及的現代，深偽技術取得容易，各種假新聞與 AI 生成影音充斥在我們身邊，在深偽技術的偵測上，日本銀行分享了一則有關偵測深偽影片中電子

身分識別(eKYC)的研究¹，研究團隊創建了一個模擬 eKYC 的真實影片和一個使用深度偽造技術製作的虛假影片，其中某兩項技術能有效識別換臉(Faceswap)的深偽影片，但對 Avatarify 所生成的深偽影片則無法與真實影片有效區分；另一項技術雖可有效辨識 Avatarify 所生成的深偽影片，但卻也將真實影片偵測為可能的深偽影片。假影片大致可以分為兩類：FaceSwap 係將一個人的臉替換成另一個人的臉；以及重製(Reenactment)，即改變一個人的表情。研究團隊使用創建的影片評估了開源的深度偽造檢測技術的性能。該評估結果顯示目前尚無適用於所有虛假影片的通用深度偽造偵測技術，因此，結合多種偵測技術來應對各種類型的深度偽造攻擊至關重要。

來自印度科學院的教授所分享的異常交易偵測模型也令人印象深刻，該系統支援單日上億交易量的分析，並採用分散式部署架構，首先所有交易資料透過 Kafka 進入系統、Flink 負責即時流量處理、Spark 負責離線批量分析與訓練、HDFS 等分散式檔案系統儲存原始數據，機器學習工作則由 Kubeflow 等工具編排。如此的技術組合使系統能在數十台伺服器上同步處理，快速萃取和分析巨量交易。模型設計上，該系統採用圖神經網路(GNNs)與機器學習結合的方式，將整個支付網路視為一個大型交易圖，以便從交易網路中發現異常資金流模式。同時結合隱藏馬可夫模型(HMM)捕捉用戶交易狀態的轉移並使用各類神經網路深度學習行為特徵。綜合這些方法，模型能同時從整體網路和個別行為兩個角度檢測異常。目前該系統的三種模型分別可單獨偵測 50%、55%及 40%的詐欺案例，但若將多模型結果結合，則能覆蓋約 88%的已知詐欺案例。惟誤報率也是關鍵指標，講者提及，銀行不希望收到過多誤報，因此模型仍需在及早攔截詐欺與控管誤報間取得平衡。

(三)國際清算銀行(BIS)推動渡鴉計畫(Project Raven)以人工智慧輔助監管的創新方案，可做為未來推動監理科技創新的借鏡

為協助中央銀行全面檢視金融體系資安成熟度，國際清算銀行創新中心(BIS Innovation Hub)於 2024 年 4 月啟動渡鴉計畫(Project Raven)，寓意由北歐奧丁主神的兩隻渡鴉來蒐集世界資訊。該計畫設計一平台允許金融機構及其第三方廠商自行上傳資安政策文件與配置數據。AI 引擎會自動對照相關標準以產生問卷回覆與差距分析，用以量化業者的資安韌性成熟度，降低因應多重監管報告的負擔，並達成資料重複利用、一份填報可適用於多重項目的目標，有效減輕人力負擔並提升效率。監理機關更可透過 Raven 平台迅速取得金融部門整體成熟度的全景視圖，

¹ Studying Detection Methods for Impersonation Attacks on eKYC Using Deepfake Videos(https://www.jstage.jst.go.jp/article/pjsai/JSAI2024/0/JSAI2024_4M3GS1003/_pdf/-char/ja)

快速識別整體與各領域的資安弱點。例如，在一次北歐區域的網路安全調查中，多家銀行利用 **Raven** 平台填報 NIST CSF 和 ISO 27001 框架的控制項成熟度，由 AI 分析生成區域基準報告，突顯當地供應鏈管理與事件通報等共通弱點，使監管機構能即時針對相關領域強化規範與投入資源。

值得一提的是，**Raven** 計畫未來進一步整合威脅情報偵測功能，定期彙集各銀行回報的事件數據，由 AI 模型交叉比對多家機構的異常情形，以發現潛在系統性攻擊趨勢並主動提示預警及因應措施。不僅是作為靜態的成熟度評估工具，更旨在成為動態的威脅偵測與協同防禦平台。

在模型設計與風險控管方面，**Raven** 團隊重視 AI 潛在風險，由於 AI 回應助手有誤導用戶的可能性，該團隊採取多重防範機制，例如：嚴格篩選訓練數據避免偏頗、設定輸出邊界避免偏離主題，並在關鍵決策階段保留人工審核，強調 AI 僅作為輔助工具，最終評估結果仍需資安專家確認。該平台架構遵循安全最佳做法，強化存取控制和資料隔離，並邀請第三方資安機構進程式碼審查和紅隊演練，更設有多國央行代表組成的委員會和產業專家測試小組，透過公私協作與滲透測試，確保在正式部署前發現並修補安全隱患。

國際清算銀行創新中心的渡鴉計畫預計於 2026 年底推出試行版本供各國央行使用，試圖為監管機關利用 AI 提升金融系統網路韌性並透過嚴謹的治理機制為業界建立 AI 風險控管標竿，強調 AI 風險管理需前置融入架構與流程，央行在導入 AI 的同時，應遵循安全即設計(Secure by design)理念，從高層治理到技術實作都須納入風險評估，例如模型可解釋性、結果可追溯、對開源工具和第三方 AI 供應商進行嚴格審查，確保資料品質與模型完整性，並保持跨界合作與資訊共享，才能在享受 AI 創新紅利的同時，有效管控 AI 所衍生的新威脅，確保金融體系穩健。

二、建議：

(一)推動「RegTech + AI」監理科技平台

對於金融主管機關如欲應用人工智慧在場外監理上，主辦方提出以下的經驗與建議分享：儲備資源打造 AI 驅動的監理科技平台，利用大數據分析和機器學習提升監管效能。例如透過統計分析標記特定風險，當場外監理是基於數據本身時，可透過機器學習利用資料庫中的數據精確建置模型，比較不同銀行間的風險指標，建立介面並從資訊中聚合某些資料以進行比較。對於非結構化數據等文字圖像資料，則可以考慮利用 AI 工具分析並提取關鍵字。對內可設立 AI 分析實驗室並聘任資料科學家與工程師，與政府其他單位合作開發共用工具。初期可著重易於實

現的領域，例如異常交易偵測，信用評等自動化著手，逐步擴大應用範圍。此舉不僅減少監管人員重複作業，也可驗證 AI 技術在監管中的適用性。

(二)建立 AI 監理沙盒與跨部門協調機制

參考歐盟及其他國際經驗推動設立 AI 監理沙盒，提供受監管機構在受控環境中試驗 AI 創新方案，透過沙盒觀察機構創新行為對現行法規的衝擊，並根據實驗結果調整規範，同時與周邊機構、資安與產業代表定期檢視 AI 技術進展與監管政策的匹配程度，並可參考歐洲央行虛擬實驗室的作法，鼓勵跨部門共建安全的資料與演算法共享平台。

同時可參考 NIST AI 風險管理框架，制定金融業專門的 AI 風險分類與評估標準，針對不同風險級別(用途、影響程度)指定相對應的解釋性與控制要求。並推動 AI 模型註冊，要求金融機構向監理單位申報其 AI 模型資訊(用途、模型架構、訓練資料來源等)，用以明確模型可解釋性、偏誤檢測與控制措施。

(三)培育專業人才，提升監理深度與廣度

專業的培養與人力的銜接缺口也是講者和與會學員反應的困境之一。根據國際清算銀行調查，多數央行預期需要大量增聘或培訓兼具資安與 AI 技能的人才。我國應前瞻性培養跨領域專家團隊，讓傳統資安團隊學習 AI 模型原理與風險，並吸納資料科學人才加入防禦陣容，透過建立了解 AI 的資安團隊，才能有效運用 AI 工具抵禦攻擊並監督 AI 系統的安全運行。

同時，人才是 AI 監管的基石，建議可與周邊機構或學術單位合作，培養兼具金融與 AI 專業的跨域人才。透過實習、交換等計畫，增強檢查人員對 AI 的技術認知與實務經驗、了解業者的 AI 應用開發，透過多元運行的人才培育計畫，使 AI 監管工作得以持續發展。

參考資料

1. Chetan Raghuprasad (2025/9/30), “Cyber threat landscape updates”.
2. Takahiro Ebisawa (2025/9/30), “Central Bank against Cyber Threat”.
3. Victor Perez (2025/9/30), “Project Voyager”.
4. Anand Kannan (2025/9/30), “Our Journey in building AI chatbots @ BIS”.
5. Zhang Zhang (2025/9/30), “AI in Banking”.
6. William Zhang & Carina Selander (2025/9/30), “Project Raven – A Cyber-Security Assessment Tool”.
7. Yogesh Simmhan (2025/10/1), “Data Management & Anomaly Detection over Billion Scale Transactions”.
8. Sukhvir Notra (2025/10/1), “AI & implications on cyber security”.
9. Yogesh Simmhan (2025/10/1), “Emerging Trends in Agentic AI & AIOps”.
10. Randy Miskanic (2025/10/1), “Implementing an AI Risk Management Framework”.
11. Bablish Joshi (2025/10/2), “IT Outsourcing and Supply Chain Risks”.
12. Bablish Joshi (2025/10/2), “Best Practices and Common Deficiencies in Cybersecurity Implementation”.
13. Angela O’Connor (2025/10/2), “Governance of AI adoption in central banks”.