

## 論著與分析

# 「人工智慧於金融業的風險監測與監理機關的內部應用」報告

劉正淙撰擬

壹、摘要

貳、監理機關對 AI 監測的現況

參、央行與監理機關對 AI 的應用

肆、對金融機構監測上的考量與可能的監測指標

伍、案例研究：AI 的第三方依賴與生成式 AI 的供應商集中

陸、總結

## 壹、摘要

本篇係以 2025 年 10 月金融穩定委員會（FSB）「監測人工智慧在金融業的採用情況及相關脆弱性」<sup>(註1)</sup> 為主軸，並結合國際清算銀行（BIS）2025 年 10 月發布「人工智慧在政策制定上的應用」<sup>(註2)</sup> 之重點，解析監理機關對應人工智慧（AI）的觀察與挑戰；前者深入分析金融機構在使用 AI 上的風險及監理機關的監測考量，後者則著重央行及監理機關內部對 AI 的應用及挑戰。

---

本文為本公司風險管理處中級辦事員劉正淙依金融穩定委員會（FSB）「監測人工智慧在金融業的採用情況及相關脆弱性」、國際清算銀行（BIS）「人工智慧在政策制定上的應用」，並輔以相關資料編撰完成。

AI 已具備提升效率、強化法規遵循、促進資料分析及發展個人化金融產品的潛力，然而 FSB 於 2024 年「人工智慧對金融穩定之影響」<sup>(註 3)</sup> 中指出，AI 的廣泛應用亦伴隨多項潛在脆弱性，包括對第三方的依賴、服務供應商的集中、市場連動性、網路安全，以及模型與數據品質等治理風險，而 BIS 則點出 AI 人才短缺亦是一大挑戰。

FSB 應 G20 之請，彙整了問卷調查及業界意見交流等，提出一系列可用於監測金融業採用 AI 情況的相關風險指標。然而，各國金融監理機關的監測工作仍屬於起步階段，普遍面臨缺乏對 AI 統一的定義、跨國間資料缺乏可比性、難以評估 AI 對機構之關鍵程度等問題。BIS 則透過各項創新專案，探討監理機關擔任 AI「使用者」與「觀察者」的發現與應留意的面向。

兩篇報告皆強調生成式 AI (Generative AI)<sup>(註 4)</sup> 發展所帶來的利與弊，其能對洗錢防制、網路風險監控等帶來監理上幫助，然同時亦可能增加金融詐欺與市場錯誤資訊的傳播能力。

## 貳、監理機關對 AI 監測的現況

2025 年初 FSB 向會員機關發出問卷調查，收到 1 個國際組織及 19 個管轄區總計 28 份的回覆。本章將依據調查結果與相關研究，分析當前監理機關對 AI 的監測情形。

### 一、監測模式

多數監理機關均有蒐集金融業對 AI 採用情況的資料，最常見的資料蒐集方式為問卷調查，其次是透過公開資料進行研究，另有部分參考私部門資料供應商的資訊。然而各監理機關的回覆中，對 AI 的定義並不一致：部分採取經濟合作暨發展組織 (OECD) 或歐盟的定義，部分則依據國內自訂之法規，且有少數尚未對 AI 明確定義。

蒐集的問卷多數屬於自願填答，資料蒐集對象通常涵蓋不同規模的金融機構，但有些僅針對大型機構調查。各監理機關對 AI 相關的調查多屬非常態性的，惟約有半數監理機關會公布調查後彙整的結果，而有部分亦採用其他監測方式，例如：建立金融業 AI 應用之清單、透過創新中心（innovation hubs）與業界對話、從監理訪談中蒐集質化資訊，以及分析金融機構之職缺與公開資訊。

## 二、脆弱性監測

相較於掌握金融業對 AI 的採用與應用，要對 AI 帶來的脆弱性進行監測更加困難。以下揭示多數監理機關監測脆弱性的項目、方法與發現：

表 1 脆弱性監測

脆弱性	監測方式與調查發現
對第三方的依賴與服務供應商的集中	多數問卷均有納入此項的調查，以了解依賴程度及與外部供應鏈的關係；少數機關更進一步調查機構對 AI 應用的關鍵性程度，並詢問金融機構在採用第三方 AI 服務供應商時所面臨的挑戰。
市場連動性	僅有少數機關蒐集 AI 決策對市場變化的連動關係，其中尤其關注跨機構間使用相似 AI 模型與數據來源會對市場的影響；須留意若機構間皆使用相同供應商之模型與數據，AI 是否會做出相同的判斷，而有「羊群效應（herding behaviour） <sup>（註 5）</sup> 」的系統性風險。
網路安全	調查網路資安相關事件與 AI 之相關性，要求金融機構說明其與 AI 相關之網路脆弱性及防護措施。
模型風險、數據品質與治理	多數問卷中均有詢問機構關於 AI 的治理機制、模型管理風險等，其中關注機構對 AI 模型決策可解釋性（explainability） <sup>（註 6）</sup> 的因應做法。

### 三、具體監測機制

#### (一)問卷

為最普遍之監測手段，這類調查為監理機關提供具體的統計基礎，然問卷調查仍存在限制，如回覆率差異、樣本偏差等問題。

#### (二)產業交流

常見方式包括研討會、工作坊，邀集產官學界參與，部分監理機關與大型科技公司合作設立創新中心或監理沙盒（regulatory sandboxes），以蒐集實務經驗與新興應用案例。

有些監理機關會定期向機構發出有關 AI 的「資訊索取（Requests for Information）」，然機構可能不願公開具體資訊。因此，監理機關亦可考慮「閉門會議」，與金融業相關利害關係人進行保密性的討論，以作為更深入的工作分析補充。

#### (三)公開資料與商業資料來源

這些資料包括企業問卷調查、專利申請、公開資訊揭露、工作職缺資訊等，它們在監測 AI 時具有重要價值，且這些資料不會增加金融機構的申報負擔，且可涵蓋不同規模與類型的金融機構，有助於呈現整體之多樣性。

表 2 監測資料來源

資料來源	監測說明
商業調查	專業的調查機構對各類金融機構進行 AI 相關議題的調查；美國 Business Trends and Outlook Survey 發現，證券與投資類金融機構的 AI 使用率最高。
AI 相關專利申請	了解金融業申請有關 AI 專利之應用種類及發展趨勢。

資料來源	監測說明
公開資訊揭露	對公開資訊（如股東年報、財報及會議紀錄與公告文件等）進行文字分析。
工作職缺	觀測金融業對 AI 相關職務所開設之職缺。

然而，這些資料指標也存在一些缺點，其內容往往缺乏針對性，無法明確反映營運效率、風險管理或 AI 在核心業務中的關鍵程度，目前多數指標著重於「採用率」，而非與特定脆弱性相關，因此 FSB 建議，在使用這些資料時應採綜合性分析，結合多元資料來源，以確保評估結果能更全面地反映金融體系中 AI 採用的情況與脆弱性。

### 參、央行與監理機關對 AI 的應用

根據調查，多數央行於過去三年間顯著提升對 AI 或機器學習（Machine Learning）的專案預算，約三分之一的受訪央行預期未來三年內將超過 5% 的業務預算投入 AI 相關項目，反映 AI 已成為重要的基礎設施，而央行大多將 AI 應用在經濟研究、貨幣政策、統計分析及金融監理等。

BIS 的「極光計畫（Project Aurora）」展示了 AI 對洗錢防制所帶來的潛力，計畫採用圖神經網絡（Graph Neural Network）<sup>（註 7）</sup>，結合隱私保護技術（如聯邦式學習<sup>（註 8）</sup>），進行跨國交易的比對分析。AI 模型可以偵測更複雜的洗錢模式，而這些模式過往常難以透過單一銀行的核對來發現。研究結果顯示，該方法檢測到複雜洗錢案件的數量可達傳統方法的三倍，同時將誤報率降低近 80%。

同時 BIS 點出，客製化模型的建置並使用特定專屬領域的資料，能比未經調校的一般 AI 基礎模型達到更高的準確度，如 BIS 的央行語言模型專案（Central Bank Language Model Project）透過收錄央行的演講稿和研究論文來調校 AI 模型，使模型對貨幣政策相關的專業術語分析準確率從約 60% 提

高至近 90%。

針對 AI 的內部使用，央行最關切的風險為隱私、網路安全與可解釋性等議題，此些與 FSB 監測金融機構的 AI 風險多有契合。而 BIS 更進一步點出人才短缺是 AI 內部應用到外部監測時的一大挑戰，近九成央行表達在招募 AI、金融科技與資安人才上遇到了困難。且央行及金融機構在生成式 AI 的應用上仍須留意民眾的「信任度」，據調查相較於 AI 所做的決策，民眾當前對人為決策仍是較為信任的，民眾尤其擔憂資料外洩及濫用的風險，因此強化 AI 治理與透明度也成為一大考驗。

## 肆、對金融機構監測上的考量與可能的監測指標

### 一、設計資料蒐集時的考量

以下設計原則可協助監理機關在可行性與監測精度之間取得平衡，並依各國之情況適度調整之：

表 3 監測上的考量

考量因素	說明
與脆弱性之相關性	可參考 FSB 於 2024 年發布之「人工智慧對金融穩定之影響」其中有關脆弱性的相關指標。
代表性	涵蓋不同類型金融機構（依業務類別、規模等），以反映整體 AI 採用狀況。
標準與分類一致性	監理機關應盡可能與國際標準或相關監理機構的定義接軌，以提升資料的明確性與可比性。
時效性	定期蒐集資料至關重要，以避免資訊過時；然應採取彈性的方式，以利監測機制能隨時因應技術環境的變化而調整。

考量因素	說明
監理與申報之負擔	盡可能降低資料蒐集所帶來的負擔與成本，監理機關可在既有的申報架構下，促進監理機關間的資料共享，避免重複作業並提升樣本代表性。

## 二、挑戰與潛在的因應對策

### (一)挑戰

1. 定義與可比性：一些機構將外部購得但經自行修改的模型視為「第三方模型」，另一些則歸類為「內部開發模型」。
2. 監測範圍與成本：許多 AI 服務供應商不在金融監管範圍內，使得追蹤其活動之能力受限。此外調查結果顯示，不到半數機關能每年進行收集資料，反映出資源與人力上的限制。
3. 各項 AI 服務的關鍵性評估：評估服務在營運中的關鍵性極具挑戰，需深入理解 AI 與營運流程的交互作用，以及全體金融體系對特定供應商、模型或訓練資料的依賴程度。單純的問卷調查通常不足以滿足此需求。

### (二)因應對策

1. 由國際組織主導，建立具一致性的 AI 分類方式與指標。
2. 簡化問卷設計，聚焦高價值問題以減少負擔並提高回覆率。
3. 結合質化訪談並借助全球監理合作倡議，以提升監測深度與資訊互通。
4. 發布 AI 金融應用之監理指導原則、強化與業界之交流，並建立標準化通報機制，且監理機關可考慮更具效率地將 AI 監測問題整合進既有的監測框架裡。

### 三、 監測指標與監測困難

#### (一) 監測指標

為協助監理機關因應前述挑戰並有效追蹤 AI 發展，以下將介紹一系列潛在之監測指標。

表 4 監測指標

監測標的 或風險	建議指標與內容
AI 採用情況 (直接指標)	<ol style="list-style-type: none"> <li>1. 建立機構之 AI 應用清單                             <ol style="list-style-type: none"> <li>(1) 應用類型：放款、保險、支付等。</li> <li>(2) AI 技術：生成式 AI、代理式 AI<sup>(註9)</sup> 等。</li> <li>(3) 關鍵程度：核心業務、低風險內部作業等。</li> </ol> </li> <li>2. 採用 AI 之機構比例 追蹤不同規模與性質的金融機構使用 AI 的比率與趨勢。</li> <li>3. 質化資料 從產業交流、公開文件（如年報與新聞稿）取得，以補充量化統計。這些資料有助於辨識主要應用方向、共通挑戰以及導入方式（如與外部供應商合作或自行開發）。</li> </ol>
AI 採用情況 (間接指標)	<ol style="list-style-type: none"> <li>1. AI 專利申請數量 機構申請專利的數量可反映對創新活動與技術投入的程度。</li> <li>2. AI 相關職務之趨勢 透過第三方資料或研究機構彙整之 AI 職務需求變化，了解金融業對 AI 技能與人力的需求。</li> <li>3. 研究發展支出 參考財報中的研究發展支出，並可結合文字分析（如投資人報告、會議紀錄），評估 AI 在機構裡的重要性與投入程度。</li> </ol>

監測標的 或風險	建議指標與內容
對第三方的依 賴與使用服務 的供應商集中	<ol style="list-style-type: none"> <li>1. 多少比例使用第三方提供之 AI</li> <li>2. AI 服務供應商清單</li> <li>3. 多少系統性重要銀行使用第三方提供之 AI</li> <li>4. AI 服務的成本與效能 透過公開來源（如大型語言模型排行榜、供應商網站或性能報告）比較主要 AI 服務的成本與效能，以衡量可替代性與市場集中風險。</li> </ol>
市場連動性	<ol style="list-style-type: none"> <li>1. 機構使用同一特定預訓練模型的數量與特徵 追蹤各機構使用相同或類似預訓練模型的情況（如模型類型、結構設計、訓練資料或目標函數），倘多家機構依賴少數模型與資料庫，則可能放大市場連動性。此指標有助於衡量模型集中度與潛在行為趨於相同之風險。</li> <li>2. AI 採用與資產價格波動的關聯分析 由統計或分析方法（如迴歸分析）評估 AI 的採用與市場波動之關聯性。監理機關可與學術界合作，共同發展具實證基礎的觀測指標。</li> <li>3. AI 自動化程度 探索 AI 之自動化交易、信貸審核等，若自動化程度高且人為干預較少，AI 驅動的市場連動風險可能上升。</li> </ol>
網路安全	<ol style="list-style-type: none"> <li>1. AI 相關外部攻擊事件數量</li> <li>2. AI 相關內部事件 如將敏感資料外洩至外部 AI 工具，或內部 AI 應用系統存在漏洞。</li> <li>3. 第三方供應商的 AI 相關事件數量 追蹤 AI 供應商（如雲端平台、模型開發商）所發生的網路事故。</li> <li>4. AI 防禦系統的應用 建立 AI 防禦系統的使用登錄資料庫，協助監理機關與機構辨識並推廣有效防禦的應用。</li> </ol>

監測標的或風險	建議指標與內容
模型風險、數據品質與治理	<ol style="list-style-type: none"> <li>1. 機構模型庫中 AI 模型的占比 蒐集受監理機構之模型清冊資料，以衡量 AI 模型在整體模型應用中的比例，並可進一步區分高風險與低風險應用</li> <li>2. 透過金融檢查挖掘與 AI 相關之風險與趨勢 透過檢查建立彙總指標，如年度內涉及可解釋性或資料治理缺失的案件數量，此趨勢資料有助監理機關掌握系統性弱點的演變。</li> </ol>
AI 驅動的金融詐欺與假訊息	<p>此類活動可能削弱信任、放大市場波動，甚至引發瞬間崩盤或擠兌，此類風險多源自外部行為：</p> <ol style="list-style-type: none"> <li>1. AI 驅動的金融詐欺事件 追蹤生成式 AI 的詐欺數量（如深偽影像）。除事件統計外監理機關應評估金融機構的防詐能力（如是否運用 AI 進行異常交易偵測）。</li> <li>2. 假訊息 包括假新聞、影響投資人行為與市場情緒的資訊干擾事件，追蹤此類事件的頻率與傳播範圍，有助於識別有哪些高風險的資訊流。</li> <li>3. 與 AI 詐欺及假訊息相關的客訴 消費者的投訴資料可作為 AI 詐欺與假訊息活動上升的早期訊號。</li> </ol>

## (二) 監測困難

AI 不對齊 (Misaligned AI systems) 係指 AI 系統的輸出或決策過程，與開發者或使用者的設定原則產生偏離，導致違規或不符合道德規範的結果。造成此狀況的原因包含 AI 模型缺乏可解釋性、訓練資料來源不透明以及模型複雜性提高等。

隨著模型的逐漸演進，監理機關越來越難以掌握模型的運作及其風險，其中包含大型語言模型輸出的正確性難以驗證及其回答的偏誤，如 AI 模型試圖填補不確定資訊時，自信地產生錯誤、虛構或無意義內容的幻覺（hallucination），更是為考證資訊正確性帶來難度。

## 伍、案例研究：AI 的第三方依賴與生成式 AI 的供應商集中

觀察顯示，金融業對生成式 AI 的依賴與集中現象普遍較其他 AI 技術更為顯著。生成式 AI 常仰賴預訓練模型為基礎，而這些模型需要有專用「硬體」與「雲端服務」支撐其開發與運行。然金融機構自行研發此類模型將面臨極高的成本與人才取得障礙，以致在實務上往往只能在「採用外部模型」與「不採用」間做出選擇。

同時，隨著生成式 AI 的持續擴張與應用，金融機構對生成式 AI 模型供應商的第三方依賴程度亦可能進一步上升，且須留意更上游的「次級供應商（nth-party）」出現營運事故、網路攻擊或供應鏈中斷時，金融機構的業務穩定性亦可能受到實質影響。後文將進一步探討監理機關目前如何監測這些關鍵脆弱性，並說明如何運用「第三方風險管理指引（Third-Party Risk Management Toolkit）」來建構更具體的監測。

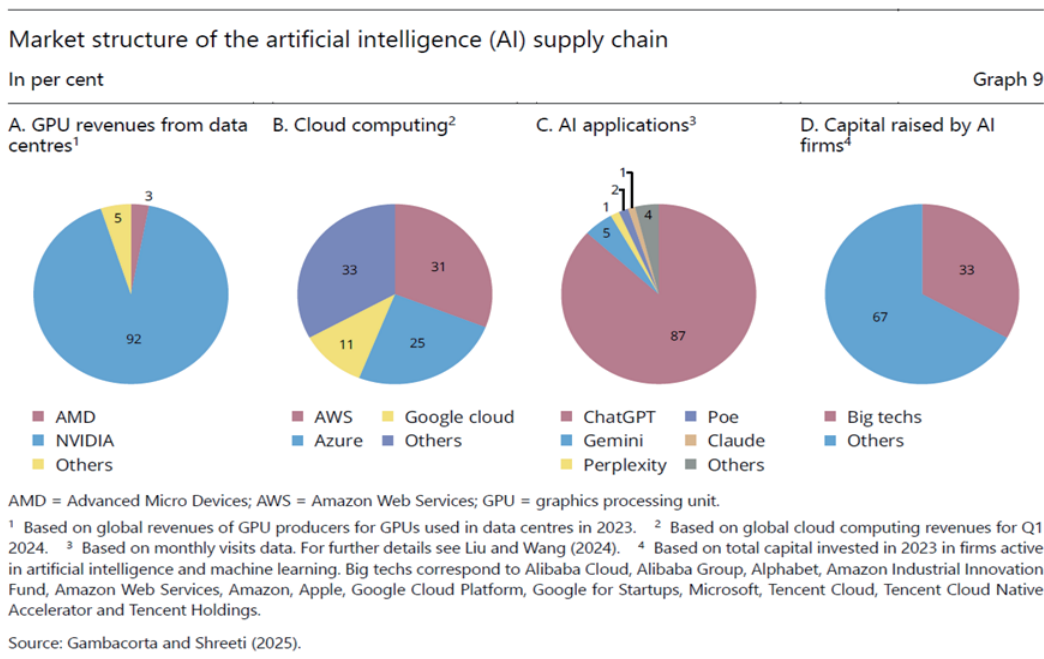
### 一、生成式 AI 的供應鏈

生成式 AI 供應鏈的結構將決定金融機構在使用時，第三方的依賴與服務供應商的集中度如何交互影響其營運脆弱性。整體而言生成式 AI 供應鏈可分為五個主要層面：

表 5 生成式 AI 供應鏈

供應鏈	說明
硬體	訓練與執行 AI 模型所需的運算晶片，如圖形處理器（GPU）及其他 AI 專用晶片。此類是目前 AI 供應鏈中最集中化的環節，少數大型供應商掌握主導地位。
運算基礎設施	主要由雲端服務構成。此類高度集中於少數科技巨擘，這些企業受惠於早期大規模投資形成的高進入門檻、高使用者轉換成本以及其垂直整合解決方案（vertically integrated solutions）帶來的競爭優勢。
訓練資料	大型資料庫的建構與管理耗費龐大資源。現行供應商多數擁有既有資料管道與大量使用者，藉由規模經濟與網絡效應強化優勢，達成資料越多、服務品質越好、吸引更多使用者並產生更多資料的「大者恆大」。
基礎預訓練模型	這些供應商常享有「先行者優勢（first-mover advantage）」，透過早期累積的資源、品牌知名度等使其難以被挑戰。不過較小型的開放權重模型（open-weight models）已逐漸出現，有望降低部分進入門檻。
用戶應用程式	此集中度通常源於數據優勢、聲譽優勢以及將人工智慧功能整合到現有軟體生態系統中所帶來的益處（如少數平台可能壟斷了客戶關係管理工具的市場）。

圖 1 AI 供應鏈的市場結構



科技巨擘對硬體、雲端與模型服務的垂直整合，可帶來便捷與高效能的解決方案，然高度集中的供應鏈結構意味著可替代性的受限，並限制了跨平台的互通性（interoperability）、推高轉換成本，且可能因單點故障（single point of failure）而引發巨大的風險。圖 1 點出，當前 AI 模型所需的圖形處理器完全由輝達主導，雲端計算由亞馬遜、微軟及谷歌累積涵蓋了三分之二的市占，AI 應用則由 ChatGPT 占有領先地位（市占 87%）。

小型語言模型（Small Language Models, SLMs）因訓練與調校所需的資料與運算資源大幅低於大型模型，亦被視為減輕依賴與集中風險的潛在替代方案。然金融機構若同時仰賴過多不同供應商，其基礎設施也可能變得複雜且難以有效管理。

## 二、現行監測下的發現

(一) 2024 年英國金融業中有 33% 的 AI 應用依賴第三方的提供，高於

2022 年的 17%。

(二) 瑞士金融市場監理局 (FINMA) 的調查顯示，雖然部分公司自行開發 AI 應用，但多數仍同時使用外部供應商提供的服務，且許多中小型機構完全依賴外部 AI 服務。

(三) 國際證券管理機構組織 (IOSCO) 與國際貨幣基金 (IMF) 一致指出：供應商集中與第三方依賴是 AI 使用過程中最主要的脆弱性之一。

### 三、須關注的重點監測面向

「第三方風險管理指引」提出了一系列監測要點，用以識別與金融機構採用 AI 相關的潛在風險。這些要點單獨存在時未必構成系統性風險，但若在服務中斷或失效的情境下相互作用，則可能引發更廣泛的金融不穩定。FSB 認為最須關注的幾項要點如下：

表 6 重點監測面向

監測面向	說明	潛在監測來源
關鍵性	關注該 AI 服務若發生故障或中斷，是否可能嚴重損害機構的存續能力及關鍵營運。	1. 依機構申報資料，建立 AI 服務及其供應商的關鍵性登錄表。 2. 問卷調查關鍵 AI 應用的數量。 3. 國際機構於報告中列示的關鍵 AI 服務與供應商。
集中度	不論機構規模之大小，關注其是否過度依賴單一或少數第三方 AI 服務供應商。	1. 第三方 AI 業務占整體之比例。 2. 關鍵 AI 服務由單一或少數供應商提供的數量。 3. AI 各層供應鏈（硬體、基礎設施、資料等）之市占率。

監測面向	說明	潛在監測來源
可替代性	AI 服務若能輕易替代或轉換，則其關鍵性相對較低；相對難以替代的服務則在中斷時恐造成重大衝擊。	1. 常用 AI 服務的成本與效能比較。 2. 在不同 AI 服務間轉換的時間與成本估計。 3. 機構使用多少垂直整合之 AI 系統。

## 陸、總結

### 一、當前的觀察

本報告檢視了金融機構採用 AI 及其相關脆弱性之監測情形，並透過建議之監測指標及「第三方風險管理指引」，協助監理機關辨識與因應潛在之風險。當前最常見的資料蒐集方式為問卷調查，然對 AI 脆弱性之了解仍屬起步階段，未來若能更有效地將指標對應至特定脆弱性、確保定期資料蒐集，並彌補第三方依賴、市場連動性等關鍵領域的監測缺口，將有助於全面強化監理工作。

### 二、對監理機關之建議

- (一) 監理機關本身亦需運用並探索 AI 工具之利與弊。
- (二) 與金融機構及 AI 業者多方交流，深入了解 AI 相關脆弱性，尤其是難以量化指標之領域。
- (三) 國內監理機關間建立更廣泛的資料共享。
- (四) 跨境合作，促進 AI 監測指標的一致性與可比性。
- (五) AI 作為自動化的輔助，最終仍是要有人為介入、由專家督導 AI 的運作與決策。

## 參考文獻

1. BIS (2025), “The use of artificial intelligence for policy purposes”.
2. FSB (2025), “Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector”.
3. Gambacorta, L. et al (2024), “CB-LMs: language models for central banking,” BIS Working Papers, no 1215.
4. Gambacorta, L and V Shreeti (2025): “The AI supply chain,” BIS Papers, no 154.

## 註釋

註 1： Monitoring Adoption of Artificial Intelligence and Related Vulnerabilities in the Financial Sector

原文網址：<https://www.fsb.org/uploads/P101025.pdf>

註 2： The use of artificial intelligence for policy purposes

原文網址：<https://www.bis.org/publ/othp100.pdf>

註 3： 詳如本公司存款保險資訊季刊第 38 卷第 2 期－金融穩定委員會（FSB）「人工智慧對金融穩定之影響」摘要報告。

註 4： 能生成新內容（如文字、影像、影片等）的 AI，通常依使用者的提示（Prompt）來運作。此類 AI 常見的基礎模型如大型語言模型（LLMs）。

註 5： 經濟學裡常用此描述經濟個體的群聚行為，會一窩蜂地做出相同反應；實例佐證說明：2005 年 7 月土耳其東部有 1,500 多隻綿羊原本在崖邊吃草，其中 1 隻羊不知何故突然跳下懸崖，其餘所有綿羊便不明就裡地集體跟進（資料來源：中央銀行／貨幣金融知識專區）。

註 6： 人工智慧模型提供清晰且可解釋的輸出或決策之能力。

註 7： 是一種專門用處理結構型數據的深度學習模型，它能利用節點（Node）與邊（Edge）所包含的關係，透過訊息傳遞計算並整合相鄰的特徵，最終能學習到整個圖或節點的樣態；在處理複雜關聯數據時具有優勢，能有效地預測和識別不尋常的樣態。

註 8： 允許多國協作訓練一個模型，但將原始數據保留在當地，可尊重數據主權，

但同時仍能獲得數據匯集的好處，使機器學習演算法能夠擁有「全視角」，從而偵測到單一銀行可能遺漏的複雜跨機構連接和洗錢模式。

註 10：指能自主執行複雜且長期任務的 AI 系統，通常可在有限人為監督下自行決策與採取行動。

註 11：公開其學習參數（權重與偏差值，weights and biases）的 AI 模型，使開發者能對特定應用進行微調。可提升靈活性、減少對第三方模型的依賴，並有助於分散 AI 生態系統的集中風險。