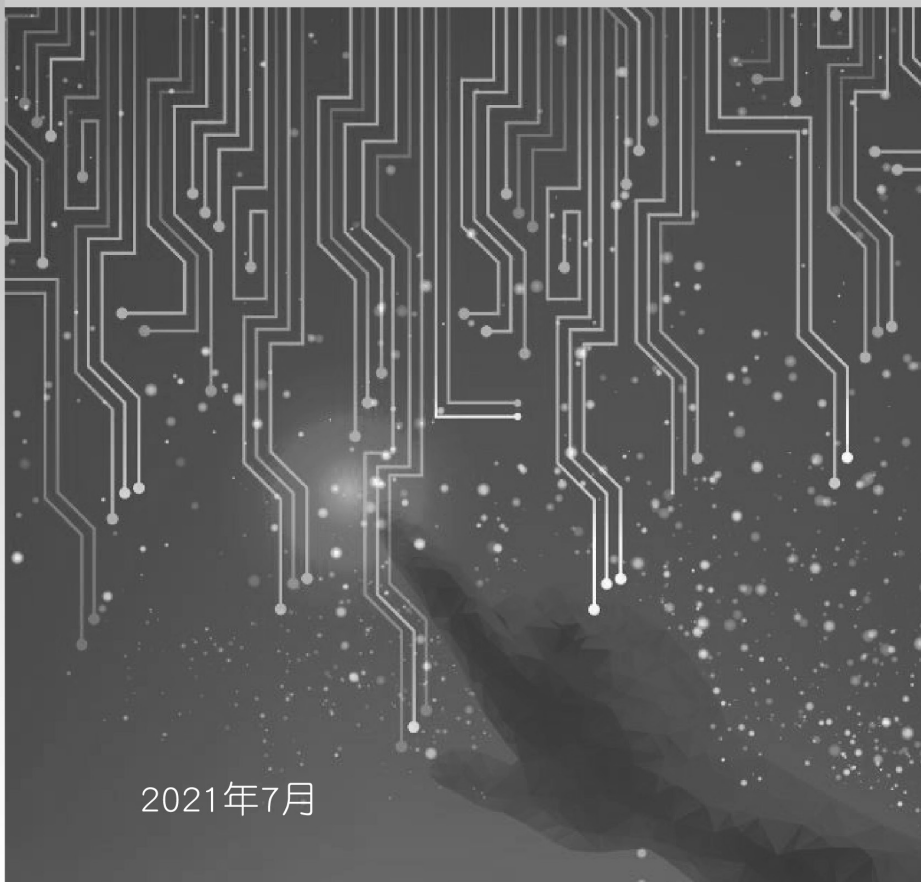
FATF

運用新科技於洗錢防制及打擊資恐之機會與挑戰



2021年7月

防制洗錢金融行動工作組織（FATF）是一個獨立的跨國組織，旨在發展與提升政策，保護全球性金融體系，以對抗洗錢、資恐以及資助大規模毀滅性武器擴散之政策。FATF 建議已成為全球防制洗錢（AML）與打擊資恐（CFT）的公認標準。

如欲進一步瞭解 FATF，請造訪網站： www.fatf-gafi.org

本文件及／或本文所含的任何地域，概不影響任何領土的地位或主權、國際疆界之界定，或任何領土、城市或地區之名稱。

引用文獻：

運用新科技於洗錢防制及打擊資恐之機會與挑戰，FATF 2021 於法國巴黎
https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-new- technologies-aml-cft.html

封面照片取自：蓋蒂圖像

致謝詞

FATF 要感謝公共和私部門的利益相關者，包括科技開發商、金融機構和其他專家，為本報告提供寶貴意見、案例研究及意見回饋。

本報告之工作由 FATF 秘書處（Inşs Oliveira）領導，並由下述 FATF 代表團之專家小組提供重要建議：加拿大、丹麥、歐洲委員會、埃及、德國、以色列、義大利、日本、馬來西亞、俄羅斯聯邦、評估防制洗錢措施特設專家委員會秘書處、新加坡、英國、聯合國和美國，還有歐洲刑警組織及歐亞防制洗錢與反恐融資組織（EAG）秘書處。

目 錄

縮寫對照表

AI	Artificial intelligence 人工智慧
AML/CFT	Anti-Money Laundering/Countering the Financing of TerrorismAML/CFT
API	Application Programming Interface 應用程式介面
CDD	Customer Due Diligence 客戶盡職調查
DL	Deep Learning 深度學習
DLT	Distributed Ledger Technology 分散式帳本科技
DNFBP	Designated Non-financial Business and Profession 指定之非金融事業或人員
FATF	Financial Action Task Force 防制洗錢金融行動工作組織
MER	Mutual Evaluation Report 相互評鑑報告
ML/TF	Money Laundering/Terrorist Financing 洗錢／資恐
MVTS	Money or Value Transfer Service 金錢或價值移轉服務
NLP	Natural Language Processing 自然語言處理
NRA	National Risk Assessment 國家風險評估
PEP	Politically Exposed Person 重要政治性職務之人
PSCF	Private Sector Consultative Forums 私部門諮商論壇
SSB	Standard Setting Body 標準制定機構
VASP	Virtual Asset Service Provider 虛擬資產服務提供商

執行摘要

1. 新科技具有使防制洗錢（AML）和打擊資恐（CFT）的措施更快、更便宜且更有效的潛力。它們可以改善 FATF 標準的實施，以推進全球 AML / CFT 工作，確保金融普及性並避免無意之間將經濟弱勢排除於金融服務之外。
2. 作為全球 AML / CFT 標準的制定者，FATF 下定決心要跟上金融部門的創新科技和商業模式，同時確保全球標準保持最新，並實現既能夠應對風險又達到負責任創新的 " 智能 " 金融部門監管。因此，FATF 審核運用新科技於 AML / CFT 之機會與挑戰，以提高對創新和具體數位解決方案的相關進展的認識。FATF 另外還研究實施這些科技方面持續存在的挑戰和障礙，以及如何緩解這些挑戰。該專案包括對監管科技（RegTech）和監理科技（SupTech）的審查和分析，這兩類科技可以提高 FATF 標準的有效性。
3. 創新的技能、方法和流程，以及使用既定科技流程的創新方式，可以協助監管者、監督者和被監管機關克服許多已知的 AML / CFT 挑戰。科技可以促進資料蒐集、處理和分析，並幫助參與者更有效和更即時地識別及管理洗錢和資恐（ML / TF）之風險。更快的支付和交易、更準確的辨識系統、監控、記錄保存以及主管當局和受監管機構之間的資訊分享也提供有利條件。
4. 在 AML / CFT 方面更多地使用基於人工智慧（AI）及其不同分支科技（機器學習、自然語言處理）之數位解決方案，可能更有助於辨識風險，應對、溝通及監控可疑活動。在公部門層面，改進的即時監控和與對應方的資訊分享能夠對受監管機構進行更明智的監督，幫助改善監管。在私部門層面，科技可以改善風險評估、客戶引導、與主管機關的關係、可稽核性、當責制和整體良好治理，還能節約成本。

5. 報告指出與開發、採納和應用這些創新解決方案或實施之相關挑戰。其中許多挑戰是由於傑出的業務和監管束縛，如傳統的 AML / CFT 合規系統和傳統的監管架構和監督機制。其中許多挑戰是由於突出的運營和監管限制，例如傳統的 AML / CFT 合規系統和傳統的監管框架和監督機制。
6. 替換或更新舊系統所涉及的複雜性和成本，使企業和政府在利用 AML / CFT 的創新方法的潛力面臨挑戰。對金融行業而言，採用新科技的成本效益分析仍然是廣泛採用 AML / CFT 創新解決方案的障礙，部分原因是實際或認知上缺乏追求創新的監管激勵。數位解決方案的可解釋性和可理解性方面的困難是金融行業和監理機關面臨的另一個重大挑戰，部分原因是相關的專業知識有限，以及金融行業和政府中的 AML / CFT 專業人士尚未意識到創新科技的潛力。在本報告所提供的資訊和分析的基礎上，加強公部門與私部門之間的溝通與合作，同時強調負責任地採用新科技，特別是在資料保護法規方面的有效性，將是克服這些挑戰和充分實現負責任的創新以加強 AML / CFT 措施有效性的關鍵。
7. 如果以負責任且適當之方式使用，AML / CFT 的創新科技可以幫助識別風險，並將合規工作集中在現有和新出現的挑戰上，但人工審查和人工介入仍然非常重要。例如，即使是在一個科技支援的監管環境中，也必須依靠人力來識別和評估新科技帶來的任何剩餘風險，並制定適當的緩解措施。將數位解決方案的效率和準確性與人類專家的知識和分析技能相結合，可以產生更強大的系統，在完全可審計和可當責下有效地應對 AML / CFT 的要求。
8. 運用新科技及創新可以幫助公部門與私部門提高其執行 FATF 標準要求之風險基礎法的有效性。對這些科技的開發、採用和監管監督必須反映出威脅和機會。它還必須確保創新工具的使用符合資料保護、隱私和網路安全的國際標準。

1. 簡介

9. FATF 的標準，是一個根據持續變化的全球洗錢和資恐（ML / TF）威脅、弱點和風險，以及在實施過程中出現的挑戰而不斷發展的工具。客戶盡職調查（CDD）和相關程序在最初採用的 30 年後，大大增加交易的透明度，使犯罪分子、資助恐怖主義者和資助武器擴散者更難濫用金融產品。同時，儘管客戶識別／核實和監控是 AML / CFT 架構的一個關鍵支柱，但它仍然存在實施上和有效性方面的挑戰。

10. 不以風險為基礎的客戶盡職調查工作可能被認為是昂貴且低效，因為它們不只浪費資源且往往不能轉化為準確的風險評估或讓客戶順利獲得金融服務。認識到創新步伐的加快、數位轉型對金融系統的深遠影響以及對 FATF 標準對有效性的追求，FATF 發起一項倡議，檢驗新科技在減輕洗錢和資恐威脅方面的潛力。

11. 在本報告中，" AML / CFT 之新科技 "[1] 指的是。

    a 用於實現關於有效執行 AML / CFT 要求的目標的創新技能、方法及程序，或

    b 利用既定的科技程序遵守 AML / CFT 義務的創新方法。

12. 與使用傳統方法和程序相比，新科技力求提高 AML / CFT 部分措施的速度、品質或效率和成本，以及更廣泛地實施 AML / CFT 架構的成本。最相關的科技是跨領域的，能夠以新的數位方式蒐集、處理及分析資料。這些科技還允許通過各種具體的解決方案來交流資料和資訊。這些能力可以以重疊的方式應用，並針對廣泛的

---

1 在本報告中，數位解決方案、數位工具、創新解決方案或系統等術語可互換使用，且本段所定義的用於 AML / CFT 之新科技也適用。

AML / CFT 目標。這些新科技的許多能力和影響在很大程度上仍是未知的，也就是說，瞭解它們目前的能力及對 AML / CFT 的潛在影響至關重要。

13. 例如，數位身分解決方案可以實現非面對面的客戶識別／驗證和資訊更新。它們還可以改善對客戶的認證，以便更安全地登入帳戶，並在產品導入和交易時加強識別和認證，促進普惠金融的同時，打擊洗錢、欺詐、恐怖主義融資和其他非法融資活動。

14. 又如，自然語言處理可以對客戶資訊進行更準確、更靈活、更及時的分析，減少不準確或錯誤的資訊，並能更有效地匹配和搜尋其他資料。更佳且更新的客戶資料代表更準確的風險評估，更好的決策，以及非故意的金融排斥情況更少。

15. 同樣，將基於人工智慧（AI）和機器學習（ML）科技的解決方案應用於大數據，可以加強對可疑交易的持續監控和申報。這些解決方案可以自動監控、處理和分析可疑交易和其他非法活動，即時將其與正常活動區分，同時減少對第一線人工審查的需求。人工智慧和機器學習的工具或解決方案還可以對正在進行的客戶盡職調查和客戶風險產出更準確和更完整的評估，這些評估可以在新的威脅出現時進行即時更新。然而，人工智慧／機器學習解決方案在科技和使用上都有極大差異，可能會帶來重大風險，本報告後面將討論這些風險。

16. 同樣，採用創新的解決方案，如應用程式介面（API）和分散式帳本科技（DLT）、資料標準化和機器可讀法規，可協助受監管機構[2] 更有效地向監管者和其他主管機關報告。這些科技還允許監

---

2 在本報告中，"受監管機構"在 FATF 標準所定義係指金融機構、虛擬資產服務提供商（VASP）和指定之非金融事業或人員（DNFBP）。

理機關、執法部門或其他主管部門向受監管機構及其客戶發出警報、申報之後續處理和其他溝通，以及受監管機構之間、受監管機構與其客戶之間的溝通。監理機關應用更先進的分析科技也可以加強檢查和監督，包括可能提供更準確和即時的回饋。

17. 在某些情況下，由於擔心是否及如何根據 FATF 的建議及各國的 AML / CFT 其監管架構運用創新科技，阻礙採用新科技 AML / CFT 的合規與監管。

1.1. FATF 對負責任的創新和數位轉型的承諾

18. 作為一個全球標準制定機構（SSB），FATF 致力於緊跟金融部門的創新科技和商業模式，並確保全球 AML / CFT 標準在數位轉型加速的環境中保持相關性和有效性。這樣，FATF 的要求才能實現 " 智能 " 金融部門監管，幫助推動負責任的創新，以促進 AML / CFT 並達到普惠金融目標。

19. FATF 於 2017 年 11 月 3 日在布宜諾斯艾利斯發表公開聲明，正式認可負責任的 AML / CFT 的金融創新，該聲明宣佈：
" FATF 全力支持符合金融行動特別工作組標準中的 AML / CFT 要求的負責任金融創新，並將繼續探索新的金融與監管科技可能帶來的機會，以有效改善 AML / CFT 措施的執行。"

20. 2017 年支持負責任的創新的公開聲明建立在 FATF 先前的努力之上，同時應對潛在非法金融風險和新興科技帶來的 AML / CFT 之監管和監督挑戰。包括發佈許多指南及最佳實務文件，更新建議以解決虛擬資產產生的問題（FATF，2019[1]），以及通過公私研討會及 FATF 的私部門諮詢論壇（PSCF）與私部門廣泛接觸。

21. 通過其他國際聲明可見負責任的創新已得到支持，即聯合國安全理事會第 2462（2019）號決議（聯合國，2019[2]），該決議呼籲所

有國家加強金融交易的可溯源性及透明度，包括通過充分利用新的金融和監管科技來改善普惠金融，並促進有效實施 AML / CFT 措施。

22. 儘管有眾所周知的好處，但在 AML / CFT 面向上有效利用創新科技受到各種因素的限制，在不同程度上影響不同的受監管機構和監管者。

23. FATF 輪值主席國德國將創新科技作為其首要任務之一，發起一項數位轉型倡議，其中包括三個項目。

- 本報告所依據的研究，審查新科技的機會和挑戰，以使私部門和監管人員更有效地實施 AML / CFT 措施。
- 對營運機構的機遇和挑戰之研究，使系統偵測及調查洗錢與資恐以及瞭解洗錢／資恐的風險，更有效率，以及
- 關於資料庫、協作分析和資料保護科技的盤點，旨在幫助私部門改善其在 AML / CFT 方面對人工智慧和大數據分析的使用，提高監管合規的效率，同時確保高水準的資料保護。

24. FATF 主席已將這一議程提交給國際論壇，強調其對增進 FATF 的標準之執行及 AML / CFT 的有效性之重要性（FATF，2020 年[3]）。

25. 本報告的目標是

- 增進認識並發掘利用新科技及新的及現有科技解決方案的機會。
- 確定有助於支持進一步採用新科技的條件、政策和作法，這些科技有助於按照各司法管轄區的監管制度提高 AML / CFT 工作的效率與效力，並通過案例研究加以闡明。

---

3 許多 FATF 關於金融科技和監管科技的立場、參與和相關文件可在其網站上找到，詳： www.fatf-gafi.org/fintech-regtech/fatfonfintechregtech/.

- 調查無法採用新科技的監管障礙或其他因素，並在相關情況下，提出 FATF 的其他專案，以探究政策調整之可能；以及
- 為政府當局和私部門利益相關者提供一套共同的定義、概念架構和建議行動，以推動負責任地開發和運用 AML / CFT 之新科技。

1.2. 範疇和方法

26. 本報告重點關注新科技如何協助各司法管轄區和受監管機構更有效地執行 AML / CFT 的標準。特別是，數位解決方案更能理解、評估和減輕風險、更能有效執行客戶盡職調查和監控以及與監管者的溝通，可能有助於實現 AML / CFT 標準的有效執行。

27. 本報告討論俗稱監管科技[4]的新科技之實施，如人工智慧、機器學習、大數據和針對客戶識別和驗證要求，以及更廣泛的 AML / CFT 合規義務之進階的認知分析／演算法。還包括監理科技[5]或監理機關使用的科技，例如，風險評估工具、資料視覺化工具或其他（Coelho 等人，2019[4]）。

28. 本報告並研究關於科技已成功部署者，其得以有效運用科技之前提條件為何？取得何種效益？以及成功使用創新解決方案後產生哪些新要求（如果有的話）？

29. 本報告還審議前途有望的科技但未成功建置的案例，並指出有效運用這些科技的挑戰或障礙。報告還探討是否需要採取全球之協

---

4 監管科技是金融科技下的一個子集，側重於提供可比現有能力更有效地促進監管要求的科技，如回饋聲明 FS16/4，金融行為管理局，關於支持監管科技的發展和採用者的徵詢意見（2016 年）中提到的。詳見： www.fca.org.uk/publication/feedback/fs-16-04.pdf

5 監理科技（suptech）是監理機關為因應監管而使用之創新科技。詳見，（Broeders D. and Prenio J., 2018[36]）

調行動，以便能夠更加利用創新科技解決方案來支持 AML / CFT 的目標，包括分析結構性挑戰，如資料品質問題、改變傳統系統、成本限制和缺乏監管激勵。

30. 在這些科技提供真正的好處並有助於以有效的方式應對威脅的情況下，FATF 會分析新科技早期採用者的案例，以使其他受監管機構和主管機關能夠以最有效的方式實施這些科技。

31. 其他未在本報告中提出分析之關於執行 FATF 標準的更好的科技範例，包括：

- 資料管理和分享工具
- 金融情報機構如何使用包括機器學習和大數據分析等分析工具。

32. 本報告依賴於一般的次級資料研究和 FATF 秘書處向政府當局、公部門與私部門專家分發之對線上數位轉型問卷[6]的回覆。秘書處並諮商主要利益相關者，以獲得更多資訊和專家意見，包括由 FATF 在 2021 年 3 月 10 日舉行的運用新科技對 AML / CFT 的機會和挑戰的線上高峰圓桌會議。

33. FATF 的數位轉型調查問卷徵求利益相關者對新科技的主要使用者（採用者）的意見，以及在該司法管轄區的 AML / CFT 和其他監管架構下基於科技實施特定解決方案的目的和附加價值。它還關注它們對使用者與監管者關係的影響和實施障礙，以及新科技與 FATF 標準和其他監管架構的關係。它還鼓勵回覆者提交能說明最佳作法和／或具體挑戰之案例研究。54% 的回覆者為私部門代表，主要是大型銀行和科技開發商。在公部門層面，大多數回覆者是由監管人員。

---

6 問卷調查尋求有關本專案中新科技的機會和挑戰的資訊。蒐集到 188 份回覆，包括案例研究和數位解決方案之例。

2. AML / CFT 之新科技：更有效地實施 FATF 標準

34. 妨礙 AML / CFT 措施有效執行的主要挑戰之一是對洗錢／資恐的威脅和風險認識不足。根據不充分的風險評估所做的決策時而不正確且無關連性，嚴重依賴人力投入及以防禦性的框選方法來應對風險，而不是採用真正的風險基礎法。

35. 無法充分識別、評估和減輕洗錢及資恐的風險，包括風險識別的基本要素（客戶識別／核實和交易監控），對 AML / CFT 的有效性構成障礙。這正是新科技可以提供最大附加價值之處。

36. 目前大多數的風險評估和風險管理工作都是基於一套預先決定的風險因子自動進行靜態分析，再結合人為判斷。舊系統[7]通過新的演算法和人工輸入的資訊進行更新，產生對風險進行解釋和行動的組合，但這些系統很少提供客戶交易或機構風險的即時概觀。

37. 此外，利用 Excel 一類的試算表軟體或靜態報告平臺這些傳統風險評估工具，資料無法進行大規模分析，限制進行關聯和分析以產生更精細的風險情況的可能性。此外，舊系統獲得的資料品質各不相同，可能無法提供符合 AML / CFT 標準所需的準確性和細節。

38. 在私部門，粗劣的風險評估可能導致 AML / CFT 架構之防禦性勾選應用，不僅效率低下，負擔沉重，更重要的是沒有反映金融機構面臨的真正的洗錢／資恐威脅。糟糕的風險評估破壞真正以風險為基礎的決策方法以保護金融系統的誠信。這有可能導致兩個截然不同的問題，對減輕新的或正在出現的風險缺乏足夠的重視（允許洗錢和資恐發生），以及在適用簡化措施的低風險情形下

---

7 在本文中，"舊系統"指的是依靠低科技（手工輸入和資料庫）流程進行資料蒐集和分析。.

過度應用風險緩解措施（給客戶帶來不必要的成本和摩擦，包括金融排斥）。

39. 在識別、評估和管理洗錢和資恐風險方面，使用新科技可以使風險分析更加動態，可以提供網路分析，並在客戶、金融機構、司法管轄區和跨境層面進行操作（見案例 1）。然而，運用這些工具的最佳情況需要一個監管和政策環境，以建構足夠的資料庫和分享、或協作分析，以及監管人員和執法部門的適當存取。

案例 1. 金融機構的動態風險評估工具

一跨國金融機構正在建立動態風險評估工具，用以：

- 使用更具深度和更豐富的資料，動態更新以反映最新的調查見解。
- 以更快的速度識別金融犯罪風險，並減少無益的警報。
- 對客戶風險進行更準確、更複雜的評估。

這個工具使用雲端計算功能來集中和處理大規模的資料。還包括新的技術、機器學習，以識別金融犯罪風險，通過：

- 納入關於金融犯罪類型和可疑活動的現有知識。
- 觀察一個實體與其他具有可疑或確認的不利特徵的實體之交易和社會聯繫。
- 量化（或捕捉）一個實體相對於具有類似特徵的同行群體的異常行為。
- 量化（或捕捉）一個實體相對於其自身歷史行為的異常行為。

40. 在識別、瞭解與管理風險方面的困難對接受調查的公共和私部門實體都有負面影響。FATF 第四輪相互評鑑報告的分析顯示，許多監理機關仍然無法按部門或機構層面對被監管實體進行適當的風險評估。相互評鑑分析顯示，由於資源和工具的短缺，許多監

理機關缺乏蒐集和處理資料的能力。一些監管者的風險評估缺乏足夠的更新，也缺乏採用風險基礎法以及向被監管實體提供足夠回饋所需的關鍵基礎。

41. 雖然數位身份和 AML / CFT 交易監控及報告解決方案的數量增加，監管科技公司激增（見附件 D），但受訪者證實，監理人員與監管者在這些科技的能力和採用方面仍有很大差距。

案例 2. 監理人員的動態風險評估工具：風險評估的數位解決方案

為金融機構或指定之非金融事業或人員之監管人員提供的現有商用監管科技工具可讓通常每年進行的 AML / CFT 風險評估過程自動進行，以便為特定週期的監管工作提供資訊。

該現有商用工具支援風險基礎法，有三個模組：

- 用於保證資料品質和調查管理的資料蒐集模組。
- 帶有風險模型的評分模組，導入調查資料，對固有風險進行評分，並與控制措施的品質評估相結合，在機構層面產生剩餘風險評級，以及
- 對部門、子部門、個別機構和個別風險因素提供與監管者相關分析的資料分析模組。

該現有商用工具使用一個有組織地開發的風險模型，在風險評分演算法中加入機器學習的降維處理。評分演算法通過將模型變數（風險因素）減少到那些報告的重大活動，消除 " 稀釋效應 "，為每個實體調整風險模型的規模。這樣做的好處是，可以識別出有風險的狹窄商業模式和小而有風險的實體。

這個解決方案以更大的相關性和精確性來識別風險，並以更低的運營成本，比非自動化替代方案更快地產生剩餘風險結果。

2.1. 風險基礎法之實施

42. *"風險基礎法應是有效的 AML / CFT 制度的基石，對適當管理風險必不可少"*。（FATF, 2014[5]）然而，儘管 FATF 為此提供指導（FATF, n.d.[6]），但 FATF 對第四輪相互評鑑的戰略審查的結論是，許多司法管轄區繼續適用大量的規範基礎法的制度。同樣，私部門仍在掙扎於採用風險基礎法，還是傾向於對 AML / CFT 採取昂貴的防禦性方法。

43. 對風險有充分的瞭解和認識，從而有能力按比例減輕和處理風險，這對有效執行 FATF 的標準至關重要。

44. 傳統上規範基礎法導致防禦性合規，而不是對不同程度的風險採用不同的緩解措施。主管機關對多報少報的反應，進一步助長防禦性行動。

45. 防禦性的 AML / CFT 架構是監管或業務不確定和／或對所應用的戰略和機制缺乏信任的結果。公部門與私部門都可能對自己的風險評估缺乏信任，因為他們對現實的理解不全面造成訊息和資料缺失，也缺少資源和工具來進行堅實、最新和全面的風險評估。

46. 提高蒐集和處理資料的能力，以及在利益相關者間分享資料的能力，可以在這一領域提供巨大的優勢，促進更加動態的風險基礎法。

47. 使用機器學習和其他人工智慧工具，可以進行即時、迅速且更加準確的資料分析，可以為上述問題提供解決方案。這類工具可以部分或完全自動化風險分析過程，使其能夠考慮到更大的資料量，並識別出不符合已經瞭解的情況的新出現的風險。這類工具還可以提供識別風險的替代手段，實際上是對傳統風險分析的結論進行半獨立的檢查。

48. 即使使用這些工具得出的結論與傳統風險分析得出的結論相同，這種確認也能使行為者對其評估的完整性和準確性打消疑慮。通

過這種方式，機器學習可以提高他們在應用風險基礎法措施時可信度，並使他們能夠更自如地向其監管者證明使用這種措施的合理性。自動化之風險評估工具也可能更容易被監管者審計，並提供更多的客觀性。

49. 實施新科技以解決這些弱點需要專業科技。然而，正如受訪者所報告的那樣，主要障礙是一些現有的監督作法和一些監管者在創新方面面臨之困難。儘管如此，案例 3 中的案例研究顯示，理想的文化轉變正在出現，一些監管者已經在與該部門接觸，鼓勵採用新科技。

案例 3. 美國金融犯罪稽查局和聯邦銀行機構

聯邦銀行機構（FBAs）和美國金融犯罪稽查局（FinCEN）於 2018 年 12 月發佈了 " 聯合創新聲明 "，鼓勵業界考慮、評估並酌情負責任地實施 AML / CFT 義務的創新方法，同時仍然遵守銀行保密法（BSA）／防制洗錢合規義務。該聲明重點關注反洗錢（交易監控）合規解決方案，但也包括更廣泛地遵守銀行保密法／防制洗錢之要件的創新解決方案，包括創新的數位身份解決方案；認可私部門負責任的創新，包括利用現有工具的新方法或採用新科技，可以經由提高銀行保密法／防制洗錢合規計畫的有效性和效率，幫助銀行識別和報告洗錢行為、資恐和其他非法金融活動。

該聲明旨在保證測試和驗證負責任的創新方法的有效性的防制洗錢試點項目不會必然導致以下幾點結果：。

1）如果試點最終被證明不成功，而招致監管部門的批評。

2）如果試點暴露了現有防制洗錢合規計畫中的漏洞，而導致主管機關採取制裁行動；或

3）如果實施創新的方法，增加額外的監管期望。

該聲明還明確指出，美國金融犯罪稽查局會為了支持負責任的 AML / CFT 創新試點動用豁免權，否則計畫可能會因為特定的監管禁令或障礙而無法實現。

該聲明還鼓勵私部門就其創新的銀行保密法／防制洗錢方法的創新試點專案與各機關進行接觸，強調早期接觸可以促進各機關對這些方法更加理解，並允許在適當和必要時澄清監管期望。

2.2. 普惠金融

50. 促進金融普及性是有效實施 FATF 標準的一個重要部分，可以從總體上減少洗錢／資恐風險。然而，緩解金融排斥仍然是一項挑戰。

51. 在世界各地，有 10 億餘人為開設銀行帳戶，或維持獲得金融服務的機會，想盡辦法拿出適當的身份證明文件。（Vyjayanti T Desai 等人，2018 年 [7]）即使身份能被識別，客戶盡職調查的程序往往以嚴格而無彈性的風險管理的方式踐行，進而導致社會中最弱勢的群體被金融排斥。

52. 大多數受訪者同意，保護個人獲得金融服務的權利和確保金融普及性是充分執行 AML / CFT 的關鍵因素，而為有效，減輕和避免這種意外後果應為優先事項。

53. FATF 重申其基於風險按比例採用其標準的承諾，以保護最脆弱的群體並支持 AML / CFT 保障措施的範圍。FATF 所出版關於 AML / CFT 措施和普惠金融的指南，以及關於客戶盡職調查的補充，旨在提高對這一問題的認識，並鼓勵各國利用 FATF 建議的彈性，向被金融排除的經濟弱勢提供健全之金融服務。（Vyjayanti T Desai 等人，2018[7]）

54. 最近的 FATF 數位身份指南（FATF，2020 年 [8]）也包括關於對數位身份解決方案在採用風險基礎法時是如何支持普惠金融的詳細情況。

55. 二十國工業集團數位普惠金融高層原則（G20，2016[9]）強調普惠金融，確認需要在數位工具和金融知識的幫助下，對識別要求採取相稱且基於風險之方法。

56. 聯合國在促進及支援為反恐目的下負責任地使用生物識別資料的努力加強 FATF 的工作，目的是防止意外後果並遵守國際法。（聯合國，2018[10]）

57. 確保普惠金融的一個關鍵因素是金融機構對 AML / CFT 採取有效的、基於風險的方法，包括客戶盡職調查要求。（EBA, 2021[11]）客戶盡職調查支持與個別客戶相關的風險評估，而不是僵化的勾選方法和對客戶廣泛分類不加區分的政策。基於科技的創新解決方案，像是數位身份證和反洗錢合規交易監控工具，可以促進以優化的成本進行更準確和最新的風險評估，並對風險評估的結論提供更大的信心，從而能夠在適當的時候更多利用簡化的客戶盡職調查。這可能是普惠金融的一個重要推動因素，迄今為止，由於不願意充分利用風險基礎法所提供的靈活性，以及金融機構基於利潤的商業決策，普惠金融一直受到阻礙。

58. 基於科技的創新解決方案，只要是基於風險基礎法並負責任的來實施，可能有助於普惠金融（Chase，2020[12]）。如案例 4 所總結[8]，可以最大限度地減少與人為控制措施不一致的相關弱點，改善客戶體驗、節省成本，並促進交易監控。傳統的身份證明要求（Kazzaz，2020[13]）可能是識別客戶最顯著的方式，但不應該是用於此目的的唯一工具[9]。例如，自然語言處理工具、生物識別及

---

8 更多關於數位身份證的好處，詳（FATF, 2020[8]）.。

9 關於使用數位金融服務的相關建議，請參考 FATF 之前出版之關於數位身份證的指引 www.fatf- gafi.org/publications/financialinclusionandnpoissues/documents/digital-identity- guidance.html and COVID-19 www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html for relevant recommendations on the use of digital financial services.

其他類似工具[10]之使用可能比強制親自出示身份證明文件更有利於客戶盡職調查過程，儘管分析人員和專家的作用和審查仍然是防止偏見和其他過度依賴科技的意外後果的關鍵。

案例 4. 數位身分證對受監管機構和個人的普惠金融的好處

對於受監管之機構而言：

1. ***降低成本：***數位身份證可以支援更便宜、更複雜的客戶引導。特別是，結合通過移動設備和智慧手機盡可能獲得更多元的金融服務，科技可以從根本上改變消費者獲得金融服務的方式。更便宜和更自動化的客戶盡職調查流程，允許更廣泛的資料庫和來源，可以讓沒有傳統信用記錄的客戶獲得金融服務或自動化經紀服務，並使這些服務更實惠。
2. ***可攜性和互通性：***系統可以在多個機構或交易中使用，將驗證的負擔減少到只有客戶導引的一種情形即可（如果初始驗證是由政府主導的，則具有特別的優勢）。
3. ***減少人為錯誤：***雖然人工輸入仍然需要且令人滿意，但資料蒐集和匹配的自動化允許在更短的時間內考慮比人工執行更多的資料點。

對個人而言：

4. ***更佳客戶體驗：***數位化的身份證明大大減少證明個人身份的負擔，例如，需要攜帶和提交多種實體形式的文件。
5. ***多種用途：***系統允許多次使用經過驗證的數位身份證用以簡化日常操作，並提高系統與服務提供者和主管機關之間的互動的效率。

[10] 廣義的"數位身份"指的是線上存在的關於個人、組織或電子設備的資訊載體

59. 科技還可以實現普惠金融，經由強化交易監控的數位工具。正如關於普惠金融的指導意見所述，強化的持續監控可用於管理與客戶身份和核實資料的可信度有關的洗錢／資恐風險，從而使洗錢／資恐風險管理不那麼嚴重地依賴於引進客戶時的客戶盡職調查。例如，在客戶只能提供不太可靠的身份證明形式的情況下—因此身份識別和驗證要素不夠健全—使用如行為分析等科技解決方案，可以支援和強化交易及業務關係監控，從而使客戶能夠接受。這些科技也可以提供一個強大的持續監控過程，並更能理解風險。

60. 在這種情況下，科技解決方案的開發可以促進＂白標＂交易（如工資、水電費和生活費的支付、政府補助支出等），在客戶風險評估允許之情況，也可以用來加強有限的帳戶的使用。這將使更多的客戶能夠獲得基本的銀行服務，同時減輕金融機構所面臨的風險。然而，重要的是要確保客戶在開戶時的盡職調查，提供足夠的資訊，以便對客戶進行有效的監控，而將影響所需要蒐集的訊息量。如果一個機構對其客戶的訊息太少及對客戶相關金融產品之預期使用方式不夠清楚，就無法有效監控。

61. 此外，如果交易監控的改進能使銀行對其他類型的金融機構（如金錢或價值移轉服務供應商）採用更堅實的合規方案更有信心，則可緩解金融排斥現象。更好的風險評估、客戶盡職調查程序和適當的監控工具可以成為更加包容和安全的金融體系之重要組成部分，且不會因作法、社會或區域背景而產生歧視。

62. 為金融包容目的之數位解決方案，例如生物識別科技，並非沒有遇到挑戰，且其實還存在風險。特別是在金融服務提供商只開發數位業務模式的情況下，讓金融排斥的情形在無法獲得電子設備、

不信任或不瞭解這些設備所帶來之可能性的人群中甚至更加惡化。目前為促進普惠金融而實施某些策略也可能導致金融排斥過程更加拖延。限制帳戶[11]可能會限制銀行帳戶預期的活動類型或功能，導致客戶體驗不盡人意，進而退出正規銀行系統。遠端登入、帳戶層級和延遲的身份證明也被認為有時會導致充分獲得金融服務更佳困難（Kazzaz, 2020[13]）。在這種情況下，創新也可以通過為金融機構監控銀行關係提供替代方案，幫助減輕依賴新科技的意外後果。例如，行為風險取向、網路分析和心理測量資料的使用可以為承保和獲得信貸提供資訊，成為數位身份證系統的優勢。

63. 重要的是，使用這些方法還可以為獲得全方位服務和盡可能不受限制地獲得金融服務開闢道路。上述提及之解決方案也有一些潛力，可以實現這種轉變（例如，科技強化的長期持續監控和行為分析，可以為客戶風險分析提供更有力的基礎，並提高與客戶身份識別和驗證缺乏可信度有關的強化盡職調查的有效性，可能允許擴展上述帳戶的功能）。

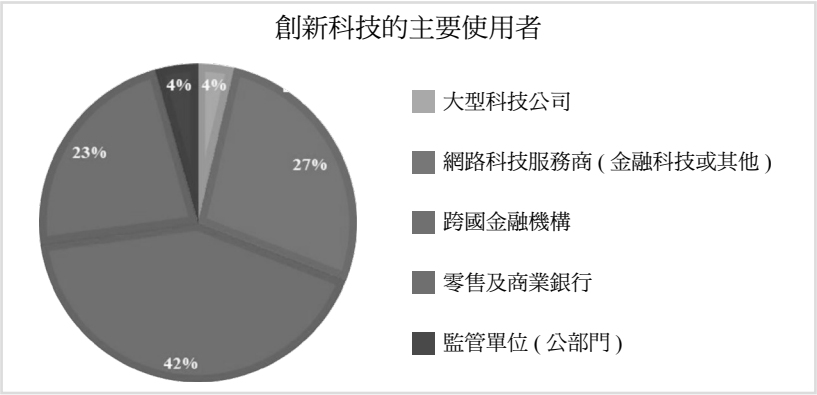
64. 歸根結底，為 AML / CFT 目的而採用的任何新科技都必須遵循問題解決途徑，不造成額外的負擔或意外的後果也同樣重要。

11 限制帳戶或基本帳戶是旨在提供最低金融服務的帳戶。這些帳戶通常對交易金額、獲得信貸的能力和網路銀行工具或支付系統有所限制。

3. 新科技為 AML / CFT 帶來之機遇

65. FATF 的數位轉型問卷要求提供關於如何為防制洗錢及打擊資恐開發和部署新科技的資訊，包括：
    - 新科技的使用者是誰？
    - 被用於哪些 AML / CFT 的功能？
    - 哪些底層科技被用來執行這些功能？
66. 關於使用新科技是誰的這個問題，如圖 1 所示，金融機構、科技開發商和跨國規模的金融科技監管實體主導對新科技的需求。

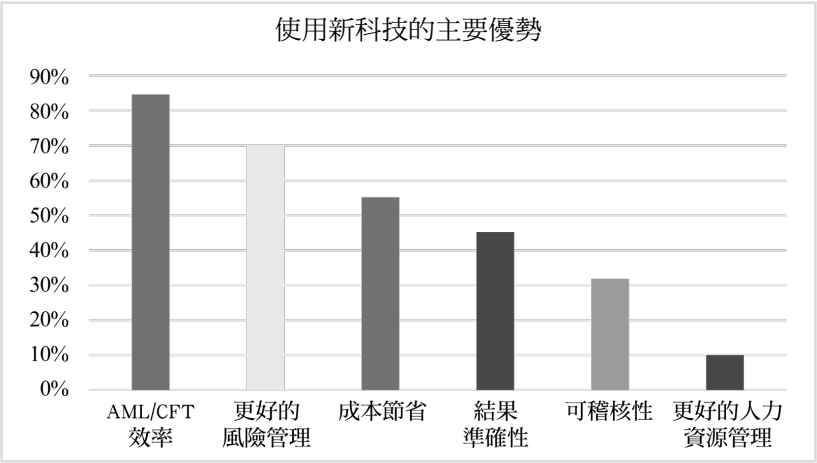
圖 1、創新科技的主要使用者



67. 受訪者認為，對新科技的採用和需求是不平等的，大型金融機構和較小的行為者之間繼續存在巨大的差距，而且在區域和國家層面上也是如此，較小的經濟體在數位創新方面落後。
68. 關於運用何種 AML / CFT 功能的問題，新科技有望經由向利益相關者提供更快、更有成本效益的工具來提高 AML / CFT 工作的有效性。85% 的受訪者同意，AML / CFT 的有效性是使用新科技的首要利益，其次為風險管理更好，如圖 2 所示。受訪者宣稱，速度、

靈活性、能力及更好的治理是新科技有助於提高 AML / CFT 成效的結果。

圖 2、使用新科技的主要優勢



69. 回覆者強調，監督人員多利用新科技更可能提高監督能力進而促進 AML / CFT 的效力。專家們提到的新科技對監管人員的好處包括：能夠

- 監督大量的金融機構[12]。
- 更清楚識別和瞭解與不同行業的個別機構有關的風險。
- 即時監控對 AML / CFT 標準的遵循情況，並在不遵循時採取行動。
- 更有效地與受監督之機構進行溝通，並執行額外的資訊要求。
- 存儲、處理和報告更多的監督資料。

---

12 數位化讓受監督實體數量的增加被認為是驅動使用監理科技的需求因素之一。其他因素包括對更準確的資料的需求、法規的複雜性增加、風險管理能力的提高，以及更有洞察力的政策和更具前瞻性的監督。（FSB, 2020[14]）

- 與其他主管機關交流資訊。

70. 私部門的優勢包括能夠：
    - 更能識別、理解和管理洗錢／資恐風險。
    - 能夠以更快、更迅速和更準確的方式處理和分析更大的資料集。
    - 更有效的客戶引導實務（數位）。
    - 實現更高的可審計性、問責制和整體的治理。
    - 降低成本，最大限度地將人力資源用於 AML / CFT 更複雜領域。
    - 提高提交可疑活動報告的品質。
71. 在更細化的層面觀察，受訪者強調新科技提供結果及資料處理結果的能力，這些結果不僅超越人類在創紀錄的時間內處理大量資訊的能力，而且由於資料標準化和匹配軟體之運用，得到更可靠、更容易與他人交流之結果[13]。
72. 52% 的受訪者認為，監管科技是 AML / CFT 領域可以確保從新科技獲得大部分的利益[14]。特別是，受訪者確認處理和分析風險評估和分析所需的大型資料集、客戶盡職調查以及交易監控，是確保從新科技中獲得最大利益的領域。
73. 回覆者強調，新科技能夠提高 AML / CFT 的能力，並釋放人力資源，用於如分析複雜的洗錢／資恐案件等更關鍵的工作。資料管理，包括以有效且具有成本效益的方式蒐集、分析和使用資訊的能力，是回覆中被提及的跨領域因素。

---

13 更多關於資訊分享的功能，詳（FATF, 2020[37]）

14 歐洲銀行監理機關於 2019 年關於監管科技的調查顯示，樣本中包含的銀行有很大一部分（42%）實施至少一個監管科技解決方案。詳：at: https://www.eba.europa.eu/financial- innovation-and-fintech/fintech-knowledge-hub/regtech-industry-survey

74. 此外，新科技還被描述為使內部系統中的資訊更加準確，儘管一些受訪者強調不斷審查的重要性，以及機器學習意味著從人類的行為和決定以及現存的機構實務中學習。
75. 及時性的因素與不需要人工干預而持續分析和更新資料的能力，也被強調為一個關鍵的優勢；特別是在舊系統和更新客戶記錄的能力方面。這對自然語言處理工具來說尤其重要，它允許在原始資料插入中存在拼寫差異或錯誤的情況下，對客戶記錄進行匹配。
76. 關於第三個問題，哪些基礎科技被用來執行這些功能，問卷調查詢問哪些科技最有可能促進 AML / CFT 的有效性。回覆指出，人工智慧（包括機器學習和自然語言處理工具）、應用程式介面（API）和用於客戶盡職調查的工具最具潛力。
77. 分散式帳本科技（或區塊鏈科技）在這項工作的前期就被提到過，認為是有潛力的科技，但發現受訪者的採用程度較低。然而，一些基於分散式帳本科技的例子、大部分仍處於發展階段，說明如後。

3.1. 人工智慧（AI）

78. 人工智慧是模仿人類思維能力，以執行通常需要人類智慧的任務之科學範疇，如識別模式、做出預測建議或決定等。人工智慧使用先進的計算科技，從不同類型、來源和品質（結構化和非結構化）的資訊智能中獲得洞察力，以自主解決問題和執行任務。有幾種類型的人工智慧，它們以不同的自主水準運作（並實現），但一般來說，人工智慧系統結合意向性、智能和適應性。
79. 機器學習是人工智慧的一種類型（分支），它訓練電腦系統從資料中學習、辨識模式，並在最低人為干預下做出決定。機器學習

涉及到設計一連串的行動，通過經驗和不斷發展的模式識別演算法來自動解決一個問題，只需要有限的或沒有人工干預，換言之，它是一種自動建立分析模型的資料分析方法。受訪者認為，人工智慧驅動的機器學習和自然語言處理能力，為受監管機構和監管者在 AML / CFT 方面提供巨大好處（見案例 5）。據報導，機器學習通過其從現有系統中學習的能力提供最大的優勢，減少人工輸入監控系統的需要，減少偽陽性和識別複雜案件，也促進風險管理。

案例 5. 機器學習的監督性使用

巴西

監管流程

巴西中央銀行（BCB）行為監督部在 2019 年時，從一套客觀指標中開發了一個優先級的模型，以確定哪些被監督的機構應在年度監督規劃（ASP）中被優先考慮。這個模型在 2020 年首次使用，作為 2021 年監督規劃的想法（作為一個原型）。

巴西中央銀行正在使用機器學習來改進此模型，以支援其在風險基礎法架構內的監督規劃。無監督的學習科技正被用來計算被監督機構的風險分數。

80. 機器學習的應用對於檢測異常和離群值識別和消除重複資訊以提高資料品質和分析非常有用。例如，深度學習（DL）是一種進階的機器學習類型，其中具有許多（深）層的人工神經網絡（受人腦啟發的演算法）以高度自主的方式從大量的資料中學習。深度學習演算法反復執行一項任務，每次都會稍作調整以改善結果，使機器能夠在沒有人類干預的情況下解決複雜問題。

3.2. 自然語言處理和軟性計算科技

81. 自然語言處理（NLP）[15]是人工智慧的一個分支，使電腦能夠理解、解釋還能操縱人類語言。模糊邏輯是一種邏輯科技，它採用不精確或近似的資料，並使用多個值對其進行處理，以產生可用的（但不精確的）產出。這種邏輯是非二進位的，使用一系列的值來替代 0 或 1。模糊邏輯系統可以對不完整的、模糊的、扭曲的或不準確的（模糊的）輸入產生有用的產出，比傳統邏輯更接近地模擬人類的決策，並更能從非常不精確的資料中提取更有用的資訊，以便用傳統邏輯得出明確的結果。模糊邏輯可以通過硬體、軟體或兩者的結合來實現。

案例 6. 模糊邏輯的應用

義大利

義大利金融情報機構（UIF）與義大利銀行金融監管總局合作，為非屬銀行的金融中介機構建立了一個用以構建反洗錢指標模糊邏輯的應用程式。目前處於實驗階段，被提出的模糊系統，允許闡述定量資料（即來自／流向高風險國家的跨境支付），以支持對這些仲介機構進行定期的 AML / CFT 風險評估。

用於計算指標的資料來源是反洗錢綜合報告（S.AR.A. 來自義大利語的縮寫）資料庫和監管部門報告。為了構建指標，非銀行金融中介機構根據其類型（如受監管投資機構、資產管理公司、支付和電子貨幣機構、信貸提供者）和主要活動（如開放式基金、封閉式基金、匯款服務、電子貨幣和其他支付服務等）被分成不同類別。

---

15 “自然語言處理（NLP）是人工智慧的一個分支，說明電腦理解、解釋和操縱人類語言。自然語言處理協助電腦用人類自己的語言與人類交流，使電腦有可能閱讀文本，聽到語音，解釋它，測量情感並衡量哪些部分是重要的。”（SAS, n.d.[15]）

82. 自然語言處理和模糊匹配工具也可以更有效地減少偽陽性和偽陰性（例如在制裁篩選過程中），但主要是克服資料品質問題，因為這些方案更善於將資訊要素聯繫起來，例如將搜尋引擎結果與重要政治性職務之人名單聯繫起來、識別欺詐企圖或監控制裁名單等等，如案例 7 所示。

案例 7. 付諸實行的自然語言處理

巴西

巴西中央銀行（BCB）在 2020 年 4 月批准自然語言處理（NLP）監理科技專案，目的是將人工智慧應用於自然語言科技處理的文件，以達到監督的目的。

通過這個專案，巴西央行計畫進一步緩解未遵守其監管職責的風險，提高監管效率，並確立相關法律與監管架構。

開發中的工具包含下述的分析：

- 社群媒體：捕捉文字材料作為監督活動的輔助資訊來源；
- 內部報告和文件：對存儲在網路系統（SisAPS －更多細節詳附件 C）中的 AML / CFT 遠端檢查範圍內之受監管機構之回應，進行分類和總結，以提高對所 提交之定性資訊的處理能力，提供對監管要求之改進；
- 外部報告和文件（解釋性說明、審計報告、相關事實和董事會紀錄）：研究、總結和分類與監督有關的資訊，如審計報告中解釋性說明的定性資訊。
- 全球互聯網研究（網頁抓取）：初期掃描公共資料進行分析，建構指標和／或形成資料庫，以取得受監管機構與涉及洗錢／資恐的資訊。在第二階段，將使用機器學習來閱讀新聞，並從中提取法律實體參與貿易型洗錢（TBML）的證據。
- 報告的自動化—檢查和後續：自動生成工作報告的描述性文字與供檢查之用之報告。

83. 廣義而言，將人工智慧應用於 AML / CFT 的過程，可以提高行為者應對風險和更有效地執行要求的能力。這些工具不是一種替代品，而是對旨在改善結果和簡化合規系統的補充。

84. 利用人工智慧和機器學習工具進行交易監控，可使受監管機構以更快、更準確和更高效的方式履行傳統職能（前提是機器經過充分和準確的訓練）（見案例 8）。這些模型對於過濾那些需要額外調查的案件很有用。在大多數情況下，為監控目的使用新科技應繼續與更廣泛的監控系統結合，其中包括對特定警報或高風險領域的部分加入人工分析。這些系統還必須提高其可解釋性及可審計性的程度，以充分遵守大多數的監督要求。

案例 8. 機器學習所增加之價值為何？

- *客戶的識別和驗證：*在遠端登入和人工智慧驗證的背景下，包括生物識別科技，機器學習和活體偵測科技可用於執行：微表情分析、反欺騙偵測、假圖偵測和人臉特徵分析。
- *監控業務關係以及行為和交易分析：*
  - *無監督的機器學習演算法：*根據客戶的行為將其分組，然後創建控制措施，可以根據風險基礎法（例如:交易閾值設置）進行更充分的設置，從而對業務關係進行量身定制的有效監控。
  - *監督的機器學習演算法：*允許根據現有的相關 AML / CFT 的要求，對資料進行更快速和即時的分析。
  - *警報評分：*警報評分有助於關注活動的模式，並發出通知或加強盡職調查需求。
- *監管更新之辨識與實施：*具有自然語言處理（NLP）、認知計算能力和機器人流程自動化（RPA）的機器學習科技可以持續掃描和解釋大量的非結構化監管資料，對其來源自動識別、分析，然後列出機構的適用要求；或（在一定程度上）實施新的或修訂的監管要求（通過編纂和生成實施工作流程），以便受監管機構之相關受監管之產品能夠合規。
- *自動資料報告（ADR）：*使用標準化的報告範本，使用自動化的數位應用程序（資料庫工具），使受監管機構的基礎細化資料可以批量提供給監管者。

1. 非詳盡的清單

3.3. 分散式帳本科技

85. 分散式帳本科技可能會改善跨境交易的可追溯性，甚至是全球規模的交易，有可能使身分驗證更加容易。為資料和流程管理目的負責任地、規範地使用分散式帳本科技也可能加快客戶盡職調查流程，因為消費者可以自我認證，甚至可以通過驗證資料的智能合約自動批准或拒絕（見案例 9）。

86. 此外，在適當的保障措施和監管環境下，交易有可能通過跨多個司法管轄區中的數個機構之間共用的單一分類帳，或通過可交互操作的分類帳進行管理。與現有架構相比，這將大大增加監控的可能性。這也意味著，隨著分散式帳本科技得到更廣泛的理解和使用，例如，可以通過智能合約在證券發行時建立合約協議，這意味著每次證券交易啟動時，其他股東將被自動通知，並依照合約設計或可成為交易的對手方。

87. 分散式帳本科技也可能為管理客戶盡職調查要求帶來好處，有助於解決使用者對此過程的擔憂，為私部門帶來更大的成本效益，並建立一個更準確和以品質為基礎的資料庫。例如，在中國，金融機構正在使用分散式帳本科技，在該系統允許的保密範圍的基礎上分享觀察名單或紅旗指標。

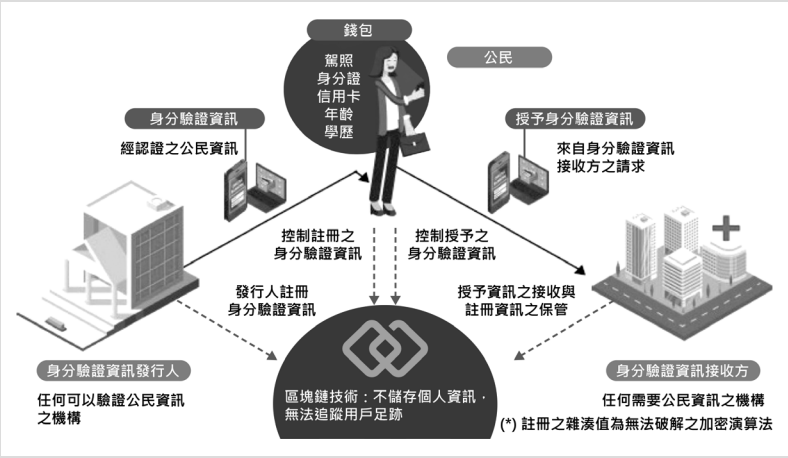
88. 儘管分散式帳本科技有其優點，但從 AML / CFT 的角度來看，它不斷對虛擬資產的監管和／或監督形成挑戰並引起重大關切[16]。與通過銀行等傳統中介機構進行的交易不同，基於分散式帳本科技的虛擬資產交易在本質上是去中心化的，讓未經中介的點對點交易可以在沒有任何監督的情況下進行。如果沒有單一的實

[16] See（FATF, 2021[38]）第五節

體或明確的地點負責這項活動，它們同樣會引起對司法的考驗。這可能會對專注於監管／監督中介機構的傳統 FATF 標準構成潛在挑戰。因此，FATF 成員應詳細監控和進一步考慮這種科技的使用。當局還可能要考慮與傳統工具相比，使用分散式帳本科技的碳足跡。

案例 9. 客戶盡職調查與分散式帳本科技

來自不同行業的九家大型私營公司相互合作，並得到當地監理機關的支援，從使用者控制的角度促進數位身分的管理模式（身分自主權）。它遵循歐洲和西班牙的標準，以授予與未來替代品的互通性。因為它使用分散式帳本科技，這個系統允許使用者從一個 " 錢包 " 中控制操作，從而簡化與合作夥伴實體的交換和身分證明及客戶盡職調查程序。該項目處於前導測試階段，預計將在 2021 年投入使用。



3.4. 客戶盡職調查的數位解決方案

89. 客戶識別／驗證和監控是 AML / CFT 架構的一個關鍵支柱，但在某些情況下，仍然存在執行方面和有效性的挑戰。當在非風險基礎上實施時，這些努力被認為成本高昂，且大多效率低下，因為它們消耗資源和時間，而這些資源和時間往往沒有轉化為準確的風險評估流程或成功的業務關係。

90. 據接受調查的私部門各方稱，客戶盡職調查措施和監控是一個極其繁瑣的過程，同時還在資料品質方面產生高度的不確定性，難以按要求更新和匹配資訊。客戶盡職調查程序也是客戶不滿意的主要原因之一。蒐集和核實資訊的過程往往是困難又費力的，充滿無休止的文件要求和額外的親自定期提交證據。此外，專家們提到，客戶盡職調查產生的風險分析過於基於規則，而不是基於行為或背景，導致難以遵循要求的非特權個人或群體受到金融排斥。

91. 將新科技應用於客戶盡職調查和監控可能有助於解決這些挑戰，辦法是根據風險、背景和個人情況，在不損害提供服務的實體或金融系統的誠信的情況下，更加簡化開戶程序。這些都有可能改善客戶體驗，並促進更有效的 AML / CFT 保障措施。例如，有證據顯示，混合方法，即在提供官方身分證的同時提供生物識別，可以提供更有力的識別和驗證過程。

92. 數位身分證為這一領域提供最好的案例研究之一，因為它已在許多司法管轄區被廣泛採用和支持（而且 FATF 已發佈關於其使用的指導意見）。有證據顯示，COVID-19 危機進一步促進對遠端金融服務提供的需求。事實上，電子身分識別和驗證是 " 反洗錢中最成熟和即時有用的科技要素 " 之一。（Richard Grint 等人，2017 年 [14]）它也是問卷調查中最受認可和經常被提及的 AML /

CFT 的良好作法之一（見案例 10）。

93. 例如，數位身分證可以改善客戶通過移動設備和智慧手機獲得金融服務的情況，同時通過生物識別資訊作為個人身分資訊的補充，確保客戶資訊的安全性和準確性。一些金融機構可以在基本身分資訊的基礎上，在客戶允許的情況下，通過蒐集客戶的額外資料，增加資料來源的多樣性，最終強化知識和能力以管理業務關係。

案例 10. 數位識別解決方案

歐盟電子身分識別條例

歐盟電子身分識別條例是第一個關於可信的電子識別和信任服務的全球跨境架構。該條例允許在一個歐盟成員國簽發的電子身分證用於訪問另一個成員國的線上公共服務。信任服務是旨在使電子商業交易更加安全、方便和有效的電子服務。歐盟電子身分識別下的信任服務包括電子簽名、電子印章、時間戳記、電子交付服務和網站認證。歐盟電子身分識別建立統一的規則和程序，以發展歐洲內部市場，使信任服務得到跨國界的承認，具有與其傳統的同等紙質程序相同的法律地位。

印度—數位實名認證（eKYC）

印度實施一個客戶憑證電子驗證系統 -- 數位實名認證（eKYC）。這個系統是經由生物辨識資料庫 Aadhaar 實施的，這是一個由印度單一身分識別管理局（UIDAI）所頒發的 12 位元識別碼。在註冊 Aadhaar 時，姓名、地址、性別、出生日期、手機號碼和電郵位址等細節被蒐集並納入印度單一身分識別管理局的資料庫。

FIs 金融機構可以使用數位實名認證應用程式介面（API）來獲取 Aadhaar 的詳細資訊進行驗證，印度單一身分識別管理局確保金融機構在處理資料時遵守既定的安全標準、保護措施和隱私標準。

客戶的認證是通過發送到記錄的手機號碼的一次性密碼，或通過生物識別科技完成的。這些關於電子實名認證的規定已於 2019 年被納入 2005 年防制洗錢（紀錄維護）規則（PMLR），規則 2（1）（ca）中定義 " 電子 KYC 認證設施 "（ca）。

中央實名認證登記制度（CKYC）

印度已經實施中央實名認證登記制度（CKYC），這是一個金融部門客戶實名認證紀錄的集中存儲，具有統一的實名認證規範，允許相互使用。

中央實名認證登記制度由印度證券化資產重組及證券權益統籌登記處（CERSAI）管理，避免客戶在建立業務關係之前不得不在多個金融機構履行實名認證手續。

中央實名認證登記制度已於 2019 年被納入防制洗錢規則，並在規則 2（1）（ac）中進行定義。

新加坡—MyInfo

新加坡在 2017 年推出首個被稱為 MyInfo 國家數位身分服務，其中包含從各政府機關匯集經政府驗證之資料。通過同意 MyInfo 的使用，居民和企業可以分享經過驗證的業務資料，從而最大限度地減少需要取得額外的實體或電子文件的處理。

使用 MyInfo 來執行客戶盡職調查，提高效率、安全性和客戶開戶流程體驗。它還使金融機構能夠在 COVID-19 大流行期間繼續導入新客戶，因為此時對遠端金融服務的需求更大。

94. 此外，能夠快速進行客戶盡職調查和客戶特徵分析的導入工具（如地理定位、信用檢查、反詐欺軟體等）也將充實客戶盡職調查和監控過程，並導向更準確地瞭解業務關係的性質以及對機構的影響。

95. 加強對科技的使用，對客戶進行篩選和匹配，對於改善合規程序有巨大潛力，因為對過時的和與區域無關的制裁、重要政治性職務之人和其他名單的依賴被認為是一個需要改善的領域（見案例11）。這些工具可以區分相似的名字和其他識別要素、克服語言差異、辨識負面新聞資訊和不同資料庫的交叉引用。自然語言處理和更進階的模糊比對工具可以為這一功能提供顯著的優勢。資料協調也將有助於消除偽陽性和詐欺企圖，因為行為者將開始依賴集中的資訊和不同的驗證系統。

96. 最後，當允許資訊分享和資料彙集之作法，旨在應對客戶盡職調查挑戰的數位解決方案將對 AML / CFT 的有效性貢獻最大，這也說明克服資料共用障礙的重要性。受訪者認為，協作客戶盡職調查是一個更有效的系統的重要元素，因此，政策制定者和監管者應集中精力解決這問題，一起找到適當的解決方案，使其與受監管機構在承擔其責任的需要上，按照風險基礎法互相協調。

案例 11. 用於客戶盡職調查的機器學習

巴西

具有系統重要性的巴西金融機構（SIFIs）在其監控和客戶盡職調查／員工／合作夥伴流程為識別新的洗錢／資恐風險，及提高分析速度和決斷發出警告的能力上，正在使用機器學習。

為此，他們擁有專業團隊、資料科學家和能夠支援大量資料的科技環境（例如：SAS、Teradata、R-Studio、Foundry、Hadoop、Python 等）。

關於監控過程和警報

通過使用分析工具和整合不同的資料庫，系統重要性金融機構創造可能發生之事態，從而減少錯誤的偽陽性警報，並提高警報分析的效率。應該指出的是，許多系統重要性金融機構正在創建各種主題情景，其結果被證明是有效的，特別是那些專注於涉及 COVID-19 大流行的情況，如用公共資源購買醫院設備和支付緊急援助。

基於梯度提升機制的機器學習演算法，一些系統重要性金融機構創建風險群組，可以通過群體而非個體分析進行決策，以便對向金融情報單位（FIU）報告警報的可能性進行評分。

一些系統重要性金融機構也在使用監督式分群演算法來訂定捕捉現金交易中的 " 離群值 " 的規則，而另一些金融機構則使用單變量和雙變量探索性分析、特徵分析和特徵工程科技來識別交易不在其範圍內的客戶。

一家系統重要性金融機構開發一種工具，使用分析科技來分析涉及警報的人之間的聯繫、對應關係、風險和地理資訊以支援其分析。

關於客戶盡職調查流程

系統重要性金融機構正在使用機器學習科技來支援其客戶風險評估，考慮與客戶註冊和金融交易有關的各種變數。

例如，一家系統重要性金融機構正在將機器學習科技（梯度提升演算法、隨機森林之決策樹演算法、投票機制之集成學習法等）與邏輯回歸相結合，選擇客戶進行強化的盡職調查。其他系統重要性金融機構正在開發工具以識別空殼公司，並根據註冊和財務資訊實施整合客戶監控。

成果

系統重要性金融機構已經在其 AML / CFT 的過程中獲得一些優勢，例如：

- 獲得有關其客戶行為的資訊品質更高，可以從客戶的角度發出警報；
- 通過識別對於被監督實體而言有更大風險之客戶發出警報，有更大的信心；
- 通過研究行為和模式，構建更有說服力的規則，減少偽陽性警報；
- 分析警報的有效性和效率；
- 對金融情報單位申報品質的改善，提供更多可疑交易的細節；
- 由於建立新的態樣規則，向金融情報部門提交的可疑交易報告的數量增加；
- 通過增加資料的關聯性，發現新的洗錢／資恐風險，以便做出更好的決策；
- 從企業集團各機構和外部供應商的登記和財務資訊中監控全部客戶的可能性。

3.5. 應用程式介面（APIs）

97. 應用程式介面是一種允許不同的應用程序進行連接和互相溝通的軟體。應用程式介面也經常被用來提供支付服務，例如，通過網站接受捐款。數位化轉型調查問卷的受訪者提到，應用程式介面是解決已確定的洗錢和恐怖主義融資問題的最常用和最相關的解決方案。

98. 應用程式介面在 AML / CFT 方面的效用在於能力，例如將客戶識別軟體與監控工具連起來，或將風險和威脅識別工具與客戶風險剖析聯繫起來，以便發生警報或改變相關的風險分類。應用程式介面允許這種整合更快地發生，而且資料集要大得多。這一點尤其重要，因為對許多金融機構來說，最困難的挑戰之一是整合許多不同的、往往不相容的系統，包括傳統科技及由不同的開發者創建的專門的工具。

案例 12. 應用程式介面的優勢

- 加強傳統銀行資料之間的互通性，擺脫架構分散的孤島式系統。
- 提高自動化程度以優化資源運用及輸出準確性。
- 提供整合且規範化的資料來源，有助於為新客戶建立一個更完整的風險剖析，例如在客戶開戶之程序。

99. 應用程式介面也為公部門提供巨大的價值，幫助他們存取營利事業登記處及其他機構之資料，以便在應對經濟的意外衝擊時為臨時監控目的進行靈活地修改，或在應對金融系統商業模式的變化時更為持久的監控[17]。

[17]（金融穩定委員會 , 2020[15]）

案例 13. 應用程式介面之應用

漢尼拔平臺

突尼西亞的金融情報機構、突尼西亞金融分析委員會（CTAF）在 2021 年 1 月推出了一項名為 " 漢尼拔平臺 " 的監管科技，對有形的跨境運輸現金進行永久監控。漢尼拔平臺是在突尼西亞金融情報機構的監督和領導下，執法機關（內政部和海關）、銀行、郵局、外匯局之間合作與協調的成果。

漢尼拔平臺旨在瞭解、識別和評估與有形的跨境運輸貨幣有關的洗錢和資恐的國家風險。

這個平臺是使用被認為是資料存儲領域最重要的現代科技之一的區塊鏈科技來設計，這項科技保證資訊的透明度，並提高其安全性，使其免受任何駭客攻擊。該平臺還依賴於連接利益關聯方（內政部、海關、銀行、郵局、外匯管理局和突尼西亞金融情報局）資料庫的應用程式介面）。

應用程式介面的使用使有關當局能夠獲得關於外幣進口量和所有與外幣有關的銀行業務的即時資料，以及執法機關查獲的外幣的即時資料。

利用該科技，有關當局有可能監控出口或進口並向海關申報的貨幣的最終目的地。它也有可能進行幾個交叉點，根據程式設計的參數獲得即時警告，甚至將資訊轉化為情報。

該平臺使突尼西亞當局能夠採取適當的措施，以減輕與貨幣實體跨境運輸有關的洗錢和資恐風險。

多帳戶整合器

IndiaStack 是一套應用程式介面，允許政府、企業、初創企業和開發人員利用獨特的數位基礎設施以實現非面對面、無紙化和無現金之服務提供來解決印度的金融問題。

India Stack 提供四個不同的科技層面，包括一個通用的生物識別數位身分，一個適用於全國所有銀行帳戶的單一介面，一個分享資料的安全方式，以及數位身分記錄自由移動的能力，消除對紙張蒐集和存儲的需求。

這一基礎設施包括 Aadhaar、eKYC、eSign、DigiLocker 及 UPI，這些工具正在促進該國開放銀行的有序發展。

美國社會安全部之許可社會安全碼驗證服務（CBSV）

許可社會安全碼驗證服務使用一個應用程式介面節點，合格的金融機構或其授權的服務提供者（許可實體）可以在個人同意的情況下，為法定的特定目的，驗證許可實體提交的個人姓名、社會安全碼和出生日期是否與社會安全局記錄中的資訊相符。許可社會安全碼驗證服務以 " 是 " 或 " 不是 " 為結果返回匹配驗證。如果社會安全部記錄顯示社會安全碼持有人已經死亡，許可社會安全碼驗證服務也會返回一個死亡指示。許可社會安全號碼驗證服務並不驗證個人的身分。

目前，許可社會安全碼驗證服務通常被提供銀行和抵押貸款服務、處理信用檢查、提供背景調查、滿足許可要求等的公司使用。許可社會安全碼驗證服務有一次性 5,000 美元的初始註冊費，以及每筆社會安全碼驗證交易的費用。

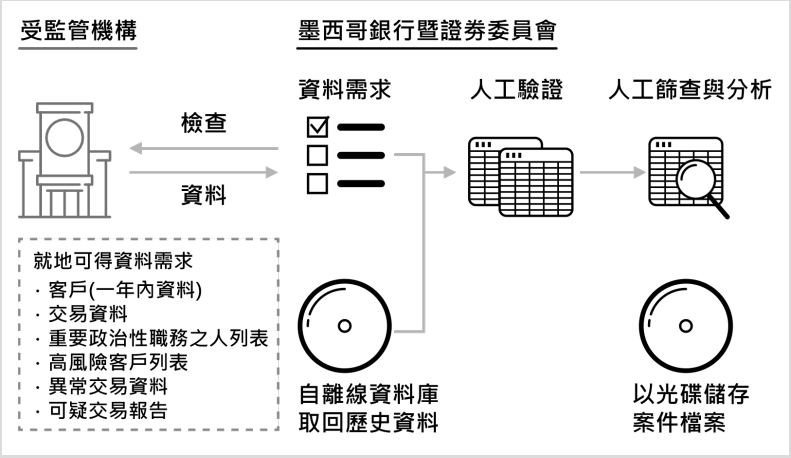
100. 除促進機構內部程序進行外，應用程式介面還促進行為者之間的溝通。

101. 監管人員在與人工智慧驅動的分析相結合的情況下使用應用程式介面時，可以提高義務申報實務的效率和以風險為基礎的監管品質。如下文案例 14 所示，這種類型的工具可以讓監管者在結合實地檢查資料和背景因素處理歷史資料，並生成自動報告以供考慮和確定行動。

102. 這種自動化分析為受監管機構提供更即時和詳細的回饋監管過程及期望的可能。

案例 14. 墨西哥

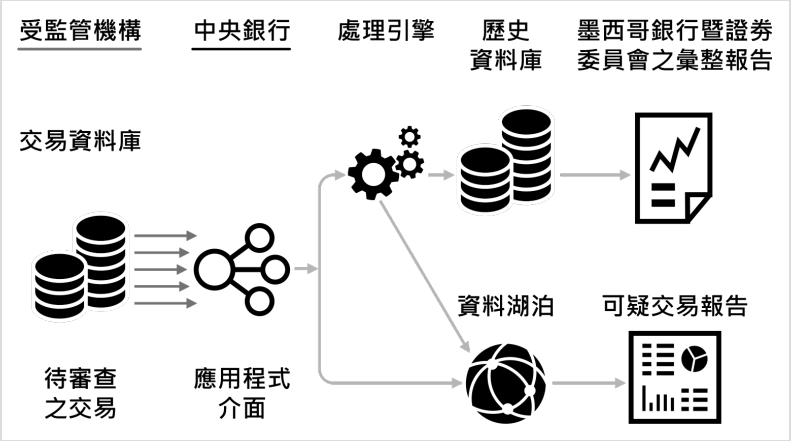
效率低下的防制洗錢資料結構，加上許多被歸類為中高風險的金融機構，導致無法在實地訪查取得的資料得到深刻見解，不然就是延遲和無效的審計成果。



出發點是什麼？

監理科技的創新解決方案：

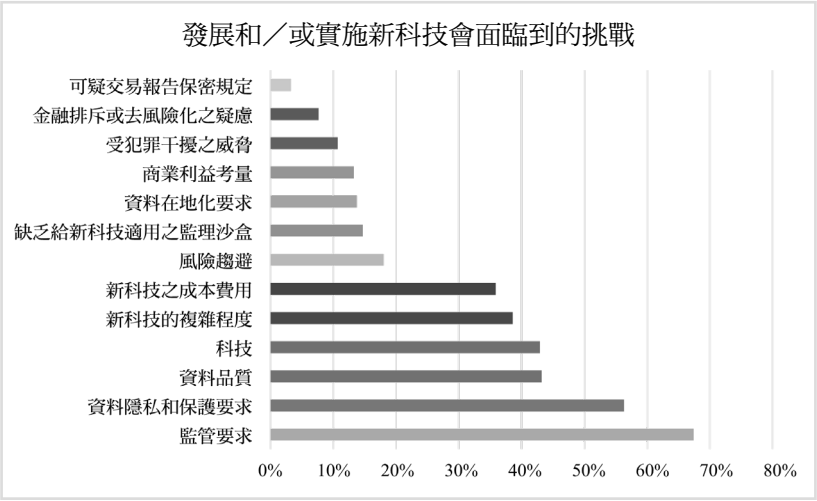
一個基於應用程式介面的防制洗錢資料結構和人工智慧驅動的分析工具，其中包括：一個集中化平臺，用於向受監管機構產生標準化、自動化的請求，通過推送或搜尋，提交存儲在資料湖泊中的原始資料。一種用於建立安全、直接的機器對機器資料傳輸的應用程式介面，將資料餵入處理引擎進行即時運行驗證測試，驗證報告的品質、內容和結構，並將處理後的資料輸送到資料湖泊中，建立一個綜合的、單一的和具存取控制的資料架構。人工智慧驅動的分析工具，使用預測分析和機器學習技術（集群分析、神經網絡、邏輯回歸、隨機森林等演算法）偵測可疑交易，並基於金融機構的潛在曝險情形來優化反洗錢警報。透過儀表板和追蹤關注名單以觀察反洗錢風險的概況。



4. 實施 AML / CFT 新科技之挑戰

103. 在 AML / CFT 架構中採用和實施新科技並非沒有挑戰。核心挑戰不是在監管方面，就是在操作方面的部分[18]。

圖 3. 發展和／或實施新科技會面臨到的挑戰



4.1. 監管方面之挑戰

104. 為本報告蒐集的資料顯示，FATF 和國家主管機關需要明確支援 AML / CFT 方面的創新。一些專家表示，希望有 " 科技積極的監管者 " —監管者願意與科技開發者接觸—而不是科技中立的態度。受訪者認為，主管機關和 FATF 缺乏明確支持，導致對新科技的興趣、投資和信任減少，儘管它們具有潛力。

18 正如所證實（Richard Grint et al, 2017[14]）

105. 新科技對監管者的可理解性和可解釋性[19]是確保支持這些工具的關鍵。受監管的機構在建置這些新科技之前，必須能夠解釋並保留創新解決方案的原理和科技細節。監管者必須能夠理解人工智慧工具所使用的模型，以確定其準確性及其與所識別風險的相關性。然而，一些回覆者表示，大多數監管者不具理解和充分監督新科技之專業知識或是資源。

106. 受訪者還提到，即使是最懂科技的監管者，在調整監管作法方面也往往進展緩慢。事實上，雖然一些司法管轄區已經通過創新活動和其他形式的監管支持促進新科技的採用（見案例 15），但這些努力並不總是轉化為監管部門對新程序和合規作法的接受。

案例 15. 利用公共基礎設施促進數位客戶盡職調查程序

丹麥金融服務局最近發佈一項關於科技倡議的公共諮詢，這些倡議可以支援受 AML / CFT 法規約束的機構致力於打擊金融犯罪，即 "AML / TEK 計畫 "。其目的是激起這個非常重要的話題的討論，並獲得確保對未來進行有啟發性的政治討論的觀點。

該分析提出有可能強化第一道防線之七項倡議之利與弊。總體上反映丹麥社會的高度數位化性質，但也提出有關權衡取捨的普遍利益的問題，特別是在打擊金融犯罪與資料保護和隱私之間。

該分析旨在為進一步討論提供基準線。大多數倡議對義務實體和客戶都有法律上的影響，同時也提出關於存取和分享有關資料的法律基礎問題。這些倡議中有三項可以支援客戶盡職調查程序的進一步數位化。

[19] 更詳細的觀點，詳（EBA, 2020[17]）

增加對相關商工登記處的使用

義務實體將其客戶盡職調查程序數位化的一個核心障礙是缺乏經過驗證的數位客戶資訊。由於丹麥當局有數個登記處有相關客戶的資訊，該分析研究允許增加對這些登記冊的使用。該分析研究對幾個登記簿中資料的存取，例如丹麥商業管理局、丹麥稅務局、護照和駕駛執照登記處、丹麥移民局登記處等機關持有的資料。

丹麥商業登記處的品質資料保證

丹麥商業登記冊中的資料是由有義務的實體自己提供的。因此，儘管大多數公司的主要資料可以通過應用程式介面存取，並受到控制環境的各式各樣影響，但不能確定能否識別所有錯誤或誤導性的登記，這影響資料可能不適用於對客戶盡職調查此一目的。因此，該分析建議研究是否有可能建立一種機制，藉由律師和合格會計師能夠核實註冊資料。

重要政治性職務之人之檢核方案

對義務實體來說，檢核政治人物及其關係是一個耗費大量人力資源的過程，需要他們獲得有關其客戶的個人資料。在丹麥，這種關係在很大程度上可以通過公共登記冊進行繪圖，儘管這引起嚴重的資料保護問題。該分析著眼於建立一個公共的 PEP 檢核方案，通過提高數位化程度來提高重要政治性職務之人檢核結果的品質並降低其成本，同時儘量減少個人資訊的蒐集。

107. 只有當系統建立在標準化資料的基礎上，關於 AML / CFT 的新科技其使用才能真正變得有效，且更容易被科技開發人員整合到他們的工具中、簡單易懂、並容易向一般人解釋，同時在需要時易於與對應方和主管機關溝通。這個問題也顯示公部門，特別是金

融情報機構，向申報機構提供可用於培訓目的之可靠的可疑活動和機器學習案件的回饋的重要性。如果可以的話，用已經積極核實為涉及洗錢或資恐的真實案件訓練機器學習系統，會比訓練人工智慧來複製人類合規人員對於是否達到合理懷疑的程度的決定提供更好的命中率。此外，金融情報機構和其他主管機關能夠通過自動化程序提供關於哪些報告最有用的回饋，這也將有助於金融情報機構培訓及通知內部合規團隊及系統。

108. 資料協調（或缺乏協調）也是被提及的另一個障礙，因為如果這些系統需要根據不同司法管轄區的要求和格式進行微調和改變，那麼投資於新科技和專業知識的成本就會成倍增加。因此，資料協調為創造一個有利於實施新科技的環境提供巨大的優勢，因為它使各行為者在目標上趨於一致，例如，一個共同的交易監控，向私部門提供回饋和風險評估。45% 的數位轉型調查問卷受訪者都有同樣的擔憂，都認為如何確保資料品質是採用 AML / CFT 科技解決方案的一個障礙。

109. 確實存在或是已被意識到的判讀爭議同樣導致在科技提供者與使用者之間建立值得信賴的關係的能力受到限制，以及無法信任經過新科技處理的資料是可靠的。儘管如此，越來越多的參與者正在大規模地登錄資料，這種業務規模的擴大意味著匹配不同複雜資料庫的能力增強。

110. 60% 的數位轉型問卷調查的回覆者認為，作為新科技提供者的第三方廠商其作用已經足夠明確，但私部門的回覆者要求就如何解釋數位時代的現行法規提供額外指導。

111. 私部門要求對使用新科技之實體的責任制、透明度和監督問題作出進一步說明。隨著採用此一領域科技的速度加快，監管者應反思受監管機構正在採用何種工具，以及這些工具的提供者（供應

商）是否應受到額外的審查，例如比照服務提供者去管理使用其科技的實體或是經由單獨的規範和監管。主管機關或許還可以考慮被監管機構和／或監理機關使用的 AML / CFT 的創新科技是否可以通過新的合作形式得到更有效的利用；例如，公私合作或擴大被監管機構對政府資料庫存取權限。然而，使用創新解決方案不應讓受監管機構的最終責任受到質疑。

112. 雖然增加採用新科技可能會強化監管的執行，但回覆者提到必須在科技整合的重要性和以人為本的前瞻性監督程序的重要性之間取得平衡[20]。為採用這種方法，大多數可用的工具仍然將人力投入和人工審查作為關鍵組成的部分，並證明這些工具不是對現有系統的替代，反而是增強其功能[21]。

113. 人們認為，人力投入和能力建設在幫助採用 AML / CFT 的新科技方面持續發揮重要作用，特別是在科技仍無法克服的部分、區域不平等或關於新議題的專門知識等方面。本報告提出許多就 AML / CFT 方面成功合作的實例，這些合作是以科技為輔，主要依靠行為者之間的交流和支持來獲得成功。例如，這些公部門與私部門行為者之間的合作方式，為識別洗錢／資恐紅旗指標的目的，能夠證明使用科技解決具體挑戰的直接好處，同時不是為有效性而完全依賴這些工具[22]。

20（金融穩定委員會, 2020[15]）, 第 32 頁 .

21 關於監理科技領域的相關發展及其與監管報告的連結的更多資料，請參見 Crisanto 等，《從資料申報到資料分享：監理科技和其他創新如何挑戰監管申報之程度現狀？，（BIS, 2020[18]）

22 例如，見打擊犯罪專案，以通過人工智慧在金融公私部門合作的方式，以智慧和全面的方式打擊破壞法制的犯罪，如人口販運、洗錢及腐敗。詳：www.uva.nl/en/about-the-uva/organisation/faculties/amsterdam-law-school/research/research- themes/labour-exploitation-human-trafficking/labour-exploitation-and-human-trafficking.html. 另見非營利性專家網路 The Knoble 的工作，該網路致力於通過協作和基於科技的方法預防金融犯罪。詳：www.theknoble.com/

114. 同樣地，與依靠從多個來源蒐集資料的系統相比，以國家發給的數位身分工具為系統似乎更可以在數位身分系統和協作平臺上採集資料取得更大的成功。資料驗證可能是一個方面，人類的威信將繼續佔據優先地位。此外，隨著新科技的使用越來越廣泛，行為者也必須考慮機器的錯誤，可接受或無法接受的程度。

115. 除其他與 AML / CFT 無關的原因外，AML / CFT 效率的提高也受到受監管機構無法與其對應方和跨國界分享資訊的限制。最終，為充分瞭解可疑交易的性質和風險，需要獲得金流之全部路徑，而這些金流路徑往往跨國界或由其他實體掌握。正如 FATF 在盤點資料庫、協作分析和資料保護的評估報告中所作的深入討論，新科技可能為克服這一挑戰提供重要價值。

116. 最後，在私部門應對措施中，安全及保護免受犯罪干擾的問題並沒有出現在已確定挑戰的清單上，而儘管從公共政策和執法角度來看，這個問題可能更加重要。儘管如此，與使用科技有關的刑事案件越來越多，例如，與身分詐欺或使用 " 錢騾 " 的犯罪活動有關，在評估新科技對受監管機構的營運和一般犯罪活動的影響時，應考慮到這一點。

4.2. 操作方面的挑戰

117. 操作方面的挑戰主要涉及適應新的作法及未經測試的系統或科技解決方案。回覆者提出的核心問題包括：新科技的成本、承辦人理解及培訓人員實施科技的能力，以及用新工具取代舊系統的問題。

118. 儘管優勢被廣泛承認，但監管者對新科技的採用程度仍落後於私部門的水平。受訪者強調，監管者需要更新自己的系統和監管策略，以便在數位時代對於 AML / CFT 能有更佳的闡釋與監管。

119. 監理機關指出最大的困難是更換舊有系統相關的成本、提供 AML / CFT 數據的優質報告以及可用的專業資源與熟練的專業人員。

120. 例如，更新舊系統的採購程序過於複雜、冗長，而且往往沒有針對正確的操作人員。一些回覆者說，監理科技的公共採購程序對科技供應商來說往往不感興趣或不明顯，因為它們需要對公共採購程序和具體治理目標的瞭解，而這正好是科技開發商缺乏的。此外，公部門尋求的科技在進入採購階段時往往已經過時，或者要求的方式過分規範，對科技供應商沒有吸引力（即要求獨家經營）。這種作法阻礙開發商為監管人員生產現成的產品。

121. 這方面的挑戰包括不願意投資於新科技，因為這些科技可能：難以與舊系統整合和／或超出受監管機構的科技能力，進而無法適當和有效地使用；變得過時，反而需要額外投資於較新的解決方案；不符合監管預期或無法滿足特定的檢查人員，後者可能缺乏評估解決方案有效性的能力或因其他原因對創新解決方案感到不自在；存在風險，包括潛在的隱私侵犯和 AML / CFT 合規失敗。特別是較小的金融機構，其內部往往缺乏能力或信心，無法在大量且不斷增加的競爭的供應商和產品中評估特定創新解決方案的有效性，也無法確定解決方案是否適合機構自身的風險狀況、客戶群和業務活動，也無法實施和管理這些模型的風險。

122. 總體而言，受訪者同意，在瞭解新趨勢和新興數位解決方案方面，一些監管者之參與不如私部門深入。監管者缺乏專業技能（和資源）及知識，增加對新科技的可理解性的挑戰，而且在大多數情況下，限制其對 AML / CFT 的有效性的潛力。

123. 一些回覆提及，由於缺乏協調所以可能無法大規模地使用新科技。這有可能使創新無法達到成本效益，並阻礙其發展。例如，最有效地運用大數據，需要跨多個實體之間提供。如果沒有這種可擴

展性，一些科技工具可能在財務上是不可行的。

124. 此外，無法開發科技以擴大規模，也加劇大型及小型實體以及不同區域之間的吸收差距。受訪者同意，只有在有更重要的激勵措施，無論是強制使用還是更大的信任環境，支持投資並證明較小的金融操作和其他非金融義務實體的改革是合理的，才有可能更廣泛地實施科技。

125. 新科技改善資料品質，但仍然依賴人力資料輸入及人工審查。機器學習工具依賴於現有的系統及其人工更新，因此可能會產生輸入＂壞資料＂的情況，然後對採用的模型產生負面影響。這包括例如學習識別可疑交易等機器學習系統被訓練用的資料。如果訓練資料包括偽陽性或其他錯誤，這些錯誤將被＂訓練＂到機器學習系統中，儘管對於人為偏見或未識別的錯誤，仍然需要一定的誤差幅度。

126. 藉由自然語言處理工具實現初始資料登錄的自動化，也可以通過儘量減少客戶或工作人員錄入資料時發生的錯誤來提高資料品質。

127. 最後，消費者對金融服務中的新科技的渴求被認為是新科技採用與否中最不重要的驅動因素之一。然而，隨著客戶盡職調查和其他以個人為中心的數位解決方案變得更加突出，其作用和消費者觀點可能會變得越來越重要。

128. 在克服已確定的監管和操作挑戰時，考慮納入客戶對傳統的客戶盡職調查和監控程序的反應或許是值得，但也要考慮新的適用方法以及這些方法對資料保護和隱私的影響。消費者可能不會影響這些科技的發展，但還是會受到改變客戶與受監管機構互動的體驗的工具的影響。雖然將新科技用於 AML / CFT 也可以有利於客戶體驗，但在採用和實施這些工具時，必須考慮到數位化的風險和意外的後果。

129. 最常提到的數位化風險為犯罪分子對系統的濫用，以及它對增加社會特定階層的脆弱性和金融排斥，即老年人、農村或遙遠的（較少連結或偏遠）社區。

案例 16. 克服操作挑戰

香港金融管理局（HKMA）採取一系列措施，以確定銀行在採用新科技時遇到的常見操作困難，並開展一系列活動，以協助銀行克服這些挑戰，首先是在 2019 年 11 月舉辦的 AML / CFT 監管科技論壇。在 2020 年一整年，在三個工作組中根據科技採用的完善程度，與約 40 家銀行進行對話，以更瞭解如何將監管科技作為加強 AML / CFT 流程的一種手段。

這項工作在 2021 年 1 月達到頂點，金管局以發表 "*AML / CFT 的監管科技案例研究和見解* " 的報告（香港金融管理局／德勤，2021 年 [15]）的形式分享實施 AML / CFT Regtech 銀行的實務經驗。該報告旨在通過分享案例研究和說明所採用的不同方法（例如，以使用案例為基礎的方法與以解決方案為基礎的方法）來建立意識，並降低採用 AML / CFT 監管科技的實際和自覺障礙。報告還提供早期採用者的見解、科技亮點和解決關鍵操作挑戰的指導（如資料和流程準備、利益關聯方的購買和行政支援，以及與供應商合作時的考量）。該報告整個架構是方便讓採用成熟度不同的銀行，可以找到他們感興趣的科技應用或與他們產生共鳴的挑戰。針對不同成熟度群體的後續活動，例如通過進行中行業分享和互動實驗室會議。

4.3. 意外後果和濫用之可能性

130. 金融機構在創新科技的使用不僅帶來重大和潛在的變革性好處，也帶來與隱私、包容、公平結果等競爭目標的潛在衝突及意外後果的風險，以及容易被故意濫用的風險。雖然人工智慧已經成為包括金融服務、醫療保健、零售和製造業等行業在內的基本工具，提高效率、降低成本，並加速研究與開發，但其日益增長的使用已引發一系列道德和法律問題，產生廣泛的要求和許多工作流以制定適當的政府及私部門標準和保障措施。

131. 人工智慧／機器學習解決方案在科技和使用方面都有相當大的差異，同時還可能會帶來重大風險。潛在的缺乏可解釋性和透明度會破壞評估人工智慧／機器學習解決方案在識別可疑交易和其他非法活動方面的準確性的能力，從而無法確定其作為 AML / CFT 法遵工具的有效性。此外，儘管演算法決策似乎提供一種足以克服人類的主觀及偏見的客觀方式，但研究人員發現，許多人工智慧演算法複製程式開發人員有意識和無意識的偏見，這些偏見隨著工具被大規模使用，不公平地將某些類型的個人或實體的金融活動作為可疑的目標，或產生拒絕他們獲得某些金融產品和服務之風險輪廓及決定。

132. 同樣地，儘管值得信賴的數位身分解決方案可以大大加強開戶時的客戶識別／核實，支援其他客戶盡職調查措施，促進普惠金融的同時並助於打擊詐欺和網路犯罪，但數位身分解決方案如果不能提供足夠的風險基礎科技保證和適當的治理，就會帶來作業風險和潛在的意想不到的後果。這些解決方案還可能被故意濫用。

133. 在不考慮風險基礎法或比例原則情況下採用數位身分解決方案，可能會加劇對本就缺乏金融服務社區的排除。例如，尋求庇護者可能無法提供為生成這類數位身分證而要求的初始文件。數位身

分證工具還有其他潛在的意外後果需要考慮，特別是與潛在的個人資訊披露有關的挑戰。

134. 當被用於金融服務時，要求客戶提供的個人資料量增加，因為基於客戶盡職調查和防制洗錢監管的目的，必須高度保證個人的真實身分。然而，為適當落實普惠金融目標，數位身分證工具在設計和操作上應具有包容性[23]。

135. FATF 要求 " 可靠和獨立的數位來源文件、資料或資訊 "（FATF, 2020[8]）。這意味著用於進行客戶盡職調查的數位身分工具為系統產生準確的結果提供適當程度的信心，必須依靠科技、適當的治理、流程和程序。

136. 為此，應查明並減輕身分識別系統中的法律、程序和社會障礙，並特別關注得不到充分金融服務的人群和可能因文化、政治或其他原因面臨被排斥風險的群體（如婦女、兒童、農村人口、少數民族、語言和宗教群體、移民、被迫流離失所者和無國籍人士）。（世界銀行，2021 年 [16]）

137. 作業風險和風險抵減措施，包括對非預期的排斥和隱私風險，是在 FATF 的數位身分指引第五節[24]中被拿來討論的。鼓勵各利益攸關方參考該文。此外，世界銀行更新的持續發展身分識別原則：邁向數位時代（世界銀行，2021 年 [16]）提供一套基本原則，用以指導數位身分系統的設計、治理和使用，目的是確保這些系統具有包容性，基於同意，保護隱私和其他權利，並且是公平和負責任的。

---

23 個人保護公約諮詢委員會關於自動化處理個人資料公約第 108 號。詳（Walshe, 2020[20]）

24（FATF, 2020[8]）第 35-45 頁

案例 17. 生物識別資料帶來的挑戰

生物識別數位身分工具可能引發潛在的人權衝突，主要涉及隱私權（如世界人權宣言第 12 條）和免於歧視的自由（如世界人權宣言第 7 條）。這種潛在的衝突反映於一些法律和公約中，現代化的歐洲委員會第 108 號公約（108+），以及歐盟通用資料保護（GDPR）條例，該條例認為 " 生物識別資料 " 是一種特殊的、需要更高程度保護之資料類別，以保障個人免受其使用的不利影響。也有人擔心，生物識別科技的廣泛範圍及其快速發展和用於多種目的，可能會使基本人權受到威脅。（CoE, 2011[17]）

如果數位身分解決方案強制以生物統計學為基礎，它們將有可能成為一種普遍的識別、追蹤或控制手段，對隱私權產生負面影響。

因此，非政府機關蒐集的生物識別資訊應被視為受保護的資訊，應遵守國際法律文件對此類資料規定的法律標準，並根據比例原則和必要性原則限制其使用。

4.4. 評估 AML / CFT 科技解決方案的有效性以及如何解決剩餘風險

138. 隨著各參與者在克服上述挑戰後開始部署新科技，受監管機構必須不斷審查這些新科技在偵測和打擊洗錢／資恐風險方面的有效性。通過對有效性進行衡量，將鼓勵受監管機構更加注重結果，確保採用的新科技符合目的，並在其生命週期內繼續發揮充分作用。

139. 這些有效性的衡量也讓公共及私部門在沒有達到預期的目的時，可以重複調整其科技解決方案。同時，有明確的衡量標準，將有助於幫助監管者評估被監管實體採用的新科技。

140. 此外，所有參與者都應評估使用新科技是否會產生剩餘風險，或者是否存在新科技無法完全替代的關鍵人為因素。必須確保的是不會過度依賴新科技，當發現有剩餘風險時，受監管機構應展示對這些風險的認識，以及在需要時管理或應對這些風險的能力。

141. 儘管如此，已經確定制定這種有效性指標和確定可接受的有效性程度或剩餘風險是具有挑戰性的，並且有分享最佳作法和／或指導的範圍。

5. 為在 AML / CFT 中使用新科技創造有利環境

142. 受訪者同意，FATF 和主管機關在克服實施 AML / CFT 新科技方面的現有監管和操作挑戰仍然有很長的路要走。然而，重要的是去檢視消除系統障礙後所產生的意外後果[25]，例如，更迅速的交易執行表示識別犯罪活動的時間減少，系統試圖發掘和預防金融犯罪的壓力則會增加。

143. 新科技運用於 AML / CFT 的機會和挑戰更多來自於監管和政策反應，而不是額外的科技發展。使用新科技的具體情況對公共和私部門都是有價值的，因為它提高 AML / CFT 的整體能力，資料蒐集及視覺化的能力更佳，監控犯罪活動的能力，同時更有效地利用資源[26]。

144. 各種推動監理科技和監管科技的方式已受到討論（BIS，2019[18]），強調高階管理層接受的重要性以及確保可解釋和可說明的必要性。受監管機構向其監管者和內部展示新科技的好處的能力是充分採用和監督的關鍵。展望未來，重點應該是利用科技來應對已確定的挑戰，並證明在實現 AML / CFT 的有效性方面的進展。

145. 監管部門與行業機構合作確認努力克服可解釋問題的其他例子，即指導行業如何解決 " 黑盒子 " 模式。（mas, 2018[18]）

146. 如案例 18 所示，一些司法管轄區和大多數大型金融部門實體已經開始採用新科技，作為常規合規工作的一部分，但強調只有當這些科技被全球大多數業者大規模採用時，才能實現其真正的附加價值。

25（世界經濟論壇 , 2020[24]），第 21 頁

26 同上，第 18 頁

案例 18. 俄羅斯聯邦金融監測局網站上的個人帳戶

俄羅斯聯邦金融監測局（俄羅斯聯邦）在其網站上積極開發個人帳戶（PA），作為與私人部門溝通的機制。個人帳戶作為IT解決方案，結合監理科技和監管科技功能。最初，個人帳戶被設計用來提交可疑交易報告和分發指定人員名單。

在 " 試驗 " 模式結束後的 2018 年間，個人帳戶成為所有報告機構的強制性規定。目前，有 8 萬個報告機構，包括 6 萬個經常使用個人帳戶的指定之非金融事業或人員。在私部門已被證明這是一種有效的風險緩解工具。

個人帳戶允許送達俄羅斯聯邦金融監測局使用的自動遠端監控系統（ARMS）中產生的資訊，以計算監督目標的風險評估。每個報告實體可以收到有關其活動，涉及內部控制的所有方面（提交可疑交易報告、風險管理、指定人員名單的使用等）的缺陷的資訊，使各機構能夠遠端減少缺陷。

這一功能對指定之非金融事業或人員部門尤為重要。每年約有 2,000 家指定之非金融事業或人員通過使用從個人帳戶收到的資訊成功地減輕缺陷。

個人帳戶作為可疑交易報告的回饋機制發揮作用。它向金融機構提供資訊流質量指數，其中包括界定義務實體報告可疑交易的有效性的若干標準。

個人帳戶允許金融情報機構交流關於洗錢／資恐風險和類型的資訊，傳播國家和部門風險評估的結果。

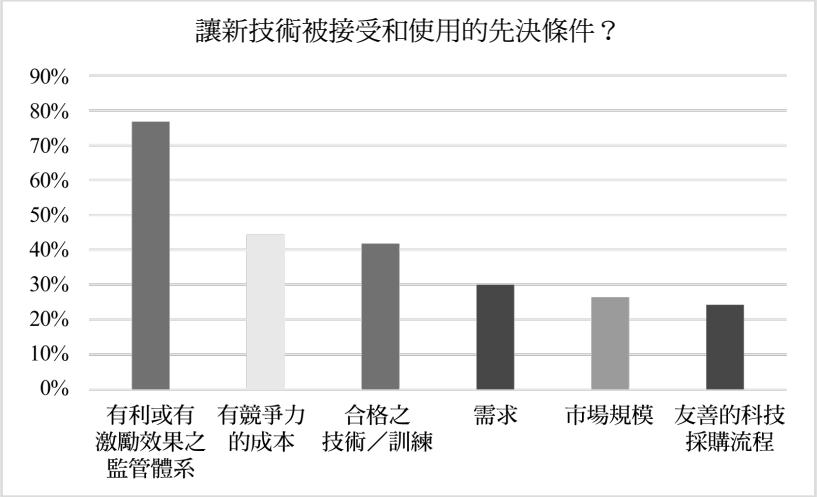
個人帳戶旨在提高私部門對立法要求的認識水準。遠端電子學習在這個過程中發揮重要作用。

PA 金融監控國際培訓和方法中心開發一些培訓課程，並放在個人帳戶中。很快將另外推出關於重要政治性職務之人和實質受益人風險管理的具體課程。

2018 年，為監管人員推出個人帳戶。它有助於俄羅斯聯邦金融監測局和監督機構之間就操作風險進行交流。

147. 如圖 4 所示，有利的監管環境、有競爭力的成本、專業知識（培訓）和規模被認為是採用新科技的關鍵前提條件。

圖 4、讓新技術被接受和使用的先決條件？



148. 監管人員對於科技應採取積極主動的方法。這將是促進採用和使用新科技的先決條件，並協助成員更有效地執行 AML / CFT 的標準。

5.1. 熟悉科技的監管者 [27]

149. 如果監管者與 FATF 對新科技表現出更積極的支持，將有助於應對受監管機構所表達的突出風險和信任問題。許多司法管轄區已經開始支持新科技，其形式包括科技衝刺、加速器、創新中心和其他合作倡議，讓私部門能夠開發、展示和測試其工具，並獲得關於其對 AML / CFT 架構適用性的回饋（見下文案例 19）。FATF 與個別監管人員都不應該對個別科技或供應商採取立場。遵守 AML / CFT 要求的責任仍由被監管機構承擔。相反，FATF 及各國主管機關的作用應該是促成創新和新方法，允許市場在適當的監管和監督範圍內為值得信賴和經過驗證的科技背書，並尊重國家政府制定的公共政策目標。

150. 雖然這些機會值得注意（更多例子，詳附件 C），但受訪者認為，這一領域的合作必須超越特定事件，監管者和被監管機構之間採取持續交流和合作的形式。機構為克服對監管處罰或制裁的恐懼，需要比受訪者所經歷的更持續的互動，例如採取適應數位時代的全面監管戰略改革或案例 20 中建議的具體實施指南的方式 [28]。

151. 提交給歐盟委員會的一份報告支持這種看法，該報告提出 " 關於監管、創新及金融的三十條建議 "（EC，2019 年 [19]），其中許多建議得到本報告結論的證實。其中，需要：澄清人工智慧和相關科技的可解釋性和可理解性，促進數位身分證的使用並取消默認的書面要求，促進科技驅動之金融服務的使用，以及制定和實施支持監管科技和監理科技之措施。

---

27 不應與認可特定科技或數位解決方案相混淆。FATF 和監理機關應保持科技中立。

28 另請參閱香港金管局的經驗作為最佳實踐的例子。（HKMA, 2020[26]）

案例 19. 創新中心、科技衝刺和沙盒實例

德國聯邦金融監管局

德國聯邦金融監管局在 2020 年啟動一個名為 "TechBridge " 的專案，為創新者建立新的制度化交流模式，包括 AML / CFT 問題。其核心部分涉及保密的個人研討會，由一名創新者和一組選定的德國聯邦金融監管局專家參加。

這些研討會可以在創新工具的研究和開發階段就開始舉行。首先也是最重要的，新工具必然會引起新的監督和／或監管問題。

進一步的選擇標準包括新工具是否會對金融市場產生重大影響並可能帶來高風險。

英國金融行為管理局

英國金融行為管理局已經採取一系列措施，鼓勵負責任地使用新科技來履行 AML / CFT 的義務。

英國金融行為管理局監理沙盒允許受監管機構在實際市場環境中測試創新產品、服務和商業模式，同時確保適當的保障措施到位。該沙盒從 2016 年 6 月開始接受申請，已經有六個完整的沙盒計畫。在所有這些佇列中，受監管機構圍繞交易監控和身分驗證測試防制洗錢創新解決方案。受監管的實體與沙盒計畫密切合作，以確保風險被識別並得到適當的緩解。主要的干預措施是為防制洗錢法規的應用提供早期指導；使受監管機構能夠反覆運作其業務模式；並指導受監管機構通過對推出新業務、服務或產品至關重要的監管程序。

2017 年 7 月，英國金融行為管理局發佈一份受博安諮詢公司委託的報告，內容是如何利用新科技來簡化 AML 之合規。

在演講中明確表示，科技提供改善反洗錢合規的機會，英國金融行為管理局鼓勵試驗和部署這種創新。英國金融行為管理局投資、批發和專家監管執行董事 Megan Butler 在題為 " 將科技用於打擊金融犯罪 " 的演講中談到英國金融行為管理局的觀點，即這些科技被用於正確的目的，可以成為遊戲規則改變者。

鼓勵監理機關和監管科技供應商之間就受監管機構使用科技進行互動和知識分享。舉辦 " 科技博覽會 "，讓現有和潛在的市場參與者展示正在開發和在市場上使用的解決方案，讓監管者更瞭解優勢，並提出關切。積極鼓勵討論目前在金融服務領域尚未或廣泛使用的新興科技如何提供益處，例如，2019 年的科技衝刺將探討 PETs 在打擊金融犯罪和洗錢方面的潛力，從而顯示機構對採用新解決方案的承諾。

瑞典金融監管局

瑞典金融監管局在 2018 年成立一個創新中心，目的是提供指導、提供資訊，並與受監管機構和在金融部門提供創新產品和服務的初創公司保持持續對話。創新中心還安排研討會和資訊聚會，並參與和金融業創新有關的外部活動。目前的一個例子是在快速發展的虛擬資產領域與來自私部門的不同服務提供者進行圓桌討論。最近在這些活動中討論的主題是新的相關法規和歐洲銀行關於 AML / CFT 領域的風險迴避和風險抵減措施的修訂準則。瑞典金融監管局的立場是，只要瑞典金融監管局的主要任務不被忽視，金融監管不應阻礙金融業的發展和創新。瑞典金融監管局對加強消費者保護的創新持積極態度，同時對金融穩定、良好運作的市場和可持續發展作出貢獻。

案例 20. 新加坡金融管理局

鼓勵金融機構為提高 AML / CFT 成果，
負責任地使用新技術 - 關鍵因素

新加坡金融管理局（MAS）與金融業者一起制定一套原則，以促進金融業者在使用人工智慧（AI）和資料分析方面的公平、道德、負責和透明（FEAT）之準則。這套準則為金融機構（FI）負責任地使用人工智慧和資料分析提供指導，以加強相關資料管理和使用的內部治理能力。

針對 AML / CFT 領域，新加坡金融管理局一直在積極與業界合作，以解決實施 AML / CFT 資料分析方面的關鍵挑戰。2019 年，新加坡金融管理局通過新加坡的 AML / CFT 行業夥伴關係（ACIP）與金融機構合作，就資料分析問題交流觀點。在研討會上，新加坡金融管理局和業界達成三個關鍵原則，即治理、模型可解釋性和模型性能，並鼓勵負責任地採用新科技。大家一致認為，隨著金融機構在應對金融犯罪方面採用更多的創新方法，在健全治理方面不應妥協。可解釋性也應是系統有效的設計重點，並應在系統開發之初就加以考慮。

152. 創新方法和協作監督也在最新興的新科技領域中被確認。分散式帳本科技已被確定為對虛擬資產的監督具有特別重要的意義。在全球範圍內制定一些倡議，以支持這些科技的發展，並創造一個有利於利益相關者能夠進行對話的環境，並克服與創新相關的一些挑戰。

153. 與通過銀行等傳統中介機構進行的交易不同，基於分散式帳本科技的虛擬資產交易往往在不使用或不參與中介機構和其他義務實體的情況下進行，它們在實現監管目標，特別是與 AML / CFT 有關的目標方面面臨障礙，原因是其獨特性質可能導致追蹤和監控交易方面的困難。隨著虛擬資產的普及，通過使用中介機構來降低風險的作法可能會在中長期內成為挑戰。

154. 因此，在虛擬資產交易和區塊鏈金融領域，一個有前景的方向是探索如何確保開發協定和電腦代碼，以促進 AML / CFT 的合規程度，同時保持創新的好處（Yuta Takanashi et. al, 2020[20]）。由於開發者、協議設計者和第三方協力廠商沒有明確受制於 FATF 建議下的 AML / CFT 義務，FATF 應考慮是否需要與其他利益攸關方進行額外的討論，例如，關於科技供應商的作用，以及區塊鏈在金融中日益增長的 AML / CFT 的使用，以確保 FATF 標準在中長期的相關性和有效性。

155. 最後，FATF 還確定支持在 AML / CFT 方面使用科技的建議行動（見附件 B），以推進 2017 年聖荷西原則，追求積極和負責的創新。這些行動指出，在開發和實施用於 AML / CFT 的新科技時，必須反映威脅和機會，確保其使用符合資料保護和隱私以及網路安全的國際標準。

案例 21. 監理機關和分散式帳本科技

日本金融廳－日本

日本金融廳積極做出貢獻之區塊鏈治理倡議網路（BGIN）於 2020 年 3 月啟動。該倡議通過採用所謂的多利益相關者方法，一直在應對以區塊鏈科技為支撐的去中心化金融系統的挑戰。金融穩定委員會（FSB，2019[21]）宣導加強多方利益相關者之間對話的重要性，並受到於 2019 年日本擔任主席國的 20 國集團（G20，2019[22]）的歡迎。鑒於傳統監管架構的局限性：監理機關與義務實體的單方面溝通，這一概念旨在通過監理機關、科技開發商、義務實體、學術界等各利益相關者之間的平等對話，形成攸關各方利益相關者所面臨的問題的共識。

區塊鏈治理倡議網路對其目標的解釋是（BGIN，n.d.[23]）：" 主導、設計可以讓多方利益相關者達成共識之合理的治理，同時加強對話、共同合作，為生態圈和整個社會帶來真正的積極影響 "，並暫時將重點放在以下方面：

- 創建一個供各方利益相關者對話且開放的、全球性的、中立的平臺。
- 為具有不同觀點的多方利益相關者之間發展一種共同的語言和理解，以及
- 通過持續提供基於開源式的可信賴的文件和代碼，建立學術支柱。

區塊鏈治理倡議網路處理與 FATF 有關的各種問題，包括，例如考慮到新興科技和市場發展，確定去中心化金融體系（Decentralized Finance）中防制洗錢／打擊恐怖主義可能的監管方法。FATF 及其

成員參與其活動可能是正面意義的，因為在這裡可以加強與各利益攸關方的對話，包括那些開發科技的人，而監管當局通常在接觸這些科技方面面臨挑戰。如金融穩定委員會報告所述，與利益相關者的這種持續接觸將最終確保遵守反洗錢／打擊資助恐怖主義行為，同時避免扼殺創新及其有利環境。

5.2. 結語

156. 本報告對新科技給 AML / CFT 帶來的機遇和挑戰提供概略的總結，在可能的情況下，提供現有最佳做法和／或具體挑戰的例子。本報告的結論並非包羅萬象，在 FATF 標準和數位轉型之間的關係上還有改善的空間。

157. 科技的創新為 AML / CFT 的效力提高提供巨大潛力。然而，它也可能導致社會某些階層，像是老年人、農村社區等，在金融方面受到更多排斥，並給社會帶來挑戰，特別是在人權、民主和法制方面。FATF 注意到，由於各行為人對新科技的不負責任或錯誤的支援和依賴，可能會出現進一步的挑戰。

158. FATF 鼓勵各司法管轄區共同努力，並與私部門機構們合作，考慮對新科技採取全面的辦法，同時考慮到其潛力以及侷限性。

附件

- 附件 A. 詞彙表
- 附件 B. 支援在 AML / CFT 中使用科技之行動建議
- 附件 C. 監理科技之案例研究
- 附件 D. 關於私部門對於 AML / CFT 應用之新科技的監管科技案例研究

附件 A：詞彙表

進階分析：進階分析是指使用複雜的技術和數位工具，來自主或半自主地檢查資料或內容，通常在超出傳統商業智慧的範圍發掘更深層次的見解，進行預測或給出建議。進階分析技術包括那些諸如資料／文本探勘、機器學習、模式匹配、預測、視覺化、語義分析、情感分析、網路和集群分析、多變數統計、圖形分析、類比、複雜事件處理、神經網絡。進階分析法通常依賴於大數據的使用。

應用程式：應用程式是為幫助使用者執行特定工作而設計的電腦軟體。

應用程式介面（API）：應用程式介面是一套用於構建和整合應用軟體的定義和協定。應用程式介面讓電子產品或服務可以隨時與其他產品和服務進行交流。

演算法：電腦演算法是一組執行特定工作的連續指令。

人工智慧（AI）：人工智慧系統是一組針對人類定義的目標，（並以不同程度的自主性運作）做出會影響真實或虛擬環境的預測、建議或決定的機器系統（OECD, 2020[14]）。人工智慧的目標是使電腦能夠自動進行某些方面的分析，盡可能地節省在枝微末節的工作上耗費的人力，並獲得人類可能無法得出的見解。人工智慧在眾多應用程式中都有幾個部分的技術組成，對於什麼是＂思考＂、什麼是＂智慧＂、什麼是＂完全自主＂，目前並沒有達成共識，而且人工智慧有幾個類別。但總的來說，人工智慧系統在不同程度上結合了意圖性、智慧和適應性等特性上建立了所謂的＂智慧型機器＂。目前最為人所知及最發達的人工智慧形式是機器學習。

大數據：金融穩定委員會將大數據定義為 " 由於越來越多地使用數位工具和資訊系統而產生的大量資料 "，像是金融交易、社交媒體和機器（如物聯網、電腦和手機資料 , FSB, 2017[15]）所產出的資料。

黑盒子：黑盒子是指人工智慧／機器學習或其他技術以不透明、非直觀的技術且不提供有關其決策和預測／結果的充分資訊，亦即黑盒子技術缺乏可解釋性。

基準化分析：基準化分析是一種確定以技術為基礎之流程、生產或服務的實際能力和相對能力之方法；透過與功能、工作或目標的最佳性能進行測試，使用由特定基準來衡量之精準資料以確定性能差距，透過無論是在特定的實體或組織內，還是在整個行業內或者由不同的行業實現。基準測試可被用作衡量或比較在新科技和傳統系統之間或是在新科技和相對之替代新科技的效能評估。

協作分析：對於協作分析，資料不會被轉移集中到一個位置，以便與其他資料庫一起分析。相反地，分析工具會反過來移到資料上。這使得保持資料的安全和讓「知道是誰、為了什麼目的、訪問什麼資料」這些事情更加容易被控制。

網路安全：網路安全指的是包含了資料保護以及移動、儲存和驗證資料的系統的所有過程，是一個比資料安全更概括的術語。

資料混合：資料混合是指將自不同來源的數據資料結合起來，形成一個更全面和更有效的資料庫進行分析（包括由多方）的過程。這些資料庫是以中心化方式組織起來的。

資料安全：資料安全是指在其生命週期內保護其資料免受未經授權的存取和資料惡化的過程。資料安全的做法包括資料加密、雜湊、記號化以及保護所有應用程式和平台的資料的金鑰管理做法。資料安全的定義比網路安全的定義更有侷限性。

資料正規化：資料正規化是為了讓不同使用者能夠處理和分析資料，將資料轉換為統一格式的過程。這種標準化對於實現大數據處理和進階分析，以及其他創新數位工具和方法的開發和應用至關重要。例如，金融資料在實體內部和實體之間都可能有所不同；資料正規化將其轉換為一種通用的形式，從而實現複雜的大規模分析。

數位身份（ID）系統／解決方案：數位身份識別系統或解決方案是一種執行識別或驗證（自然人或法人）身份的識別系統、產品或服務，將已驗明正身的身份與數位憑證結合起來，然後將數位憑證和其他可能的驗證要件來建立（確認）聲稱的人是擁有身份的人（即，他就是他所宣稱的那個人）。

分散式帳本技術（DLT）（亦稱區塊鏈）：分散式帳本技術指的是一種能夠讓數台電腦（通常是位於多個實體或地點）同時存取、驗證和更新分佈於其上的不可更改帳本（電子記錄）的技術協議，意即分散式帳本技術可以創建一個分散式數位資料庫。

深度學習（DL）:深度學習是一種具有多（深度）層的人工神經網絡（受人腦啟發的演算法）以高度自主的方式從大量的資料中學習的進階機器學習技術。深度學習演算法反復執行同一項工作，每次都會稍作調整以改善結果，使機器能夠在沒有人類介入的情況下解決複雜問題。

數位化技術：此項技術是利用數位化技術和數位化資料來改變商業模式，對於工作的完成方式產生影響，改變客戶和公司的互動方式，並提供新的收入和創造價值的機會。

資訊數位化：數位化是將資料、資訊、文字、圖片、聲音或其他類似的表現形式轉換為可由電腦處理的數位形式（即二進位碼）。

動態資料：動態資料指的是連續且資料點不停變動的即時數位資料，因此資料庫隨著時間的推移不斷變化，這與靜態或持續而不受時間影響的資料不同。

可解釋性：在使用新技術的背景下，可解釋性是指基於技術的過程、解決方案或系統可被解釋（分析）、理解和說明。可解釋性提供了對解決方案如何運作和其產生之結果的充分理解，是可信的和負責任的使用的基本條件。可解釋的人工智慧技術提供了用於實現結果的資料、變數和決策點的透明度。

金融科技：金融科技泛指在金融領域為了各種不同的目的使用之新興數位技術。一開始金融科技主要是指利用基於技術的創新來提供諸如移動支付解決方案、線上借貸服務、演算法儲蓄和投資工具、虛擬貨幣支付、募資（眾籌）和接受存款（遠端存款服務、行動銀行）等面向客戶的全新金融產品和服務。金融科技現在還包括使用新興技術提供如使用演算法、大數據、人工智慧和機器學習，以及用於收購清算、結算和其他收購仲介公司的連結分析，例如證券、衍生品、零售金融和支付，以及監管合規活動（見下文監管科技定義）等的自動化中、企業後臺功能。其他應用仍有待開發。

模糊邏輯：模糊邏輯是人工智慧的一個子集合，它接受一個開放的、範圍不精確的資料（不精確的輸入），以一種產生的輸出包括在是與否（例如，肯定是、可能是、不確定、可能不是、肯定不是）之間的一系列居中可能性的方式處理多個值。模糊邏輯系統對不完整的、模糊的、扭曲的或不準確的（模糊的）輸入產生明確的輸出，比傳統的是／否邏輯更接近人類的決策。模糊邏輯可以通過硬體、軟體或兩者的結合來實現。

物聯網（IoT）：由所有支援網際網路的設備和機器組成之全球網路，這些設備和機器與網際網路相連，在沒有和人互動的情況下利用嵌入式感測器、處理器和通訊硬體在收集、發送、分享資料同時採取行動。物聯網產生了大量的即時資料，這些資料可以被分析並用來創造預期行動或商業成果（見大數據）。

可交互運作性：是指不同的資訊技術系統和應用程式軟體間，能夠實時地溝通、交換資料和不間斷使用資訊的能力，使所有參與者在所有系統中操作。

機器學習：機器學習其中一種人工智慧類型（子集合）是用來 " 訓練 " 電腦系統，它能夠從資料、識別模式來學習，並在最小的人為介入下做出決定。機器學習涉及到透過經驗和不斷發展的模式識別演算法設計一連串的行動，在有限的或沒有人類干預的情況下自動解決一個問題；也就是說，它是一種可以自動建立分析模型的資料分析方法。

機器可讀規則：機器可讀規則用電腦程式取代了用自然法律語言編寫的規則，以便能夠使用人工智慧進行監管申報。

自然語言處理（NLP）：自然語言處理是人工智慧的一個分支，使電腦能夠理解、解釋和操縱人類語言。自然語言處理使人類可以與機器對話。

強化隱私技術：" 專業的加密能力，允許在底層資料上進行計算，而資料所有者不一定會洩露該底層資料。同樣的技術可以確保資料所有者對搜索查詢沒有可見性，查詢和結果仍然是加密的（或不披露），只有請求者得知 "。（Maxwell, 2020[16]）因此，這個術語包含了一系列使用加密的技術，主要在資料使用過程中允許保護隱私。

即時分析：即時分析是一個系統處理和分析實時載入的資料，並幾乎馬上（接近即時）產生有意義（例如，資訊、預測或決策）輸出的機器學習過程。

即時資料（RTD）：即時資料是在收集後立即傳送的資訊，確保所提供資訊的及時性。即時資料能夠實現即時分析，可以是動態的、也可以是靜態的（例如，一個在特定時間、特定位置即時寫入的資料）。

監管科技（RegTech）：監管科技利用比現有技術更有效的新技術來遵守監管要求，是金融科技的一個子集合。

負責任創新：當創新技術在防制洗錢／打擊資恐、消費者保護、網路安全和隱私保護等面相能勝任其目的並符合適用的監管要求，就是負責任的創新。

智慧機器：智慧機器是使用人工智慧演算法的電腦硬體和軟體系統，被設計使用即時資料來做決定。與只能做出機械或事先安排的被動機

器不同，智慧型機器使用結合來自感測器、數位資料和遠端輸入，即時分析這些不同來源的資訊，並根據從中得出的見解採取行動。智慧型機器透過使用進階的計算過程模仿人類智慧，根據計算結果即時分析得出結論。

靜態資料：靜態資料指的是一個固定的，資料在被收集後保持不變的資料庫。

監督式學習：監督式學習是一種透過向演算法提供已知結果的輸入資料來指導演算法預測模型的機器學習過程，即利用實例來訓練模型。輸入／輸出對（標記的資料）為演算法提供回饋，演算法使用訓練資料庫來調整模型以最小化誤差。例如，一個訓練集可能包含不同種類已經被標籤的動物圖片，允許演算法將預測的標籤與正確的標籤進行比對。監督式學習使用驗證資料庫，來衡量演算法在學習模型方面的進展，並使用測試資料庫來評估模型在還未見過資料上的表現，以確定模型是否有效地學習了訓練資料，並能歸納到新資訊。

監理科技（SupTech）：監理科技是指監理機關用於支援監督和審查之新技術。

非監督式學習（亦稱非監督式機器學習）：非監督式學習是使演算法能夠在無人工介入下，分析和協同未標記的資料庫以發現隱藏的模式、資料分組或異常情況的一個機器學習過程。該演算法對可用資料進行分析，並在沒有解答的情況下，透過推論和基於開放觀察和直覺，對同類事物進行分組，來確定相關性和關係。它的建模會隨著演算法接觸的資料量增加而變得更加準確和完善。

附件 B：支援在 AML / CFT 中使用科技之行動建議

負責任地使用包括數位身份和先進的交易監控和分析解決方案（包括協作分析）之新技術，可以幫助公部門和私部門能有效地、依風險基礎法實施防制洗錢金融行動工作組織的建議，同時促進金融包容性。

以下原則推進 FATF 在 2017 年支持的聖荷西原則*追求積極和負責任的創新*。防制洗錢／打擊資恐的新技術其開發和使用必須不僅反映威脅還要能帶來機會，確保其使用符合資料保護和隱私以及網路安全的國際標準。

1. 政府和私部門為提高防制洗錢／打擊資恐的有效性一起創造有利的創新環境。
   i. 促進應用防制洗錢／打擊資恐措施的創新解決方案並加強對其監督和檢查，包括風險評估、客戶盡職調查和其他要求。
   ii. 更新內部原有舊系統或用新技術取代這些系統的最佳實務做法。
   iii. 新防制洗錢／打擊資恐解決方案的適當保障措施和特點，包括：流程和結果的可解釋性和透明度、人工監督、尊重隱私和資料保護、強大的網路安全、以及與全球、國家和技術標準保持一致的最佳做法。
2. 在應用新技術時確保隱私和資料保護。
   i. 確保在部署新技術處理個人資料時具有有效法律依據。
   ii. 根據國家和國際法律架構保護個人資訊。
   iii. 根據明確、具體和合法的目的處理資料，同時遵守國內和國際間規則。

iv. 支持負責任地開發和採用保護隱私的創新技術，以便在保護隱私的同時，實現強大的防制洗錢／打擊資恐的資訊分享和分析。

3. 設計支持金融包容性促進防制洗錢／打擊資恐的創新。
   i. 通過制定和應用減輕金融包容性障礙的創新解決方案。
   ii. 確保負責任的創新與防制洗錢金融行動工作組織促進金融包容性之目標相一致。
4. 制定和宣傳靈活的、技術中立的、基於結果的、符合風險基礎法的創新政策和監管方法
   i. 在伴隨著結構和組織變化的背景下，全面考慮新技術的影響，其可能產生的意外後果，以及其對防制洗錢／打擊資恐的有效性和金融包容性的總體影響。
   ii. 必要時發佈和／或更新明確的政策聲明、指引、使用案例、最佳做法或法律規定，以告知和鼓勵負責任地使用新技術來進行防制洗錢／打擊資恐的工作。
   iii. 向關聯方和受監管實體提供相關政策和決策過程之資訊並徵求意見。
5. 實行知情監管
   i. 為了能夠對其使用進行知情的監管和監督建立新技術方面的專業知識，包括為具體的防制洗錢／打擊資恐的目的。
   ii. 在防制洗錢／打擊資恐的監督和檢查中確定明確的、定義清晰的新技術用途。
   iii. 瞭解與新技術相關的風險和利益，以及保持其利益的適當風險緩解措施。
   iv. 使用技術來加強防制洗錢／打擊資恐的監管。

6. 推動和促進合作

   i. 與所有有關當局合作和協調，以促進採取全面、協調的方法，包括資料保護和隱私權主管機關去瞭解和處理在防制洗錢／打擊資恐方面使用新技術的風險和益處。

   ii. 或可考慮發展合作環境，以促進跨政府和／或公、私部門對新技術和創新解決方案的研究和開發。

   iii. 國際間共同制定關於使用新技術進行防制洗錢／打擊資恐的原則，以幫助確保其符合人權、改善國際相關技術標準和信任體系對防制洗錢／打擊資恐的實施、網路安全、資料隱私和保護措施。

附件 C：案例研究

Brazil

The 巴西中央銀行的監管支援綜合系統（SisCom，2018 年起稱 APS-Siscom）是一個基於網路的系統，由一套可以在安全的環境下與受監管機構（SE）互動的強大研究成果支援，在以下各方面促進監管工作：

- 一個簡單和安全的方式，要求和接收來自受監管機構的政策、手冊、管理報告、審計報告、有關特定客戶和特定交易的實名認證文件，以及受監管機構寫在系統中的回覆。
- 檢查過程中的互動功能，以澄清任何疑慮和要求補充資訊或解釋。
- 使檢查程序標準化，允許各種檢查同時進行。
- 檢查範本。巴西中央銀行的監管人員可以為一組受監管機構、受監管機構部門或某一受監管機構特別創建量身定做整合資料夾，這些資料存儲在一個組合中供以後使用。通過查詢功能，監管人員可以知道哪些請求被發送給多少個機構。
- 編制報告：APS-Siscom 自動提供監督報告，這些報告可以很容易地組合成審計用的檔案資料。
- 在檢查結束時，不足和違規情況將通過系統進行通報，並要求受監管機構也通過 APS-SisCom 提交一份改正計畫，供主管批准。
- 所有的要求完成日期都由 APS-SisCom 控制並發出信號，APS-SisCom 根據商業智慧報表中的完成情況，提供最新的缺陷和違規情況統計。
- 搜尋功能允許監管部門蒐集對特定受監管機構進行的每一次檢查資料，以跟蹤進展。

2018 年，Siscom 被納入巴西中央銀行新的監督平臺 SisAPS 中，該平臺整合多種系統和資料庫。SisAPS 為檢查員、監督員和管理人員實施，為團隊在每次檢查中正在開展或已經開展的工作提供記錄功能，以及管理資訊和監督報告。

APS-SisCom 為巴西中央銀行的監管團隊提供巨大的生產力，促進檢查程序，使巴西中央銀行不需要對受監管機構進行耗時的訪問

APS-SisCom 蒐集的資料也被納入一種方法，使建設銀行能夠按照不同的風險類別對銀行和非銀行金融機構（NBFI）進行細分和監督。監管人員對定量和定性資料進行處理和分析，為他們提供不同的視角：

- 對特定監管要求的遵守程度；
- 風險評估，使用評級分類法。

因此，這一工具和方法能夠對分佈在巴西大地上的數百家中小型企業進行有效的 AML / CFT 監督。

香港金融管理局：監理機關在鼓勵使用網路分析之作用

香港金融管理局（HKMA）與銀行密切合作，在過去幾年中採取一系列措施，鼓勵探索和負責任地採用 AML / CFT 的監管科技，包括通過其金融科技監理沙盒和線上討論以及 2019 年 11 月舉辦的 AML / CFT 監管科技論壇。在眾多應用程式中，香港金融管理局已將網路分析科技應用的發展確定為香港金融管理局的監管重點之一，其支持銀行在通過與香港欺詐和洗錢情報工作組建立公私夥伴關係所取得的成果增加價值。在整個 2020 年，香港金融管理局一直在與銀行接觸，以更好地瞭解影響網路分析科技應用的因素和依賴性，這有助於香港金融管理局作為監管者準備回應，特別是對那些詢問 " 如何開始準備使用網路分析 " 的銀行。

香港金融管理局最近分享一個銀行的案例，該銀行幾年來一直在研究網路分析的潛在應用（HKMA, 2021[27]）。該銀行自 2013 年起採用分析科技，詳細介紹如何利用分析科技來提高銀行識別顯示出高洗錢／資恐風險的網路的能力。金管局說明這家銀行如何克服某些挑戰以及已經取得的一些成果。

為繼續支持加快銀行業採用的科技路線圖，香港金融管理局已將監管科技作為其 2021 年 AML / CFT 監管計畫的重點，並在最近出版物中詳細說明它將如何利用其中作法來建立行業對關鍵科技的接受度，並為所有銀行在 AML / CFT 工作中探索和使用監管科技創造條件，包括網路分析。

新加坡金融管理局

問題陳述

新加坡金融管理局對金融機構（FI）的洗錢和資恐（ML / TF）風險管理進行監督。為提高新加坡金融管理局的監督效率，新加坡金融管理局進行風險監督，以發現系統性風險，並針對高風險地區和金融機構進行更密切的監督檢查。新加坡的金融機構就潛在的非法資金流動和金融犯罪問題提交可疑交易報告，這些報告為我們的風險監督提供有用的資訊。複雜的類型往往涉及多個金融機構的多個帳戶，這可能表現為在一段時間內提交多個可疑交易報告。因此，新加坡金融管理局開發一個可疑交易報告網路分析工具，以 明我們跨金融機構、不停地為新加坡金融管理局發覺事情的全貌。

洞見和成果

使用可疑交易報告網路分析工具，有助於新加坡金融管理局確定甄別表現出可疑行為的個人／實體的相關群組，以及參與我們監督分析和審查的金融機構。這有助於提高我們在防制洗錢監督中確定風險優先次序和目標的能力。從網路分析中發現的見解和新出現的風險也通過各種平臺與金融部門分享，包括我們的 AML / CFT 行業夥伴關係（ACIP）、行業研討會，或通過對所有金融機構的諮詢說明和監督指導。這些由資料驅動的參與提高行業的風險意識，並反過來促使金融機構加快採用創新的資料分析科技來打擊金融犯罪。

除推進我們的監管目標外，從可疑交易網路分析工具中獲得的洞察力也有助於我們國家打擊金融犯罪的努力。在新加坡，有一個機關間委員會，將相關的執法單位和監督機關聚集在一起，進行 ML / TF 重點案件之調查和制定風險緩解計畫。通過我們的可疑交易報告

網絡分析發現的幾個相關網絡已提交至該委員會，供各機關審議和共同協調行動。

在初始階段，我們的網路分析的資料來源主要由可疑交易報告中固定的資料欄位中之資訊組成。我們正在加強資料庫，以提高我們網路分析工具的影響力。我們首先開發自然語言處理（NLP）模型，從可疑交易報告中的非結構化文本資料中提取資訊，例如，解釋客戶交易的不尋常性質和交易對照方之間關係的敘述，將之納入我們的網路分析。再來，我們的分析工具也已經開始吸收更多的交易資料和公司的概況資訊。這些改進將加強我們的能力，以識別不為人知的聯繫，並檢測和優先考慮系統性風險問題，以便監督和機構間跟進。

馬來西亞

推動有效實施電子化實名認證監管要求的沙盒架構

馬來西亞中央銀行（BNM）在 2016 年建立的金融科技監理沙盒（Sandbox），在促進金融業的創新方面發揮關鍵作用。它作為一個有效的平臺，讓馬來西亞中央銀行在制定正式的行業監管要求之前，監控科技發展對行業的潛在影響。

沙盒的優勢體現在貨幣服務業（MSB）的創新商業模式的增長上。在 2017 年之前，馬來西亞的貨幣服務業者不允許在沒有與新客戶面對面接觸的情況下進行任何交易，除非首先與客戶建立業務關係並進行客戶盡職調查措施。兩家數位貨幣服務業者能夠透過監理沙盒測試他們的創新商業模式，包括通過電子化實名認證解決方案，使用非面對面的產品導入流程，在這樣的環境中，與創新科技相關的風險可以得到充分的緩解。

考慮到從 " 沙盒 " 中獲得的經驗教訓，馬來西亞中央銀行在 2017 年底引入對貨幣服務業部門進行非面對面產品導入核查的監管要求。這使得更多合格的貨幣服務業參與者能夠實施電子化實名認證驗證，並採取適當的保障措施，如與客戶建立獨立聯繫和設定交易限額。迄今為止，已有七家匯款公司獲准為新客戶的產品導入進行電子化實名認證。馬來西亞中央銀行還採取一種漸進的方式來推出監管要求，以支援符合行業準備情況的創新解決方案。例如，電子化實名認證驗證首先被引入到匯款領域，並在 2019 年被擴展到貨幣兌換領域。

此外，為加快和簡化各行業參與者的作法，貨幣服務業在 2020 年發佈適用於所有金融機構的 AML / CFT 政策文件和電子化實名認證政策文件的修訂版，規定對各機構採用電子化實名認證科技的監管期望。

附件 D. 關於私部門對於 AML / CFT 應用之新科技的監管科技案例研究

案例研究：機器學習驅動之 AML 智慧警報管理與姓名檢核系統

一金融機構與一家新加坡的監管科技（RegTech）公司合作進行防制洗錢（AML）合作。這次合作成效就是一個全面的機器學習解決方案，將使金融機構能夠得出更快、更精確的資訊，以防止和發現可疑的洗錢活動。該解決方案解決銀行防制洗錢架構內的兩個主要流程，即交易監控和姓名篩選，有效地創建工作流程，根據風險水準對警報進行優先排序，協助合規部門專注於那些最重要的警報。

該解決方案結合監督式和無監督的機器學習科技，旨在更快、更準確地檢測可疑活動和識別高風險客戶。它提供一種智慧方式，通過將交易監控和姓名篩選警報隔離成 L1、L2 和 L3 三個風險層級，其中 L3 是最高風險層級。

交易監控模組能夠根據風險分數對已知的警報進行優先排序，並察覺新的或未知的可疑模式。姓名篩選模組有以下三個核心部分，透過多種複雜的姓名排列組合來加強姓名檢核，透過預測功能減少具不確定性的命中，以及透過初級和次級資訊使偵測能力更準確。這些功能有助於準確區分誤報及正確警報。

這個工具的特點是具有自動、持續學習的自主學習機制，以及正在申請專利的可解釋人工智慧架構，以便徹底理解並進行高品質的調查。該架構用商業使用者可以理解的方式，解釋機器學習模型的每個警報預測背後的理由。

當它發現一個可疑的活動模式時，工具中防制洗錢套件也會創建一個 SMART 規則，並將其添加到防制洗錢態樣庫中，從而使機器學習模

型能夠檢測到類似的模式，以便在未來發出警報。這意味著，隨著時間的推移，該解決方案將繼續過濾誤報的數量，並實現更準確的追蹤。因此，銀行的員工將能夠利用節省下來的時間，對可疑案件進行更深入的調查，或快速有效地關注其他案件。

案例研究：風險管理解決方案

一家跨國金融機構正在使用大數據和自動化的 " 語意監控 " 來檢測和瓦解國際貿易中的金融犯罪。

語意監控是將來自不同系統和來源的資料連接在一起的能力，以創造背景和意義，從而識別重要的聯繫並提高準確性。它採用先進的演算法，允許更複雜的評分和分析方法。

採用此一科技，可以對客戶活動進行持續評估，並對風險進行評分。這種等級的語意監控提高準確性和決策性，同時通過基於分析和情報的防制洗錢解決方案提供前所未有的對資料關係的洞察力。

它的主要好處是：通過更少和更高品質的警報來提高對客戶的關注，識別與洗錢有關的高風險活動，提供客戶歷史交易和風險狀況的完整背景，提供交易和非交易事件分析的能力。

案例研究：機器人流程自動化解決方案

一家金融機構正在開發基於機器人流程自動化（RPA）解決方案的舉措，以提高流程的效率，如調查可疑交易、篩選名字以確定重要政治性職務之人、實名認證入職和重新認證。一些自然語言解決方案（翻譯）也被使用。

目前專門針對反洗錢檢測領域的機器學習解決方案包括基於規則的模型與資料分析相結合，基於原則為基準的模型與警報評分方法相結合，加強以原則為基準的模型（使用外部資料，如公司註冊資料）（在這種情況下與機器人流程自動化無關）。

案例研究：數位身分解決方案

一個會員制機構正在提供解決方案以支持創新。該專案旨在開發一個方案，為消費者制定單一的數位身分符合所有相關的監管要求（實名認證和防制洗錢），作為在英國金融服務進行自己安全識別的主要手段。

該組織正在與政府密切合作，開發一個國家信任體系，因此該計畫將允許消費者通過具互通性的標準和科技在多個部門使用他們的數位身分，它將依靠各種接入點和需要數位身分認證的設備的擴散來綜合服務和體驗。它還將依賴於生物識別／視頻實名認證、機器學習、自然語言處理和區塊鏈／分散式帳本科技的增加使用。

這個數位身分計畫將允許消費者重新使用他們經過驗證的身分和相關的實名認證屬性來開啟和訪問線上金融服務。

案例研究：風險管理與合規公司專注於解決資料品質與資料一致性

對交易資料進行適當風險評分的關鍵因素之一是，識別所有提到的當事人和地域。鑒於各種交易格式，再加上人為錯誤和／或不良行為者試圖混淆其身分，這可能被證明是一種挑戰。為克服這些挑戰，監管科技團隊採用各種科技來獲得和規範資料。

這個風險和合規監理機關提供以科技為基礎的資料處理服務，以促進對 AML / CFT 義務的遵守。在任何項目的開始和資料獲取之前，將與利益相關者、中小企業和必要的科技團隊進行一系列的對話，以確定關鍵資料元件（KDEs）。一旦資料到手，團隊會創建一個原始資料的副本（黃金來源，即最佳資料來源），以保持完整性和可稽核性。接下來，它進行高水準的分析，以更好地瞭解資料的完整性並確定差距。

字串正規化也是這個過程的一個重要部分。去除特殊字元、多餘的空白區域和常見的公司術語（LLC、OOO、Limited）只是為更好地分組、分類和識別而採取的幾個步驟。

機構提取是任何風險模型的一個重要組成部分，並因 " 受汙染 " 或不完整的資料而變得複雜。雖然在資料獲取過程中，人們關注的是被識別的關鍵資料元件，但僅僅依靠這一點可能會錯過 " 隱藏 " 的實體。

一種常用的科技是自然語言處理（NLP），該科技用以識別部分的言語。自然語言處理提供掃描整個資料庫的能力，以尋找可能表示特定個人或公司的名詞。雖然自然語言處理很有幫助，但結果仍然需要額外的分析和清理，因為交易資料很少遵循典型的語法。因此，這些掃描是通過標記化字串的內部智能功能來補充的。

使用從早期規範化實體所提取的資料，該團隊創建一個獨特的列表，同時仍然保持追溯其原始來源。

參考文獻

區塊鏈治理倡議網路（n.d.）, *區塊鏈治理倡議網路（BGIN）, 相關詳*, https://bgin-global.org/about/. [23]

國際清算銀行（2020）, *金融穩定學院政策實施的洞見*, http://www.bis.org/fsi/publ/insights29.pdf. [31]

國際清算銀行（2019）, *防制洗錢之監理科技應用程式, 金融穩定學院政策實施的洞見 N.8,* https://www.bis.org/fsi/publ/insights18.pdf. [34]

Broeders D. and Prenio J.（2018）, *金融監管的創新科技（監理科技）早期使用者經驗*, https://www.bis.org/fsi/publ/insights9.pdf. [36]

Chase, I.（2020）, *如何做對：普惠金融需要更好的激勵措施*, *皇家聯合研究所*, https://rusi.org/commentary/doing-what-right-financial-inclusion-needs-better-incentives. [12]

CoE（2011）, *1797 號決議（2011）, 全面考慮生物識別科技對人權影響的必要性*, https://pace.coe.int/pdf/8b5e492cf90ea25e1c1f2f459c42bc9570713dd10154b339883da5da4c3 09a89/resolution%201797.pdf. [17]

Coelho et al.（2019）, *防制洗錢的監理科技應用*, https://www.bis.org/fsi/publ/insights18.htm. [4]

歐洲銀行業管理局（2021）, *Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector,* https://www.eba.europa.eu/eba-highlights-key-money-laundering-and-terrorist-financing-risks- across-eu. [11]

歐洲銀行業管理局（2020）, *歐洲銀行管理局、大數據與進階分析*, http://www.eba.europa.eu/sites/default/documents/files/document_library/Final%20Report%20 on%20Big%20Data%20and%20Advanced%20Analytics.pdf. [30]

歐洲聯盟委員會（2019）, *關於監管、創新與融資的 30 條建議*, https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/docu ments/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf. [19]

FATF（2021）, *虛擬資產和虛擬資產服務商年度評論第二版*. [38]

FATF（2020）, *數位身分指南*, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html. [8]

FATF（2020）, *FATF 在德國擔任輪值主席國之優先事項*, http://www.fatf-gafi.org/media/fatf/documents/German-Presidency-Priorities.pdf. [3]

FATF（2020）, *盤點資料庫、協作分析及資料保護*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/data-pooling- collaborative-analytics-data-protection.html. [37]

FATF（2019）, *虛擬資產與虛擬資產服務商之風險基礎指引*, FATF, http://www.fatf- gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html. [1]

FATF（2014）, *FATF 闡明所謂風險基礎法：個案處理非全面迴避風險*, http://www.fatf-gafi.org/documents/documents/rba-and-de-risking.html. [5]

FATF（n.d.）, *FATF 指引 - 風險基礎法*, [6]
http://www.fatf- gafi.org/documents/riskbasedapproach/?hf=10&b=0&s=desc（fatf_releasedate）.

金融穩定委員會（2020）, *主管機關與被監管機構對監理科技和監管科技之使用* , p. 32, http://www.fsb.org/2020/10/the-use-of-supervisory-and-regulatory- technology-by-authorities-and-regulated-institutions-market-developments-and-financial- stability-implications/. [28]

金融穩定委員會（2019）, *去中心化金融科技 - 針對金融穩定、監管與治理影響之報告*, [21]
http://www.fsb.org/wp-content/uploads/P060619.pdf.

金融穩定委員會（2017）, *金融服務中的人工智慧與機器學習*, [25]
https://www.fsb.org/wp-content/uploads/P011117.pdf.

G20（2019）, *G20 大阪高峰會領導人宣言*, [22]
http://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_l eaders_declaration.html.

G20（2016）, *高層次數位普惠金融原則*, https://www.gpfi.org/sites/gpfi/files/documents/G20-HLP-Summary_0.pdf. [9]

香港金融管理局（2021）, *AML / CFT 監理機關：個案研究與洞見* , http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and- circular/2021/20210121e1a1.pdf. [27]

香港金融管理局（2020）, *數位創新時代之 AML / CFT 監管*, [35]
http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and- circular/2020/20200929e1a1.pdf.

香港金融管理局／勤業眾信聯合會計師事務所（2021）, *AML / CFT 監管科技：個案研究與洞見*, http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and- circular/2021/20210121e1a1.pdf. [15]

Kazzaz, Z.（2020）, *COVID-19 的緊急救助：快速開戶和監督之監管工具*, p.13, http://www.findevgateway.org/sites/default/files/publications/submissions/72016/Emergency% 20 [13]

新加坡金融管理局（2018）, *行業觀點 - AML / CFT 所採用的數據分析方法*, http://www.mas.gov.sg/regulation/external-publications/industry-perspectives-adopting-data- analytics-methods-for-amlcft. [18]

Maxwell, N.（2020）, *創新科技和評述論文：利用隱私保護分析處理金融犯罪之案例研究*, http://www.future-fis.com/uploads/3/7/9/4/3794525/ffis_innovation_and_discussion_paper_-_case_studies_of_the_use_of_privacy_preserving_analysis_-_v.1.3.pdf. [26]

OECD（2020）, *人工智慧原則*, https://www.oecd.ai/ai-principles. [24]

Richard Grint et al（2017）, *新科技和防制洗錢合規, 英國金融行為監理局*, http://www.fca.org.uk/publication/research/new-technologies-in-aml-final-report.pdf. [14]

SAS（n.d.）, *五種應該知道的人工智慧科技*, https://www.sas.com/en_us/insights/articles/analytics/five-ai-technologies.html. [29]

UN （2019）, *聯合國安理會（UNSC）2462 號決議（2019 年 3 月 28 日）, UN Doc S/RES/2462, para.20,* https://undocs.org/en/S/RES/2462（2019）. [2]

UN （2018）, *於反恐活動中負責任使用與分享生物辨識科技之建議作法大綱* , https://www.un.org/sc/ctc/wp- content/uploads/2018/06/Compendium-biometrics-final-version- LATEST_18_JUNE_2018_optimized.pdf. [10]

Vyjayanti T Desai et al.（2018）, *“全面身分識別之挑戰：10 億為沒有身分證明的人是誰？”* , https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity. [7]

Walshe, P.（2020）, *數位身分* , https://rm.coe.int/t-pd-2020-04rev-digital-identity-tc- en/1680a0c051. [32]

世界經濟論壇（2020）, *另闢蹊徑：接下來的金融服務創新演變* , http://www.weforum.org/reports/forging-new-pathways-the-next-evolution-of-innovation-in- financial-services. [33]

世界銀行（2021）, *識別可持續發展之原則：邁向數位時代* , https://documents.worldbank.org/en/publication/documents- reports/documentdetail/470971616532207747/principles-on-identification-for-sustainable-dev. [16]

Yuta Takanashi et. al（2020）, *呼籲各方利益相關者就利用區塊鏈科技建立之金融生態系統建立治理機制進行溝通 , Part 2 of 2,* https://stanford-jblp.pubpub.org/pub/multistakeholder-comm-governance2/release/1. [20]