ISACA

稽核從業人員之機器學習參考指引

第二部分：合規風險

稽核

目錄

摘要

機器學習（ML）作為人工智慧（AI）的一個子集，正迅速被全球企業與政府廣泛採用。然而，現有的資訊科技（IT）稽核流程與管理控制可能無法充分辨認、衡量並有效管理這項新技術所帶來的獨特風險。

本白皮書是此系列的第二部分，作為第一部分的延伸與補充。第一部分已概述機器學習的基礎概念以及當前稽核應考量的重點，而本部分則聚焦於與 ML 相關的合規風險。本文件概述了各產業及不同地區與 ML 相關的法規與法律，包括《一般資料保護規則》（GDPR）、《加州消費者隱私保護法》（CCPA）、美國聯邦儲備理事會發布的《模型風險管理監理指引》（SR 11-7）等其他相關規範。此外，本白皮書也提供 ML 稽核實務中的治理框架與關鍵角色指引。

本白皮書提供了一套系統化且全面的 ML 資料合規稽核指引，透過解析 ML 的典型開發週期，協助資訊稽核人員掌握該領域的合規風險點。透過這些觀點，資訊稽核人員可以為管理階層提供可行的建議，以強化合規並降低風險。

機器學習合規概述

機器學習合規性與資料合規性密切相關

正如本白皮書第一部分所強調，現代機器學習（ML）演算法的開發、訓練與測試仰賴大量資料。當資料包含個人資訊、資料隱私、公平性與治理相關議題時，各類法規對資料蒐集與使用設立了相應的限制，以保障個人資料安全並維護消費者權益。然而，在 ML 領域專家深入研究之前，大規模 ML 應用對於消費者的實際影響並不總是如此顯著。對 ML更為深入探究是源自Facebook® 吹哨者 Frances Haugen。《麻省理工科技評論》（MIT Tech Review）[1]曾刊登一篇關於她舉報內容的文章，揭露了一個令人震驚的故事：Facebook 的 ML 模型如何影響青少年用戶。Facebook 內部團隊過去曾透過設計戰術，例如調整通知內容與頻率，來提升用戶黏著度。其中一個關鍵指標是「L6/7」，意即在過去七天內至少有六天登入 Facebook 的用戶比例。[2]L6/7 指標只是 Facebook 測量「用戶參與度」的眾多方式之一，該參與度衡量的是人們在 Facebook 平台上的使用情況，無論是發佈貼文、留言、按讚、分享，或是單純瀏覽內容。[3] 透過 L6/7，Facebook 工程師先前分析的每一次用戶互動都被轉交給 ML 演算法來處理，進而形成更快速、更個人化的回饋迴圈，調整並優化每位用戶的動態消息，以提升參與度數據。Facebook 的 ML 模型因其將「參與度為核心」的排序機制應用於易受影響的青少年群體以最大化利益而引發倫理爭議。同時，此事件也提升了大眾對 ML 在資料蒐集層面的關注，突顯出隱私與安全是資料合規的關鍵因素之一。

案例研究：Facebook 的機器學習設計策略與青少年心理健康的關聯

Facebook 旗下的 Instagram® 內部研究發現，該平台正在使青少女的心理健康問題加劇惡化。2020 年 3 月的一份簡報中，研究人員指出：「32% 的青少女表示，當她們對自己的體型感到不滿時，Instagram 讓她們的感受變得更糟。」[4]在美國參議院聽證會上，Facebook 吹哨者 Frances Haugen 的證詞指出，這一現象與 Facebook 基於參與度的排序系統（engagement-based ranking system）有關，並表示該系統「導致青少年接觸到更多關於厭食症的內容」。[5]此外，一名前人工智慧研究人員也發現：「那些習慣發布或參與憂鬱資訊的人，存在著罹患憂鬱症的可能性，並容易陷入日益消極的惡性循環，且進一步的惡化其心理健康。」[6]這議題的解決方案目前尚未明朗且仍在調查中，並充滿爭議。美國《通訊端正法》（Communications Decency Act, CDA）第 230 條保護 Facebook 等科技平台，使其無須對平台上的內容傳遞承擔法律責任。Haugen 建議應對第 230 條有關 ML 演算法排序進行更具針對性的例外條款，以消除基於參與度的排名機制。隨著 ML 演算法的應用越來越廣泛，機器學習合規與資料合規變得更加重要。

[1] Hao, K.; "The Facebook Whistleblower Says Its Algorithms Are Dangerous. Here's Why," *MIT Technology Review*, 5 October 2021, www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms/

[2] Hao, K.; "He Got Facebook Hooked on AI. Now He Can't Fix Its Misinformation Addiction," *MIT Technology Review*, 11 March 2021, www.technologyreview.com/2021/03/11/1020600/facebook-responsible-ai-misinformation

[3] *Ibid.*

[4] Smith, A.; "Facebook Knew Instagram Made Teenage Girls Feel Worse About Themselves – But That They Are 'Addicted' to App," *Independent*, 14 September 2021, https://www.independent.co.uk/tech/facebook-instagram-girls-worse-addicted-app-b1920021.html

[5] *Op cit* Hao

[6] *Op cit* Hao

機器學習合規因產業和地區而異

隨著過去十年間 ML 模型應用場景的不斷擴展，與其對應的法規和法律也逐步建立，以確保資料主體的權利，並規範企業的合規要求。

不同產業與地區的 ML 合規要求各不相同，以下**表一**是具代表性的機器學習規範(包括但不限於此)。

除了這些法律與規範外，環境、社會與治理（ESG） 已成為資料合規領域的新興議題，這一點可以從財務報告中 ESG 揭露數量的增加中看出。[7] 由於 ESG 具有社會科學背景，並且更強調質性（qualitative）而非量化（quantitative） 因素，因此 ESG 所揭露資料的蒐集過程可能存在挑戰。[8]例如，企業對於「社會正義立場」的資料蒐集方式，若存在不確定性，則其揭露的有效性將受到質疑。

表1：機器學習遵循規範範例

管轄地	名稱	描述
歐盟	歐盟《一般資料保護規則》(GDPR)[9]	GDPR 是歐盟及歐洲經濟區內關於資料保護與隱私的法律。該法規是歐盟隱私法與人權法的重要組成部分，特別是《歐盟基本權利憲章》第 8 條。
美國	《健康保險可攜性與責任法案》(HIPAA)[10]	HIPAA 是一部美國聯邦法律，用以要求建立全國標準，以防止在未經患者同意或知情的情況下洩露敏感的患者健康資訊。
美國加州	《加州消費者隱私保護法》(CCPA)[11]	CCPA 適用於在美國加州營運並蒐集加州居民個人資料的營利企業。符合以下條件之一的企業需遵守 CCPA：年營收超過 2,500 萬美元；擁有 50,000 名以上的消費者、家庭或設備的個人資訊；超過 50% 營收來自於銷售消費者個人資訊。CCPA 要求企業明確表達消費者個人資訊的處理目的與方式。
美國	《模型風險管理監理指引》(SR 11-7)[12]	美國聯邦儲備理事會與通貨監理局發布的《模型風險管理監理指引》，這項指引方針適用於銀行機構及其監管機構，以評估企業在模型風險管理方面的作為。該指引適用於美國聯邦儲備理事會監管的所有銀行，並依銀行的規模、性質、複雜度及模型使用範圍進行調整。
英國	AI稽核框架指引[13]	英國資訊委員辦公室(ICO)的諮詢指引草案針對兩大受眾：以合規為重點的專業人士，例如資料保護官（DPO）、法務總監、風險管理人員，以及英國資訊委員辦公室的稽核人員；技術專業人士，包括 ML 專家、資料科學家、軟體開發人員和工程師、資通安全專家與資訊風險管理人員。
美國	信用機會平等法(消費者信用保護法第七章)[14]	該法案基於種族、膚色、宗教、國籍、性別、婚姻狀況、年齡、公共援助身分或消費者信用保護法下的合法權利，嚴禁歧視個人。此外，該法規要求放款方在拒絕信貸申請時提供具體理由，並要求放款方須向首要抵押貸款的申請人提供房產評估報告和其他書面評價資料。

[7] CFAInstitute.org, “What is ESG Investing?,” 22 February 2022, https://help.cfainstitute.org/s/article/What-is-ESG-Investing. Also refer to ISACA, “Governance Roundup: What Are You Doing About Environmental, Social and Governance Factors in Your Enterprise?” USA, 2022, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004OiXgEAK

[8] Silk, D.M.; D.B. Anders; S.V. Niles; “GAO Report Highlights Dearth of ESG Disclosure,” Harvard Law School Forum on Corporate Governance, 17 July 2020, https://corpgov.law.harvard.edu/2020/07/17/gao-report-highlights-dearth-of-esg-disclosure/

[9] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), EUR-lex, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434#tocId9

[10] HHS.gov, “Health Information Privacy,” www.hhs.gov/hipaa/index.html

[11] California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa

[12] Board of Governors of the Federal Reserve System, SR 11-7: Guidance on Model Risk Management, 4 April 2011, https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm

[13] Information Commissioner’s Office, “Guidance on the AI Auditing Framework: Draft Guidance for Consultation,” https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf

[14] 15 USC Chapter 41, Subchapter IV: Equal Credit Opportunity, http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter41-subchapter4&edition=prelim

環境、社會與公司治理（ESG）因素

2020 年 7 月，美國聯邦審計署（GAO）指出，投資者需要更完整的 ESG 相關資訊，以評估企業面臨的挑戰。為應對這一需求，美國證券交易委員會（SEC）於 2021 年 3 月成立 ESG 與氣候議題專責小組，其主要目標是識別「在現行法規下，證券發行人對氣候風險的揭露是否存在重大缺漏或不準確」。[15]美國證券交易委員會的專責小組任務還負責分析投資顧問與基金ESG策略相關揭露與合規議題，並協調該機構資源的有效利用；專責小組利用複雜資料分析技術萃取並評估已公開的 ESG 資訊，辨認潛在違規行為。[16]

隨著企業承諾提供更有價值的資訊，並確保揭露的準確性，監管機構對合規的一致性要求也日益提高。加拿大永續金融行動委員會（SFAC）計劃於 2022 年底前提供強制性氣候資訊揭露的建議。[17]國際氣候倡議（iCI），一個關注全球性氣候議題的私募股權聯盟，已發布關於溫室氣體排放的會計與報告標準，提供給私募股權行業參考。

由於不同產業與地區的風險胃納各有不同，ML合規的採納速度也有所不同。

另一項自願性資訊揭露工具，氣候相關財務揭露工作小組（TCFD） 被廣泛認可為傳達氣候相關財務資訊的權威指南，目前已有超過 1,900 家機構承諾支持 TCFD。[18]

如同大多數的違規案例，若企業未能主動評估資料合規，可能會面臨監管機構的調查與訴訟，進而產生巨額罰款、及成本與聲譽風險。

現行法規與新興領域（如 ESG）的發展，印證了《*哈佛商業評論*》[19]的一篇文章的觀點：AI 和 ML 的監管正逐步擴展至所有產業。為了未來做準備，建議稽核人員在企業的 ML 與 AI 開發週期中落實合規審查。然而，由於不同產業與地區的風險胃納各有不同，ML合規性的採納速度也有所不同。

機器學習稽核的資料合規

在評估資料合規情形時，稽核人員應考量所有資料來源，包括任何與 ML 模型訓練相關的移轉資料，這些資料可能受資料隱私或公平性相關法規的約束。

雖然資料集的複雜性與抽樣策略通常由資料科學家負責，但稽核人員可以從開發生命週期的角度，驗證資料轉變過程與 ML 模擬的結果。如同大多數的違規案例，若企業未能主動評估資料合規，可能會面臨監管機構的調查與訴訟，進而產生巨額罰款、及成本與聲譽風險。

[15] Macpherson, M.; "Implications for Artificial Intelligence and ESG Data," *The AI Journal*, 6 October 2021, https://aijourn.com/implications-for-artificial-intelligence-and-esg-data

[16] *Ibid.*

[17] Segal, M.; "Canada Sets Mandatory Climate Disclosure as a Top Priority for Sustainable Finance Council," *ESG Today*, 20 May 2022, https://www.esgtoday.com/canada-sets-mandatory-climate-disclosure-as-top-priority-for-sustainable-finance-council/

[18] *Op cit* Macpherson

[19] Candelon, F.; R. Charme di Carlo; M. De Bondt; T. Evgeniou; "AI Regulation Is Coming," *Harvard Business Review*, September-October 2021, https://hbr.org/2021/09/ai-regulation-is-coming

在 GDPR、CCPA 和英國資訊委員辦公室的AI 稽核指引等關鍵監管框架中，以下是資料合規性的一些重要考量：

- **ML 模型使用個人資料的合法性、公平性與透明度—**ML 模型於開發生命週期的不同階段中處理個人資料，並用於多種用途，也因此存在風險。例如：「如果企業未能適當區分不同的資料處理操作，並為每項操作識別適當的合法依據，可能會違反資料保護法中的『合法性原則』。」[20] 稽核人員應確認企業對每項資料處理目的均有對應的合法依據，以告知管理層並提出確信「企業遵守合法性原則」。

稽核人員應確認這些個人資料使用的權利適用於 ML（機器學習）開發生命週期的所有階段。具體而言，稽核人員應確保企業在開發和部署 AI 時，已考量個人相關的資訊、存取、更正、刪除、限制處理及資料可攜性的權利。

- **資料最小化與資料安全—**如果 ML 模型能夠在處理較少個人資料的情況下達到相同效果，則企業必須遵循資料最小化原則。除了減少資料保護的負擔，企業可利用資料最小化原則來確保，「個人資料在處理過程中具備適當的安全機制，以防止未經授權的存取、非法處理、意外遺失、銷毀或損壞。」[21] 除了確認資料最小化原則的運用，稽核人員還應驗證所有個人資料的存取與儲存過程是否有完整記錄與文件化，以便監測適當安全風險控制的有效性。
- **當責與治理—**在歐洲，當企業使用 ML 系統來處理個人資料時，必須執行「資料保護影響評估（DPIA）」[22]。DPIA 讓企業有機會去檢視自身使用 AI 系統的方式、資料處理的目的，以及潛在風險。此外，根據 ML 系統的設計與部署方式，企業需在隱私與其他商業利益之間做出權衡。稽核人員的責任在於理解這些權衡機制，並確保企業採取適當措施來管理潛在風險。例如，在受 GDPR 監管的國家，Facebook 基於參與度的 ML 排序模型(見本白皮書前章節：「ML合規與資料合規密切相關」)可能被禁止使用某些敏感個人資訊，這可能會降低模型的表現。
- **消費者知情權—**CCPA 規定，消費者有權要求企業揭露其蒐集、使用、共享或銷售的個人資訊及其原因。因此，在 ML 稽核過程中，稽核人員應確保企業對 CCPA 所涵蓋不同的個人資訊有明確認知，尤其稽核人員應考量[23]：
  - 所蒐集的個人資訊類別
  - 具體蒐集的個人資訊項目
  - 企業所蒐集個人資訊的來源類別
  - 企業使用個人資訊的目的
  - 企業與那些第三方共享個人資訊
  - 企業向第三方銷售或揭露的個人資訊類別

根據資料保護相關法律與法規，個人擁有與其個人資訊相關的權利，其中包括與自動化決策相關的權利。在GDPR（一般資料保護規則）的適用範圍內，稽核人員應確認這些個人資料使用的權利適用於 ML（機器學習）開發生命週期的所有階段。具體而言，稽核人員應確保企業在開發和部署 AI 時，已考量個人相關的資訊、存取、更正、刪除、限制處理及資料可攜性的權利。此外，稽核人員需驗證所有個人資訊的移動與儲存過程均已完整記錄並文件化。

[20] Ahmed, H.; "Auditing Guidelines for Artificial Intelligence," @ISACA, 21 December 2020, www.isaca.org/resources/news-and-trends/newsletters/atisaca/2020/volume-26/auditing-guidelines-for-artificial-intelligence

[21] *Ibid.*

[22] GDPR.eu, "Data Protection Impact Assessment (DPIA)," https://gdpr.eu/data-protection-impact-assessment-template/?cn-reloaded=1

[23] State of California Department of Justice, Office of the Attorney General, "California Consumer Privacy Act (CCPA): Frequently Asked Questions (FAQs)," https://oag.ca.gov/privacy/ccpa#:~:text=The%20CCPA%20requires%20business%20privacy.the%20Right%20to%20Non%2DDiscrimination

模型合規

現有多項 ML 合規框架可供企業參考，例如 ISO/IEC 23053:2022(基於機器學習（ML）的人工智慧（AI）系統框架)，此框架適用於所有產業及各種規模的組織。[24]

此外，也有特定產業相關的 ML 監管框架提供有用的指引。「監管與監督函件(SR)11-7」即是用於監理模型風險的一個例子。(SR)11-7由美國聯邦儲備理事會與美國通貨監理局（OCC）聯合發布。如同圖二所示，為模型風險管理的合規要素提供指引，包括：模型風險管理、模型開發、實施及使用、模型驗證及模型文件管理。

除了理解 ML 模型週期的整合性，稽核人員還應了解關鍵利益關係人（如資料科學家與 ML DevOps 管理者）在合規與治理中的角色。

持續關注風險與控制校準及風險管理權責，能夠幫助稽核人員評估控制措施的有效性，以及對風險容忍度的變化保持警覺。

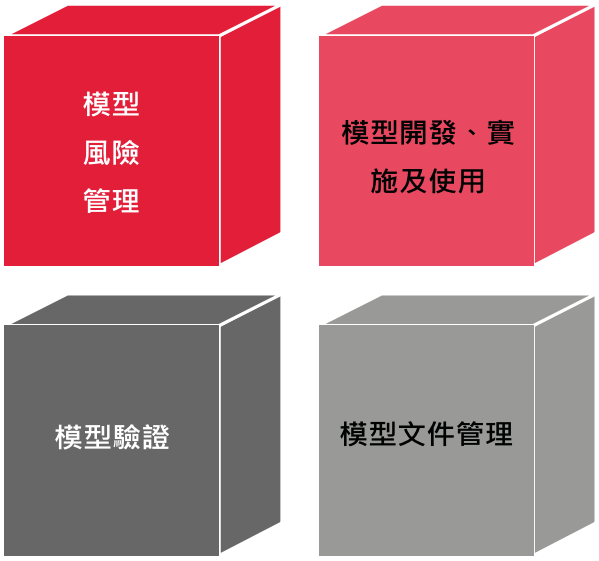
模型風險管理

一般而言，機器學習模型的風險實現通常來自兩個主要原因，一個模型可能：

- 模型本身存在根本性錯誤，導致輸出結果不準確，無法滿足設計目標或業務需求。
- 不正確或不適當地使用模型，或因誤解其限制及假設，導致不當應用。

從稽核角度評估 ML 風險時，稽核人員應明確辨認每項風險及其對應的控制措施。持續關注風險與控制校準及風險管理權責，能夠幫助稽核人員評估控制措施的有效性，以及對風險容忍度的變化保持警覺。

圖2：(SR) 11-7: 模型風險管理之監管指引



模型開發、實施及使用

ML 模型開發流程始於「確保設計與模型的預期用途一致」的目標陳述。在模型實施前，稽核人員應評估模型的開發方式是否能夠滿足其設計目標(如資料量體是否足夠)。一旦模型開始運作，稽核人員應持續監測模型的使用情況，以確保其能夠持續符合原先開發的目的。

模型驗證

模型驗證是指一系列流程與活動，用於確保模型的性能符合預期，並與其設計目標及業務用途保持一致。有效的驗證機制不僅能確保模型的穩健性，也能辨認其潛在限制與假設，並用以評估對模型的潛在影響。模型驗證應由具備適當專業能力與影響力的專業人士執行。

[24] ISO, ISO/IEC 23053: 2022 Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML), June 2022, https://www.iso.org/standard/74438.html

美國聯邦儲備理事會與美國通貨監理局建議機器學習模型驗證框架應包含三個核心要素：

- **包含發展性證明的概念健全性評估 (Evaluation of Conceptual Soundness)** - 健全的機器學習模型開發流程將提供充分的文件證明，以支持所有選擇的模型，包括整體理論架構、關鍵假設、資料來源及具體數學計算方法。

機器學習模型的開發與驗證文件應具備充分的細節，使未接觸該模型的相關人員能夠理解模型運作方式，並熟悉其限制與關鍵假設。

- **包含流程驗證與標竿測試的持續性監測 (Ongoing Monitoring)** - 一般認為機器學習模型在訓練完成後會維持不變，但實際上，數據分佈可能發生變化，導致現有模型失效並影響其效能。因此，監測變化對確保機器學習模型持續符合業務需求具有相當的重要性。
- **包含歷史數據回測的結果分析 (Outcome Analysis)** - 結果分析的目標在於建立實際結果與預期目標間的合理範圍，並評估觀察到的偏差原因，以確保模型的適用性。

整體而言，模型驗證有助於降低模型風險，透過辨認模型錯誤、矯正措施及適當的使用方式，提升模型的可靠性。驗證過程亦評估模型的基本假設、理論基礎及方法，藉此提供模型風險的來源與範圍資訊。

模型驗證還能透露模型效能隨時間衰退的情況，並透過分析結果與預測或預期值之間的分佈，設定可接受的誤差範圍。如果模型結果持續落在該範圍之外，則應重新開發模型。

模型文件管理

機器學習模型的開發與驗證文件應具備充分的細節，使未接觸該模型的相關人員能夠理解模型運作方式，並熟悉其限制與關鍵假設。完整的文件有助於確保業務持續性，使政策遵循更為透明，並協助追蹤建議、回應及例外事項。因此，開發人員、使用者、控制與合規單位以及監督人員皆可受益於有效的文件管理。

驗證報告 (Validation Reports) 是文件紀錄的重要部分，應明確說明已審查的模型面向，特別是在邊界條件下可能存在的缺陷，並確定是否有需要進行調整或實施補償性控制措施。為確保驗證報告對企業具備實質意義，報告應包含清晰的管理摘要，說明模型的目的，並提供易懂的模型與驗證結果的概述，包括主要限制與關鍵假設。

為確保驗證報告對企業具備實質意義，報告應包含清晰的管理摘要，說明模型的目的，並提供易懂的模型與驗證結果的概述，包括主要限制與關鍵假設。

值得注意的是，稽核人員與負責驗證的工作人員應擁有明確的權限，以對模型開發人員及使用者提出挑戰，並向管理階層反映其發現的問題。此外，稽核人員及其他參與驗證工作的團隊應依據美國聯邦儲備理事會監理指引的建議，將所觀察的問題與缺陷納入其中。

機器學習稽核的治理與關鍵角色

在機器學習模型風險管理框架中，開發與維持強大的治理架構、政策與控制機制至關重要。即使模型開發與驗證均達標準，若治理功能薄弱，整體模型風險管理的有效性仍會降低。

此外，現代機器學習應用的開發是一項大工程，其中包含多個專業領域，如系統架構、演算法設計、資料蒐集與準備、系統訓練與測試等。

因此，稽核人員應了解開發週期中的關鍵角色，以確保專業技能被適當運用並發揮價值。

機器學習工程角色

機器學習工程角色包含專業技術人員，負責建立端到端的機器學習模型。

稽核人員應將自身定位為值得信賴的顧問，以協助降低機器學習模型所暴露的風險。圖3 提供可能的工程角色列表，該列表可能因產業不同而有所變動。

現代機器學習應用的開發是一項大工程，其中包含多個專業領域，如系統架構、演算法設計、資料蒐集與準備、系統訓練與測試等。

管理角色

管理角色包括工程經理、總監、風險及合規團隊，該團隊通常由風險長或法務領導。這些企業治理領袖應考量世界經濟論壇於 2022 年發布的《Empowering AI Leadership: AI C-Suite Toolkit》中的機器學習模型管理實務。[25]

圖 3 :機器學習工程角色

角色	描述
資料科學家	資料科學家與企業利害關係人密切合作，以確定資料如何幫助企業達成目標。他們設計資料建模流程、創建演算法與預測模型，以提取企業所需的資料，並協助分析資料及提供洞察報告。[26]
機器學習工程師	機器學習工程師專注於研究、構建及設計自動化 AI 系統，以自動執行預測模型。他們負責設計與開發能夠自我學習並做出預測的 AI 演算法，這些演算法構成了機器學習的核心。
資料工程師	資料工程師負責在資料集中尋找趨勢，並開發演算法，使原始資料對企業更具價值。此角色需要具備深厚的技術能力，包括 SQL 資料庫設計、多種程式語言的運用，以及 ETL (擷取、轉換、載入)流程的專業知識。
機器學習營運(MLOps)	MLOps 團隊確保已部署的模型能夠維持良好狀態、達成預期效能且不會對企業造成不良影響。此角色對於保護企業免受因部署但未維護或未監測之模型所帶來的風險極為重要。

[25] World Economic Forum, “Empowering AI Leadership: AI C-Suite Toolkit,” 12 January 2022, https://www.weforum.org/reports/empowering-ai-leadership-ai-c-suite-toolkit/?

[26] Doyle, L.; “What Does a Data Scientist Do?,” Northeastern University Graduate Programs, 13 August 2020, www.northeastern.edu/graduate/blog/what- does-a-data-scientist-do/

本框架倡導建立涵蓋全體員工以資料為導向的文化，並依據國際內部稽核協會（IIA）所提出的「三道模型」[27]，確保企業運作順暢：

- **第一道角色**—資料科學家、資料工程師、機器學習（ML）模型開發人員、執行與營運團隊： 負責規劃、設計、開發、部署及運作資料、人工智慧（AI）及機器學習（ML）模型，包含自動化與軟體開發。主要職責包含運行及監控資料、軟體及模型。
- **第二道角色**—經理、總監、監管人員及品質保證團隊： 負責評估資料、AI 及 ML 模型、自動化及軟體的風險，並一同為企業戰略發展負責。持續監測第一道線的運行狀況也屬第二道線職責。
- 第**三道角色**—內部與外部稽核人員、倫理專家： 監督前兩道的工作，確保企業符合法規、政策及企業策略，並確保技術應用符合道德及社會責任。內部稽核人員應定期審查控制措施與流程，而倫理專家則以倫理角度評估企業決策、策略、文化及使命。

為配合採用與人工智慧/機器學習治理相關的三道模型架構，建議企業成立倫理委員會。成員應涵蓋不同背景的主管與員工，以確保 AI/ML 的應用符合道德規範。

為配合採用與人工智慧/機器學習治理相關的三道模型架構，建議企業成立倫理委員會。

某些企業可能會聘請外部專家加入該委員會，以獲取內部無法獲得的專業知識或不同視角，增強治理機制的有效性。

結論

人工智慧（AI）和機器學習（ML）的採用為企業創造了無限的機會。

例如，透過AI與ML，企業能夠更快速且全面地運用歷史資料，以支持決策制定，或優化流程，更好地滿足客戶需求。

機器學習的應用開闢了一個全新的稽核領域，這個領域充滿了挑戰與複雜性，但同時也極具發展潛力。

然而，這些機會也伴隨著挑戰。從理解這項新技術所帶來的風險，至因應帶有倫理考量的潛在合規要求，機器學習的應用開闢了一個全新的稽核領域，這個領域充滿了挑戰與複雜性，但同時也極具發展潛力。

當資訊稽核人員進入機器學習合規領域或持續發展該領域的技能時，他們可以透過結構化的方法來應對ML稽核的挑戰。

首先，了解組織對機器學習的策略觀點及相關利害關係人的角色至關重要。這些背景資訊能幫助稽核人員從業務角度更好地理解ML的開發週期（風險管理、模型開發、實施與使用、模型驗證及文件紀錄）。

這使得資訊稽核人員能夠評估合規風險的暴露程度及獲得洞見，以支持他們向管理層提供具體可行的建議，以強化合規性並降低風險。

[27] The Institute of Internal Auditors, “The IIA’s Three Lines Model: An Update of the Three Lines of Defense,” www.theiia.org/globalassets/site/about- us/advocacy/three-lines-model-updated.pdf

附錄：推薦資源

數十年來，機器學習一直是電腦科學領域最活躍的學術研究方向。研究人員與統計學家的努力，讓這個領域從抽象概念發展到成熟應用。儘管從業人員無需深入理解ML演算法的全面理論概念，但若希望加深對機器學習的理解，建議參考以下資源：

歐洲議會與理事會於2016年4月27日通過的歐盟（EU）法規《第2016/679號規則》，即《一般資料保護規則》（GDPR），規範了自然人在個人資料處理與自由流通方面的保護，並取代了個人資料保護指令(95/46/EC)。
EUR-lex, https://eur- lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434#tocId9

Hao, K.; "The Facebook Whistleblower Says its Algorithms are Dangerous. Here's Why." *MIT Technology Review*, 5 October 2021, www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms

Intersoft Consulting, "Principles Relating to Processing of Personal Data: GDPR: Articles 5.1 and 5.2," https//:gdpr- info.eu/chapter-5/

Pearce, G.; "Beware the Privacy Violations in Artificial Intelligence Applications," *ISACA* NOW Blog, 28 May 2021, www.isaca.org/resources/news-and-trends/isaca-now- blog/2021/beware-the-privacy-violations-in-artificial-intelligence-applications

歐盟GDPR第5.1條規定了七項關鍵原則，構成一般資料保護機制的核心：

個人資料應該：

(a) 以合法、公平且透明的方式處理（「合法性、公平性與透明度」）；

(b) 出於特定、明確且合法的目的蒐集個人資料，並且不得以非上述目的的方式進行額外處理；然而，為公共利益、科學或歷史研究或統計目的所進行的額外處理，將不被視為與原始目的不相容（「目的限制」）；

(c) 充分、攸關且僅限於實現處理目的所必須的範圍（「資料最小化」）；

(d) 準確且在必要時及時更新；應採取一切合理措施，以確保任何不準確的個人資料被及時刪除或更正（「準確性」）；

(e) 以允許辨認資料主體的形式保存，時間不得超過達成處理目的所須的期限；若出於公共利益、科學或歷史研究或統計目的需要，則可存儲更長時間，前提是必須實施GDPR要求的適當技術與組織措施，以保障個人權利與自由（「儲存限制」）；

(f) 以確保個人資料安全的方式進行處理，包括防止未經授權或非法處理，以及防止意外遺失、破壞或損害，並應採取適當的技術或組織措施（「完整性與保密性」）。[28]

第5.2條補充：

資料控制者應對第5.1條的合規性負責，並能夠證明其符合該條款的要求（「當責」）。[29]

[28] *Op cit* European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

[29] *Ibid*.

致謝

ISACA 謹此致謝：

開發領袖

Victor Fang, Ph.D.
CEO, AnChain.AI Inc., 美國

校審專家

Ibrahim Sulaiman Alnamlah
CISA, COBIT 2019, ITLv4, ISO/IEC 27001 LA
沙烏地阿拉伯
Chetan Anand
CDPSE, CCIO, CPISI, ISF IRAM2, ISO 9001 LA, ISO 22301 LA, ISO 27001 LA, ISO 27701, ISO 31000, SQAM, Lean Six Sigma
Green Belt, Agile Scrum Master, Fellow of Privacy Technology, NLSIU Privacy and Data Protection Laws
印度
Shigeto Fukuda
CISA, CDPSE
日本
Kevin Fumai
CDPSE, CCSK, CEET, CIPM, CIPP/US/E, CIPT, FIP, PLS
美國
Shamik Kacker
CISM, CRISC, CDPSE, CCSK, CCSP, CISSP, ITIL Expert, TOGAF 9
美國
Harmendra Nitish Koladoo
CISA, CDPSE, CEH, CHFI, ISO 27001 LA
Hong Kong SAR, China
Frank Oelker
CISA
德國
Christian Nyanor Ohene
CISA, CEH
迦納
Jian Qin, Ph.D.
CISA, CISSP, PMP, ODSC Machine Learning Certification
美國

校審專家(續)

Xitij U. Shukla, Ph.D.
CISA
印度
Ioannis Vittas
CISA, CISM, COBIT 2019 Foundation, BCCLA
希臘
Wickey Wang
CISA, Six Sigma Green Belt
美國
Yap Kai Yeow
CISA, CISM, CRISC, CAMS
新加坡

ISACA 董事會

Pamela Nigro, Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, 美國
John De Santis, Vice-Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., 美國
Niel Harper
CISA, CRISC, CDPSE, CISSP
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, 德國
Gabriela Hernandez-Cardoso
Independent Board Member, 墨西哥
Maureen O'Connell
NACD-DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., 美國
Veronica Rose
CISA, CDPSE
Senior Information Systems Auditor–Advisory Consulting, KPMG Uganda, Founder, Encrypt Africa, 肯亞
David Samuelson
Chief Executive Officer, ISACA, 美國
Gerrard Schmid
Former President and Chief Executive Officer, Diebold Nixdorf, 美國
Bjorn R. Watne
CISA, CISM, CGEIT, CRISC, CDPSE, CISSP-ISSMP
Senior Vice President and Chief Security Officer, Telenor Group, 美國
Asaf Weisberg
CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., 以色列
Gregory Touhill
CISM, CISSP
ISACA Board Chair, 2021-2022
Director, CERT Center, Carnegie Mellon University, 美國
Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, 美國
Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, 美國
Rob Clyde
CISM, NACD-DC
ISACA Board Chair, 2018-2019
Independent Director, Titus, Executive Chair, White Cloud Security, Managing Director, Clyde Consulting LLC, 美國

關於 ISACA

ISACA® (https://www.isaca.org) 是一個推動個人與組織追求數位信任的全球性社群。 50 多年來，ISACA 為個人與企業提供知識、證書、教育、培訓與社群，以促進其職涯發展、改造其組織並建立一個更值得信賴及合乎倫理道德的數位世界。 ISACA 是一個全球性專業協會與學習型組織，擴展其在資訊安全、治理、確信、風險、隱私及品質等數位信任領域工作的165,000 名成員的專業技能。它已在全球 188 個國家共設立225 個分會。 ISACA 透過其 One In Tech 基金會，為資源不足及代表性不足的人們提供 IT 教育與職涯發展途徑之支援。

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

電話: +1.847.660.5505

傳真: +1.847.253.1755

支援: support.isaca.org

網站: www.isaca.org

提供回饋：

www.isaca.org/audit-practitioners-guide-to-ML-part-2

參加ISACA線上論壇：
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/

免責聲明

ISACA 設計並完成本創作「稽核從業人員之機器學習參考指引，第二部分：合規風險」（著作），主要作為專業人士的教育資源。ISACA 並不聲稱使用本著作任何內容將確保有成功的結果。 該著作不應被視為包含所有適當的資訊、程序及測試或排除合理指導獲得相同結果的其他資訊、程序與測試。 在確定任何特定資訊、程序或測試的適當性時，專業人員應將本身之專業判斷應用於特定系統或資訊科技環境所呈現的特定情況。

權利保留

中文版致謝名單

ISACA台灣分會 高進光理事長

翻譯: 林煒傑

校稿: 陳政龍

編輯排版: 游恬欣