

ISACA全球AI脈動調查解析： AI治理、資安、風險管理與 稽核的關鍵因應策略

陳政龍

CISA, CGEIT, CDPSE, PMP, CEH

ISACA台灣分會 副會長

電腦稽核協會 常務理事/國際事務委員會主任委員

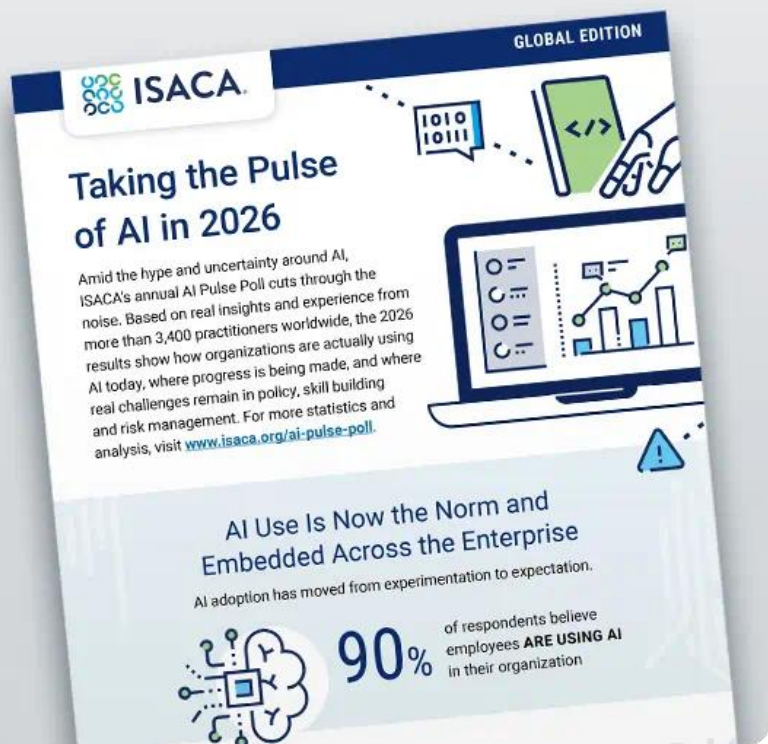
國家太空中心 稽核長

2026年全球AI 脈動調查 《2026 AI Pulse Poll》



揭開人工智慧炒作的迷霧

在不間斷的新聞報導與市場熱潮之下，人工智慧（AI）如今在各類組織中的實際發展究竟如何？



掌握 2026 年 AI 發展脈動

AI 的應用已從試驗探索階段，邁向日常運用；然而，組織的整備能力仍未能跟上其發展速度。ISACA《2026 年 AI 脈動調查》彙整了全球 **3,400 多位數位信任領域專業人士** 的調查結果，深入探討以下重點：

- 全球實務工作者目前如何運用 AI
- 他們所面臨日益升高的 AI 風險
- AI 治理、專業能力及監督機制仍存在哪些缺口



AI 應用已成為常態 深度融入企業各個層面

AI 不再只是試驗性技術，現在已成為企業營運的常態。



90%

的受訪者表示，
其組織內的員工
目前正在使用 AI。

◆文字內容生成 ◆提升生產力 ◆自動化作業 ◆資料分析



InfoSec
Taiwan
國際資安展大會

2026

重新定義信任邊界
THE NEW TRUST BOUNDARY

影子 AI 仍是一項重大風險(隱憂)

即使未獲組織明確授權，相關使用情形仍持續存在。



81%

的受訪者表示，其組織內的員工
正使用生成式 AI。



InfoSec
Taiwan
國際資安盛會

2026

重新定義信任邊界

THE NEW TRUST BOUNDARY

全球

最常見的 AI 應用包括

-  **62%** 提升生產力
文字內容生成
-  **50%** 自動化重複性工作
-  **49%** 分析大量資料
-  **37%** 客戶服務（例如：聊天機器人）
-  **36%** 改善決策品質



77%

的受訪者表示，組織使用 AI 時，會將其可能造成的相關環境議題納入考量；**57%** 的個人受訪者在使用 AI 時也會考量相關環境議題。

歐洲

最常見的 AI 應用包括

-  **69%** 文字內容生成
-  **63%** 提升生產力
-  **54%** 自動化重複性工作
-  **52%** 分析大量資料
-  **37%** 客戶服務（例如：聊天機器人）



80%

的受訪者表示，組織使用 AI 時，會將其可能帶來的相關環境議題納入考量。



InfoSec
Taiwan
國際資安展大會

2026

重新定義信任邊界

THE NEW TRUST BOUNDARY

AI 政策持續改善，但仍未能跟上發展速度

AI 治理仍未跟上 AI 導入的速度。雖然組織已持續強化，
但多數仍缺乏必要的防護機制。

全球

38%

(較 2025 年提升28%)

30%

25%

7%

歐洲

42%

(較 2025 年提升31%)

31%

23%

5%

已建立正式且完整 AI 政策

已制定有限範圍
的AI 政策

尚未建立有效
AI 政策

不確定是否
具有 AI 政策



InfoSec
Taiwan
國際資安展大會

2026

重新定義信任邊界
THE NEW TRUST BOUNDARY

您的組織是否具備明確文件化流程， 在 AI 系統發生問題時能予以關閉或停用？

(例如：遭惡意使用者攻擊，或 AI 系統產生不良結果)

- 39% 不清楚
- 25% 無
- 16% 流程建置中
- 12% 是，定期測試
- 8% 是，未定期測試



不清楚資安事件發生時，
停止 AI 系統運作所需
時間。



ONLY
9%

非常同意組織已充分重視
AI 導入相關倫理標準。



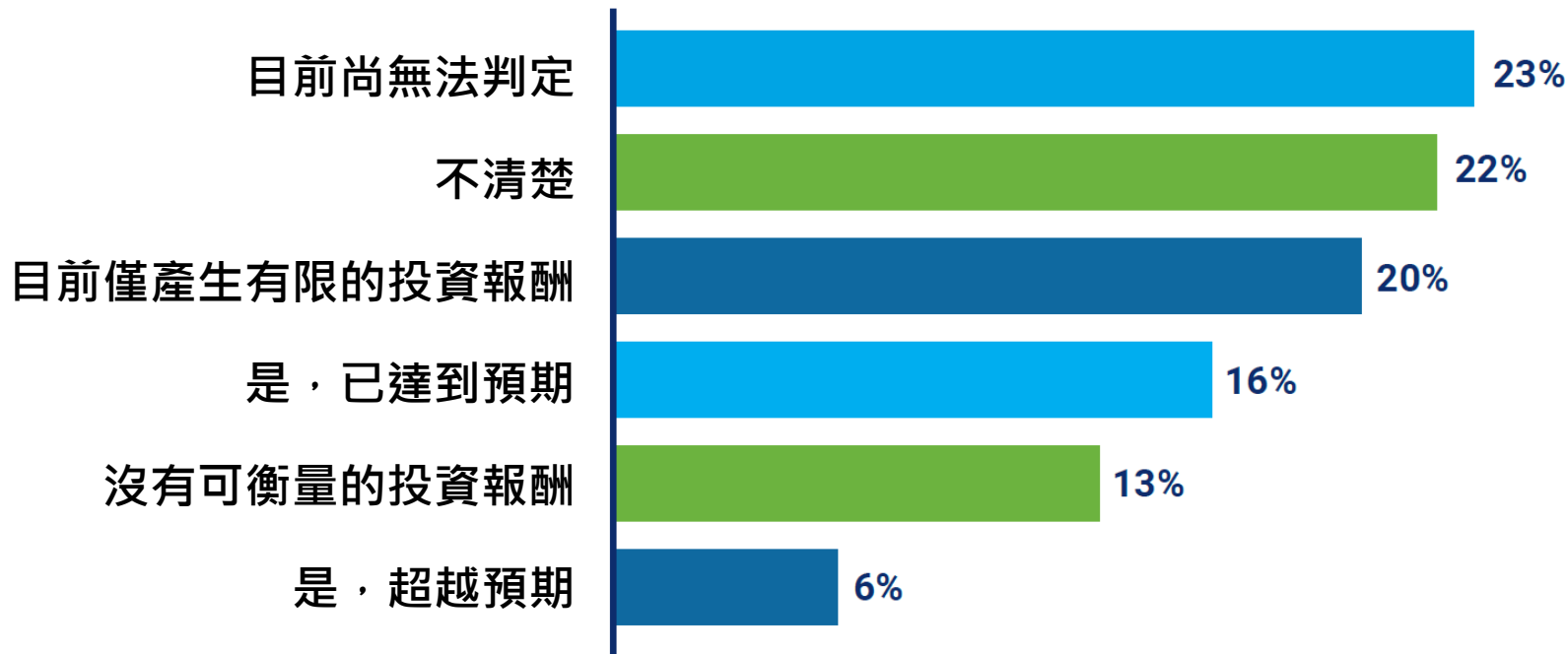
InfoSec
Taiwan
國際資安大會

2026

重新定義信任邊界
THE NEW TRUST BOUNDARY

AI 投資報酬率仍不明確

(您的組織導入 AI 後，是否已產生可衡量的投資報酬率 (ROI) ？





AI 素養已成為 必要能力

78
%

的受訪者表示，AI 技能對其專業工作而言非常重要或極為重要，高於去年的 72%。



AI 技能需求提升 增加培訓投入

33
%

的組織已為全體員工提供 AI 培訓，高於 2025 年的 22%。



InfoSec
Taiwan
國際資安展大會

2026

重新定義信任邊界
THE NEW TRUST BOUNDARY

全球

主要 AI 風險

最常被提及的 AI 風險包括：

- 1  **82%** 錯誤資訊與蓄意誤導
- 2  **74%** 侵犯隱私
- 3  **60%** 社交工程
- 4  **58%** 智慧財產權損失
- 5  **42%** 工作職位流失

歐洲

主要 AI 風險

最常被提及的 AI 風險包括：

- 1  **87%** 錯誤資訊與蓄意誤導
- 2  **75%** 侵犯隱私
- 3  **60%** 社交工程
- 4  **59%** 智慧財產權損失
- 5  **41%** 工作職位流失



InfoSec
Taiwan
國際資安展大會

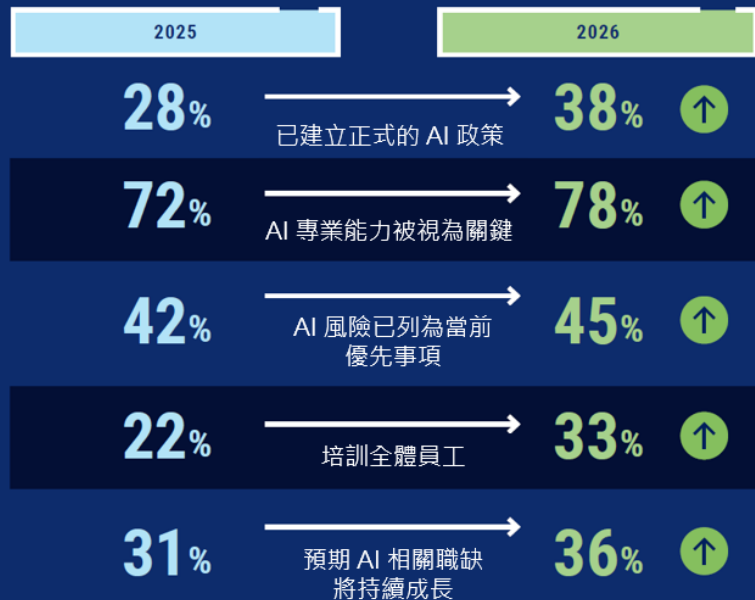
2026

重新定義信任邊界
THE NEW TRUST BOUNDARY

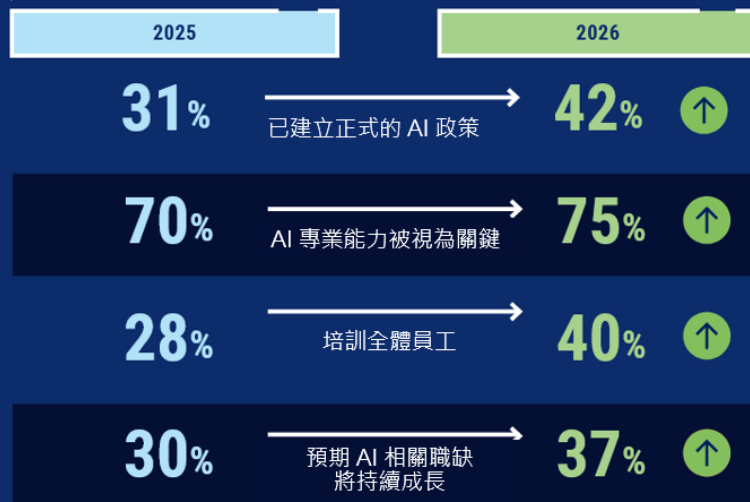
重點摘要

今年與去年相比有哪些改變？

全球



歐洲



InfoSec
Taiwan
國際資安展大會

2026

重新定義信任邊界

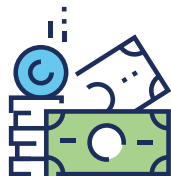
THE NEW TRUST BOUNDARY



《2026 AI Pulse Poll》



AI 已無所不在
--治理仍未跟上



AI 投資報酬率 (ROI)
--仍有待驗證



AI 人才能力是關鍵
--投入資源仍然不足



InfoSec
Taiwan
國際資安盛會

2026

重新定義信任邊界
THE NEW TRUST BOUNDARY



ISACA in 2026

為職涯賦能、讓信任扎根

Fueling Careers. Strengthening Trust.



智連未來 CONNECT
創新無界 CREATE
共榮新局 CONTRIBUTE

人工智慧、治理、資安、隱私、稽核/審計
內部控制、量子運算、風險管理

未來



2025.10.13~14 國際電腦稽核協會(ISACA)全球領導人會議(GLS)【英國倫敦】



We are a Global Community

47%

North America

21%

Europe

20%

Asia

3%

Central/South
America

5%

Africa

3%

Oceania

195k+
MEMBERS

為職涯賦能、讓信任扎根

Fueling Careers. Strengthening Trust.



隱私



安全



風險



品質



治理



確信

ISACA by the Numbers

Global Non-Profit Professional Association for Individuals and Enterprises



195k+

Members



231

Chapters



2.8k+

Global chapter
leader volunteers



429k+

Certifications issued



14k+

Enterprises served

People Are Our
Top Priority



ISACA 證照

Skillsoft 經常評為**最高薪酬資訊證書**之一



CISA、CISM 榮獲 2025 年 SC 最佳專業認證獎項！

入圍名單：

<https://www.scworld.com/news/2025-sc-awards-finalists-best-professional-certification-program>

探討IT認證與薪資之間的關係

www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/exploring-the-relationship-between-it-certifications-and-salaries

AVERAGE SALARIES IN
2023 (US)

\$**154k+**
CISA

\$**167k+**
CISM

\$**164k+**
CGEIT

ISACA專業認證

COBIT

An ISACA® Framework

IT RISK

FUNDAMENTALS

An ISACA® Certificate

IT AUDIT

FUNDAMENTALS

An ISACA® Certificate

CYBERSECURITY

FUNDAMENTALS

An ISACA® Certificate

**ARTIFICIAL
INTELLIGENCE**

FUNDAMENTALS

An ISACA® Certificate

BLOCKCHAIN

FUNDAMENTALS

An ISACA® Certificate

CLOUD

FUNDAMENTALS

An ISACA® Certificate

**CYBERSECURITY
AUDIT**

An ISACA® Certificate

DATA SCIENCE

FUNDAMENTALS

An ISACA® Certificate

Digital Trust

Ecosystem Framework

IoT

FUNDAMENTALS

An ISACA® Certificate

ADDITIONAL
CERTIFICATES

2

COBIT certificates

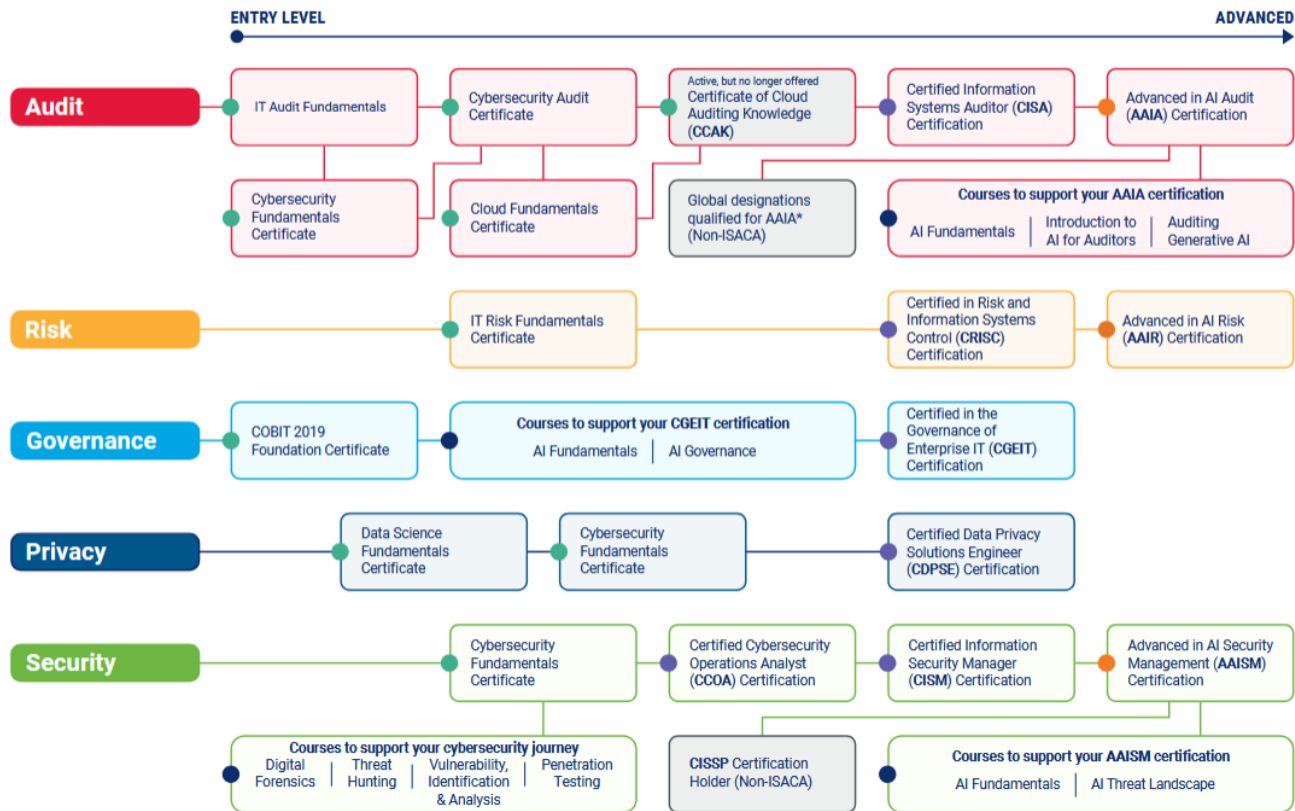
8

Foundational Certificates

3

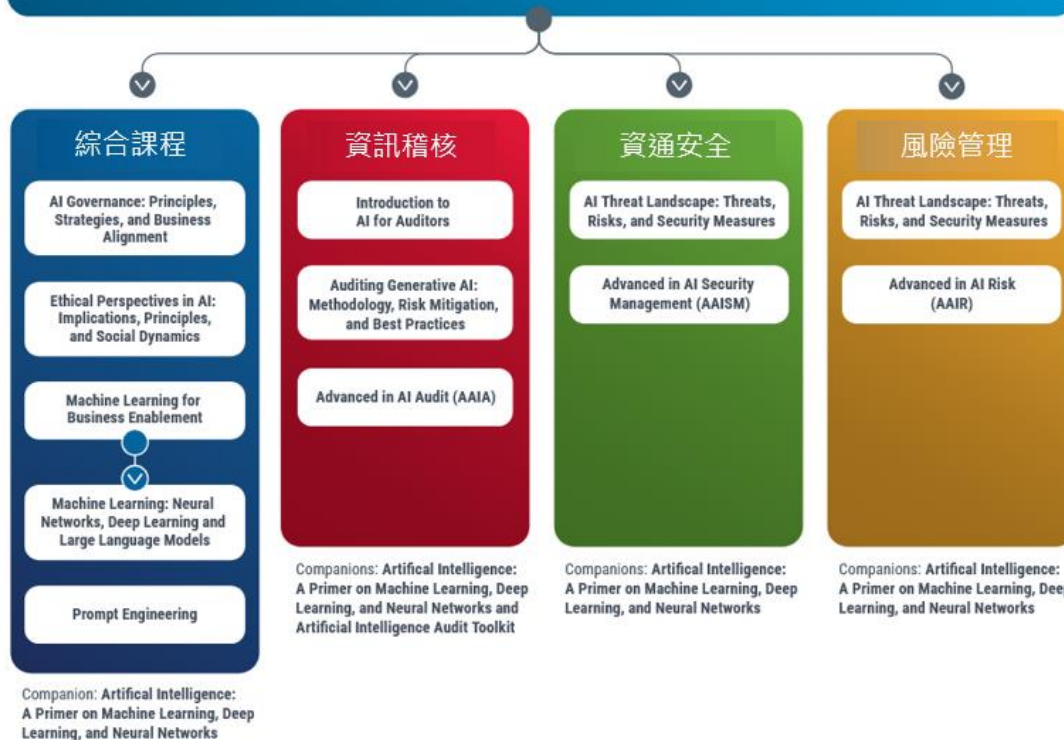
Emerging Tech
Fundamentals Certificates

ISACA 專業發展藍圖



基礎課程

AI Fundamentals



InfoSec
Taiwan
國際資安組織大會

2026

重新定義信任邊界
THE NEW TRUST BOUNDARY



ISACA®



ISACA Is Now the CAICO for CMMC

ISACA 在 CMMC 生態系統中的新角色為何？



ISACA 已獲授權成為 CMMC 評估師與講師認證機構 (CMMC Assessor and Instructor Certification Organization, CAICO)，目前負責管理 資通安全成熟度模型驗證 (Cybersecurity Maturity Model Certification, CMMC) 生態系統內個人的培訓、考試及專業認證作業。

ISACA 將代表美國戰爭部 (Department of War, DoW) 的 CMMC 計畫管理以下認證資格：

- CMMC 認證專家 (CMMC Certified Professional, CCP)
- CMMC 認證評鑑員 (CMMC Certified Assessor, CCA)
- CMMC 認證主導評鑑員 (Lead CCA)
- CMMC 認證講師 (CMMC Certified Instructor, CCI)

什麼是 CMMC？



資通安全成熟度模型驗證 (Cybersecurity Maturity Model Certification, CMMC) 是一套評估架構及評鑑員認證制度，作為提升對於符合各項標準要求之資安措施的信任程度。這些標準由美國國家標準暨技術研究院 (National Institute of Standards and Technology, NIST) 所發布。CMMC 的目的，是驗證美國戰爭部承包商所使用、用於處理、傳輸或儲存敏感資料的資訊系統，是否符合強制性資訊安全要求。其核心目標在於確保由合作夥伴或供應商儲存與處理的：受控未分類資訊 (Controlled Unclassified Information, CUI) 聯邦合約資訊 (Federal Contract Information, FCI) 均受到適當保護。任何希望與美國戰爭部進行業務往來的組織，都必須取得 CMMC 所要求的特定等級認證，以證明其具備符合要求的資安實務能力。CMMC 的評估與認證制度，用於確認國防承包商是否具備充分保護政府資訊的能力。

CMMC 正式實施始於 2025 年 11 月 10 日，並將在後續三年間逐步提高要求，預計於 2028 年 11 月完成全面導入。此計畫將影響超過 20 萬個組織。

新增認證資格



CMMC Certified
Professional (CCP)

CMMC
認證專家



CMMC Certified
Assessor (CCA)

CMMC
認證評鑑員



Lead CCA

CMMC
認證主導評鑑員



CMMC Certified
Instructor (CCI)

CMMC
認證講師

www.isaca.org/cmmc

會員權益



開創新的職涯發展路徑

取得 CMMC 認證專家 (CCP)、認證評鑑員 (CCA) 或主導評鑑員 (Lead CCA) 資格，成為執行或支援 CMMC 合規評估所需的專業人才。



全球認可

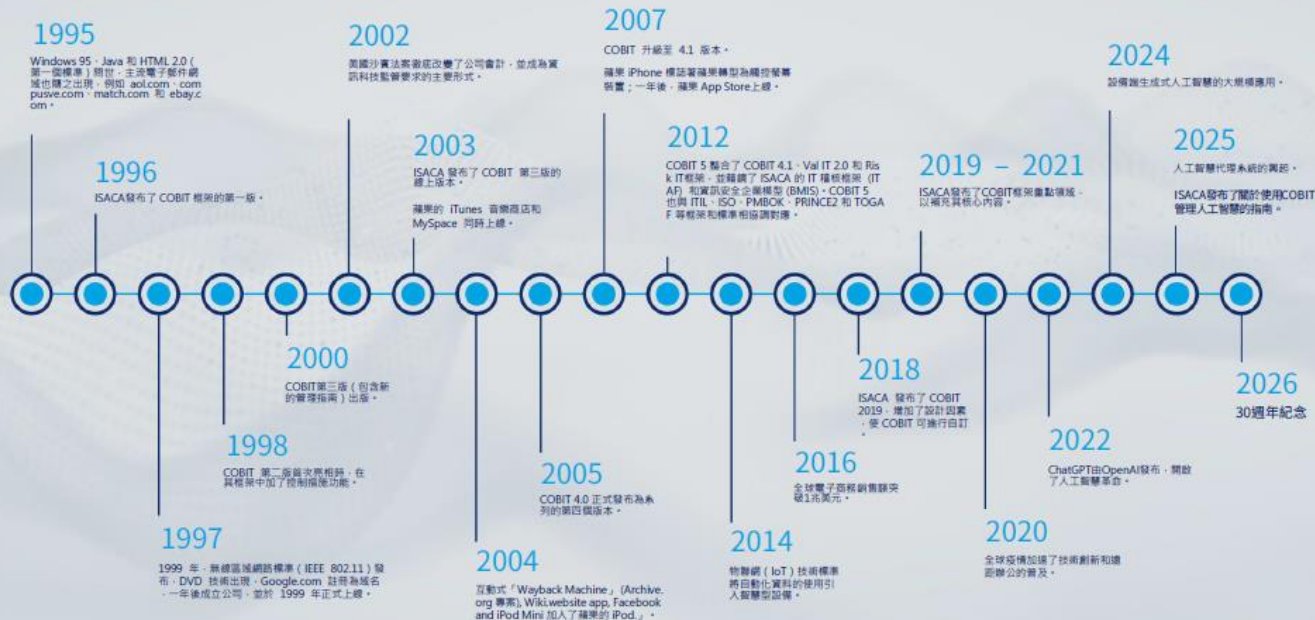
ISACA 社群正引領資安專業發展方向，並構成因應當今資安與數位信任挑戰所需的關鍵人才力量。



延續發展與專業成長

現有 ISACA 認證，包括 CISA 與 CISM，皆可能成為申請 CCA 的先決資格之一；而這些新認證將進一步擴展您的專業能力版圖。加入此計畫不會影響您目前持有的 ISACA 認證或會員資格。

慶祝 COBIT 成立三十週年



運用 COBIT 實現 AI 系統的有效治理



風險類別	風險情境範例
倫理使用風險	偏見和歧視 - 人工智慧系統無意中放大了訓練資料中的偏見，導致對特定群體的不公平對待（例如，有偏見的招募建議）。 意想不到的後果 - 人工智慧系統會以開發者未曾預料的方式學習和行動，這可能會導致有害的後果。
政策與治理風險	缺乏問責制 - 人工智慧決策的歸屬不明確，導致發生錯誤或造成損害時無法追究責任。 不符合全球標準 - 人工智慧系統未能滿足跨境監管要求（例如 GDPR、歐盟人工智慧法案），導致罰款或營運延誤。
技術和基礎設施風險	演算法故障 - 由於設計、資料或部署方面的錯誤，人工智慧模型產生錯誤的預測或分類。 對抗性攻擊 - 駭客操縱人工智慧輸入（例如圖像或文字）來利用其弱點並產生預期結果。
營運和組織風險	過度依賴人工智慧 —— 員工過度依賴人工智慧的輸出結果，缺乏關鍵監督，導致對有缺陷的系統盲目信任。 未能與策略目標保持一致 —— 人工智慧投資專注於熱門技術，而不是解決實際的業務問題。
新興和策略風險	生成式人工智慧的濫用 - 生成式人工智慧會產生有害內容（例如，露骨的圖像或極端主義宣傳），進而影響品牌聲譽。 針對人工智慧的法律先例 —— 新的訴訟或法律裁決限制了組織部署或使用人工智慧系統的方式。

2026 年隱私發展現況



- ◆ 設有隱私長（ Chief Privacy Officer, CPO ）的企業，較容易獲得董事會充分支持；而隸屬於 CPO 的隱私團隊，也對維護資料隱私的能力更具信心。
- ◆ AI 無法彌補資源不足與預算受限所帶來的挑戰。由於 AI 在隱私相關工作的應用程度，與企業是否具備成熟的隱私治理計畫呈現高度正相關，可見隱私專業人員已普遍認知，AI 解決方案本身亦伴隨風險，並非解決隱私治理未獲適當重視的萬能解方。



InfoSec
Taiwan
國際資安盛會

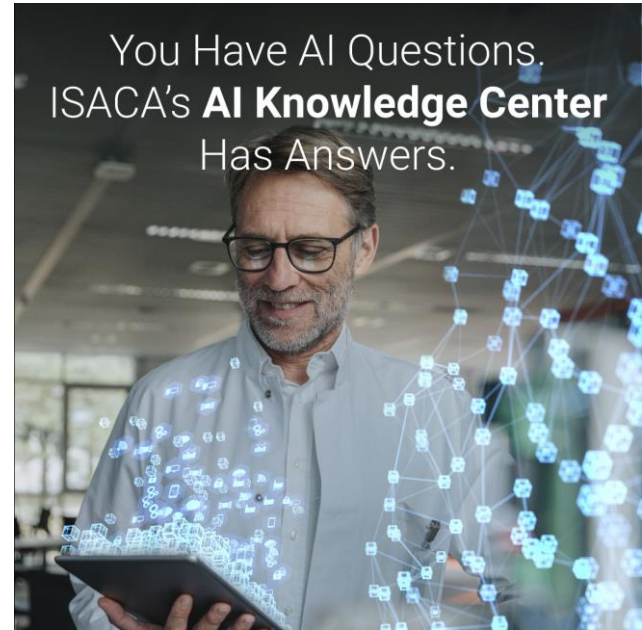
2026

重新定義信任邊界
THE NEW TRUST BOUNDARY

**We Are Digital
Trust Leaders**

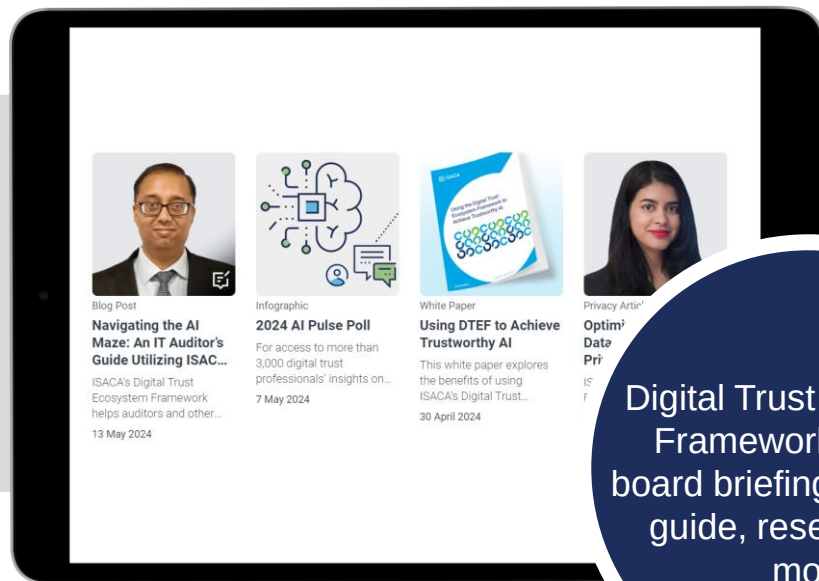


Newly-launched AI resources and training



www.isaca.org/ai

Digital Trust Ecosystem Framework and Resources



Blog Post

Navigating the AI Maze: An IT Auditor's Guide Utilizing ISAC...

ISACA's Digital Trust Ecosystem Framework helps auditors and other...

13 May 2024



Infographic

2024 AI Pulse Poll

For access to more than 3,000 digital trust professionals' insights on...

7 May 2024



White Paper

Using DTEF to Achieve Trustworthy AI

This white paper explores the benefits of using ISACA's Digital Trust...

30 April 2024



Privacy Article

Optimizing Data Privacy

ISACA's Digital Trust Ecosystem Framework helps auditors and other...

13 May 2024

Digital Trust Ecosystem Framework, course, board briefing, interactive guide, research, and more



The Ultimate
DIGITAL TRUST
Product Suite Has Arrived

www.isaca.org/digital-trust

2025 IMPACT

8,100+

HOURS SPENT VOLUNTEERING
BY ISACA MEMBERS AND GUESTS

2,462

VOLUNTEER ACTIVITIES COMPLETED

51

COUNTRIES REPRESENTED

SAVE THE DATE

**3 October
2026**



Content Types

1. Print/Web

1. Blog posts
2. Web articles
3. *ISACA Journal* articles
4. Case studies
5. White papers
6. Frameworks and standards
7. Books/publications
8. Miscellaneous: ISACA glossary, Engage online community

2. Tools

1. Question, Answer and Explanation (QAE) database
2. Audit programs
3. Other items (career tools, toolkits, templates)

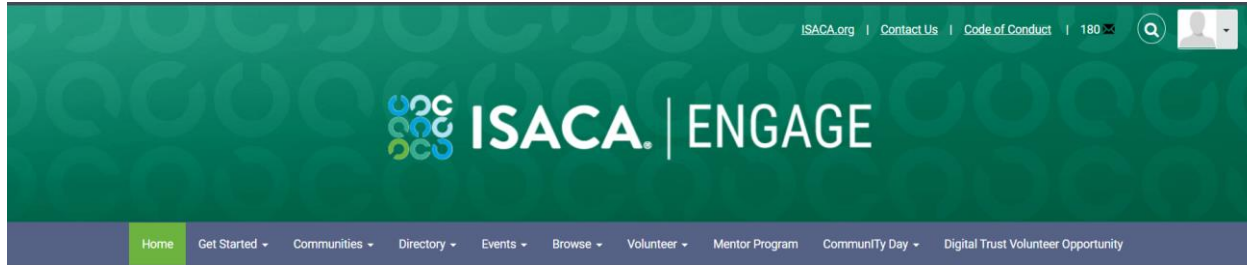
3. Podcasts

4. ISACA Video Content



Engage With Your Peers

<https://engage.isaca.org/home>



- Exchange ideas in the online forums
- Reach out to speakers, authors and experts
- Volunteer! Share your time and expertise with ISACA

ISACA職業道德規範(Code of Professional Ethics)

國際電腦稽核協會 (ISACA) 制定了職業道德規範，以指導協會會員和證書持有人的職業行為與個人行為。

協會會員和ISACA證照持有人應：

1. 支持實施並鼓勵遵守適當的標準和程序，以有效治理和管理企業資訊系統及科技，包括稽核、控制、安全和風險管理。
2. 依照專業標準，客觀、盡職、專業上的注意執行職務。
3. 以合法誠信的方式，維護利害關係人之權益，並保持高標準的行為和品行，且不損害其專業或協會的形象。
4. 維護活動過程中所取得資訊的機密與隱私，除司法機關要求予以揭露的情況外。不應將此類資訊用於圖利個人，或發布予不適當的團體。
5. 維護其專業領域內的能力，並同意在合理範圍內，從事預期能以必要的技術、知識所完成的活動。
6. 向適當團體告知所執行工作的結果，並揭露他們需要知道的所有重要事實；如不揭露時，可能導致報告結果失真。
7. 提升利害關係人對治理和管理企業資訊系統和科技的瞭解，包括稽核、控制、安全和風險管理，以支持其專業教育訓練。

未遵守職業道德規範，將導致對協會會員或證照持有人的行為進行調查，最終可能遭受到紀律懲戒處分。



InfoSec
Taiwan

國際資安組織大會

2026

THE NEW
TRUST BOUNDARY

重新定義信任邊界

Thank you for your support and attention

感謝各位的支持與關注