



InfoSec
Taiwan
國際資安組織大會

2025
07.09-10

DATE : 2025 / 07 / 10

AI時代稽核人員必懂 的機器學習

PRESENTER : DEREK_LIN 林煒傑

自我介紹



現任

- 財金資訊股份有限公司 內部稽核
- 中華民國電腦稽核協會專業發展委員會 委員

曾任

- 上市櫃科技製造業、零售貿易業 內部稽核

專業認證



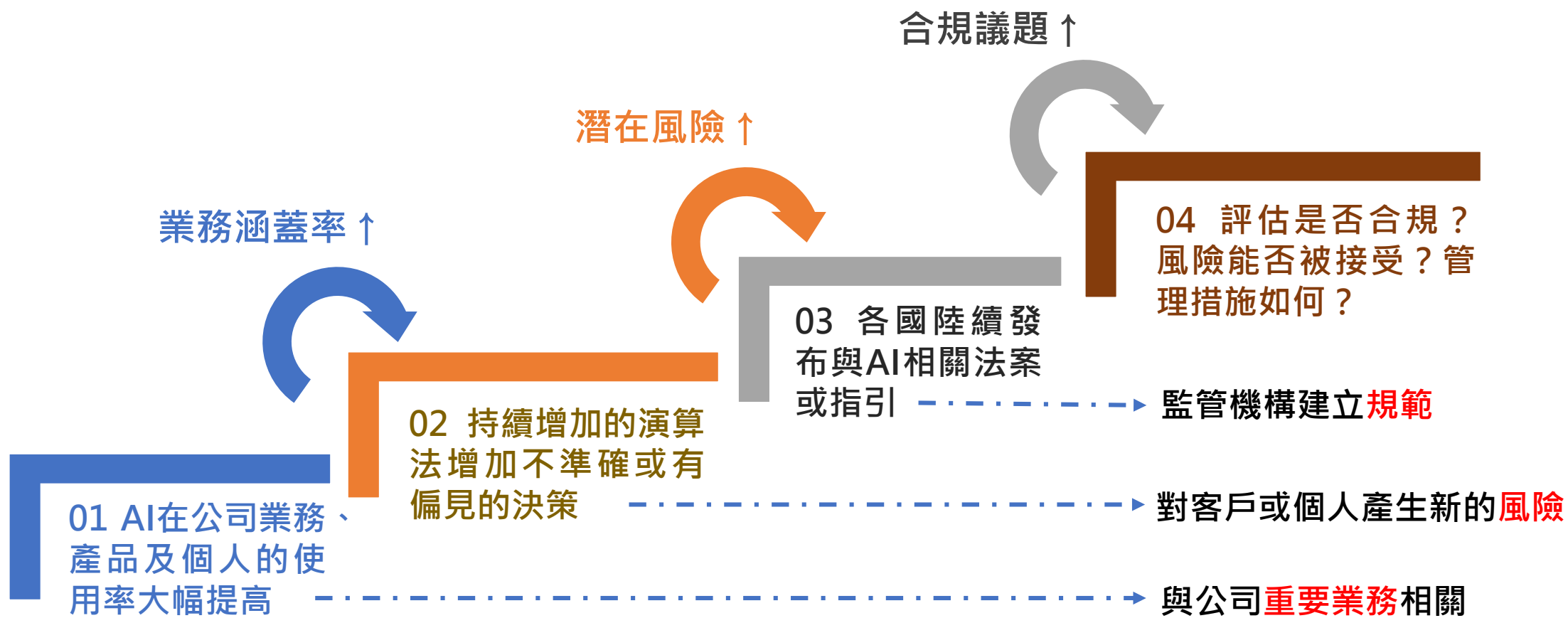
專長

內部稽核、電腦稽核、電腦輔助工具軟體應用、數據分析、作業流程優化、風險管理等

分享的主題

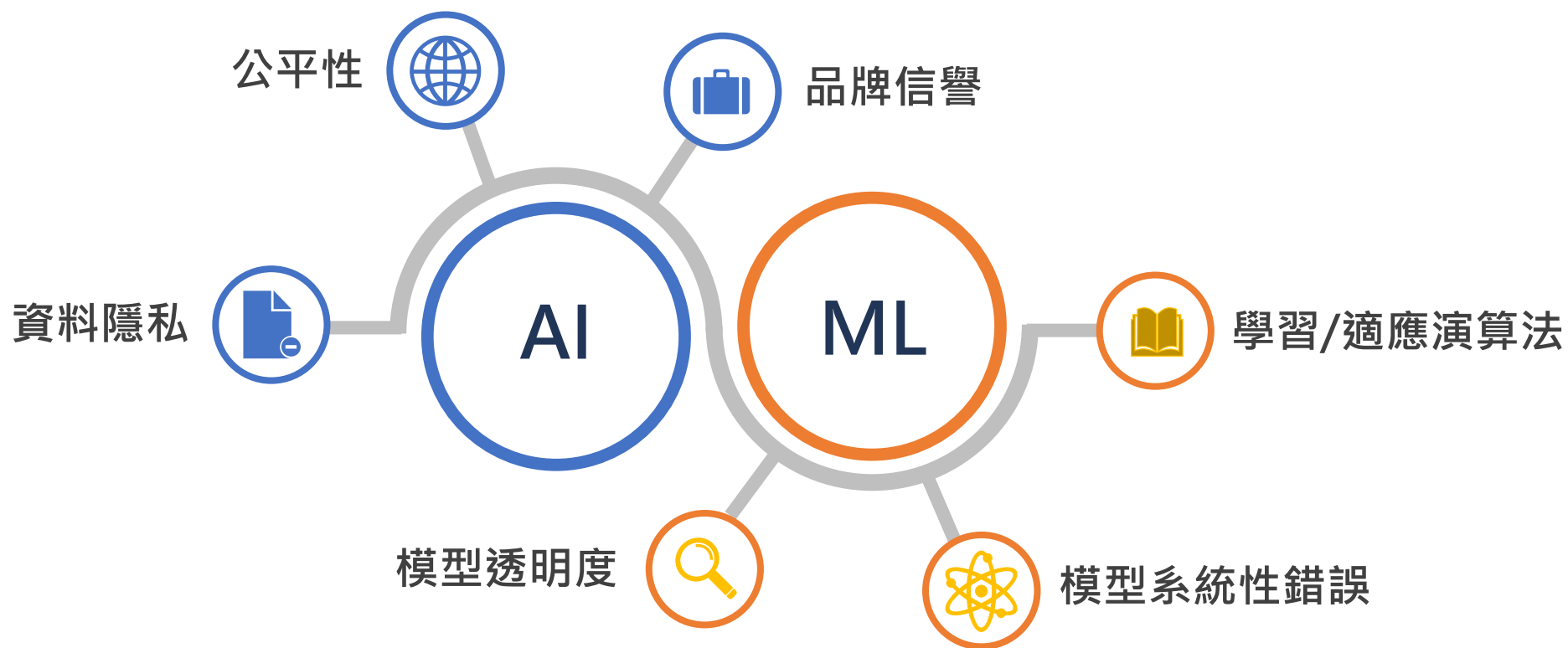
- 為何稽核 AI/ML 很重要？
- AI/ML 基礎概念
- 六大科技風險與稽核人員需思考面向
- ML合規議題
- 稽核人員在ML扮演什麼角色？

為何稽核 AI/ML 很重要？



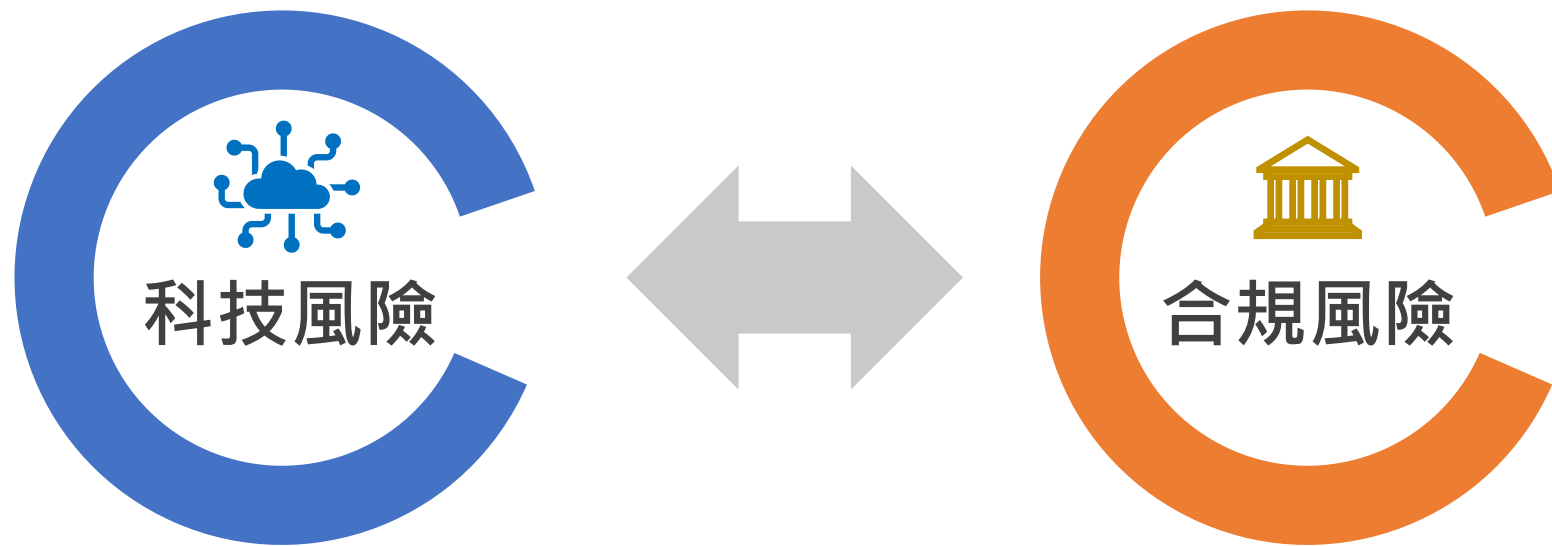
為何稽核 AI/ML 很重要？(續)

使用AI及ML的主要挑戰...

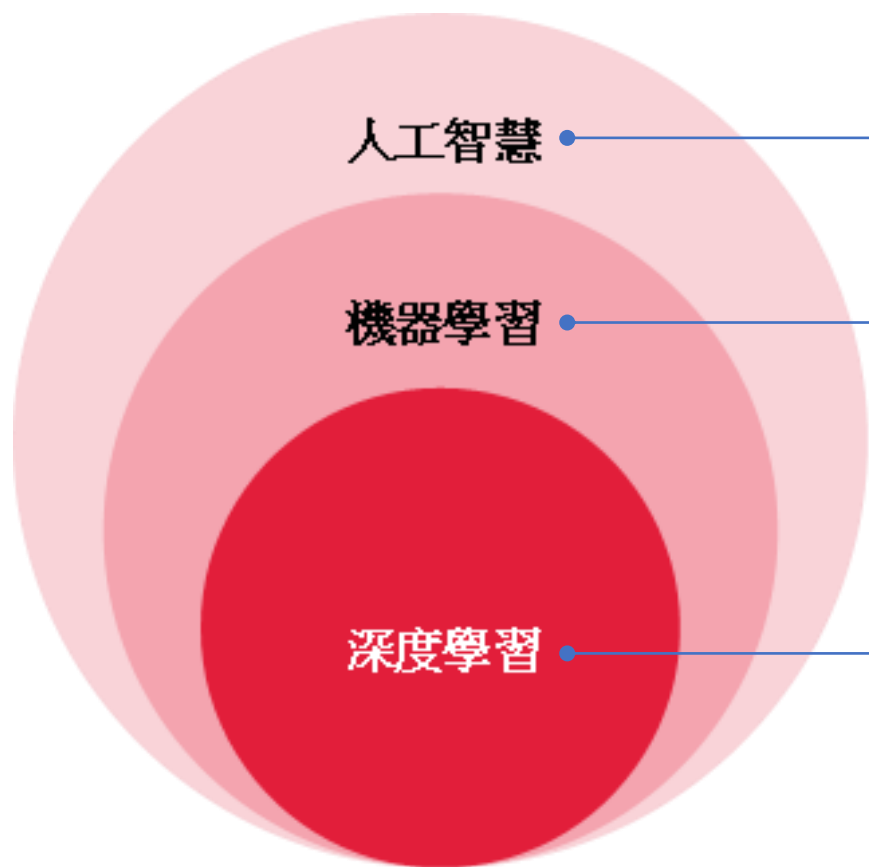


為何稽核 AI/ML 很重要？(續)

對稽核來說，可從哪裡開始...



AI/ML 基礎概念

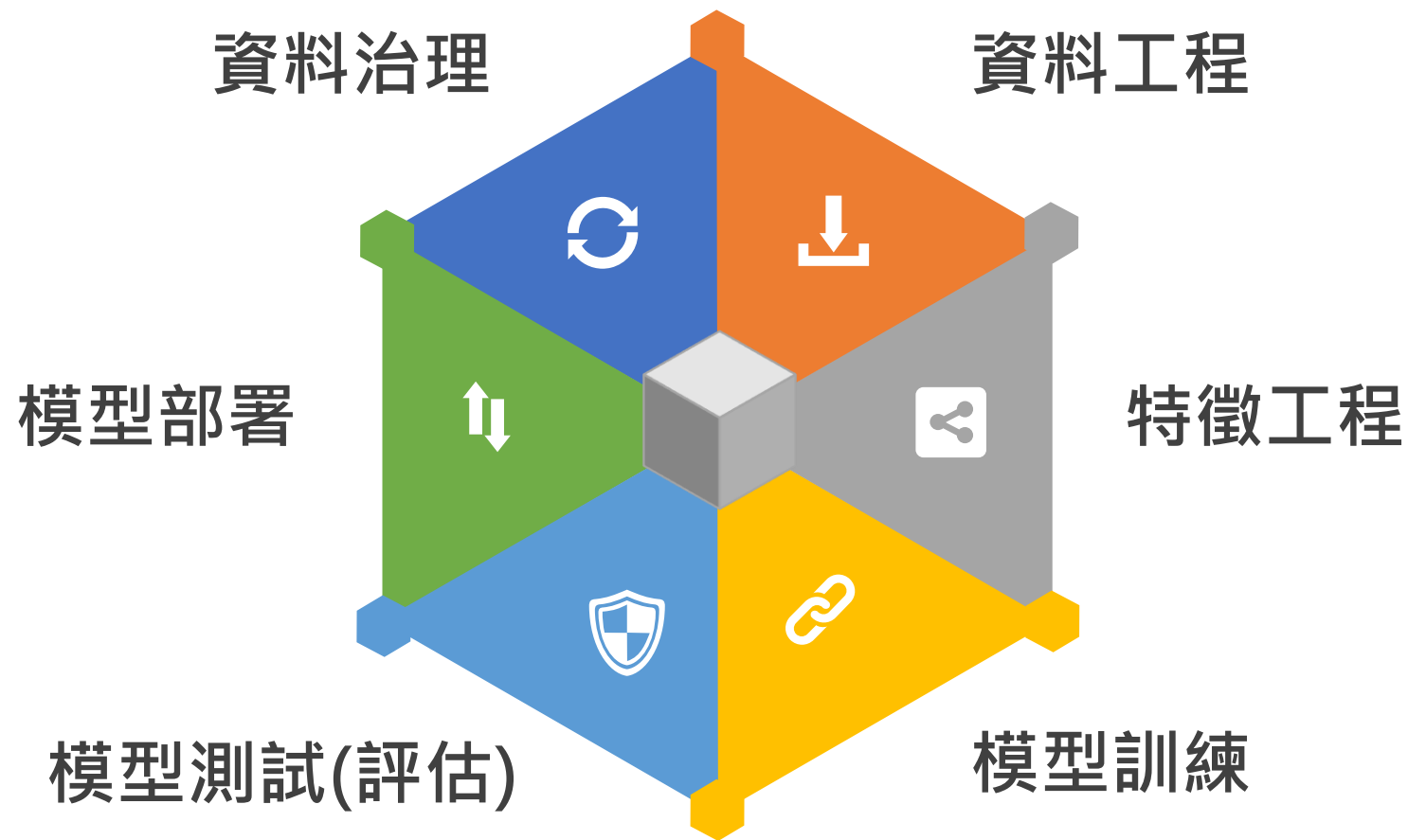


AI 由專門從資料中「學習」的演算法所組成。

利用統計模型「彙總」來自大量資料集型態，這些型態爾後可用於預測新資料。

基於人工神經網路的機器學習類型，其中透過使用多層處理從資料中提取更高層次的特徵。

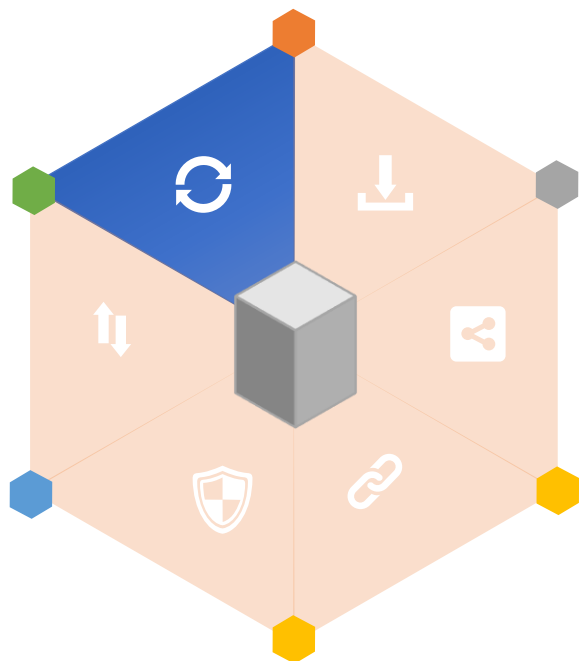
六大科技風險與稽核人員需思考面向



六大科技風險與稽核人員需思考面向(續)

資料治理

了解整體控制環境



當責 | 高層參與、職能分工、監督



資料品質 | 垃圾進、垃圾出？



資料安全 | 存取保護措施...



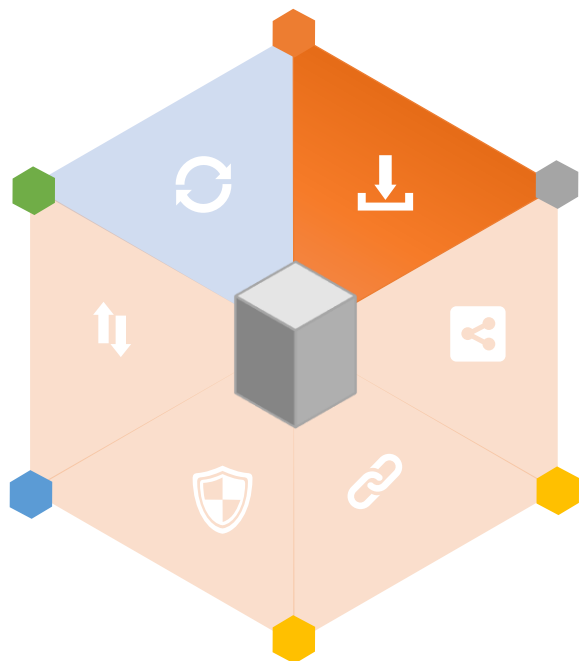
資料授權 | 開源資料授權限制

六大科技風險與稽核人員需思考面向(續)

資料工程



想想...如果平時查核，會怎麼做？



資料蒐集

→ 來源？準確/完整？格式？

資料探索

→ 找出有用的資料

資料清理

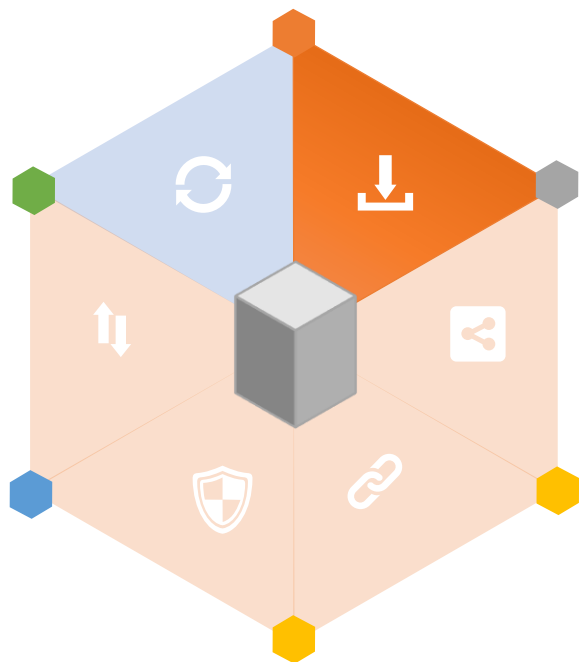
→ 整合、標準化、結構化

六大科技風險與稽核人員需思考面向(續)

資料工程



想想...如果平時查核，會怎麼做？



資料匿名

→ 監管要求？
個資、健康資訊？分析前匿名化？

資料模式、ETL

→ 資料存在哪？怎麼存取及分析？

資料公平性

→ 涉及歧視與偏見的資料？

六大科技風險與稽核人員需思考面向(續)

特徵工程

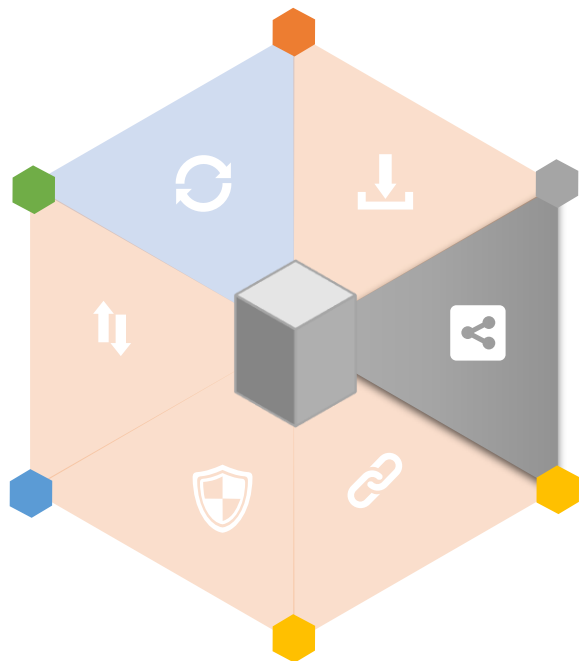


好的特徵，讓ML預測更準確

預測房價時...可能的特徵會有哪些？

- ① 平方公尺數
- ② 臥室/浴室數量
- ③ 房屋類型
- ④ 地區犯罪率
- ⑤ 學區評分...等

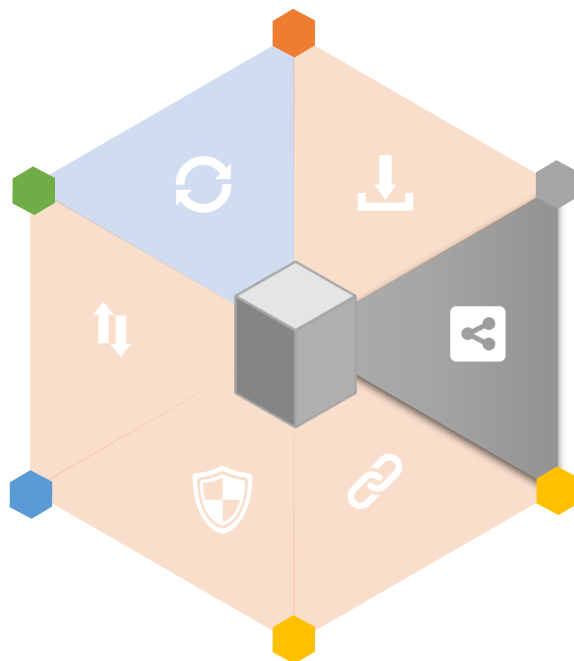
原始資料→提取特徵→創建模型→
預測房價



六大科技風險與稽核人員需思考面向(續)

特徵工程

稽核人員需思考面向...



項目	描述
資料插補	水管堵住，影響性能
異常值處理	辨認及移除異常值，避免系統性錯誤
特徵衍生或轉換	時間戳記→年月日時分秒 不同資料，轉換相似規模
公平與隱私	特徵是否有偏見、歧視？ 與外部資料關聯，是否有隱私疑慮？

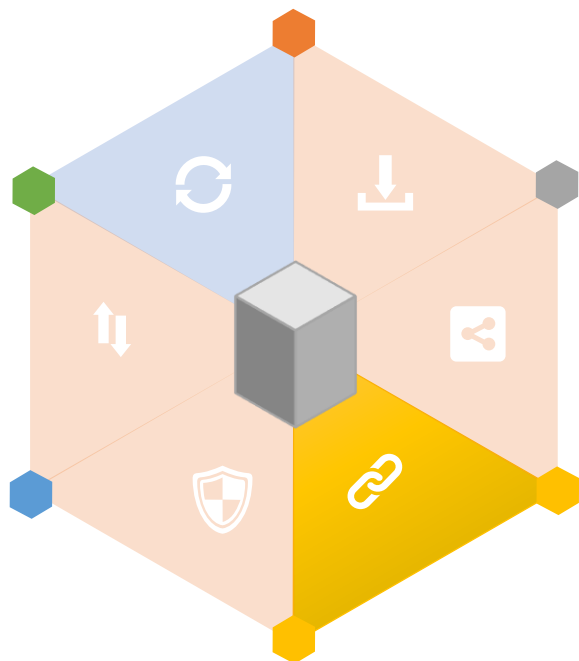


六大科技風險與稽核人員需思考面向(續)

模型訓練

模型訓練是建立 ML 模型的核心

如果你是一位神奇寶貝訓練家，剛捕捉到一隻神奇寶貝，你會希望怎麼好好訓練它？



訓練資料

- 資料來源？
- 統計數據？
- 訓練跟測驗的比例？
- 怎麼處理有偏差的情況？

模型方法論

- 訓練方法假設？
- 使用哪些技巧(演算法)？
- 訓練的環境(模型)？
- 訓練方法或環境的限制？

透明性

- 可解釋性與透明度
- 訓練環境與方法邏輯清楚嗎？還是難以解釋如何判斷？



六大科技風險與稽核人員需思考面向(續)

模型評估

衡量模型的性能→這個模型夠好嗎？

不是性能超強，而是接近資料與模型之間的平衡。

從下圖，讓我們來想像一下...一對情侶的日常情景...

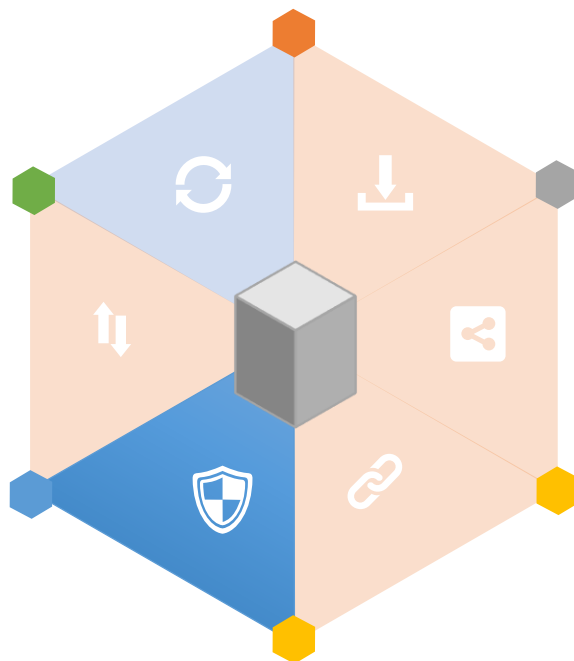
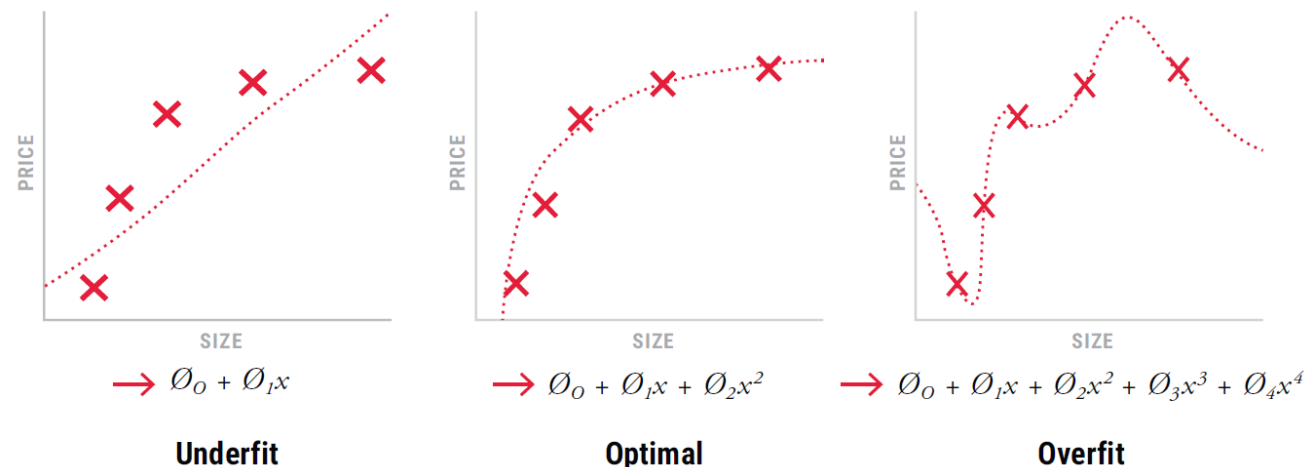


FIGURE 2: ML Models That Are Underfit, Optimal and Overfit

Linear regression model to predict housing prices

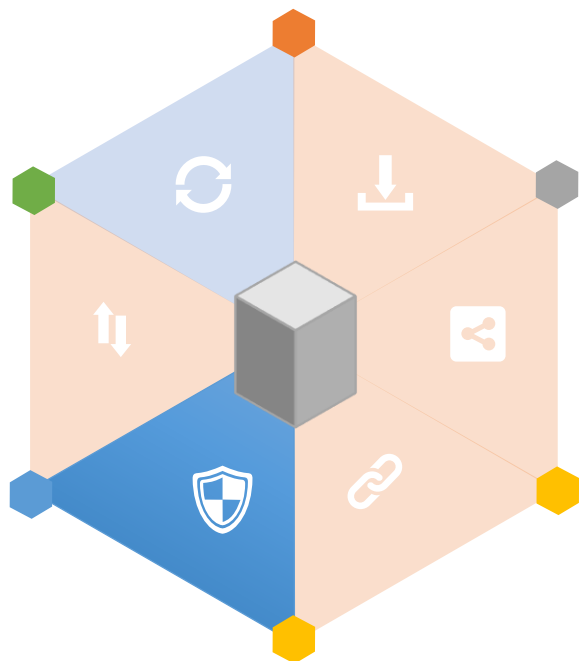


男生是模型，女生是資料

Source: Ng, A.; "Machine Learning," offered by Stanford University through Coursera, <https://www.coursera.org/learn/machine-learning>

六大科技風險與稽核人員需思考面向(續)

模型評估



評估ML模型的方法

K-fold Cross-Validation

- 資料分成K組，透過反覆訓練，會產生偏差較低的模型。
- 想像一下...男女朋友的例子...

Confusion Matrix and Its Derived Metrics

- 以表格呈現預測值與實際值的混和比對，確認準確率、靈敏度、特異度等資訊。
- ROC曲線及AUC分數
- 再想像一下...



六大科技風險與稽核人員需思考面向(續)

Confusion Matrix and Its Derived Metrics

FIGURE 3: Confusion Matrix

Confusion Matrix		Actual			
		Positive (P)	Negative (N)		
Predicted	Positive (PP)	True positive (TP)	False positive (FP)	Precision	TP/PP
	Negative (PN)	False negative (FN)	True negative (TN)	Recall	TP/P
		Sensitivity	Specificity	Accuracy (TP + TN) / (P + N)	
		TP/P	TN/N		

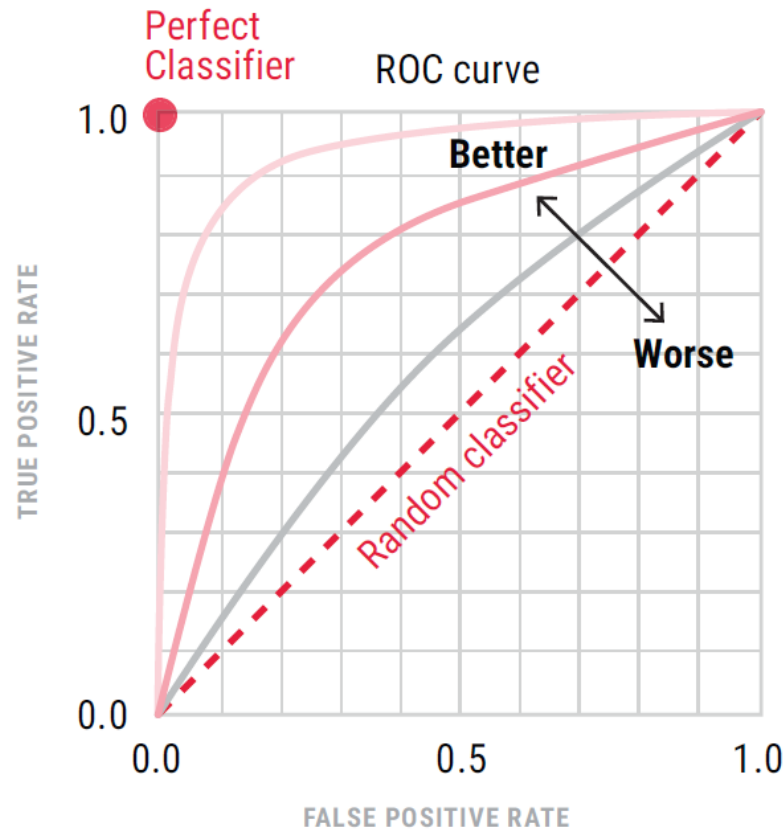
- 靈敏度or真陽率：TP/P
 - 準確度：(TP+TN)/(P+N) ...
- 用圖形來解釋會變什麼樣子？



六大科技風險與稽核人員需思考面向(續)

Confusion Matrix and Its Derived Metrics - ROC Curve and AUC Score

FIGURE 4: ROC Curve



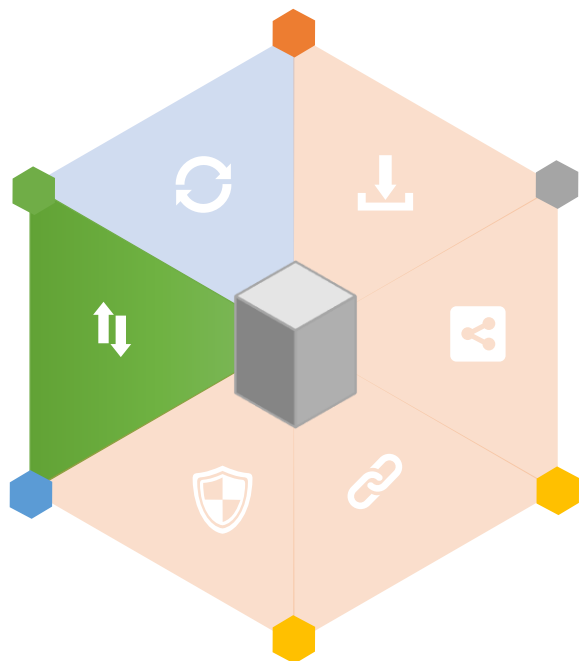
真陽性率(TPR)與偽陽性率(FPR)交叉繪製的ROC曲線

越靠近完美分類點(Perfect Classifier)，AUC分數越接近1，代表ML模型性能越好。



六大科技風險與稽核人員需思考面向(續)

模型部署及預測

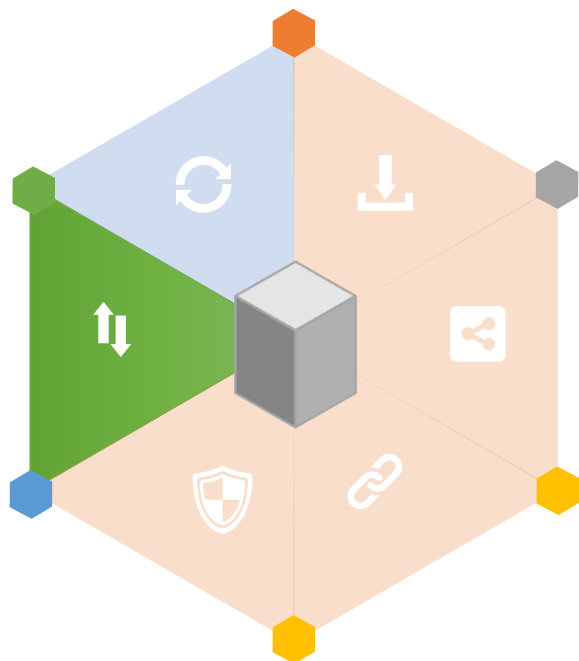


經過重重關卡，終於要上線(出門)了...
稽核人員要做什麼？

1. 持續確認模型參數與輸入資料依使用案例定期更新。
2. 檢查ML模型的營運環境是否實施持續性監控來應對新資料情境。

六大科技風險與稽核人員需思考面向(續)

模型部署及預測



該階段的服務水平協議(SLAs)通常會有哪些？

- ① 硬體(有形的)
 - CPU、GPU、設備種類、硬體規格等
 - 專車接送、住5星級酒店、燭光晚餐等
- ② 軟體(無形的)
 - 作業系統、軟體庫版本等
 - 懂察言觀色、音樂氣氛、情緒價值給滿等
- ③ 等待時間與吞吐量
 - 每次預測耗時多久？需處理多少預測量？
 - 臉色不對勁時，花多少時間正確預測並處理情緒與反應？
 - 可以處理多少需求？

ML合規議題

合規風險...稽核需要知道什麼？



- 資料來源、資料轉變過程、模擬結果等
- 確認不同資料及處理目的均合法
- 資料最小化、安全機制
- 消費者知情權

- 模型週期有哪些面向？
- 試著從內部控制有效性的角度切入...

ML合規議題(續)

參考The Supervision and Regulation Letter (SR) 11-7

模型風險管理

- 錯誤模型...
- 不正確使用

模型開發、實施及使用

- 確保開發符合原先設計目標
- 確保運作符合原先開發目標

模型驗證

- 確保性能符合預期及符合業務用途
- 假設、資料來源、計算方法等...

模型文件管理

- 確保業務連續性
- 開發、驗證、管理等...

風
開
驗
文



稽核人員在ML扮演什麼角色？

參考國際內部稽核協會(IIA)的三道模型

第一道

規劃、設計、開發、部署、運行模型，包含自動化與軟體開發等

資料科學家、資料工程師、模型開發人員等

第二道

評估資料、模型、自動化與軟體風險，監督第一道

風控、監管人員、QA等

第三道

確保符合企業策略、合法合規、道德與社會責任，監督第一、二道。

稽核人員、倫理專家等



結語

稽核人員的宿命不是被討厭，而是持續學習。

只要目標在，路就不會消失。



CYBER
GEOPOLITIC :
ONE INTERNET
NO MORE



InfoSec
Taiwan

國際資安組織大會

2025

07.09-10

CYBER GEOPOLITIC : ONE INTERNET NO MORE

指導單位 |  數位發展部數位產業署
Administration for Digital Industries, MODA

主辦單位 |  TWDDC 台灣資安大聯盟
Taiwan Digital Defense Consortium

 TWESA
台灣數位安全聯盟
Taiwan Cyber Security Alliance

共同主辦 |

 CSA
cloud security alliance
Taiwan Chapter

 CSCIS
CENTRE FOR
STRATEGIC CYBERSPACE +
INTERNATIONAL STUDIES

 fido
ALLIANCE
simpler
stronger
authentication

 ISACA
Taiwan Chapter

 ISC2
CHAPTER

TAIPEI

 OWASP Taiwan Chapter
The Open Source Application Security Project

 PM
Project
Management
Institute
Taipei, Taiwan

 The HoneyNet Project
Taiwan Chapter

 WHPC
WOMEN IN HPC

Thanks!

Do you have any questions?

林煒傑 Derek Lin

lwc6320192@gmail.com