

## 打造穩健的 AI 落地應用方案

# 透過 ISO 42001 規範 進行 AI 與 Data 治理

人工智慧管理系統 (AIMS) 國際標準 ISO 42001 相關的 AI 治理和 Data 治理議題可說是相輔相成，想要深化 AI 和 Data 在 ISO 42001 的關聯性，便須突顯 ISO 42001 在 AI 治理與 Data 治理的整體生命週期環節中扮演的樞紐角色。

文／梁日誠

要讓 AI 在組織內可持續且可被信任地 (Responsibly) 運作，僅有模型或演算法管控仍屬不足，需要一個涵蓋 AI 管理系統 (對應 ISO 42001 國際標準) 的 AI 治理 (對應 ISO 38507 國際標準) 框架來涵蓋政策、角色職責、風險、稽核與持續改善。

### AI 治理與 Data 治理 相輔相成不可偏廢

而這正是 ISO 42001 的定位：協助組織建立、實施、維護及持續改進的 AI 管理系統 (AIMS)，把 AI Systems 的相關利害團體所關注的特定議題 (如：可解釋度不足、持續學習導致行為改變、資料品質等) 整合進既有治理流程。ISO 42001 亦須將 AI 管理需求融入日常業務流程。

同時，涉及資料 (Data) 的 AI Systems (如：Machine Learning) 離不開資料品質，品質不佳的情況，如：資料偏差、代表性不足、即時性缺口等，都會直接影響模型的公平、可靠與穩定。資料品質的部分可參考 ISO 5259 系列標準補強實務面的作法，ISO 5259 系列標準說明如下：

- ISO 5259-1：名詞、概念與資料生命週期 (DLC) 模型。
- ISO 5259-2：資料品質特徵與量測 (如：Accuracy、Completeness、Representativeness、Timeliness 等)。
- ISO 5259-3：資料品質管理的要求與指引 (從資

料動機、規格、規劃、取得、前處理、增強、供應到退役)。

- ISO 5259-4：資料品質流程框架 (DQPF)，把各流程細化到可操作的步驟 (如：標註、品質評鑑與改善)。

- ISO 5259-5：資料品質治理框架，為 AI/資料品質決策、角色職責與風險管理提供高階指引。

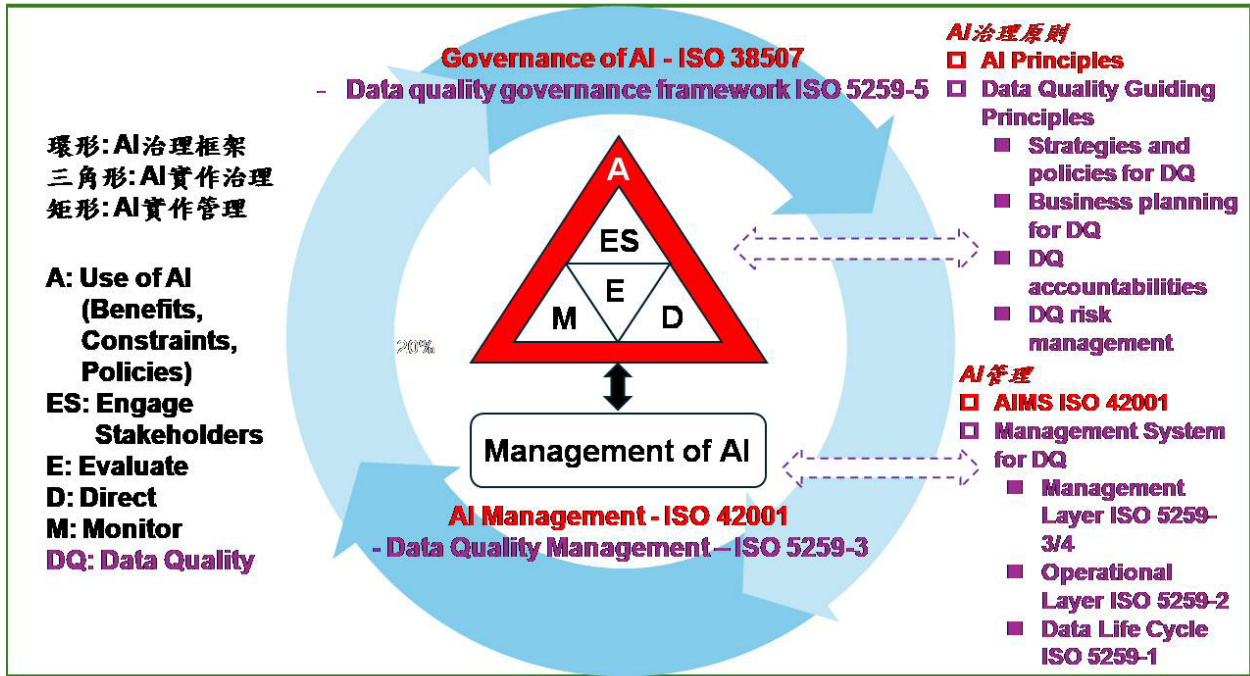
- ISO 5259-6：資料品質視覺化框架，旨在透過圖形化方法協助利害關係人評鑑資料品質測量結果。(PS：此項仍在制定中)

整體而言，ISO 42001 提供「應或須做什麼」的管理框架 (如：控制措施與對應的實作指引)，而 ISO 5259 系列則提供「怎麼做」的具體方法 (如：量測、流程與治理)，兩者缺一不可。

### AI 治理與資料治理標準間的對應關係

ISO 38507 提供了 Governance of AI 的 AI 治理框架，也可充分整合 Data 治理於其中，配合 AI 管理與 Data 管理 (如：管理層面、運作層面、DLC) 的進一步整合，提供了 AI + Data 治理的國際標準應用參考，如<圖A>。

AI 管理中用於風險處理的 ISO 42001 國際標準的資料相關的控制措施 (於 Annex A) 及實作指引 (於 Annex B) 與 ISO 5259 系列標準間，具備相互對應的關係，可參考<表A>。



圖A: AI 與 Data 治理的國際標準應用。

## AI 與 Data 生命週期的整合

AI 系統生命週期與資料生命週期 (DLC) 是治理與管理的實踐架構，各自的階段說明如下：

### AI 系統生命週期 (對應 ISO 22989)

包含了 Inception、Design & Development、Verification & Validation、Deployment、Operation & Monitoring、Reevaluation、Retirement 等階段，這些階段在 ISO 42001 透過 A.6 - AI System Life Cycle 下的控制措施被要求並參考 B.6 對應的實作指引。

### 資料生命週期 (DLC, 對應 ISO 5259-1)

包含了 Data Requirements、Data Planning、Data Acquisition、Data Preparation、Data Provisioning、Data Decommissioning；ISO 5259-3 資料品質管理生命週期 (DQMLC) 則納入 Data Motivation and Conceptualization(A)、Data Specification(B)、

Data Planning(C)、Data Acquisition(D)、Data Preprocessing(E)、Data Augmentation(F)、Data Provisioning(G)、Data Decommissioning(H) 等階段。

以資料探勘與資料科學等領域的業界實務常用的 CRISP-DM 方法論為例，其業務流程步驟可與 AI 系統生命週期與 DLC/DQMLC 相對應，案例說明如 <圖B>，展現了業界實務可充分採用或轉換 AI 與資料相關國際標準的可能性。

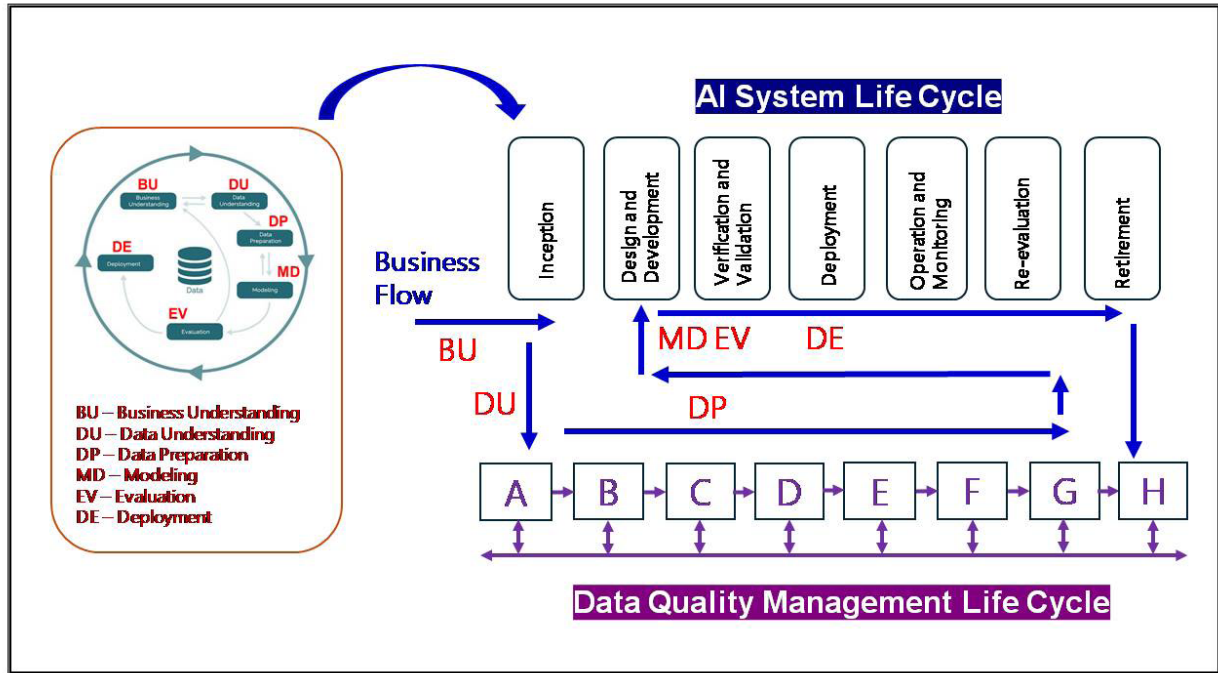
## 實踐 AI+Data 的治理與管理

為確保 AI 與資料治理能順利落地，可參考以下的具體的行動清單：

- 與 AI 利害相關團體互動 (Engagement) 時，納入 Data 考量。
- 定義 AI 政策與目標，並將資料品質原則納入其中。
- 建立角色與權責，明確資料所有者、品質負責人

ISO 42001 控制措施 (Annex A) 與實作指 引 (Annex B)	控制措施重點 (Annex A: 應、Annex B: 宜)	對應 ISO 5259 系列標準	對應說明案例
A.7.2、B.7.2 Data for development and enhancement of AI system	為 AI 系統的開發與增強，定義、 文件化並實施資料管理流程。	ISO 5259-3 ISO 5259-4	ISO 42001 要求建立資料管 理流程，而 ISO 5259-3 提 供了組織層級的要求與指 引，ISO 5259-4 則提供了 可執行的詳細流程步驟。
A.7.3、B.7.3 Acquisition of data	確定並文件化 AI 系統所用資料 的取得與選擇細節。	ISO 5259-1 ISO 5259-3	ISO 5259-1 定義了資料生 命週期中的「資料取得」 階段，而 ISO 5259-3 則提 供了該階段的管理要求， 如：資料來源的考量與處 理。
A.7.4、B.7.4 Quality of data for AI systems	定義並文件化資料品質要求，並 確保開發和運行中的 AI 系統所 用資料符合這些要求。	ISO 5259-2 ISO 5259-3 ISO 5259-4 ISO 5259-5	ISO 42001 提出了明確 的資料品質要求，而 ISO 5259-2 提供了衡量品質的 具體度量，ISO 5259-3 和 ISO 5259-4 則提供管理與 評鑑的流程，ISO 5259-5 則負責高階治理與監督。
A.7.5、B.7.5 Data provenance	定義並文件化 AI 系統中資料沿 革的記錄流程。	ISO 5259-1 ISO 5259-4 ISO 5259-6	ISO 5259-1 引入了資料沿 革 (Data provenance) 的概 念，ISO 5259-4 提供了版 本控制和變更管理的流程 來記錄沿革，而 ISO 5259- 6 則可以協助將這些資訊 視覺化，以提高透明度。
A.7.6、B.7.6 Data preparation	定義並文件化選擇資料準備方式 與方法的準則。	ISO 5259-3 ISO 5259-4	ISO 42001 要求定義資料 準備的標準，ISO 5259-3 和 ISO 5259-4 則詳細說明 了資料準備階段 (如：清 理、去重、標註、增強) 宜執行的具體活動和流程。

▀ <表A> ISO 42001資料相關的控制措施與 ISO 5259 系列標準對應。



圖B·業界實務與 AI/Data 生命週期互動案例。

與使用者之間的關係。

- 實施資料規格與量測，定義關鍵資料品質門檻，並使用 ISO 5259-2 進行量測。
- 設計可稽核的資料生命週期，將 ISO 42001 的資料相關控制措施（如：A.7.2~A.7.6）整合進 DLC /DQMLC 中。
- 識別、分析、評估及處理 AI Bias 時，納入資料議題。
- 建立監控機制，持續追蹤資料與模型漂移，並觸發再訓練或再評估。
- 建立分層的治理與彙報機制，確保董事會、管理階層與營運層的責任歸屬與透明度。

基本上，ISO 42001 協同 ISO 38507 提供 AI 治理與管理系統的整體架構，至於 ISO 5259 系列則是提供資料品質的生命週期與相關的量測與流程方法，可將三者串接起來，透過引用 ISO 22989 的 AI 系統生命週期，將業界實務與專案納入 AI 與資料品質生命週期的遞迴循環中，並務實地把可信任、負責任的 AI 具體地進行實踐。

而 ISO 5259-3 中的資料品質管理要求，也可

與 ISO 42001 合併進行第三方稽核或符合性評鑑，有效建立相關利害團體對組織 AIMS 的信心。



作者: 梁日誠 (Lead CCA<sup>®</sup> PII CISSPI CISSOI CPTTE CCSOI CDREI CCISOI ISMI ISAI AIMPI FIAAIS FHCA-EU AI ActI CAIEI CAIPCI CDEI CDAI DSFMI FHCA-GDPRI IDPPI ICEPI GRCAI GPM-bi IMPCI, ^ Pending), 現為加拿大 SCC/MC ISO/IEC JTC1/SC42、SC27、ISO/TC22/SC32、IEC/TC65 技術組成員, ISO 42001/ISO 27001/ISO 27701/ISO 22301/ISO 20000-1/IEC 62443-2-1 稽核師及講師, TCIC 環奧國際驗證公司全球營運總經理。