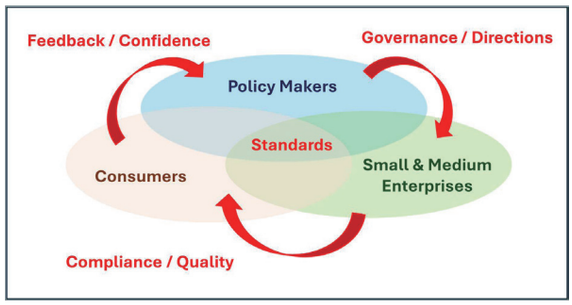
ISO 42001 助力 AI 轉型之路

歐美 AI 法規陸續底定 導 ISO 42001 將事半功倍

透過 AI 進行轉型，已經是當前企業重要課題，如何保障 AI 的投資，成為重要的考量因素，透過國際標準 ISO 42001 的導入將可降低應用上的風險，未來更可順利與國際要求的 AI 法規進行合規。

文／梁日誠

在全球 AI 治理的發展中，如何透過「標準」來支持「法規制定」與「合規展現」已成為各國共同凝聚的趨勢。ISO 述及國際標準的貢獻與優勢在於連結政策制定者（Policy Makers）、中小企業（SMEs）與消費者（Consumers），形成一個持續互動的循環，國際標準不僅是一種技術工具，更是一套可被法規化、可落實合規、可驗證的國際共通語言。如同 **<圖一>** 所揭示。



圖一，標準與市場治理互動關係。

以人工智慧管理系統國際標準 ISO 42001 為例，ISO 42001 提供了組織建立 AI 治理所需的如：管理系統、風險管理、控制措施等負責任作法，而這也正好呼應**歐盟 AI Act** 對高風險 AI 系統的合規要求。

同時，ISO 42001 也能與**美國 NIST AI RMF（AI 風險管理框架）**對應，成為企業將風險控制轉化為治理流程的實務依據。對台灣地區而言，行政院近期揭露的 **AI 基本法（草案）**，若能在制度中納入 ISO 42001 與 AI 相關風險管理（如 **ISO 23894**）及資料品質標準（如 **ISO 5259 系列**），不僅有助於加速 AI 治理的合規落地，也能引導國內產業以國際通用的標準來接軌全球 AI 市場。

因此，ISO 標準不僅幫助政策制定者「立法更快、更精準」，也讓中小企業「合規更省、更有效」，並進一步鞏固消費者的信任，在 AI 應用與日俱進的今天，這是一條「**由標準驅動法規，並以法規強化標準**」的治理之路。

歐盟人工智慧法規的合規展現優勢

ISO / IEC 42001 是全球第一個「**人工智慧管理系統（AI Management System — AIMS）**」國際標準，採用 ISO 管理系統標準，並針對 AI 系統的特性提出專屬要求，標準涵蓋如 AI 系統生命週期、風險管理、資料品質、控制措施、可信任性（Trustworthiness）與持續改進等核心領域，為組織導入 AI 治理建立國際一致的基礎。

歐洲標準制定組織 CEN / CENELEC 的JTC 21 Artificial Intelligence 工作組，正在與 ISO / IEC JTC1 / SC42 依維也納協議協力制定如「Artificial

ISO 42001章節	EU AI-QMS標準草案章節	EU AI Act 基礎要求
第4章 組織環境	**第 4 章 品質管理系統**	Article 17(1)，Article 11(1)
第5章 領導	**第 5 章 管理責任**	Article 17(1)
第7章之 資源	**第 6 章 資源管理**	Article 17(1)
第7章之 文件化資訊	**第 4.6 文件化資訊**	Article 11(1)
第8章 運行	**第 7 章 產品實現**	Article 17(1)
第9章 績效評估	**第 8 章 後市場監控**	Article 17(1), Article 72
第10章 改進	**第 8 章 後市場監控**	Article 17(1)

表一，ISO / IEC 42001、EU AI-QMS 標準草案與 EU AI Act 對應關係。

intelligence — Quality management system for EU AI Act regulatory purposes」（**EU AI-QMS 標準，Work Item Number：JT021039**，目前為制定階段），預計將成為**「調和標準」（Harmonized Standard）**。

其設計架構參考 ISO 42001，並增修如相關於 EU AI Act 第 17 條（Article 17）的特定 QMS 要求，成為 EU AI Act 合規的實施工具。在 EU AI-QMS 標準草案中，將 ISO 42001 章節、EU AI-QMS 標準草案章節與 EU AI Act 基礎要求進行對應，綜合整理關係例舉可見於 **<表一>**。

根據 EU AI Act 第 17 條，「高風險 AI 系統」提供者應建立並維持 QMS，當 EU AI-QMS 標準被歐盟官方引用並刊登於 「Official Journal of the EU（OJEU）」後，凡能展示其 QMS 符合該調和標準（Harmonized Standard，EU AI-QMS標準）的企業，其對應於 EU AI Act第 17 條之處，將具備 Presumption of Conformity（預設適足，Article 42）的地位。

換言之，組織若導入 ISO 42001，增修納入 EU AI Act 的特定法規要求於 AIMS，並通過調和標準的符合性評鑑或驗證，不僅能有效掌控合規成本，更能在歐盟市場中快速獲得其 QMS 的「預設適足」的地位，這將是台灣與國際 AI 產業進入歐盟的重要合規捷徑之一。

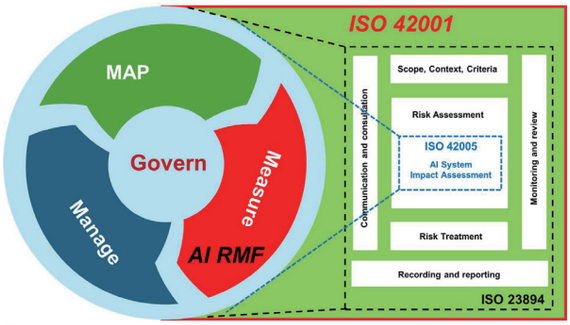
惟因 EU AI Act 的合規並非單一條款，若有其他條款如風險管理系統（Article 9）的 EU AI Act 合規展現需求，可同時遵循 AI Risk Management 標準（**prEN 18228，Work Item Number: JT021024**，制定中）。於 EU AI-QMS 標準草案中，ISO 42001 被爰引的方式包含：於必要參考文件（Normative References）中列舉、於註解（NOTE）中引用、於條文中直接適用（Apply）做為要求、於附錄中列舉對應關係等。

美國人工智慧市場的合規展現路徑

在美國的人工智慧領域，AI 治理主要依循著數個總統令（EO）來發展，NIST AI RMF（Risk Management Framework）是廣為美國聯邦相關市場接受的「可信任與負責任 AI」的治理框架，這包含治理（Govern）、對應（Map）、量測（Measure）、管理（Manage）等重要功能，並後續發展出 AI RMF：Generative Artificial Intelligence Profile（NIST AI 600-1）等規範。NIST 在近期的 Control Overlays for Securing AI Systems（COSAiS）專案中，AI RMF也與SP 800-53、NIST SP 800-218A、Draft NIST AI 800-1、NIST AI 100-2E2025 等，共同分析於 AI 系統的資安與隱私保護議題。

目前 NIST 正積極的推廣 AI RMF 與國際標準的介接，其中包含了與 ISO 42001 AI 管理系統、ISO 23894 AI 風險管理、ISO 42005 AI 系統衝擊評鑑等三個標準的「交互對應（Crosswalk）」文件，也使得運作 ISO 42001 的機構得以使用，NIST 所

出具的文件來針對美國人工智慧市場的利害相關團體進行合規展現，反之亦然，ISO 42001 相關國際標準與 AI RMF 間的關係示意圖如 **<圖二>**。



圖二，ISO 42001 相關國際標準與 AI RMF 間的關係示意圖。

ISO 42001 可做 AI 基本法的治理支點

行政院甫於八月下旬揭露的「人工智慧基本法（草案）（AI 法草案），提出 AI 發展應兼顧創新推動與人民權益保障，並在法條中建立永續發展、人權保障、資料治理、風險分類與高風險 AI 責任機制等治理基礎。AI法草案的核心精神，在於為台灣 AI 發展定錨，既要鼓勵產業創新，也要確保系統具備可信性與可歸責性。

對照 AI 法草案要求，ISO 42001 人工智慧管理系統標準正好提供了一個完整的治理骨架。

在基本原則上，AI 法草案強調永續性、透明性、公平性與可歸責性，ISO 42001則透過組織脈絡、領導責任、可信任性、資源配置與績效評估條款，要求組織將這些價值原則制度化並內嵌於 AI 生命週期。

在風險管理上，AI 法草案規定風險分類與高風險 AI 責任機制，ISO 42001 對應的規劃、AI 系統衝擊評鑑、風險評鑑與風險處理（包含控制措施），提供了實務機制，協助組織落實分級管理並強化可歸責性。

在資料治理上，AI 法草案要求個資保護與資料品質提升，ISO 42001 的資料治理與品質管理規範，可支撐「**隱私保護 by Design 與 by Default**」以及資料再利用的合規實作;在驗證與可歸責性上，AI 法草案要求 AI 系統須具備可驗證性與人為可控性，ISO 42001 的文件化、內外部稽核、績效監測與持續改進條款，能提供合規依據，確保 AI 的運作可追溯、可審查與可驗證。

ISO 42001 的可信任性中，在資安與隱私保護的領域上，和 ISMS／ISO 27001 與 PIMS／ISO 27701 的整合能力，也讓現有法規如資通安全管理法與／或個人資料保護法的適用單位與被要求單位（如受託者被要求通過第三方驗證時的國際／國家／團體標準的選擇），在面對涉及 AI 的資通系統與資通服務的議題上，有了較周全考量的選擇。

從產業角度觀之，ISO 42001不僅僅是「合規的工具」，更是企業在全球 AI 市場建立信任與競爭力的關鍵。當台灣的企業於數位轉型時導入 ISO 42001，不僅能回應「人工智慧基本法（草案）」的要求，同時也能與國際間如歐盟 AI Act 的 EU AI-QMS 調和標準（制定中）與美國 NIST AI RMF 對接，甚或於多個司法管轄區域，形成國際合規的一致語言。

這代表台灣產業若能適時甚或超前佈署採用 ISO 42001，未來在跨國市場中不但能降低合規成本，更能以「負責任、可信任 AI」的形象強化國際間的競爭優勢。

作者: 梁日誠 (Lead CCA^I CCP^I PI^I CISSPI CISSOI CPTEI CCSOI CDREI CCISOI ISMI ISAI FHCA-EU AI ActI CAIEI CAICSOI AAISMI CertifAIEd AI EthicsI CIAIPI GAILI 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。