ISO/IEC 42001:2023

Information Technology Artificial Intelligence Management System

Leading with confidence : How ISO standards are shaping the future of AI governance

Eng. Mohamad Fawaz

ISO 42001 Webinar | ASQ Ottawa 2026

SMG: Sustainable Management Group

smg-aw.com

For over 30 years: Independent · Expert · Built Around Your Needs

Who We Are

A leading provider of independent conformity assessment services offering:

· Registration / Certification
· 2nd Party & 1st Party Audits
· Franchise Audit Services
· Risk Management Solutions
· Training & Development Programs

Serving organizations from small businesses to government entities across multiple industries and jurisdictions.

Our Mission

Promote the use of standards and management system requirements through conformity assessment, training, specialized auditing, and risk management solutions.

Our Vision

To become a referenced entity for improving quality of life through the advancement and adoption of business excellence.

What We Stand For

Independence is the foundation of everything we do. Our assessors remain fully objective — no stake in your outcome other than delivering accurate and honest results.

We believe standards are essential to improving quality of life — for businesses, communities, and individuals alike.

We go beyond basic compliance. Our goal is to help organizations achieve certification through genuine performance and grow sustainably over time.

Introduction

Artificial Intelligence

Artificial intelligence (AI) is increasingly **applied across all sectors** utilizing information technology and is expected to be one of the main economic drivers. A consequence of this trend is that certain applications can give rise to societal challenges over the coming years

ISO 42001:2023 (Page vi)

The Importance of AI

Artificial Intelligence

John McCarthy, a pioneer of artificial intelligence who first coined the term in 1955, defined AI as "the science and engineering of making intelligent machines."

Computer systems that perform tasks normally requiring human intelligence — visual perception, speech recognition, decision-making, language translation.

Oxford Dictionary

Augmented Intelligence

AI as a tool that enhances human capabilities: humans remain in control while AI amplifies judgment, creativity and decision quality.

The purpose of AI and cognitive systems should be to augment, not replace, human intelligence. This technology can enhance and extend human capability and potential.(IBM)

The question is no longer whether to use AI, it is how to govern it responsibly.

Definitions from ISO/IEC 22989 (AI concepts & Terminology)

3.1.3 Artificial Intelligence (AI)

research and development of mechanisms and applications of AI systems (3.1.4)

3.1.4 AI system

Engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives

Much of the research has focused on programming machines to perform tasks intelligently, such as playing chess. However, today, the emphasis has shifted towards machines that can independently learn and adapt.

Applications equipped with AI aim to learn, understand, comprehend, problem solve and make decisions like humans would and attempt to do with human-like creativity.

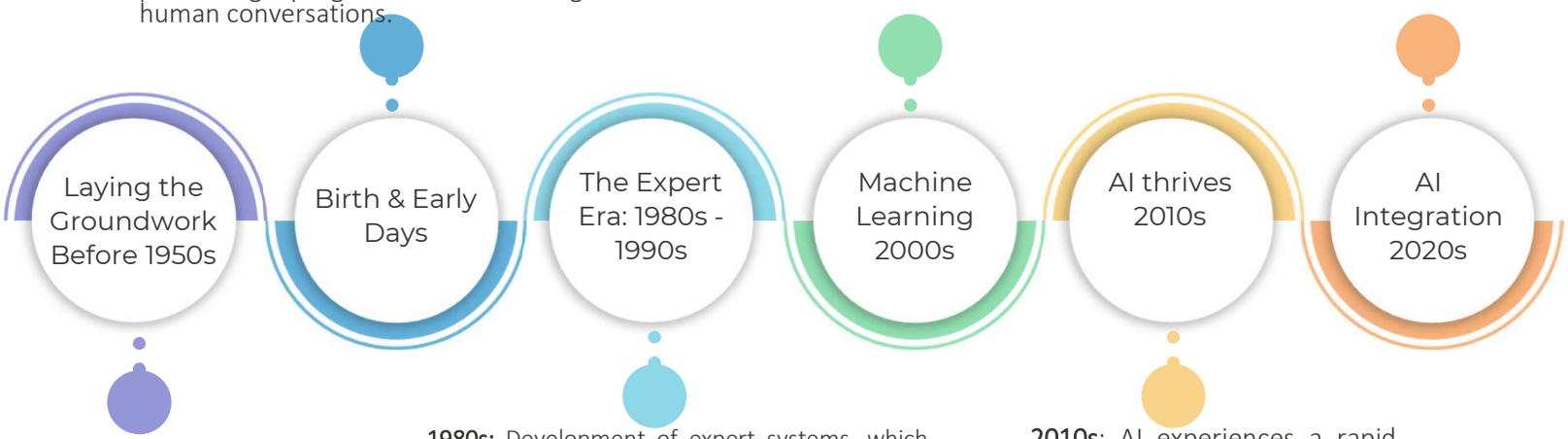
AI: A Journey Through Time

1956: The term "artificial intelligence" was officially coined at the Dartmouth Summer Research Project on AI (DSRPAI).

1960s: Early research saw the development of natural language processing programs l simulating human conversations.

2000s: Machine Learning Takes Center Stage: A period of significant advancements in Machine Learning algorithms, fueled by increased computing power and vast amounts of data. This era saw AI start to truly scale.

2020s: AI becomes deeply embedded across industries and daily life. We're seeing widespread integration into business processes, critical infrastructure, and even creative fields, leading to profound societal and economic shifts.



1940s: Alan Turing's "The Bombe" machine was developed to crack Germany's Enigma code during World War II, a foundational step in computational intelligence

1980s: Development of expert systems, which replicated human decision-making.
1981: Japan's ambitious Fifth Generation Computer Project invested over $400 million to advance AI.
1997: A landmark year! IBM's Deep Blue chess program made history by defeating world champion Garry Kasparov, showcasing its ability to process 200 million moves per second.

2010s: AI experiences a rapid acceleration, moving beyond niche applications into mainstream products and services. Think voice assistants, recommendation engines, and advanced image recognition.

From National Standards to ISO 42001

1920	ISA (International Federation of National Standardizing Associations) founded
1947	ISO officially begins operations — name from Greek ἴσος (isos) = 'equal'
1987	ISO 9001 — Quality Management System
2017	ISO/IEC JTC 1/SC 42 — Subcommittee on Artificial Intelligence established
2022	ISO/IEC 22989 (AI Concepts and Terminology) + ISO/IEC 38507 (Information Technology) + ISO/IEC 23053 (Framework for Artificial Intelligence Systems using Machine Learning) published
2023	ISO/IEC 23894 (Guidance on Risk) published: the family grows
Dec 2023	ISO/IEC 42001:2023: World's First AI Management System Standard

Uses Harmonized Structure (HLS) — compatible with ISO 9001, ISO 27001 and all major management system standards

The Legal & Regulatory Landscape for AI

EU AI ACT	EU AI Act (2024): world's first comprehensive AI law, risk-based classification: unacceptable / high / limited / minimal risk
PIPEDA	PIPEDA / Bill C-27 (CPPA) (2026): privacy obligations for AI systems processing personal data - Canada's federal privacy framework for AI systems
NIST	NIST AI RMF (USA)(2023): voluntary risk management framework for AI: widely adopted globally
China	Generative AI Services Regulation and Deep synthesis Regulations
UK	UK AI Framework: principles based: existing regulators (e.g., ICO, CMA) apply five core principles to their respective fields, focusing on safety, transparency, and accountability to foster flexibility and innovation while managing risks.
OECD	OECD AI principles: adopted by 47 countries: serve as the foundational, intergovernmental standard for AI governance.

Key Definitions — ISO/IEC 42001:2023 Clause 3

3.7	**Risk** Effect of uncertainty — can be positive OR negative
3.9	**Competence** Ability to apply knowledge and skills to achieve intended results
3.21	**Control** Measure that maintains and/or modifies risk
3.24	**AI System Impact Assessment** Formal documented process to identify, evaluate and address impacts on individuals, groups and societies
3.25	**Data Quality** Characteristic that data meets the organization's requirements for a specific context
3.26	**Statement of Applicability (SoA)** Documentation of all controls with justification for inclusion or exclusion

Without Data, There Is No AI — Data Quality (3.25) is a governance requirement, not an afterthought. Biased data produces biased AI.

Scope & Purpose of ISO 42001

"Specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving an AI management system within the context of an organization."

— ISO/IEC 42001:2023, Clause 1

Applicable To

ANY organization — regardless of size, type or nature

Providers, users and developers of AI systems

Purpose

Develop, provide and use AI systems responsibly

Manage risks and meet obligations to interested parties

Not a Technical Standard

A management system standard: it governs HOW organizations manage AI, not HOW AI is built technically

Who Uses ISO 42001? Key Stakeholders

AI Providers & Producers

- AI platform, product and service providers
- AI developers, designers, testers and deployers
- AI operators, domain experts, impact assessors

Example: A company building an AI recruitment tool

AI Customers & Users

- Organizations and individuals using AI systems
- AI system integrators and data providers
- Procurers of AI products and services

Example: HR department using an AI CV-screening tool

AI Subjects & Authorities

- Data subjects and individuals affected by AI decisions
- Policymakers, regulators and oversight bodies
- Governing bodies and AI governance professionals

Example: Regulator auditing an AI lending system

ISO 42001 ensures every stakeholder understands their role, responsibilities and accountability across the full AI lifecycle.

Benefits of ISO/IEC 42001:2023

Risk Management

Structured framework to identify, assess and treat AI-specific risks before they materialize

Regulatory Alignment

Aligns with regulations such as EU AI Act, GDPR, NIST AI RMF and reduces compliance complexity across jurisdictions

Trust & Credibility

Demonstrates responsibility to customers, regulators and the public

Governance Clarity

Clear roles, responsibilities and accountability structures for all AI-related activities

Human Oversight

Embeds meaningful human oversight into AI processes, especially for high-risk decisions

Societal Protection

Requires fairness and impact assessments: protects individuals and groups from discriminatory AI outcomes

Objectives Principles of Responsible AI

1. **Fairness**
   AI must not discriminate decisions equitable across all groups

2. **Accountability**
   Clear ownership: humans remain answerable for AI outcomes

3. **Transparency**
   Disclose AI use; systems must be understandable to all stakeholders

4. **Explainability**
   AI decisions must be explainable to those affected by them

5. **Reliability & Safety**
   AI systems must perform as intended without causing harm

6. **Privacy & Security**
   Personal data processed by AI must be protected at all times

7. **Human Control**
   Meaningful human oversight, especially in high-risk decisions

8. **Ethics & Values**
   AI must align with societal values and fundamental human rights

9. **Availability & Quality of training and test data**
   AI systems need training, validation and test data in order to train and verify the systems

10. **Robustness**
    The ability (or inability) of the system to have comparable performance on new data as on the data on which it was trained or the data of typical operations

ISO/IEC JTC 1/SC 42

42

Published ISO standards *

49

ISO standards under development *

ISO/IEC TS 4213:2022
Information technology — Artificial intelligence — Assessment of machine learning classification performance

ISO/IEC 5259-1:2024
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 1: Overview, terminology, and examples

ISO/IEC 5259-2:2024
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures

ISO/IEC 5259-3:2024
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 3: Data quality management requirements and guidelines

ISO/IEC 5259-4:2024
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 4: Data quality process framework

ISO/IEC 5259-5:2025
Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 5: Data quality governance framework

ISO/IEC AWI 25872-1 [Under development]
Artificial intelligence — Knowledge enhancement for pretrained machine learning models — Part 1: Framework

ISO/IEC AWI TS 26312 [Under development]
Information technology — Artificial intelligence — Identification and treatment of unwanted bias in AI by healthcare

ISO/IEC AWI TS 26320 [Under development]
Artificial intelligence — Corpus development and maintenance for natural language processing systems

ISO/IEC AWI 42003 [Under development]
Information technology — Artificial intelligence — Guidance on the implementation of ISO/IEC 42001

ISO/IEC CD 42007 [Under development]
Information technology — Artificial intelligence — High-level framework and guidance for the development of conformity assessment schemes for AI systems

ISO/IEC DIS 42102 [Under development]
Information technology — Artificial intelligence — Framework for characterizing AI system methods and capabilities

ISO/IEC CD TR 42103 [Under development]
Information technology — Artificial intelligence — Overview of synthetic data in the context of AI systems

The ISO/IEC AI Standards Family

ISO/IEC 42001:2023	AI Management System
ISO/IEC 22989:2025	AI Concepts and Terminology
ISO/IEC 23894:2023	AI Risk Management
ISO/IEC 23053:2022	Framework for AI Systems Using ML
ISO/IEC 38507:2022	Governance of IT
ISO/IEC 42005:2025	AI System Impact Assessment
ISO/IEC 42006:2025	Requirements for bodies providing audit and certification of AIMS
ISO/IEC TR 24028:2020	Overview of Trustworthiness in AI
ISO/IEC AWI 42003 (Under development)	Guidance on the implementation of ISO/IEC 42001

How ISO 42001 Is Structured: 10 Clauses — Harmonized Structure (HS)

	Introduction	
1–3	Scope / References / Definitions	
4	Context of the Organization	PLAN
5	Leadership	PLAN
6	Planning	PLAN
7	Support	DO
8	Operation	DO
9	Performance Evaluation	CHECK
10	Improvement	ACT

Annexes

A — NORMATIVE

38 Reference Controls (A.2–A.10)
Selected via Statement of Applicability (SoA)

B — NORMATIVE

Implementation Guidance for all Annex A controls
Best practice

C — INFORMATIVE

AI-related objectives & risk sources
Includes discrimination, fairness, transparency

D — INFORMATIVE

AIMS across sectors & integration
with ISO 27001, 9001, 27701

Clause 4 — Context of the Organization

INTENT: Understand the environment in which the AIMS operates, before building it.

ACTIONS (SHALL)

✓ Determine external issues (legal requirements, market trends, cultural expectations)

✓ Determine internal issues (governance, AI maturity, risk appetite, contractual obligations)

✓ Assess whether climate change is a relevant issue (MANDATORY, must be documented)

✓ Identify the organization's AI roles: provider, producer, customer, partner, subject, authority (per ISO/IEC 22989)

✓ Determine interested parties and their requirements (4.2)

✓ Define and document the scope of the AIMS (4.3)

OUTPUT

- Documented scope of the AIMS
- List of interested parties and their requirements
- Climate change relevance determination
- Documented AI system roles

Clause 5 — Leadership

INTENT: Top management drives and owns the AIMS: leadership cannot be delegated.

5.1 Leadership & Commitment

Approve & align AI policy with strategy · Integrate AIMS into business processes · Allocate resources · Hold people accountable · Promote continual improvement

Board members shall educate themselves on AI history and concepts. This will help them ensure proper governance. **(ISO/IEC 38507:2022)**

5.2 AI Policy

Document AI policy: purpose, framework for objectives, commitment to requirements & improvement · Communicate internally and to interested parties · Align with security, privacy, quality and ethics policies · Review at planned intervals

5.3 Roles & Responsibilities

Assign responsibility for AIMS conformance and performance reporting · Define roles: AI owner, ethics officer, data governance lead, compliance manager · Establish confidential mechanism for reporting AI-related concerns

ANNEX A CONTROLS	A.2.2 AI Policy	A.2.3 Policy Alignment	A.2.4 Policy Review	A.3.2 Roles & Responsibilities	A.3.3 Reporting of Concerns

OUTPUT: Documented AI Policy · Roles & responsibilities matrix · Concern reporting process

Clause 6 — Planning: AI Risk Assessment (6.1.1 / 6.1.2)

INTENT: Identify and treat AI-specific risks before they materialize — using a consistent, documented process.

ACTIONS (SHALL)

- ✓ Establish AI risk criteria — acceptable vs unacceptable risk
- ✓ Define process producing consistent, valid, comparable results
- ✓ Identify risks that could prevent achieving AI objectives
- ✓ Analyze risks: consequences + likelihood + level of risk
- ✓ Evaluate and prioritize risks for treatment
- ✓ Retain documented information on all risk assessments

Annex C.3 — AI Risk Sources

⚠ Discrimination & bias in automated decisions

- Poor data quality / biased training data
- Lack of transparency and explainability
- Model drift and performance degradation
- Loss of human oversight / over-automation
- Privacy violations, safety hazards

ANNEX A CONTROLS	A.5.2 Impact Assessment Process	A.5.3 Impact Documentation	A.5.4 Individual Impacts	A.5.5 Societal Impacts

OUTPUT: Risk register · Documented risk assessment process

Clause 6 — Risk Treatment · Impact Assessment · Objectives (6.1.3 / 6.1.4 / 6.2)

6.1.3 AI Risk Treatment · Controls: Annex A (all 38 — selected via SoA)

- Select risk treatment options; determine necessary controls
- Compare all selected controls against the 38 Annex A controls — justify any exclusions
- Produce Statement of Applicability (SoA): included/excluded controls with justifications
- Obtain management approval for risk treatment plan and residual risks

6.1.4 AI System Impact Assessment · Controls: A.5.2 / A.5.3 / A.5.4 / A.5.5

- Assess consequences for individuals, groups and societies from deployment, intended use and foreseeable misuse
- DISCRIMINATION is a primary concern — especially in hiring, credit, healthcare and justice AI
- Document results; feed into risk assessment (6.1.2)

6.2 AI Objectives · (Annex C.2)

- Establish measurable AI objectives aligned with AI policy at all relevant functions and levels
- Objectives: fairness, accountability, transparency, safety, privacy, robustness, maintainability

ANNEX A CONTROLS

A.5.2	A.5.3	A.5.4	A.5.5
Impact Assess. Process	Impact Documentation	Individual Impacts	Societal Impacts

OUTPUT: SoA · Risk treatment plan · Impact assessment records · AI Objectives

Clause 7 — Support

INTENT: Provide the people, resources, information and communication structures the AIMS needs to function.

7.1 Resources · A.4.2 / A.4.3 / A.4.4 / A.4.5 / A.4.6

Document ALL resources: data (provenance, quality, bias, categories, retention), tooling (algorithms, ML models), computing (cloud/edge/hardware), human expertise (data scientists, ethics specialists, domain experts, oversight roles)

7.2 & 7.3 Competence & Awareness

Determine competence needed; provide training; retain evidence. All persons aware of: AI policy, their contribution to AIMS effectiveness, and implications of non-conformance.

7.4 Communication · A.8.2 / A.8.3 / A.8.4 / A.8.5

Determine what, when, with whom and how to communicate. Disclose when users interact with AI. Provide adverse impact reporting channels. Communicate incidents to affected parties.

7.5 Documented Information

Maintain, control and protect all AIMS documentation — scope, policy, risk assessments, SoA, audit records. Ensure availability, integrity and version control.

ANNEX A CONTROLS	A.4.2 Resource Documentation	A.4.3 Data Resources	A.4.4 Tooling Resources	A.4.5 Computing Resources	A.4.6 Human Resources	A.8.2 AI system Info for Users	A.8.3 Reporting to interested parties	A.8.4 Communication of Incidents	A.8.5 Disclosure of AI interaction

OUTPUT: Resource docs · Competence evidence · Communication plan · Controlled documented information

Clause 8 — Operation

INTENT: Execute the plan — implement and control all AI processes in practice. This is the DO phase of PDCA.

8.1 AI Lifecycle · A.6.1.2 / A.6.1.3 / A.6.2.2 / A.6.2.3 / A.6.2.4 / A.6.2.5 / A.6.2.6 / A.6.2.7 / A.6.2.8

Specify requirements; document design & development; verify & validate; deploy with deployment plan; operate with continuous monitoring; maintain technical documentation and event logs throughout the lifecycle

8.1 Data Management · A.7.2 / A.7.3 / A.7.4 / A.7.5 / A.7.6

Data management processes; acquisition controls; quality requirements; provenance tracking; data preparation criteria — without quality data, there is no quality AI

8.1 Responsible Use · A.9.2 / A.9.3 / A.9.4

Define processes for responsible use; document objectives for use; implement human oversight mechanisms proportionate to the risk level of the AI system

8.1 Third Parties · A.10.2 / A.10.3 / A.10.4

Allocate responsibilities between organization, suppliers and customers; establish supplier requirements and monitoring; address customer expectations and needs

ANNEX A CONTROLS	A.6.1.2 – A.6.2.8	A.7.2 - A.7.6	A.9 .2 – A.9.4	A.10.2 – A.10.4
	AI Lifecycle	Data Management	Responsible Use	Third Parties

OUTPUT: Operational procedures · Event logs · Supplier agreements · Risk & impact assessment records

Clause 9 — Performance Evaluation

INTENT: Measure, monitor and review whether the AIMS is working as intended.

9.1 Monitoring, Measurement, Analysis & Evaluation

- Determine what to monitor: AI system performance, fairness metrics, incidents, compliance status
- Define methods, frequency and responsible parties — retain results as documented evidence
- Evaluate the performance and effectiveness of the AIMS itself

9.2 Internal Audit

- Conduct at planned intervals — does AIMS conform to requirements and is it effectively implemented?
- Plan audit programme: objectives, criteria, scope, frequency
- Select objective auditors; report results to relevant managers; retain audit evidence

9.3 Management Review — Inputs & Outputs

- Top management reviews AIMS suitability, adequacy and effectiveness at planned intervals
- Inputs: previous actions, changes in context/interested parties, nonconformities, audit & monitoring results, improvement opportunities
- Outputs: decisions on continual improvement and any needed AIMS changes — retain as documented evidence

OUTPUT: Monitoring records · Internal audit reports · Management review minutes and decisions

Clause 10 — Improvement

INTENT: The AIMS must continuously evolve: AI risks, technology and regulations change rapidly.

10.1 Continual Improvement

Suitability Is this the right AIMS for our context? **Adequacy** Is it sufficient to meet requirements?
Effectiveness Is it achieving intended results?

Use inputs from: management reviews · audit results · monitoring data · stakeholder feedback

10.2 Nonconformity & Corrective Action

- React: control and correct the nonconformity; address its consequences
- Investigate root cause — determine if similar nonconformities exist elsewhere
- Implement corrective actions; review their effectiveness; update the AIMS if necessary
- Retain evidence of nonconformities, actions taken and results — A static AIMS is an ineffective AIMS

OUTPUT: Corrective action records · Continual improvement evidence · Updated AIMS documentation

ISO 42001: Governance for Responsible AI

ISO/IEC 42001:2023 is not a technical standard.
It is a management system: a governance framework ensuring organizations develop, provide and use AI responsibly, transparently and accountably.

Without ISO 42001	With ISO 42001
Uncoordinated AI decisions	Structured governance framework
No AI-specific risk criteria or assessment process	AI risks identified, assessed and treated systematically
Accountability for AI outcomes undefined or undocumented	Roles, responsibilities and accountability formally assigned
Discriminatory AI impacts go undetected and unaddressed	Impact assessments required (Fairness and discrimination assessed)
No verifiable evidence of responsible AI practice	Documented, auditable management system (Third party certifiable)

Annex C: Discrimination · Lack of Transparency · Loss of Human Control · Privacy Violations · Safety Hazards

Sustainable Management Group

Your Partner Towards Quality Improvement, today and into the AI Era.

Get In Touch

Ontario - Canada

+1 613 702 2818

Quebec - Canada

+1 514 442 9528

Email

info@smg-aw.com

LinkedIn

linkedin.com/company/smg-sustainable-management-group

smg-aw.com

Thank you