Introduction to AI and Data ISO Standards
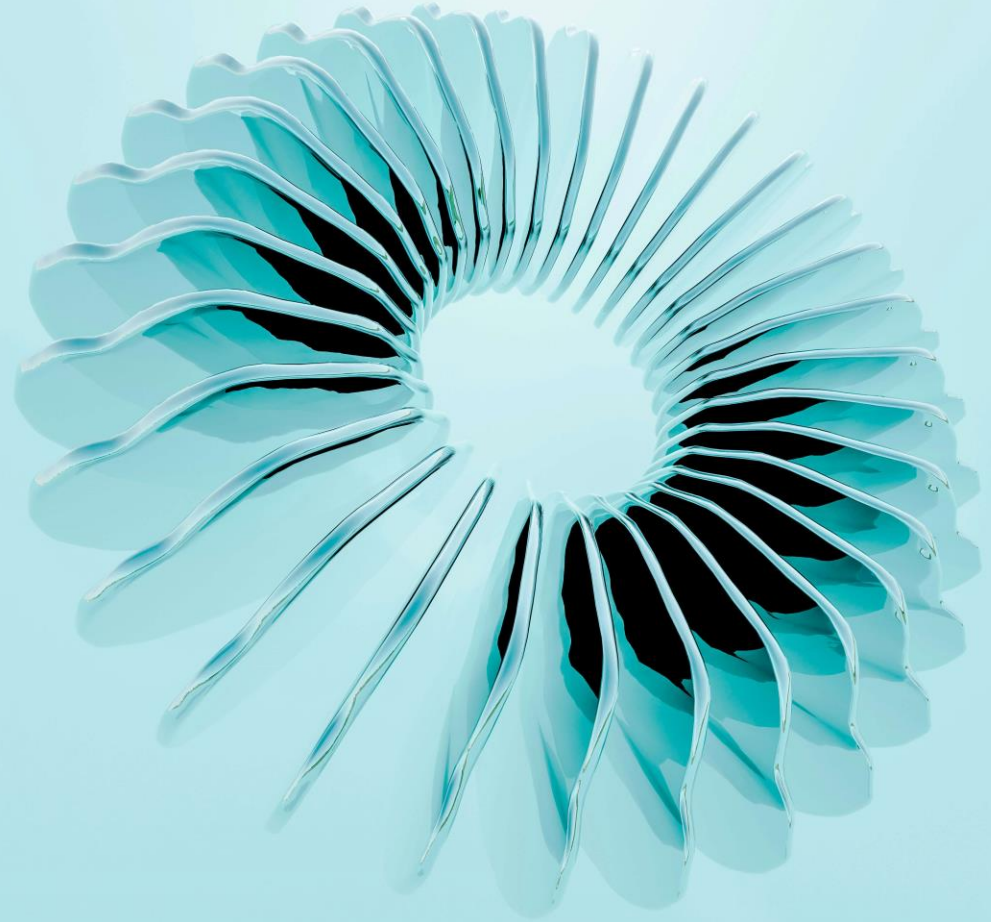
Webinar

Nemko Digital

January 27, 2026

Topics today

1. Introduction to Nemko Digital
2. Overview of AI and ISO in coherence
3. Double-clicks and discussion
    i. AI quality model
    ii. Functional safety
    iii. ISO and Data Governance
    iv. ISO 42001
4. Towards implementation
5. Conclusion & prices
6. Q&A

With you today

CA Gurunandan Savnal
Digital Trust Expert
PeopleSys Consulting

CA, CISA, CFE, CDPSE, COSO Internal Control, CRP, CEH, Lead Cybersecurity Manager – ISO 27032, Lead Auditor ISO 27001, 22301, ISO 37001, ISO 37301, ISO 42001

- **Member International ISO Technical Committees:** Risk Management & Sustainable Finance

- **Member National Committees:** Risk Management Implementation Guidelines, Risk Maturity Framework

Bas Overtoom
Sr. AI Trust Expert
Nemko Digital

- **Experienced AI & Data Executive:** +10 years of consultancy experience, driving AI and data transformations for top global organizations.

- **Responsible AI Advocate:** Passionate about RAI to address business, social, and environmental challenges.

- **Global Business Expertise:** Strong international background i.e., 7 years in Asia, fostering cross-cultural collaboration. Leads global BD at Nemko Digital, promoting AI Trust worldwide.

- **VC Advisor for AI Scale-Ups:** Supports AI startups within a prominent Dutch VC fund to achieve global growth.

Pep van der Laan Ph.D.
AI Trust & Tech Expert
Nemko Digital

- **Scaling AI impact**: +10 years in realizing business value through scaling AI and ML from initial proof-of-concept to enterprise-wide solutions.

- **Strategy advisory:** Extensive experience shaping the AI & Data transformation and architecture for global leaders and national champions across industries.

- **AI & Data capability building:** Led a team of 90 data scientists through the transformation from the traditional consulting model and introducing modern delivery and development practices.

- **Growing Digital Trust:** Recognized for consistently bridging the gap between the developer and AI risk communities, building mutual understanding
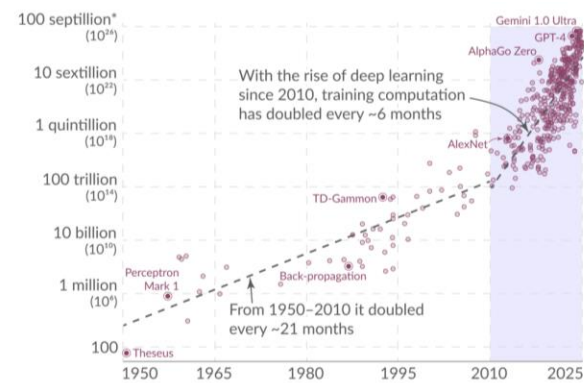
Introduction Nemko Digital

Building trust in AI is a complex challenge

Complicating factors

Speed of innovation

Training FLOPs of AI systems

Evolving regulation

EU Acts and Directives related to AI, Data, and Cyber

Domain	EU Regulation	Applicability
Artificial Intelligence	AI Act	Adopted / 2026
Data protection and governance	General Data Protection Regulation (GDPR)	In force
	Data Act	In force
	Data Governance Act	In force
	ePrivacy regulation	In draft / TBC
Cyber security and digital resilience	Cyber Resilience Act (CRA)	In force
	Network Information Security Directive (NIS2)	Adopted / 2027
	Digital Operational Resilience Act (DORA)	In force
	Cybersecurity Act	In force
Product Safety and Conformity	Product Liability Directive – revised	Adopted / 2026
	Radio Equipment Directive (RED)	In force
	Machinery Regulation – revised	Adopted / 2027
	General Product Safety Regulation (GPSR)	In force
Market and Critical Infrastructure	Digital Services Act (DSA)	In force
	Digital Markets Act (DMA)	In force
Sector-specific	European Health Data Space (EHDS)	Adopted / 2026

Changing tech stack

New/enhanced capabilities due to GenAI
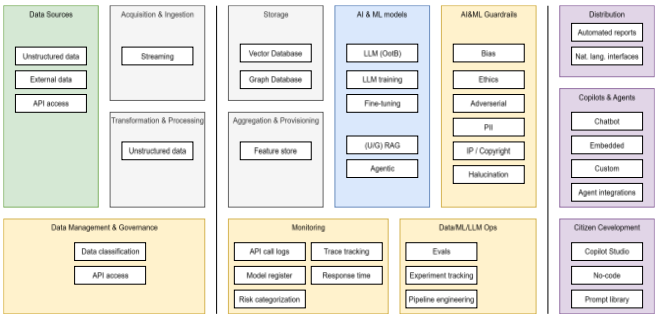
AI in everything

Multiple standards

Human interaction

Nemko: Compliance without Complexity

Strong heritage

1933 — Established by the Norwegian government as *Norges Elektriske Materiellkontroll*

1991 — Became independent self-owned private foundation

1992 - 2003 — Established offices and laboratories around the world

2020 — Launched Cybersecurity services

2024 — **Established *Nemko Digital* to consolidate AI Trust services**
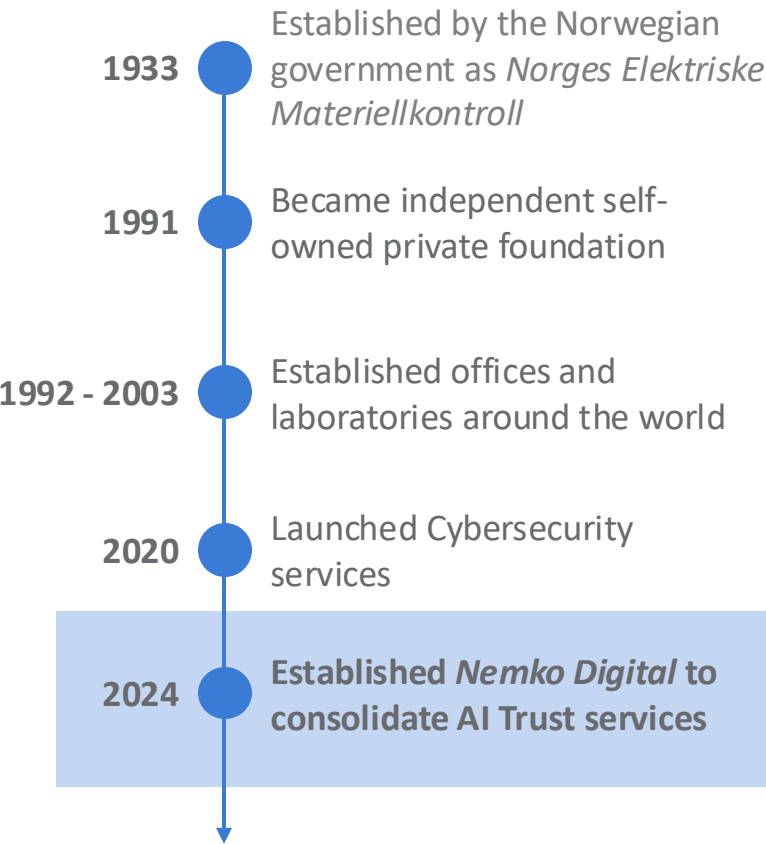
Global reach & local presence

28 locations on **3** continents

Over **850** employees worldwide.

Offering services in more than **150** countries

Serving **7,000** customers across **80** countries.

In June 2025, Nemko signed a strategic partnership with KSA to shape the future of AI certification and trust in Korea and beyond

Proven track record

Roster of clients and services (not exhaustive)

SAMSUNG   Panasonic   LG

JOTRON   WÄRTSILÄ   KÄRCHER

What is top-of-mind for our clients?

We deliver Digital Trust through end-to-end compliance and advisory support, combining technical, regulatory, and process expertise.

Regulatory Compliance — Beyond AI

ISO Readiness
ISO 42001, ISO 27001... — Beyond AI

Global Market Access — Beyond AI

Nemko AI Trust Mark

Technical Assurance / AI Testing

AI Assurance Tools

Governance Maturity — Beyond AI
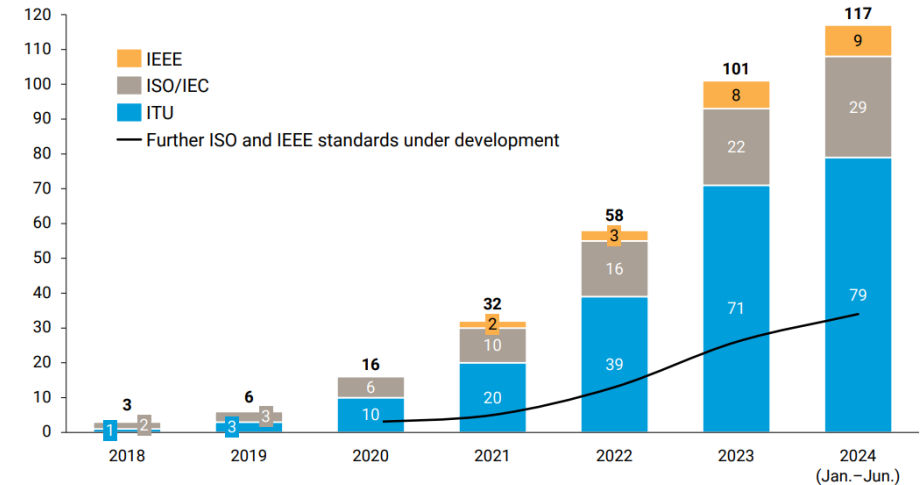
Strategy and roadmaps — Beyond AI

Why ISO standards

Which standards are worth investing time and effort in?

Navigating AI Standards becomes ever more important, but also increasingly complex. What really makes a difference for your company? What will be the benefits of conformity? What is required to get there?

Interoperability and integration

Trust, transparency and compliance

Risk Management and Quality Assurance

Global Market Access

Competitive Advantage and Innovation

Growing number of AI-related standards

Legend:
- IEEE
- ISO/IEC
- ITU
- — Further ISO and IEEE standards under development

Year	ITU	ISO/IEC	IEEE	Total
2018	1	2		3
2019	3	3		6
2020	10	6		16
2021	20	10	2	32
2022	39	16	3	58
2023	71	22	8	101
2024 (Jan.–Jun.)	79	29	9	117

Sources: IEEE, ISO/IEC, ITU, World Standards Cooperation (based on June 2023 mapping, extended through inclusion of standards related to AI).

Welcome to the ISO AI Standards Universe (selection)

AI Lifecycle processes

✦ AI Lifecycle (5338)

✦ Data lifecycle for AI (8183)

✦ AI Quality Model (25059)

Policies and Organization

✦ IT Governance of Data (38505)

✦ IT Governance of AI (38507)

✦ AI Applications (5339)

✦ AI Concepts and Terminology (22989)

Management Systems

✦ AIMS (42001)

✦ Cybersecurity MS (27001)

✦ Privacy Information MS (27701)

Data Management

✦ Master Data (8000 series)

✦ Data Quality (25012, 25024)

✦ ML Data Quality (5259)

Risk Management

✦ AI Risk Management (23894)

✦ Functional Safety for AI (TR 5469)

Let's hear from you!

Which ISO standards are currently implemented or certified in your organization? [Multiple answers possible]

- ❑ ISO/IEC 27001 (Information Security)
- ❑ ISO/IEC 27701 (Privacy Information Management)
- ❑ ISO 9001 (Quality Management)
- ❑ ISO/IEC 42001 (AI Management System)
- ❑ ISO 22301 (Business Continuity)
- ❑ ISO 14001 (Environmental)
- ❑ None yet
- ❑ Not sure
- ❑ Others

Welcome to the ISO AI Standards Universe (selection)

AI Lifecycle processes

✦ AI Lifecycle (5338)

✦ Data lifecycle for AI (8183)

✦ AI Quality Model (25059)

Policies and Organization

✦ IT Governance of Data (38505)

✦ IT Governance of AI (38507)

✦ AI Applications (5339)

✦ AI Concepts and Terminology (22989)

Management Systems

✦ AIMS (42001)

✦ Cybersecurity MS (27001)

✦ Privacy Information MS (27701)

Data Management

✦ Master Data (8000 series)

✦ Data Quality (25012, 25024)

✦ ML Data Quality (5259)

Risk Management

✦ AI Risk Management (23894)
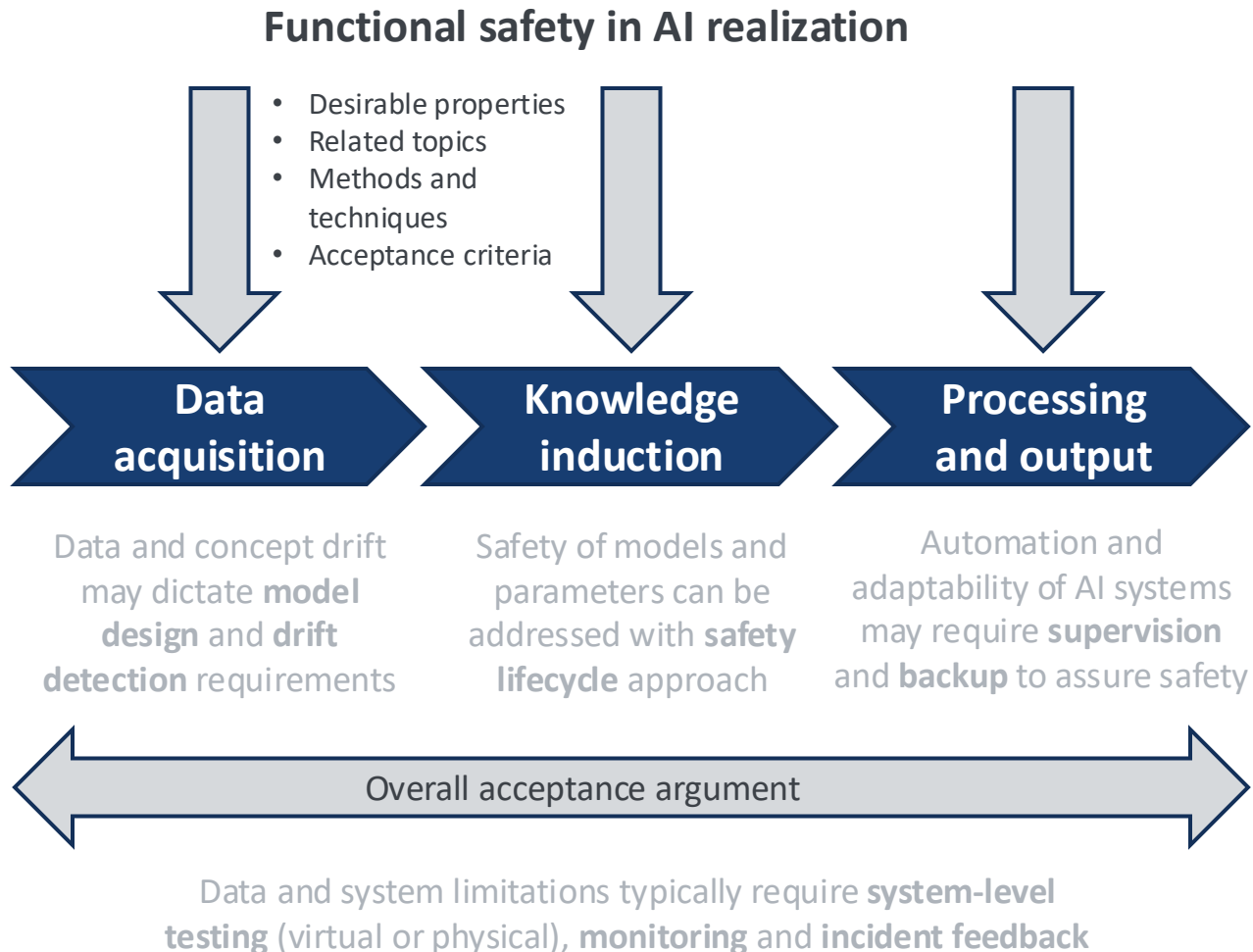
✦ Functional Safety for AI (TR 5469)

Quality Model for AI Systems (ISO 25059)

The quality model for AI systems (as a product and in use) illustrate nicely how AI differs from other technologies

AI System Product Quality
- Functional suitability — Correctness, Adaptability
- Performance efficiency
- Compatibility
- Usability — Controllability, Transparency
- Reliability — Robustness
- Security — Intervenability
- Maintainability
- Portability

AI System Quality in Use
- Effectiveness
- Efficiency
- Satisfaction — Transparency
- Freedom from Risk — Societal & Ethical risks
- Context Coverage

Functional safety for AI Systems (ISO TR 5469)

The specific nature of AI and ML technologies provides specific challenges regarding functional safety

Functional safety in AI realization

- Desirable properties
- Related topics
- Methods and techniques
- Acceptance criteria

Data acquisition → **Knowledge induction** → **Processing and output**

Data and concept drift may dictate **model design** and **drift detection** requirements

Safety of models and parameters can be addressed with **safety lifecycle** approach

Automation and adaptability of AI systems may require **supervision** and **backup** to assure safety

Overall acceptance argument

Data and system limitations typically require **system-level testing** (virtual or physical), **monitoring** and **incident feedback**

Key drivers for requirements

AI Level
- Impact on safety **direct** or **indirect**?
- AI used in **operation** or just in **development**?
- Decision making **autonomous** or not?

AI Class
- Can **requirements** be defined?
- Under **existing standards** for functional safety?
- Needs **complementary requirements**?
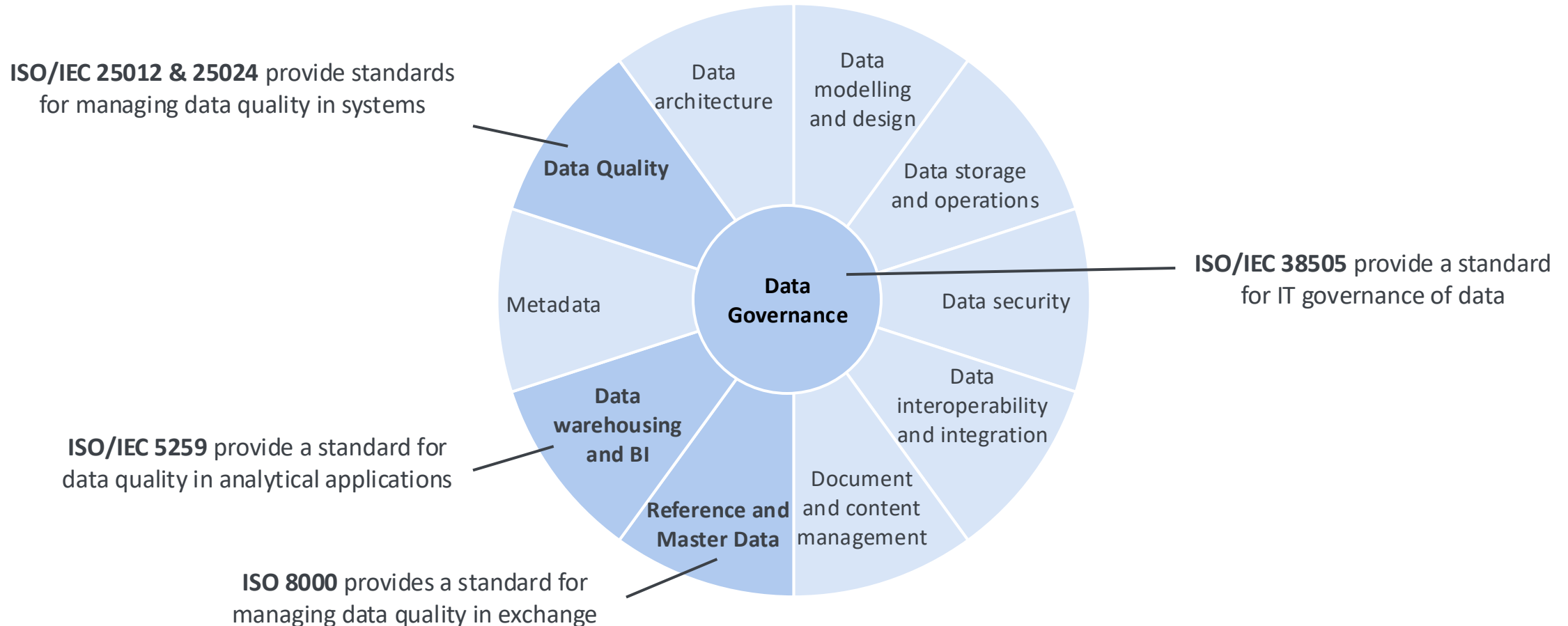
Industry standards (examples)
- Automotive (ISO 26262)
- Machinery (IEC 62061)
- Process industries (IEC 61511)

Data management and governance

ISO standards can contribute to data management objectives in accordance with the leading DAMA DMBOK framework
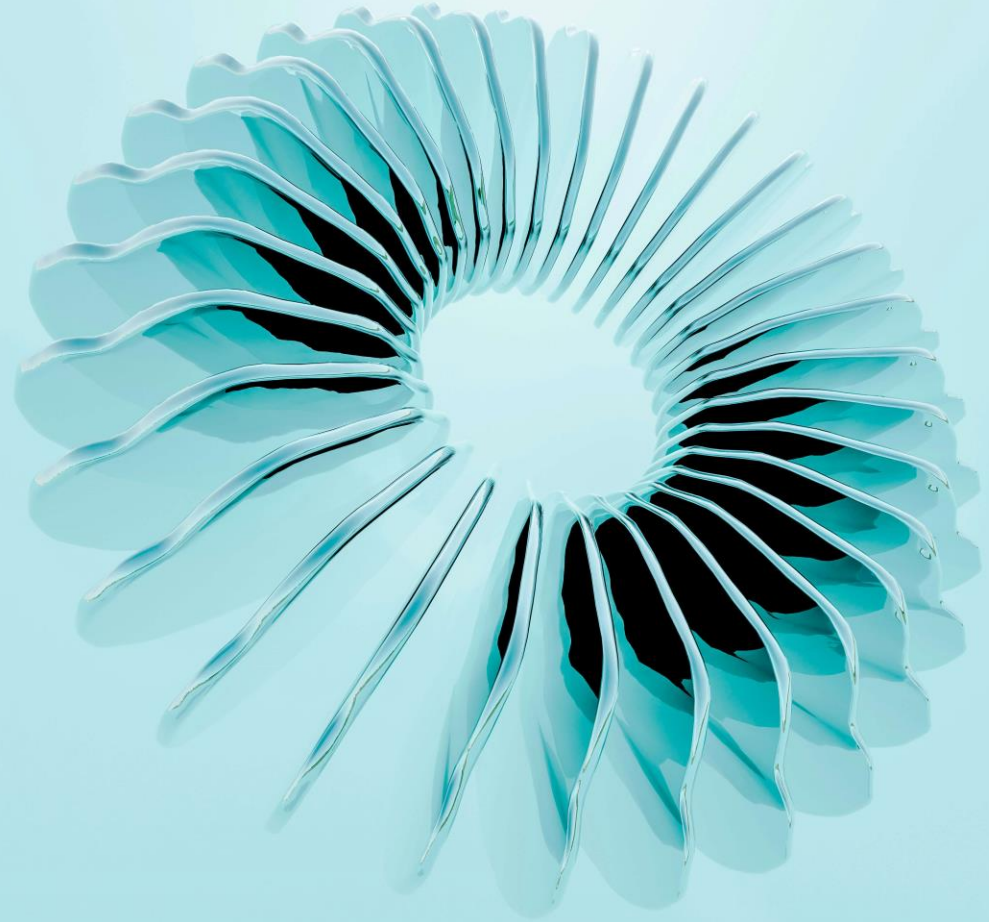
DAMA DMBOK
Framework for Data Management

ISO/IEC 25012 & 25024 provide standards for managing data quality in systems

ISO/IEC 38505 provide a standard for IT governance of data

ISO/IEC 5259 provide a standard for data quality in analytical applications

ISO 8000 provides a standard for managing data quality in exchange

Data architecture

Data modelling and design

Data storage and operations

Data Quality

Metadata

Data Governance

Data security

Data warehousing and BI

Data interoperability and integration

Reference and Master Data
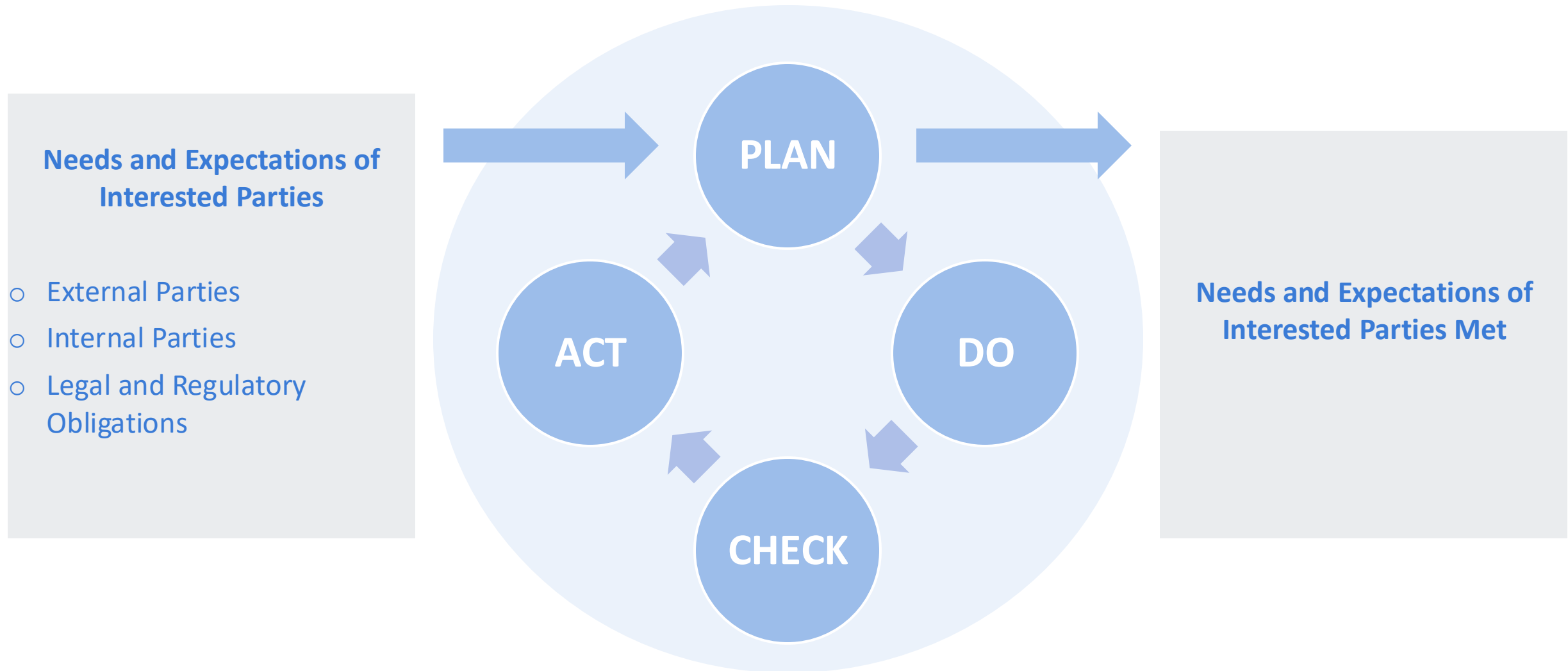
Document and content management
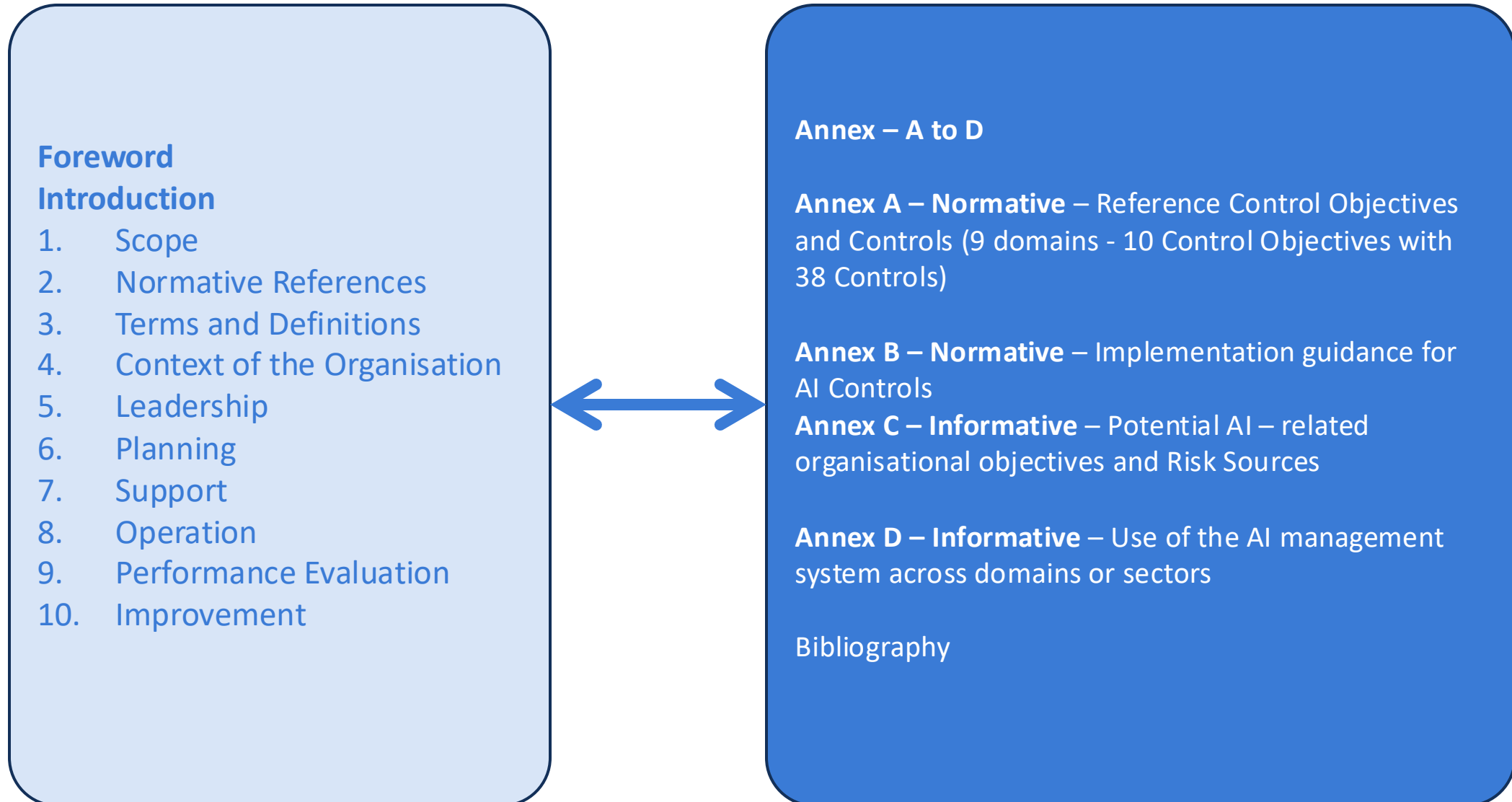
ISO/IEC 42001 in detail

ISO/IEC 42001:2023

- Requirements and guidance for establishing, implementing, maintaining and continually improving an AI management system.

- **PDCA framework**

- Use by an organization providing or using products or services that utilize AI systems.

- Organizations are expected to **focus** their application of requirements on **features that are unique to AI.**

- Certain features of AI, such as the **ability to continuously learn and improve** or **a lack of transparency or explainability,** can warrant different safeguards if they raise additional concerns compared to how the task would traditionally be performed.

- The adoption of an AI management system to **extend the existing management structures is a strategic decision for an organization**.

Plan – Do – Check –Act (The Familiar PDCA Model)

Needs and Expectations of Interested Parties

o External Parties
o Internal Parties
o Legal and Regulatory Obligations

PLAN

ACT

DO

CHECK

Needs and Expectations of Interested Parties Met

High Level Structure – ISO/IEC 42001:2023

Foreword

Introduction

1. Scope
2. Normative References
3. Terms and Definitions
4. Context of the Organisation
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Improvement

Annex – A to D

Annex A – Normative – Reference Control Objectives and Controls (9 domains - 10 Control Objectives with 38 Controls)

Annex B – Normative – Implementation guidance for AI Controls

Annex C – Informative – Potential AI – related organisational objectives and Risk Sources

Annex D – Informative – Use of the AI management system across domains or sectors

Bibliography

Overview of controls

A.2 Policies for AI
AI Policy
Alignment with other policies
Review of the AI policy

A.3 Internal Organization
Roles & Responsibilities
Reporting of concerns

A.4 Resources for AI
Documentation of resources
Data resources
Tooling resources
System & computing
Human resources

A.5 Impact of AI systems
AI impact assessment
Documentation of impact
Individuals & groups
Society

A.6 AI Lifecycle
Responsible AI guidance
Responsible AI process
System requirements
Design documentation
Verification & validation
System deployment
Operation & monitoring
Technical documentation
Recording of event logs

A.7 Data for AI
Data for AI development
Data acquisition
Data quality
Data provenance
Data preparation

A.8 Interested parties
User documentation & info
External reporting
Incident communication
Info for interested parties

A.9 Use of AI systems
Responsible use process
Responsible use objectives
Intended use

A.10 Third-parties
Allocation of responsibilities
Suppliers
Customers

Related standards
(selection)

ISO 27001
Information Security Management System

ISO 27701
Privacy Information Management System

ISO 9001
Quality Management System

ISO 42001 Standard: Interconnections with Other ISO Standards

ISO/IEC 42001:2023 establishes an Artificial Intelligence Management System framework that extensively references other ISO/IEC standards. This mapping identifies over 30 interconnections across Clauses 4-10, Annex A, and Annex B, helping organizations understand dependencies between ISO 42001 and referenced standards

>30

Total References

ISO/IEC standards referenced throughout the document

7 and 9

**7 Clauses and
9 Annex Objectives**

Clauses 4 to 10
Annex A and Annex B

Most Referenced Standards:
The Foundation of AI Governance

ISO/IEC 22989:2022

AI Concepts and Terminology

4 references across Clauses 4, 4.1, A.4, A.7, B.7, B.29. Provides foundational AI terminology, concepts, and role definitions essential for understanding AI system stakeholders and lifecycle management.

ISO/IEC 38507

Governance of AI

4 references in Clauses 5.2, 6.1.1, A.2, B.2, B.20. Addresses board-level governance considerations and strategic direction for AI systems within organizational structures.

ISO/IEC 25024

Data Quality

2 references in A.7.4, B.7.4. Critical for ensuring data quality characteristics and measurement approaches for analytics and machine learning systems.

ISO/IEC 19944-1

Big Data Reference Architecture: 3 references (A.7.3, B.4.3, B.7.3) providing data categorization and acquisition frameworks

ISO 37002

Whistleblowing Management: 2 references (8.1, B.3.3) for concerns reporting mechanisms and protection from reprisals

ISO/IEC 5259 Series

Data Quality Framework: 2 references (B.4.3, B.7.4) describing quality dimensions for AI data

Implementation Roadmap: Key Interconnections by Domain

01 **AI System Governance & Leadership**

ISO/IEC 38507 for board-level AI governance and ISO/IEC 38500:2015 for corporate IT governance frameworks

02 **Data Management & Quality**

ISO/IEC 25024 and 5259 series for data quality, ISO/IEC TR 24027 for bias assessment, ISO 8000-2 for provenance

03 **Privacy & Data Protection**

ISO/IEC 29100 for PII framework, ISO/IEC 27001 and 27701 for security and privacy management

04 **Risk Management Framework**

ISO/IEC 23894 for AI risk assessment, ISO Guide 73 for risk vocabulary, and ISO/IEC Guide 51 for safety aspects

05 **AI System Life Cycle**

ISO/IEC 5338 for lifecycle processes, ISO/IEC TR 24029-1 for neural network robustness, ISO 9241-210 for human-centered design

06 **Audit & Compliance**

ISO 19011 for auditing management systems and ISO 37002 for whistleblowing mechanisms

Critical Implementation Insight: Organizations should implement ISO 42001 as part of an integrated management system approach, aligning governance, risk, and compliance processes across all referenced standards to maximize synergies and avoid duplication. Establish cross-functional teams to coordinate multi-standard compliance and use this mapping to prioritize standard adoption and training.
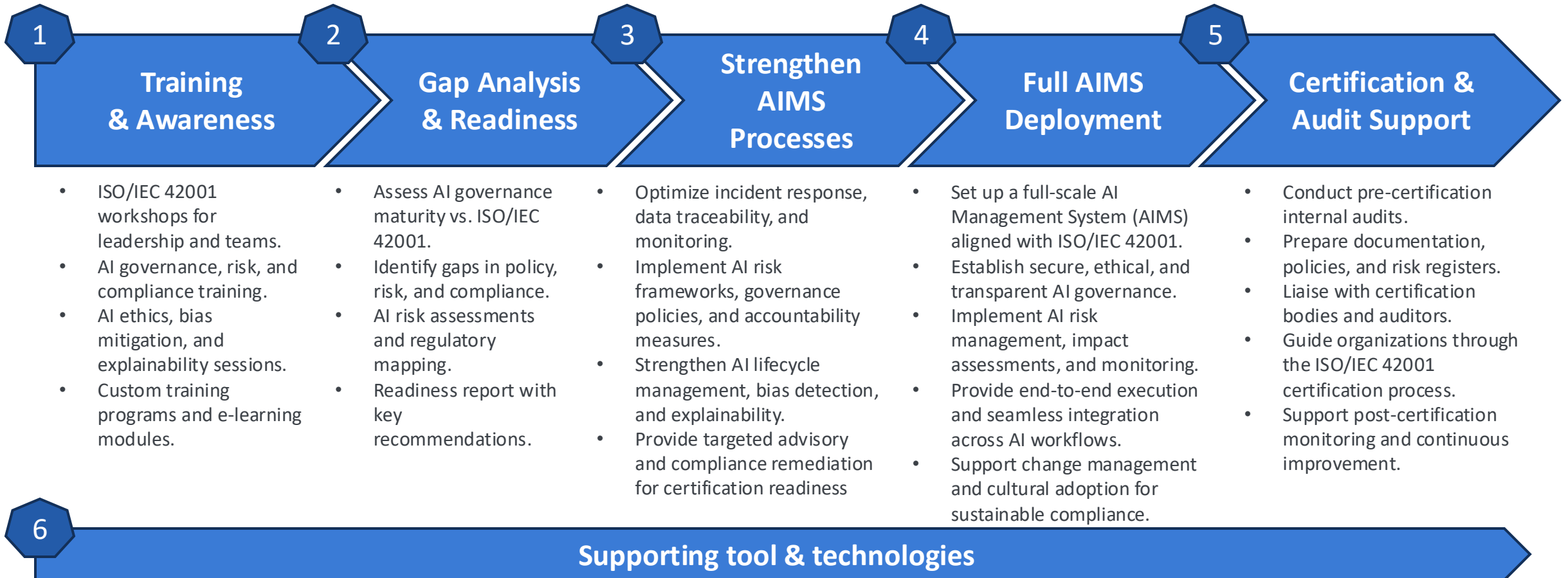
Towards implementation

Deploying ISO/IEC 42001 to drive AI quality and robustness

Achieving ISO/IEC 42001 certification requires a structured approach to AI governance, risk management, and compliance. Our end-to-end support ensures organizations strengthen their AI Management Systems (AIMS), optimize key processes, and seamlessly navigate certification requirements.
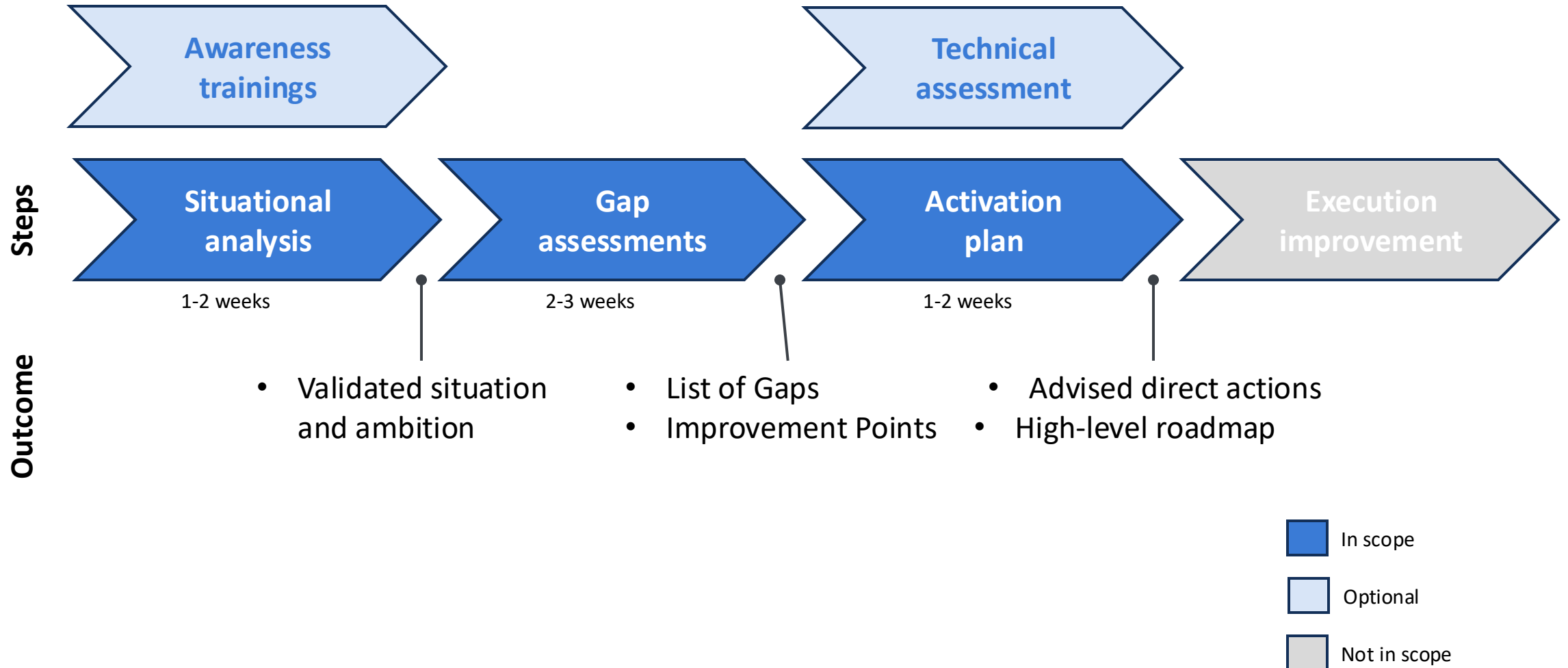
1 Training & Awareness

- ISO/IEC 42001 workshops for leadership and teams.
- AI governance, risk, and compliance training.
- AI ethics, bias mitigation, and explainability sessions.
- Custom training programs and e-learning modules.

2 Gap Analysis & Readiness

- Assess AI governance maturity vs. ISO/IEC 42001.
- Identify gaps in policy, risk, and compliance.
- AI risk assessments and regulatory mapping.
- Readiness report with key recommendations.

3 Strengthen AIMS Processes

- Optimize incident response, data traceability, and monitoring.
- Implement AI risk frameworks, governance policies, and accountability measures.
- Strengthen AI lifecycle management, bias detection, and explainability.
- Provide targeted advisory and compliance remediation for certification readiness

4 Full AIMS Deployment

- Set up a full-scale AI Management System (AIMS) aligned with ISO/IEC 42001.
- Establish secure, ethical, and transparent AI governance.
- Implement AI risk management, impact assessments, and monitoring.
- Provide end-to-end execution and seamless integration across AI workflows.
- Support change management and cultural adoption for sustainable compliance.

5 Certification & Audit Support

- Conduct pre-certification internal audits.
- Prepare documentation, policies, and risk registers.
- Liaise with certification bodies and auditors.
- Guide organizations through the ISO/IEC 42001 certification process.
- Support post-certification monitoring and continuous improvement.

6 Supporting tool & technologies

We help organizations select, implement, utilize, and enhance scalable AI governance tools to ensure ISO/IEC 42001 compliance, enabling robust risk management, monitoring, and transparency while driving AI innovation at scale.

Project approach Gap assessment & readiness

Steps

Awareness trainings

Technical assessment

Situational analysis

1-2 weeks

Gap assessments

2-3 weeks

Activation plan

1-2 weeks

Execution improvement

Outcome

- Validated situation and ambition
- List of Gaps
- Improvement Points
- Advised direct actions
- High-level roadmap

In scope

Optional

Not in scope

Call to action

Stay updated!