HUX AI
Empowering humanity, shaping tomorrow

RESEARCH INTERNSHIP REPORT

ISO 42001 Starter Guide

AUTHORS
BURÇİN KIZILCIKLI, EGE UĞUR AMASYA, HAYRİYE ANIL,
İDİL KULA, NESİBE KIRIŞ CAN, ONUR PİŞİRİR

ADVISOR & MENTOR
IŞIL SELEN DENEMEÇ

ADVISOR & EDITOR
MERVE AYYÜCE KIZRAK

PUBLISHED
OCTOBER 2025

Licensing Notice

The views and opinions expressed in this report are those of the author(s) and do not necessarily reflect the official position of any affiliated organisation or institution.

The material is provided “as is,” without warranties or representations of any kind, including accuracy, completeness, or fitness for a particular purpose. The author(s) and publisher disclaim any liability arising from the use or interpretation of the information contained herein.

Please cite this work as:
Kızılcıklı, B., Amasya, E. U., Anıl, H., Kula, İ., Can, K. N. and Pişirir, O., “ISO 42001 Starter Guide,” HUX AI, 2025, licensed under CC BY-NC 4.0 via Wikimedia Commons.

Legal Notice

The views and analyses expressed in this report are those of the individual authors and contributors. They do not represent the official position of HUX AI. This publication is for informational purposes only and does not constitute legal or commercial advice.

Table of Contents

Executive Summary

As AI becomes advanced day by day, organisations are automating critical functions at a growing pace. While efficiency and innovation drive the adoption of AI, significant risks, such as non-compliance, ethical breaches, and loss of stakeholder trust, must also be addressed. Risk management is essential for organisations to remain competitive in this environment.

Global standards for AI governance are emerging; however, the definition of a trustworthy AI system still remains unsettled. Aligning with established frameworks, such as the EU AI Act, the NIST AI Risk Management Framework, and ISO 42001, provides organisations a strategic advantage. These standards support reliability, accountability, transparency, and thorough documentation. Following them reduces compliance risks and strengthens stakeholder confidence.

Although interest in ISO 42001 is increasing, most guides lack actionable insights. They often emphasize abstract Clauses and definitions, with few practical tools or real-world examples. This leaves many organisations struggling to apply the standard effectively.

This guide addresses that gap by providing a clear, practical interpretation of ISO 42001 for organisations at any stage of AI adoption. It defines key implementation roles, explains each Clause of the standard, and demonstrates real-life applications. The fictional case study of “X Corporation” illustrates the implementation of an AI-based HR tool from concept through deployment and oversight.

The guide utilizes visual aids, including detailed and comprehensive tables and diagrams, to enhance clarity and usability. It also maps ISO 42001 Clauses with practical insights from the fictional story of “X Corporation”, providing step-by-step guidance. The result is a concise, actionable, and sector-agnostic resource for organisations applying AI governance principles when deploying AI.

Explaining ISO 42001

Artificial intelligence (AI) has moved beyond its original development space in innovation labs. The technology of AI operates as a force that influences hiring practices and customer service delivery, healthcare systems, financial operations, and essential infrastructure management. The primary challenge for businesses today is ensuring the ethical and legal compliance of AI systems while exploring its new capabilities.

ISO/IEC 42001:2023 (ISO 42001) is the world's first standard that tackles the current AI management challenge. It establishes a standardized framework for AI Management Systems (AIMS), encompassing structured policies, processes, and controls that enable organisations to oversee AI development, deployment, and maintenance effectively. The standard follows a similar approach to ISO 27001 by providing a systematic framework for AI management.

For businesses, the value is clear:

- The standard enables organisations to transform their AI projects into monitored and documented systems that receive ongoing improvement.
- The standard helps organisations reduce their exposure to biased systems, privacy violations, and other non-compliance with regulations.
- The standard enables organisations to demonstrate their trustworthiness to customers, regulators, and business partners through third-party certification.

Other Relevant Standards

ISO 42001 exists as an independent standard. It is supported by a family of related international standards that help organisations address terminology, governance, risk, data quality, and societal concerns in AI.

- **ISO/IEC 42005:2025**— AI System Impact Assessment
- **ISO/IEC 5259 Series:2024** — Data Quality for Analytics and ML
- **ISO/IEC 23894:2023** — AI Risk Management
- **ISO/IEC 38507:2022** — Governance of AI
- **ISO/IEC 22989:2022** — AI Concepts and Terminology
- **ISO/IEC 23053:2022** — Framework for AI Systems Using ML
- **ISO/IEC TR 24368:2022** — Ethical and Societal Concerns
- **ISO/IEC TR 24027:2021** — Bias in AI
- **ISO/IEC TR 24028:2020** — Trustworthiness in AI

How ISO 42001 Differs from Other AI Standards

The AI governance landscape is not crowded. Three comprehensive frameworks dominate today:

- NIST AI RMF (U.S.) → Voluntary guidance to identify and manage risks. Useful as a risk vocabulary, but not certifiable.
- EU AI Act (Europe) → The first comprehensive binding law with fines and enforcement. Compliance is mandatory for certain operators of AI systems and general-purpose AI models placed on the EU market or used within the EU.
- ISO 42001 (Global) → A voluntary, certifiable standard. Independent auditors verify whether an organisation's AIMS meets the requirements.

The NIST framework provides security management principles, but the EU AI Act requires legal compliance, and ISO 42001 provides an auditable management system. The framework functions as a voluntary system that enables businesses to show their readiness and responsibility.

What Does "AI Management System (AIMS)" Mean in Practice

An AIMS represents the organisational structure that defines AI development and deployment methods, as well as monitoring procedures, through established policies and processes, and designated roles. It includes:

- Defining and documenting which AI systems and processes are in scope.
- Risk and impact assessments need to be performed at every stage of the AI lifecycle.

- The documentation process encompasses all necessary controls to maintain fairness, privacy, transparency, data quality, and accountability.
- Training employees and clearly assigning responsibilities across teams.
- Monitoring and measuring performance through measurable KPIs, internal audits, management reviews and corrective actions.

AI governance becomes a continuous, sustainable business process through this framework, which transforms it from a single project into an ongoing management system.

What is in scope	ISO 42001 can be applicable to any organisation that develops, deploys, or uses AI systems, regardless of their the size or sector and the type of technology . The standard covers traditional machine learning models such as and credit scoring and demand forecasting, as well as newer generative systems like chatbots and image generators. The scope encompasses all AI-related activities of the organisation, including but not limited to healthcare services, employment, and financial services. organisations establish AIMS boundaries to ensure governance and management control over all systems and processes that fall within their scope of responsibility.
Who should use it	The standard is not limited to large technology companies. It is designed for organisations of any size, from startups to multinationals, across every sector. The standard establishes a common framework that enables boards, regulators, auditors, and vendors to align their AI governance objectives, accountability and compliance. Startups can benefit from implementing the ISO 42001 standard as their operational framework to achieve sustainable growth, market credibility, which may help with funding and investor support.
When does it apply	ISO 42001 standard applies to the entire lifecycle of AI systems. organisations that obtain certification in advance can avoid costly last-minute compliance expenses, meet their procurement requirements, and demonstrate readiness to their partners and regulatory bodies. Early adopters can gain advantages like improved access to funding, stronger stakeholder confidence and leadership in AI governance.

*Click **here** to view the blueprint map and literature map details dynamically or download.*

CAUTION-1: *To illustrate the principles and actions outlined in the ISO 42001 standard, the following guide presents an hypothetical business scenario. Each chapter engages with the main story from its respective angle throughout the Guide. Please note that this is a hypothetical use case scenario, structured for reference purposes only, and not intended for professional compliance needs.*

CAUTION-2: *Due to the intertwined nature of ISO 42001, each Clause chapter is inevitably related to principles and requirements in other Clauses. The examples under the Clauses do not exclude other related principles and subject matter that are linked to the Clause or requirements under other standards or frameworks.*

Use Case: Main Story of X Corporation

X Corporation plans to hire 120 new employees over the next six months to enhance its customer service and field operations. With an average of 500 applications per day, manual screening led to significant delays and inconsistencies. To address this issue, the CEO of X Corporation decided to purchase an AI-embedded HR tool provided by an external provider. The tool scans candidate/applicant CVs, ranking the most suitable candidates for open positions.

The defined scope of the tool was limited to pre-screening and recommendations. Its primary purpose was to streamline the hiring process, enhance consistency, and facilitate fairer decision-making. This commitment to fairness was a key consideration in the development and implementation of the system. However, the system also carried notable risks because it collected, processed, and retained personal data. These included ethical and legal risks related to the handling of personally identifiable information (PII), as well as risks of discrimination and bias that could result in unfair exclusion of candidates.

To manage these risks and align with best practices, X Corporation established an AIMS in compliance with ISO 42001.

The organisation conducted a formal context analysis to document internal and external factors, identify its role as AI system controller, and ensure compliance with GDPR and anti-discrimination regulations, as well as other applicable legal requirements. It defined the scope of the AIMS as limited to pre-screening and ranking, excluding other HR functions such as payroll and performance management, and documented all findings.

Audience, Scope & Roles

ISO 42001 Role and Resposibility Matrix

1. Executive / Governance

Role	Key Responsibilities	Relevant Key Clauses
Executive Sponsor / Chief AI Officer (CAIO)	Overall accountability for AIMS, setting strategic priorities, Resource allocation, and budget approval, reporting to senior management	ISO 42001: 5.1, 5.3
AI Governance & Compliance Officer	Coordination of ISO 42001 implementation, ensuring alignment with GDPR and EU AI Act, Development of policies and procedures, and regulatory reporting	ISO 42001: 4.1, 4.2, 9.2
AI Ethics Lead	Integration of ethical principles, Fairness and accountability assessment, Sustainability perspective, Resolution of ethical dilemmas	ISO 42001: 5.2, 6.2
Legal & Policy Counsel	Contract management, Tracking regulatory requirements, Legal risk assessment, Intellectual property management	ISO 42001: 4.2, 8.2
Stakeholder Engagement Lead	Management of stakeholder dialogue, Transparency and communication strategy, Building public trust, Operating feedback mechanisms	ISO 42001: 7.4, 9.3

2. Data

Role	Key Responsibilities	Relevant Key Clauses
Data Engineer / Data Steward	Design and management of data pipelines, ensuring data quality, Data security and access control, and data documentation	ISO 42001: 7.5, 8.3
Data Scientist / ML Engineer	Model development and training, Model evaluation and optimization, Feature engineering, Defining performance metrics	ISO 42001: 6.3, 8.4
Data Provider	Provision of datasets, Data licensing and usage rights management, Providing data updates, Data quality assurance documents	ISO 42001: 7.5.2
Diversity & Inclusion Advisor	Bias analysis in datasets, Representation and fairness assessment, Accessibility verification, Inclusive design recommendations	ISO 42001: 6.2.3, 8.4.2

3. Design / Engineering

Product Manager / AI Designer	Defining purpose and scope, Determining user and stakeholder requirements, Establishing success criteria, Product roadmap management	ISO 42001: 6.3, 8.1
AI Engineer	Model integration, Development of AI components, System optimization, Technical documentation	ISO 42001: 8.4, 8.5
Domain Expert	Defining sector-specific requirements, contributing to risk assessments, validating use cases, and transferring domain knowledge	ISO 42001: 6.2, 8.2
UX / Human Factors Specialist	Design of human oversight mechanisms, Explainability interfaces, User feedback systems, Appeal and recourse processes	ISO 42001: 6.2.4, 8.5.3
Systems & Software Engineer	Technical architecture design, API and integration development, System scalability, and infrastructure management	ISO 42001: 7.1, 8.5
Cybersecurity & Privacy Officer	Security-by-design, Privacy-by-design, Threat modeling, Implementation of security controls	ISO 42001: 8.6, A.6

4. Deployment / Operation

Role	Key Responsibilities	Relevant Key Clauses
AI Operator / MLOps Engineer	Management of production systems, Model deployment and updates, System health monitoring, Performance optimization	ISO 42001: 8.5, 8.7
Monitoring Lead	Real-time performance tracking, Model drift detection, Operational risk management, Alert system management	ISO 42001: 9.1, 9.2
Resilience & Incident Lead	Business continuity planning, Incident response processes, Preparedness for misuse scenarios, Recovery coordination	ISO 42001: 8.8, 10.2
Procurement & Vendor Relations Lead	Responsible procurement management, Vendor assessment and audit, Contract management, Third-party risk management	ISO 42001: 8.9, A.7
Training & Awareness Lead	AI literacy programs, Employee awareness training, raising responsibility awareness, and development of training materials	ISO 42001: 7.3

5. Auditing / Monitoring

AI Evaluator / Tester (TEVV)	Testing, validation, and verification, Bias and fairness testing, Performance evaluation, Technical documentation review	ISO 42001: 8.4.3, 9.2.2
Internal Auditor (AIMS Auditor)	Conducting internal audits, Readiness level assessment, Identifying improvement opportunities, Preparing audit reports	ISO 42001: 9.2
External Auditor / Certification Body	Independent certification audit, Conformity assessment, Certification decision, Surveillance audits	ISO 42001: 9.3
Knowledge & Documentation Manager	Records management system, Documentation of design decisions, Maintaining audit trails, Information access control	ISO 42001: 7.5
Continuous Improvement Lead	Analysis of lessons learned, Management of corrective actions, Design of preventive actions, Coordination of system updates	ISO 42001: 10.1, 10.2, 10.3

For how teams collaborate across functions, see **Annex A, Table A.1.**
For responsibility assignments across AIMS activities, see **Annex A, Table A.2.**

Clause-in-Cards

Context (Clause 4)

Before building an AIMS, it is important to map out the conditions under which your organisation operates. This requires looking outward at the environment around you, inward at your structures, and across the people affected by your systems.

1. Knowing Your organisation

Every organisation is influenced by elements that exist both within and outside the organisation:

- External elements encompass regional laws and regulations, competitor strategies, customer expectations regarding AI, environmental factors, etc.
- A company's internal factors consist of its established values and strategic goals, risk tolerance, its decision to create AI systems, purchase them or use them as part of its operations, etc.
- The organisational position you hold and your background and expertise shape your relationship with AI, as you may be developing AI systems or using them as a provider or consumer. Every position at the company has its own specific responsibilities.

2. Understanding Stakeholders

The wide range of individuals affected by AI includes employees and customers, as well as policy-makers, the general public, and individuals involved in data processing. The organisation needs to establish its essential interests first before selecting the most important ones to develop its response plan.

3. Determining the Scope of the AIMS

Defining boundaries for AI use within your organisation leads to better operational direction. The process involves determining which business sectors rely on AI, which systems will be integrated into AIMS, and which operations will remain outside of it. organisations achieve resource distribution effectiveness through boundary establishment, which also helps maintain consistent employee expectations across the entire organisation.

4. AIMS

Establishing, implementing, maintaining, continually documenting the AIMS in accordance with the standard.

X Corporation first considered its role in relation to the AI system. It was identified that the system needed to comply with GDPR rules and anti-discrimination regulations for its work with external businesses. The company grew quickly inside but struggled because it did not have enough staff to handle the workload. The organisation identified its essential stakeholders, along with their anticipated requirements. These included job candidates who sought privacy and fairness, the HR department needing fast and uniform processes, management teams seeking efficient operations, and society demanding ethical AI practices. The analysis shows that X Corporation established the boundaries of its AIMS. The AI system would begin evaluating candidates before human evaluators had completed their selection process. The research examined employee onboarding and training procedures, but did not include other HR activities, such as performance evaluations and payroll management. X Corporation ensured that all this information is formally documented.

Leadership (Clause 5)

The AI Management leadership system needs both transparent operational processes and dependable actions with established member conduct accountability. The organisation receives direction from management, which defines its principles and establishes clear roles for all members.

1. Demonstrating Leadership and Commitment

Top management needs to actively integrate AIMS. The organisation needs to provide essential resources while ensuring that AI governance aligns with the business strategy and fosters an environment that promotes ethical AI practices and continuous improvement by integrating the PDCA (plan-do-check-act) cycle.

2. Setting an AI Policy

The organisation requires an AI policy that should define its purpose and fundamental operational framework. The policy should outline the reasons for utilizing AI, along with the core values that guide its implementation, the methods for fulfilling legal obligations and regulatory requirements, and the expectations of stakeholders. The process of policy communication enables both internal and external groups to understand the established expectations.

3. Defining Roles, Responsibilities and Authorities

Leadership must distribute governance, operational, and oversight responsibilities to maintain clear accountability throughout all stages of AI development.

The implementation of specific roles leads to improved monitoring outcomes, uniform operational procedures, and increased trust in AI management systems.

The leadership at X Corporation implemented an AI-based hiring tool, made possible through their strategic decision. Senior management understood that adopting AI was not just a technical move but a strategic choice that required oversight. The CEO and executive team dedicated resources to project execution, ensuring the project supported the company's expansion objectives.

Top management approved an AI policy built on fairness, transparency, and accountability, communicated it to all departments, and committed to conducting regular management reviews to ensure the AIMS remained suitable, adequate, and effective.

The organisation developed an AI policy to manage the initiative through particular tool usage restrictions for pre-screening and ranking functions. Yet, HR managers retained complete authority and responsibility to make all hiring decisions. The policy established a framework based on fairness and transparency, which adhered to GDPR and anti-discrimination regulations, and communicated through both internal and external channels to foster trust. The organisation established formal roles and responsibilities, including HR managers for human oversight, compliance officers for regulatory monitoring, and internal auditors for implementation oversight. The framework established separate roles that created an accountable system, which led stakeholders to trust how AI was being used.

Planning (Clause 6)

An AIMS needs more than good intentions to operate effectively. Implementing responsible AI systems requires systematic planning to identify potential risks and opportunities, which allows for the creation of specific action plans and the establishment of measurable targets for AI deployment.

1. Acting on Risks and Opportunities

The first step in planning is to identify potential positive and negative outcomes. organisations should recognize the risks and opportunities that may impact their goals and determine the appropriate actions to take. These actions should be integrated into daily AIMS processes and regularly evaluated, such as on a monthly or quarterly basis.

Risk Criteria:

- Setting specific risk criteria through a basic likelihood and impact measurement system, categorizing risks as Low, Medium, and High.

- Set the rule: Low = accept; Medium = treat & monitor; High = escalate/avoid.
- Defining thresholds for stopping, escalating, or adding controls, and naming the owner who approves exceptions.

2. Running AI Risk Assessments

Risk assessment functions as an ongoing procedure that maintains its connection to the AI policy.

Per-Use Assessment:

- For each system or use-case, list the top risks (e.g., bias, safety, privacy) and who/what could be affected (people, processes, services).
- Score each risk using your standardized scoring system and record any applicable laws, regulations, or ethics guidelines.
- Ensure traceability by keeping a record of how each identified risk links to control objectives and mitigation actions.

3. Treating Risks

The assessment results should demonstrate the degree of control measures that organisations have implemented. The risk treatment plan requires documentation and management approval to become a final document. Any residual risk remaining after treatment has to be documented and accepted by the management.

Planning the treatment:

- The relevant parties should approve all risk management strategies, which include avoidance, mitigation, transfer, and acceptance.
- The list contains specific tasks that require identification of the required steps, their responsible owners, and achievement targets, as well as final deadlines.
- The controls for the identified risks may include implementing additional data verification processes and testing protocols, as well as human oversight and security protocols, user notification systems, and continuous monitoring systems.
- The system requires clear accountability, because it needs owners who should fulfill predetermined time requirements.
- The treatment plan is to be periodically reviewed.

4. Assessing AI Impacts

organisations need to assess how their AI systems affect human communities and their populations in addition to their impact on the wider social environment.

Conducting the assessment:

- Identify groups that would benefit from the change and those that might be negatively impacted, while also establishing protective measures.
- For each AI use case, identify top risks such as bias, privacy, or safety.
- Score risks using the agreed scale and link them to relevant laws or guidelines.
- Document results so they can inform decisions and next steps.

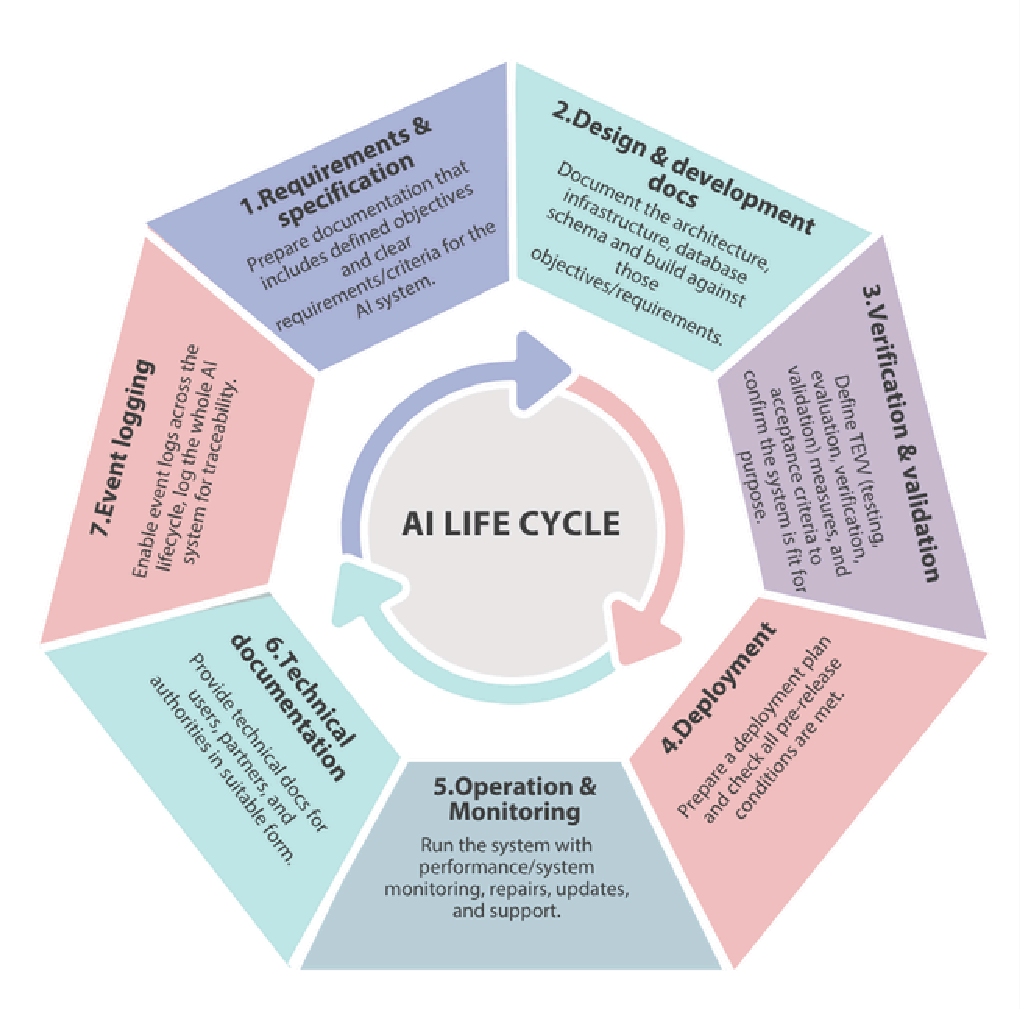
5. Setting Objectives and Planning for Change

Organisations need to establish measurable objectives that incorporate elements of accuracy, transparency, robustness, and security, aligning with their AI policy framework. Each objective needs to have a designated owner who will be responsible for its completion, along with defined timeframes and necessary resources. Objectives must be periodically reviewed to evaluate progress and effectiveness, as well as ensuring consistency with the outcomes of the risk and opportunity assessment.

Planning for Changes:

- Review all potential effects of the change before beginning the rollout process and getting required approvals.
- The team should track results as they work on backup plans and document all their actions.
- Share updates openly with stakeholders to ensure expectations remain aligned.
- The proposed changes are to be subjected to impact assessment and approval before implementation.
- After implementation, changes are to be reviewed in order to verify that objectives were achieved and no new unacceptable risks were introduced.

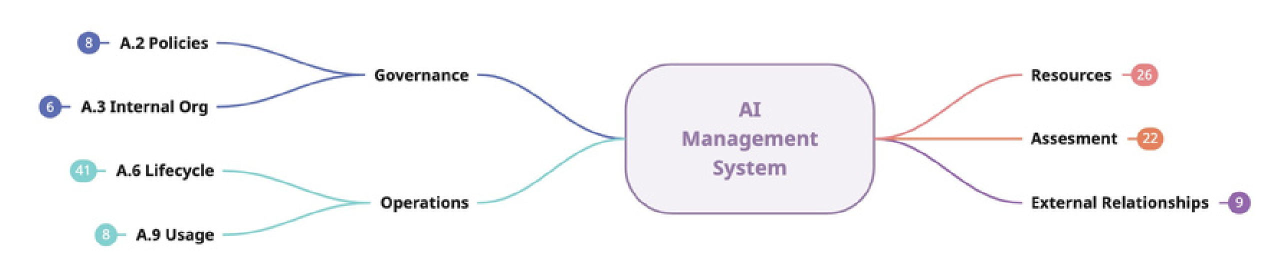
Figure 1. Building AI Lifecycle Checkpoints


1.Requirements & specification
Prepare documentation that includes defined objectives and clear requirements/criteria for the AI system.
2.Design & development docs
Document the architecture, infrastructure, database schema and build against those objectives/requirements.
3.Verification & validation
Define TEVV (testing, evaluation, verification, validation) measures, and acceptance criteria to confirm the system is fit for purpose.
4.Deployment
Prepare a deployment plan and check all pre-release conditions are met.
5.Operation & Monitoring
Run the system with performance/system monitoring, repairs, updates, and support.
6.Technical documentation
Provide technical docs for users, partners, and authorities in suitable form.
7.Event logging
Enable event logs across the lifecycle, log the whole AI system for traceability.
AI LIFE CYCLE

Management guidance: Set clear objectives for responsible AI and document both these goals and the supporting design and development processes.

Questions on data kind, type, structure, origin, evaluation, storage, and AI use: ***Annex B, Table B.1.*** Questions on intended use, technical approach, domain, autonomy level, and risk tier: ***Annex B, Table B.2.***

Figure 2. AI Management System



*Click **here** to view the mind map details dynamically or download the shapes by clicking on the nodes.*

The Product Manager and HR Lead defined the purpose of the HR tool as performing candidate screening and recommendation functions, but the organisation would make all final hiring decisions. The risk assessment system used a basic scoring system, which classified risks into three categories: Low = accept & monitor, Medium = check & monitor, and High = stop or fix. For instance, the practice of rejecting too many candidates from certain groups and exposing personal data falls under high-risk activities.

The Data Scientist and AI Evaluator conducted evaluations to determine potential risks related to bias, privacy, fairness, and accuracy. The Data Engineer/Steward was responsible for ensuring compliance with all personal data regulations. The Human Factors/UX Researcher ensured that candidates received clear explanations and access to appeal processes. The MLOps/Systems team built the infrastructure framework, implemented monitoring systems, and established a system shutdown capability.

The team established specific targets, which included achieving an accuracy rate of ≥85% while delivering transparent explanations for each recommendation, protecting data security, and resolving system problems within thirty minutes. The system underwent controlled management during changes, including job type additions and model retraining through approval processes and testing phases with rollback capabilities for resolving issues.

In addition to managing risks, the organisation identified opportunities for improvement such as enhancing explainability, improving user feedback mechanisms, and reducing decision latency. The organisation later documented them.

Support (Clause 7)

An AI Management System requires organisational support to achieve success. The organisation needs to dedicate resources and build skill sets while promoting awareness, maintaining proper communication, and ensuring accurate documentation practices. These resources should include human, technological, financial, and environmental components. The combination of these elements enables organisations to handle AI operations in a responsible and enduring manner.

1. Providing Resources

The AIMS requires dedicated personnel and technological resources, and financial support to establish and sustain its operations. The organisation needs to acquire specialized skills by hiring experts, purchasing necessary equipment and infrastructure, and allocating funds for employee development.

The organisation needs to conduct periodic resource assessments to maintain alignment with technological advancements and organisational requirements. Periodic resource assessments must be conducted in order to ensure adequacy and continual improvement, as well as maintaining alignment with technological advancements and organisational requirements.

2. Building Competence

AI management for responsible operations needs more than technical expertise. Staff members require knowledge of ethics, as well as risk management and governance principles. organisations should develop employee competence through training programs, mentoring sessions, workshops, and professional certification opportunities to ensure that persons doing work under the organisation's control are competent. Periodic evaluations of the effectiveness of these competence-building activities must be ensured.

3. Raising Awareness

All staff members should understand the AI policy, their specific duties, and the consequences of non-compliance with established requirements, as well as the AI objectives and the implications of non-conformity with the AIMS requirements of the organisation. The most effective way to sustain employee awareness involves continuous communication and practical guidance, along with periodic reminders, rather than relying solely on single, isolated training sessions.

4. Communicating Effectively

organisations should establish communication pathways to achieve successful internal and external information exchange. The organisation is to determine internal and external communications relevant to the AIMS, including what will be communicated, when, with whom, and how. The AIMS performance and AI initiatives should be reported to stakeholders through regular newsletters, meetings, and public updates. The practice of transparency helps organisations build trust with their stakeholders.

5. Maintaining Documentation

The organisation should provide simple access to all AIMS-related policies and procedures and maintain consistent updates of these documents. The organisation is to establish and maintain documented information required by the AIMS and the Standard. This documentation should be controlled to ensure accuracy, traceability, availability, and protection from unauthorized access or loss of integrity. A documented information management system helps maintain accurate and traceable data, which serves both internal teams and external review purposes. The organisation should implement version control and regular review processes to ensure documents remain current and reliable.

The management team dedicated funds for employee education while exploring a potential partnership with an outsourced AI ethics specialist, and they also upgraded their IT systems. The organisation provides AI policy training to all employees to enhance their understanding of the system. Competence evaluation was conducted periodically to confirm that personnel remained qualified and effective in their roles. The organisation offers internal guides that outline employee oversight responsibilities and establish notification procedures for potential system issues. The organisation maintains open communication by sending regular updates to both leadership personnel and all staff members. The X corporation utilizes email notifications, website disclaimers, and FAQs to inform external stakeholders, including clients, regulators, and job applicants. The X corporation employs a comprehensive document management system to track AI tool configurations, risk assessments, audit reports, and training logs.

Operation (Clause 8)

The approved plan should be followed by the team, with intervals determined, controls applied, changes managed, and records kept of what was done and the reasons behind it.

1. Executing the Plan

Processes need clear criteria so that controls can be applied consistently with the implementation of the controls defined in Clause 6 (Planning), and to verify that they are effective in practice:

- The measures defined during planning — such as data checks, testing, human oversight, and privacy and security safeguards — are implemented.
- Monitor the results and compare them with the previously agreed-upon acceptance levels.
- Decisions, along with both expected and unexpected outcomes, are captured to inform the next cycle.

2. Managing Work and Version

As AI systems evolve, visibility and consistency become increasingly important:

- Templates and simple tools help make risk assessments comparable across versions.
- Risks that support or hinder objectives should be identified, along with their potential impact on individuals, society, or the organisation.
- Assessing the risks and comparing them to established criteria and prioritizing the necessary treatments.
- Each release retains its evidence and approvals, ensuring traceability and accountability over time.

3. Monitoring & Re-checking Risks

Risks will evolve; reassess on a schedule and after significant changes:

- Applying the treatment plans and choosing one of the options (avoid, mitigate, transfer, accept) and reviewing them regularly, and after significant updates.
- Fairness, drift, and latency checks ensure the system remains within safe limits.
- Assessment plans are updated when models, data, or use cases evolve.
- Alerts and logs provide early signals when adjustments may be needed.

4. Impact Assessments & Evidence

Performing a formal AI system impact assessment to identify potential effects on individuals, groups, and society caused by the system's development, deployment, or use, explicitly considering the deployment context, intended purpose, and possible misuse:

- Impact reviews consider the context, purpose, and possible misuse of AI.
- These reviews are conducted regularly, particularly after significant changes, such as retraining or regulatory updates.
- Checklists or forms from established frameworks (OECD, EU AI Act, NIST AI RMF) help keep results consistent.
- Evidence, such as reports, approvals, metrics, and corrective actions, is maintained to ensure accountability remains traceable and clear.

The team started executing the Plan by performing all necessary steps to fulfill the requirements. The Data Engineer/Data Steward performed data collection and processing to gather the required information, creating the data inventory and conducting quality assessment tasks. The Data Scientist/ML Engineer operated the model while actively checking the system to verify both accuracy levels above 85% and fairness thresholds at 80% or higher.

The MLOps/Systems team developed an auditable, secure system that included immediate kill switch functionality and version rollback capabilities for resolving system problems. The AI Evaluator conducted scheduled tests to evaluate both system fairness and robustness levels. The system would trigger a project management tool ticket when thresholds failed to meet requirements, and the team could restore previous versions when needed. Improvements were initiated. The UX/Human-Factors lead verified that explanations and the appeal path functioned correctly during production operations.

After significant updates (e.g., adding a new role, retraining the model, or onboarding a new data source), the team conducted a brief risk assessment and impact assessment (using OECD/NIST/EU templates) and archived the evidence. All planned and unplanned changes were documented, including the person who made the change, the reason for the change, the decision made, and the outcome, ensuring the system remained traceable and auditable.

Performance Evaluation (Clause 9)

When the system is in operation, the organisation should ensure that the AIMS remains suitable, adequate, and effective. This evaluation integrates structured monitoring, periodic internal audits, and formal management reviews, all of which are supported by evidence and clear accountability.

1. Tracking and Evaluating Performance

Ongoing monitoring shows whether systems are meeting expectations:

- Focus areas include accuracy, fairness, latency, and user experience.
- Methods and tools should be consistent so results are comparable.
- Reviews are scheduled, and findings are measured against criteria and objectives.
- Reports, dashboards, alerts, and decisions are retained as evidence.

2. Conducting Internal Audits

Audits provide an independent view of how well the AIMS is working:

- Periodic audits confirm alignment with policies, documented requirements, and regulations.
- Each audit has clear objectives, scope, and criteria.
- Auditors must be impartial and not directly responsible for daily operations.
- Specialists such as data protection officers, HR staff, or external consultants can contribute to broader oversight.
- Results record strengths, nonconformities, and areas for improvement, with follow-up actions documented.

3. Reviewing Management Oversight

Top management evaluates the overall effectiveness of the AIMS at planned intervals:

- Inputs include monitoring data, audit results, regulatory changes, and stakeholder feedback.
- Outputs include policy updates, improvement actions, and resource allocation.
- Outcomes and new objectives are documented, with responsibilities clearly assigned.

As part of routine monitoring, X Corporation's hiring AI showed a drop in fairness, with the selection rate decreasing to 78%. Automated alerts flagged the issue, triggering an immediate investigation. An internal audit program was established to define audit frequency, scope, and auditor independence. In the quarterly internal audit, the Compliance and Quality Assurance team, independent of the development group, reviewed the system and found that drift detection thresholds had been set too high, allowing bias to pass unnoticed.

Audit findings, management review inputs, and corrective actions were documented and retained as evidence of conformity. At the subsequent management review, executives assessed the findings, directed resources to enhance monitoring tools, and mandated fairness testing before deployment. All evidence, corrective actions, and decisions were recorded, ensuring the process stayed transparent and traceable.

Improvement (Clause 10)

An AIMS cannot be treated as a fixed framework. Once systems are in use, they must evolve to remain suitable, adequate, and effective. This means learning from experience, correcting what goes wrong, and embedding improvements so issues do not repeat.

1. Driving Continual Improvement

Organisations should look for ways to strengthen their AIMS over time:

- New processes, safeguards, and tools can be adopted as they emerge.
- A culture of learning helps improvements spread across teams.
- Awareness of changes in policy, regulation, or user expectations ensures the system stays relevant.

2. Responding to Nonconformities

When things go wrong, a timely and structured response is necessary:

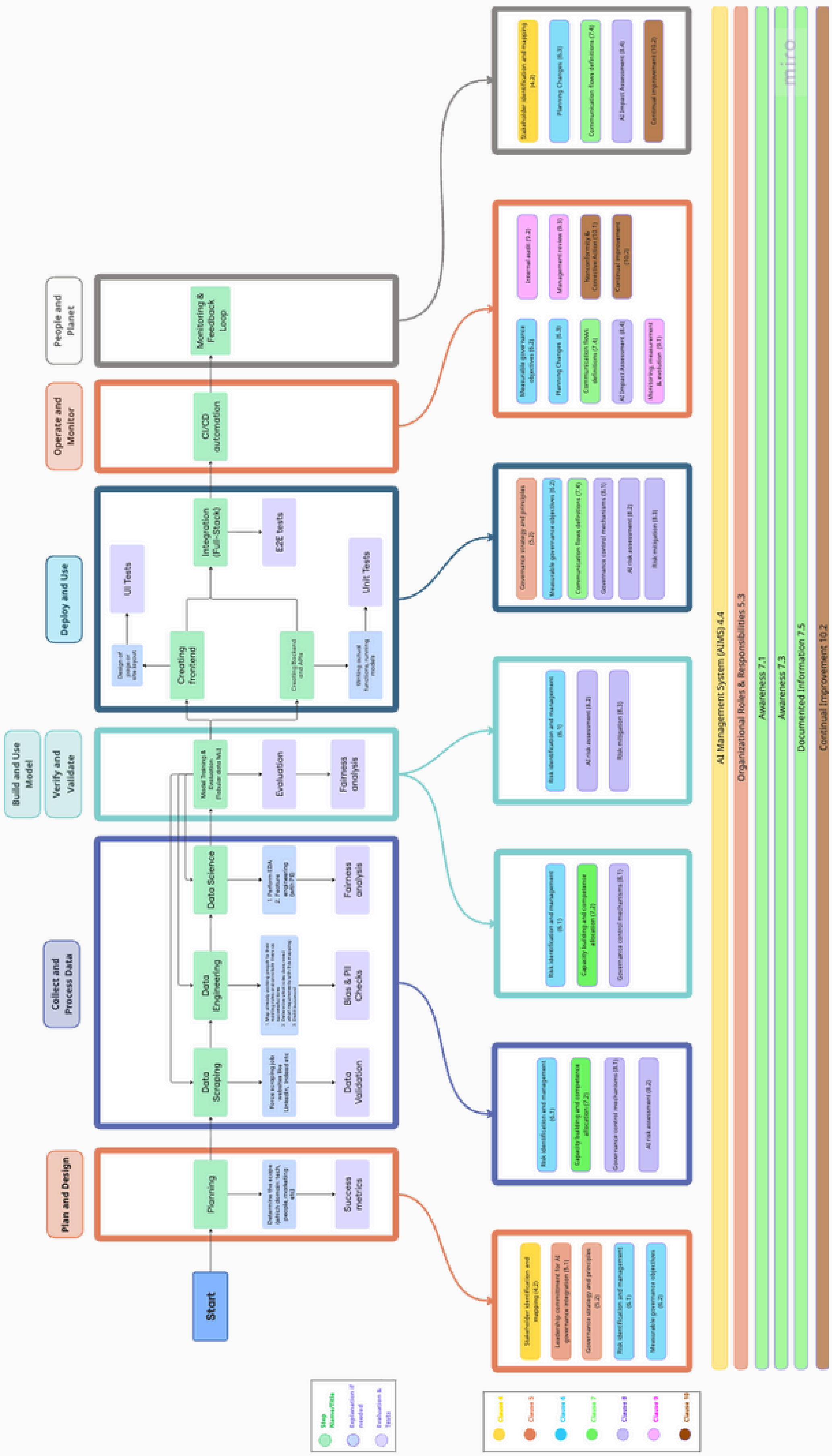
- **React:** Contain the issue quickly, correct it, and reduce any impact on those affected.
- **Evaluate:** Review what happened, why it occurred, and whether similar risks exist elsewhere.
- **Act:** Apply corrective measures, confirm their effectiveness, and update AIMS processes or controls as needed.
- **Record:** Keep clear evidence of the issue, the response, and the results to support accountability.

X Corporation’s R&D team found a new optimizer published in a peer-reviewed paper and tested its potential through small-scale experiments and an MVP model. Early results showed gains in accuracy, fairness, consistency, and stability under distribution shifts.

Based on these results, the Data Science Team retrained the hiring tool with the new optimizer and deployed the updated model to production. Post-deployment monitoring, led by the Quality Assurance (QA) Team, confirmed that candidate ranking accuracy increased from 82% to 91%, and fairness metrics remained within compliance thresholds.

The AI Governance Specialist documented the improvement in the AIMS records. The Risk Management Team scheduled quarterly reviews to track long-term performance and ensure sustained benefits. All corrective actions, evaluation outcomes, and continual-improvement records were retained as documented information.

Figure 3. AI Lifecycle Map


Start
Plan and Design
Planning
Determine the scope (which domain: tech, people, marketing etc)
Success metrics
Collect and Process Data
Data Scraping
Data Engineering
Data Science
Data Validation
Bias & PII Checks
Fairness analysis
1. Perform EDA 2. Feature engineering (with PII)
Build and Use Model
Verify and Validate
Model Training & Evaluation (Tabular data ML)
Evaluation
Fairness analysis
Deploy and Use
Creating frontend
Design of page or site layout
UI Tests
Creating Backend and APIs
Writing actual functions, running models
Unit Tests
Integration (Full-Stack)
E2E tests
Operate and Monitor
CI/CD automation
People and Planet
Monitoring & Feedback Loop
Stakeholder identification and mapping (4.2)
Leadership commitment for AI governance integration (5.1)
Governance strategy and principles (5.2)
Risk identification and management (6.1)
Measurable governance objectives (6.2)
Capacity building and competence allocation (7.2)
Governance control mechanisms (8.1)
AI risk assessment (8.2)
Risk mitigation (8.3)
Communication flows definitions (7.4)
Planning Changes (6.3)
AI Impact Assessment (8.4)
Monitoring, measurement & evaluation (9.1)
Internal audit (9.2)
Management review (9.3)
Nonconformity & Corrective Action (10.1)
Continual improvement (10.2)
AI Management System (AIMS) 4.4
Organizational Roles & Responsibilities 5.3
Awareness 7.1
Awareness 7.3
Documented Information 7.5
Continual Improvement 10.2
miro
Step Name/Title
Explanation if needed
Evaluation & Tests
Clause 4
Clause 5
Clause 6
Clause 7
Clause 8
Clause 9
Clause 10

*Click **here** to view the AI lifecycle map details dynamically or download.*

End-to-End Story of the Use Case

X Corporation aimed to hire 120 employees in six months to improve its customer service and field operations. However, manual screening led to delays and inconsistencies due to the average of 500 applications received each day. To address this challenge, the company purchased an AI-embedded HR tool that scans and ranks them by suitability. While this tool sought to expedite hiring, ensure fairness, and improve consistency, it also raised risks related to personal data, legal and ethical issues, and potential bias. Accordingly, X Corporation implemented an AIMS aligned with ISO/IEC 42001 standards. The organisation also defined the scope of the AIMS as limited to the pre-screening and ranking functions of its recruitment process, while documenting internal and external factors, relevant stakeholders and applicable legal frameworks.

The company limited the tool's scope to pre-screening and ranking, while keeping final hiring decisions in human hands. The company aligned with the applicable legal frameworks including the GDPR and anti-discrimination laws, defined clear stakeholder expectations, and excluded other HR functions from the scope. Leadership viewed the project as a strategic and technical initiative, providing resources and aligning it with the organisation's growth goals. Top management approved an AI policy emphasizing fairness, transparency, and accountability. The top management communicated it across departments and committed to periodic reviews. Roles were clearly defined; HR oversaw decisions, compliance ensured adherence to legal requirements, auditors monitored progress, and an AI policy reinforced fairness, transparency, and accountability.

In the planning phase, the team set risk levels and their scores, and reviewed risks such as bias, privacy, fairness, and accuracy, as well as personal data regulations. Meanwhile, the Human Factors ensured clear explanations and offered appeals. The MLOps team designed the infrastructure, monitoring systems, and kill switches. Careful change management was introduced for system updates.

In addition to managing risks, the organisation identified opportunities for improvement, such as enhanced explainability, improved user feedback mechanisms, and reduced decision latency. The organisation also included them in a document.

To support implementation, the company allocated budgets for staff training, improved IT infrastructure, and launched internal awareness and communication strategies. A document management system was introduced to track configurations, audits, risk assessments, and training logs, ensuring traceability.

Competence requirements were defined for staff taking part in AI operations. The effectiveness of trainings were periodically evaluated to verify that employees remained competent in their assigned roles.

During execution, data was processed and validated, models were implemented and monitored against thresholds, and fairness/robustness tests were conducted. Any breaches triggered alerts, tickets, and immediate fixes, while explanations and appeals were verified in production. Following significant updates, the team conducted risk assessments and documented the resulting changes.

During monitoring, the HR AI tool detected a decline in fairness, with the selection rate dropping to 78%. Automated alerts flagged the issue, and a review showed that bias detection thresholds were set too high. In response, management fine-tuned the monitoring tools and strengthened fairness testing. All actions and decisions were archived for accountability.

An internal audit program was established, which defined audit frequency, scope, and responsibilities. Auditors independent from daily operations reviewed the AIMS, and results were reported to top management. Management reviews incorporated audit results, stakeholder feedback, and regulatory changes.

Finally, X Corporation's R&D team developed a new optimizer, validated it in research and pilot testing, and retrained the hiring tool. After deployment, accuracy rose from 82% to 91%, and fairness levels returned to safe limits. The governance team documented the improvements and established quarterly reviews to ensure everything remained on track. All corrective actions, evaluation results, and continual improvement records were retained for purposes of evidence of conformity and accountability.

In conclusion, X corporation successfully integrated an AI hiring tool that boosted efficiency and fairness while ensuring accountability. By aligning with ISO/EIC 42001 and maintaining human oversight, evaluating competence, documenting opportunities, and performing audits and management reviews, the company built confidence and trust in its responsible use of AI.

Conclusion

The ISO 42001 standard provides a widely accepted, auditable framework for AI adoption goals of organisations, and our guide:

- Introduces ISO 42001 and AI Management System (AIMS)
- Translates the concepts, Clauses, and requirements of the ISO 42001 document into plain language, illustrating them through a detailed use case and diagrams.
- Lists relevant standards and frameworks and explains their relations.
- Defines the key roles necessary for implementing the standard.
- Introduces each Clause on a theoretical basis.
- Grounds each Clause in real-world applications by providing examples and types of tools that can be used, illustrated through a fictional case study of X Corporation's complete lifecycle steps in implementing an AI HR tool.
- Incorporates abundant tables and diagrams to ensure engagement and understandability.
- The document is easy to read and follow.
- The fictional story example of X Corporation draws an example for organisations and gives perspective on how applications of the principles of ISO 42001 can be applied in a real organisational context.

In today's ever-innovating world, adopting a reliable AIMS is essential for long-term success, enabling organisations to manage risks, build trust, and align AI with societal expectations. Still, as seen in the fictional case of X Corporation, negative connotations may arise, such as fines due to non-compliance, loss of stakeholder trust resulting from a security breach, or a violation of ethical and societal expectations. The ability to tackle these risks determines who thrives and who trails in the modern-day market.

Achieving reliability, accountability, and transparency is possible with the right mix of standards and frameworks. Getting compliant with ISO 420001 supports organisations to help withstand regulatory scrutiny and earn the trust of stakeholders and consumers.

This is also important for achieving a healthier and safer AI ecosystem and economy for the good of society. However, not all organisations have resources for compliance. At times, businesses lack access to sufficient resources for compliance under poor financial conditions, due to factors such as geopolitics, disability, and gender. To get to that fair point, there is a need for orientation towards trustworthy AI adoption.

Acknowledging the access gap, this guide aims to lead organisations in AI adoption and development. Our approach merges abstract Clauses with practical insights through examples. It is designed to be easily understood by any interested reader. Thus, organisations can have a better comprehension of ISO 42001 and be more adaptable in turning standards into action.

Annex

ANNEX A - Audience, Scope, and Roles

Table A.1 Cross-Role Collaboration Canvas

	Executive	Data	Design	Operation	Auditing
Executive					
Data					
Design					
Operation					
Auditing					

Legend: ● High collaboration | ◐ Medium collaboration | ○ Low/reporting relationship

Table A.2 RACI Canvas for Key AIMS Activities

Activity	Executive Sponsor	Governance Officer	Data Steward	AI Engineer	MLOps Engineer	Internal Auditor	Ethics Lead
AIMS Policy Development							
Risk Assessment							
Data Quality Management							
Deployment & Operations							
Performance Monitoring							
Internal Audit							
Incident Response							
Continuous Improvement							

RACI Legend: R = Responsible | A = Accountable | C = Consulted | I = Informed

ANNEX B - Planning (Clause 6)

Table B.1 Data for an AI System

Question	Potential Answers
What kind of data is being used?	Personal data (names, health records, financial info)? Non-personal data (sensor data, machine logs, public datasets)? Synthetic data (generated for training)?
What is the type of data?	Numeric, text, categorical, image, audio, video, time-series
What is the structure of the data?	structured/unstructured; CSV/JSON/Parquet schema/version

Where does it come from?	Internal systems (CRM, ERP, IoT sensors, transaction records)? External providers (third-party datasets, vendors)? Open data sources (government portals, public benchmarks)? User-generated content (social media, customer uploads)?
How is it evaluated?	Quality checks (completeness, accuracy, timeliness)? Bias detection (are some groups underrepresented)? Relevance (is the data fit for the AI's purpose)?
How is it stored and protected?	Cloud vs on-premise? Encryption, anonymization, or pseudonymization? Access controls (who can see/use the data)? Retention periods (how long is it kept)?
How is it used in AI systems?	Training data vs operational (real-time) data. Static datasets vs continuously updated data streams. Shared across multiple AI systems or dedicated?

Table B.2 Use of an AI System

Question	Potential Answers
What is the intended use?	e.g., "Assist agents by drafting email replies to customer tickets in English."
What technical approach does it follow?	Machine Learning, Deep Learning NLP, Computer Vision, Reinforcement Learning Generative AI (LLM, image) Rule/Expert-based
Which domain does it serve?	Customer support - HR/recruiting - Credit/risk Healthcare triage - Mobility/navigation - Fraud/security Retail/personalization - Manufacturing QA Public sector/social services - Education
What level of autonomy does it have?	Assistive (AI suggests; human decides) Augmentative (shared control; human approves) Autonomous (acts automatically with guardrails)
What risk tier does it fall under?	Minimal (good practices) Limited (transparency duties) High (full controls: risk management, data governance, logs, human oversight, accuracy/robustness/security) Prohibited (not allowed)

References

Ampcus Cyber. (2024). Understanding and Implementing ISO 42001 The AI Management System Standard. https://www.ampcuscyber.com/downloads/whitepaper/understanding-implementing-iso-42001-ai-management-system-standard.pdf

Cloud Security Alliance. (2024). AI Resilience: A Revolutionary Benchmarking Model for AI Safety. https://cloudsecurityalliance.org/artifacts/ai-resilience-a-revolutionary-benchmarking-model-for-ai-safety#

Coalfire. (2025). ISO IEC 42001 Readiness Assessment Checklist. https://assets.coalfire.com/prod/resources/Whitepapers/ISO-IEC-42001-Readiness-Assessment-Checklist.pdf

Deleram Golpayegani et al. (2024). AI Cards: Towards an Applied Framework for Machine-Readable AI and Risk Documentation Inspired by the EU AI Act. https://arxiv.org/abs/2406.18211

Deloitte. (2024). AI and Risk Management. https://www.deloitte.com/content/dam/assets-shared/legacy/docs/perspectives/2022/deloitte-gx-ai-and-risk-management.pdf

Eriksson et al.. (2025). AI Benchmarks Interdisciplinary Issues and Policy Considerations. https://publications.jrc.ec.europa.eu/repository/handle/JRC142931

ISO. (2023). ISO/IEC 42001:2023 Artificial Intelligence Management System. International organisation for Standardization Cloud Security Alliance. (2024). Using AI for Offensive Security. https://cloudsecurityalliance.org/artifacts/using-ai-for-offensive-security

Kimberly Lucy, Microsoft. (2025). Overview of ISO/IEC 42001 (AI Management System)and AI system conformity assessment. https://www.unido.org/sites/default/files/files/2025-07/Microsoft%20-%20Overview%20of%20ISO%20IEC%2042001.pdf

KPMG. (2025). ISO/IEC 42001 Certification: Global Standard for AI Management Systems (AIMS). https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/ISOIEC-42001-certification.pdf.coredownload.inline.pdf

Lorenzo Ricciardi Celsi, and Albert Y. Zomaya. (2025). Perspectives on Managing AI Ethics in the Digital Age. https://www.mdpi.com/2078-2489/16/4/318

Mohammed Bahja, Noureddin Sadawi, Amir Shurrab, Zahra Alhabsi. (2025). NEXUS and ISO 42001: Building Robust Governance for Responsible Enterprise AI. https://www.researchgate.net/publication/396463851_NEXUS_and_ISO_42001_Building_Robust_Governance_for_Responsible_Enterprise_AI

NIST (Tabassi et al., 2023). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). https://www.nist.gov/publications/artificial-intelligence-risk-management-framework-ai-rmf-10

OECD (2022), OECD Framework for the Classification of AI systems. *OECD Digital Economy Papers*, No. 323, OECD Publishing, Paris, https://doi.org/10.1787/cb6d9eca-en

Sensiba. (2024). ISO/IEC 42001:2023 Readiness Guide. https://sensiba.com/resources/white-papers/iso-iec-420012023-readiness-checklist/

Sid Ahmed Benraouane. (2024). AI Management System Certification According to the ISO/IEC 42001 Standard: How to Audit, Certify, and Build Responsible AI Systems. https://doi.org/10.4324/9781003463979

Serdar Biroğul, Özkan Şahin, Hüseyn Əsgərli. (2025). Exploring the Impact of ISO/IEC 42001:2023 AI Management Standard on organisational Practices. DOI:10.54569/aair.1709628

Standards Australia & CSIRO- National AI Center. (2024). Guide for Australian Business: Understanding 42001 AS ISO/IEC 42001:2023, Information Technology – Artificial Intelligence- Management System. https://www.standards.org.au/documents/understanding-42001-ai-management-system-standard-whitepaper

Standart Fusion. (2024). THE ISO 42001 Compliance Checklist. https://www.standardfusion.com/learnings/iso-42001-interactive-checklist

The Alan Turing Institute. (2025). AI Skills for Business Competency Framework https://www.turing.ac.uk/skills/collaborate/ai-skills-business-framework

Tamas Szadeczky, Zsolt Bederna. (2025). Risk, regulation, and governance: evaluating artificial intelligence across diverse application scenarios. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/103308

Thippa Reddy Gadekallu et al. (2025). Framework, Standards, Applications and Best Practices of Responsible AI: A Comprehensive Survey. https://arxiv.org/abs/2504.13979

Vanta-A-lign. (2025). The ISO 42001 Compliance Checklist. https://www.vanta.com/downloads/the-iso-42001-compliance-checklist

Vector Institute. (2025). Principles in Action: A Playbook for Responsible AI Product Development [PDF Report]. Vector Institute. https://principlesinaction.vectorinstitute.ai/files/Playbook.pdf

World Economic Forum. (2024). Responsible AI Playbook for Investors. World Economic Forum. https://www.weforum.org/publications/responsible-ai-playbook-for-investors/

World Economic Forum. (2025). WEF - Future of Jobs Report 2025. https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf

World Economic Forum. (2024). AI Value Alignment: Guiding Artificial Intelligence Towards Shared Human Goals. World Economic Forum. https://www3.weforum.org/docs/WEF_AI_Value_Alignment_2024.pdf

Contact us!

Thank you for reading this research and opinion report. If you have any questions or would like to discuss our findings further, please don't hesitate to contact us.

☎ +44 7400715479
✉ info@huxai.tech
➤ huxai.tech