



ELEVATE

ISO 42001 Audit-Ready AIMS Manual

Your AI Management System, end-to-end: scope, governance, risk, controls, and continuous improvement; built the way auditors expect.

CONTENT

Overview.....	3
Organization Context.....	5
Leadership	8
Planning.....	10
Support	14
Operation.....	17
Performance Evaluation.....	19
Management Review	21
Improvement.....	23
Source.....	25



ISO 42001 Audit-Ready AIMS Manual

Overview

Introduces the AIMS purpose, scope, and commitment to responsible AI.

Overview

The organization provides (or uses) Artificial Intelligence (AI) systems and is required to establish, implement, maintain, and continually improve an AI Management System (AIMS). This AIMS Policy is intended to assist the organization in developing, providing, and using AI systems in a responsible manner to pursue the organization's objectives, meet requirements, comply with obligations (such as regulatory, customers, and other interested parties), and to meet expectations.



Artificial Intelligence Management System Policy

Organization Context

Defines the context, scope, and interested parties of the AIMS.

Organization Context

Understanding the Organization and Its Context

The organization will determine external/internal issues relevant to the organization's purpose and impact the ability to achieve intended AIMS results. The organization will determine if climate change is a relevant issue. The intended purposes of the AI systems developed, provided, or used by the organization will be considered. The organization's roles with respect to AI systems will be determined.

Interested Parties' Needs/Expectations

The organization will determine the interested parties relevant to the AIMS, the interested parties' relevant requirements, and which requirements will be addressed through the AIMS.

Scope of the AIMS

AIMS' boundaries and applicability will be determined to establish the AIMS' scope. The organization will consider external and internal issues as well as related requirements.

The scope of the AIMS will be documented. The scope of the AI management system will determine the organization's activities with respect to this document's requirements on the AI management system, leadership, planning, support, operation, performance, evaluation, improvement, controls and objectives.

- Description of the organizational boundaries with documented justification of exceptions
 - o key process
 - o department(s)
 - o whole organization
 - o organization stakeholders
- Description of organizational structure (including AIMS)
- Identification of AI-related business processes and information assets with owners)
- Identification of the 'decision-making direction and processes'
- Description of information system boundaries in terms of:
 - o Network (internal, wireless, etc.)
 - o Operating systems (windows, linux, etc)
 - o Applications (CRM, software management, ERP, utilities, database)
 - o Database (customer records, medical data, research/development, etc.)

- o Processes: information transport, storage, processing
 - o Telecom (routers, firewalls, etc)
- Description of physical locations (internal/external) and physical infrastructure

Scope Statement

[Define scope of AIMS for appropriate size, nature, and complexity; available to interested parties.
Should be: simple; understandable; precise]

AI Management System (AIMS)

The organization will establish, implement, maintain, continually improve, and document an AI Management System (AIMS) including required processes and interactions according to the ISO 42001 standard.



Artificial Intelligence Management System Policy

Leadership

Establishes governance, responsibilities, and leadership commitment.

Leadership

Leadership and Commitment

Executive management will demonstrate leadership and commitment with respect to the AIMS by:

- ensuring the AI Governance policy and AI objectives are established as well as compatible with the organization's strategic direction;
- ensuring the AIMS requirements are integrated into the organization's business processes;
- ensuring required AIMS resources are available;
- communicating importance of AIMS effectiveness and conforming with the AIMS requirements;
- ensuring the AIMS achieves its intended results;
- directing and supporting persons contributing to AIMS effectiveness;
- promoting continual improvement; and
- supporting other relevant roles demonstrating leadership as it applies to their areas of responsibility.

AI Governance Policy

Executive management will establish an AI Governance Policy appropriate to the organization's purpose, provides a framework for setting AI objectives, includes a commitment to meet applicable requirements, and includes a commitment to continually improve the AIMS. The AI Governance Policy will be documented, relevant to other policies, communicated, and available to interested parties, as appropriate. Controls and control objectives will be established related to the AI Governance Policy.

Roles, Responsibilities and Authorities

Executive Management will ensure responsibilities and authorities for relevant roles are assigned and communicated within the organization. Executive Management will assign responsibility and authority to ensure the AIMS conforms to the ISO 42001 standard (and related policies) and report on the performance of the AIMS to executive management.



Artificial Intelligence Management System Policy

Planning

Identifies risks, impacts, and objectives for responsible AI management.

Planning

Actions to Address Risks and Opportunities

The organization will consider issues and requirements when planning for the AIMS as well as determine the risks/opportunities needing to be addressed to give assurance the AIMS achieves intended results, prevent/reduce undesired effects, and achieve continual improvement. The organization will establish and maintain AI risk criteria to support the ability to distinguish between acceptable and non-acceptable risks, perform AI risk assessments, conduct AI risk treatment, and assess AI risk impacts.

AI Risk Assessment

The organization will define and establish an AI risk assessment process informed by and aligned with AI policies and objectives. The AI risk assessment process will be designed to ensure repeated AI risk assessments can produce consistent, valid, and comparable results. The AI risk assessment process will identify risks to aid in (or prevent) achieving AI objectives. AI risks will be analyzed to assess the potential consequences to the organization, individuals, and societies if the risks were to materialize. AI risks will be analyzed to assess, where applicable, the realistic likelihood of the risks and to determine the levels of risk. The AI risk assessment process will evaluate the AI risks to compare the results of the risk analysis with the risk criteria and prioritize the assessed risks for risk treatment. The organization will retain documentation about the AI risk assessment process.

AI Risk Treatment

Taking the risk assessment results into account, the organization will define an AI risk treatment process to:

- select appropriate AI risk treatment options;
- determine controls necessary to implement the AI risk treatment options chosen and compare the controls with those in ISO 42001 Annex A to verify no necessary controls are omitted;
- consider the controls from ISO 42001 Annex A relevant to the implementation of the AI risk treatment options;
- identify additional controls necessary (beyond those in ISO 42001 Annex A) to implement all risk treatment options;
- consider ISO 42001 Annex B guidance to implement necessary controls;
- produce a statement of applicability (SoA) containing the necessary controls and provide justification for inclusion/exclusion of the controls [Note: Justification for exclusion can include where the controls are not deemed necessary by the risk assessment and

where they are not required by (or are subject to exceptions under) applicable external requirements.]; and

- formulate an AI risk treatment plan.

Designated management must approve the AI risk treatment plan and any acceptance of residual AI risks. Necessary controls will be aligned to objectives, available as documentation, communicated within the organization, and made available to interested parties as appropriate. The organization will retain documentation about the AI risk treatment process.

AI System Impact Assessment

The organization will define a process to assess the potential consequences for individuals/groups/both and societies resulting from the development, provision, or use of AI systems. The organization will determine the potential consequence of an AI system's deployment, intended use, and foreseeable misuse on individuals/groups/both and societies by performing an AI system impact assessment. The AI system impact assessment will take into account specific technical and societal context where the AI system is deployed along with applicable jurisdictions. The organization will document the results of the AI system impact assessment. Where appropriate, the results of the AI system impact assessment will be made available to relevant interested parties defined by the organization. The organization will consider the results of the AI system impact assessment within the risk assessment process.

AI Objectives and Planning

The organization will establish AI objectives at relevant functions and levels. The AI objectives will be consistent with the AI policy, measurable (if practicable), take into account applicable requirements, monitored, communicated, updated as appropriate, and available as documentation. The organization will determine what will be done, what resources are required, who is responsible, when objectives will be completed, and how results are evaluated when planning on how to achieve the organization's AI objectives.

AIMS Objectives

- To ensure responsible AI use, the AIMS will comply with regulatory and contractual requirements as well as foster a culture of AI ethics/compliance throughout the organization to ensure responsible AI practices across the entire organization.
- To mitigate risks/liabilities, the organization will demonstrate due diligence in AI system design/operation along with continuous monitoring/assessments of AI system performance/behavior making adjustments in order to maintain high standards of reliability/integrity.
- The AIMS will inspire confidence among stakeholders related to AI system reliability and ethical use by promoting responsible AI innovation/development along with adhering to

ethical AI principles/guidance.

- To minimize potential impact of AI system failures (or security breaches), the AIMS will enhance the organization's response to AI-related incidents in order to reduce costs (including legal, finance, and reputational costs).

Planning for Changes

When the organization determines the need for changes to the AIMS, the changes will be carried out in a planned manner.



Artificial Intelligence Management System Policy

Support

Ensures resources, competence, communication, and document control.

Support

Resources

The organization will determine and provide the resources needed for the establishment, implementation, maintenance, and continual improvement of the AIMS.

Competence

The organization will determine the necessary competence of person(s) doing work under its control impacting AI performance. The organization will ensure persons are competent on the basis of appropriate education, training, or experience. Where applicable, the organization will take actions to acquire the necessary competence and evaluate the effectiveness of actions taken. The organization will make available appropriate documentation as evidence of competence.

Awareness

The organization will ensure persons under its control will be made aware of the AI Governance Policy, their contribution to the effectiveness of the AIMS (including the benefits of improved AI performance), and the implications of not conforming to the AIMS requirements.

Communication

The organization will determine the internal/external communications relevant to the AIMS including: what the AIMS will communicate; when to communicate; with whom to communicate; and how to communicate.

Documentation

The organization's AIMS will include documentation required by the AIMS policy and documentation determined by the organization to be necessary for the effectiveness of the AIMS.

Creating and Updating Documentation

When creating and updating documentation, the organization will ensure appropriate identification and description of the documentation such as title, date, author, or reference number. Documentation will be maintained in an appropriate format considering language, software version, graphics, and media (such as paper or electronic form). Documentation will be reviewed and approved for suitability and adequacy.

Control of Documentation

Documentation required by the AIMS and by this policy will be controlled to ensure it is available (and suitable) for use (where and when needed) and it is adequately protected (from loss of confidentiality, improper use, or loss of integrity). To control documentation, the organization will address the following activities (as applicable): distribution, access, retrieval, and use; storage and preservation (including preservation of legibility); control of changes (such as version control); and retention and disposition. Documentation of external origin determined to be necessary for the planning and operation of the AIMS will be identified as appropriate and controlled.



Artificial Intelligence Management System Policy

Operation

Controls AI system operations and lifecycle activities.

Operation

Operational Planning and Control

The organization will plan, implement, and control the processes needed to meet requirements and implement necessary actions by establishing criteria for the processes along with implementing controls over the processes according to the criteria. The organization will implement determined controls related to the operation of the AIMS (such as AI system development and usage lifecycle related controls). The effectiveness of these controls will be monitored and corrective actions will be considered if intended results are not achieved. Documentation will be available to the necessary extent to ensure confidence of the processes have been carried out as planned. The organization will control planned changes and review the consequences of unintended changes. The organization will take action to mitigate any adverse effects, as necessary. The organization will ensure externally provided processes, products, or services relevant to the AIMS are controlled.

AI Risk Assessment

The organization will perform AI risk assessments according to this policy and at planned intervals (or when significant changes are proposed or occur). The organization will retain documentation of the results of all AI risk assessments.

AI Risk Treatment

The organization will implement the AI risk treatment plan according to this policy and verify its effectiveness. When risk assessments identify new risks requiring treatment, the risk treatment process will be performed for these risks. If risk treatment options defined by the risk treatment plan are not effective, these treatment options will be reviewed and revalidated following the risk treatment process and the risk treatment plan will be updated. The organization will retain documentation of the results of all AI risk treatments.

AI System Impact Assessment

The organization will perform AI system impact assessments according to this policy and at planned intervals (or when significant changes are proposed to occur). The organization will retain documentation of the results of the AI system impact assessments.



Artificial Intelligence Management System Policy

Performance Evaluation

Monitors, audits, and evaluates AIMS effectiveness and performance.

Performance Evaluation

Monitoring, Measurement, Analysis, and Evaluation

The organization will determine the following related to performance evaluation:

- what needs to be monitored and measured;
- the methods of monitoring, measurement, analysis, and evaluation, as applicable, to ensure valid results;
- when the monitoring and measuring will be performed; and
- when the results from monitoring/measurement will be analyzed/evaluated.

Documentation will be maintained and available as evidence of the results. The organization will evaluate the performance and the effectiveness of the AIMS.

Internal Audit

The organization will conduct internal audits at planned intervals to provide information on whether the AIMS conforms to the organization's own AIMS requirements, the requirements of the ISO 42001 standard, and the AIMS is effectively implement as well as maintained.

Internal Audit Program

The organization will plan, establish, implement, and maintain an audit program to include frequency, methods, responsibilities, planning requirements, and reporting. When establishing the internal audit program, the organization will consider the importance of the processes concerned and the results of previous audits. The organization will define the audit objectives, criteria, and scope of each audit. The organization will select auditors and conduct audits to ensure objectivity as well as impartiality of the audit process. The organization will ensure results of the audits are reported to relevant managers. Documentation will be made available as evidence of the implementation of the audit program along with the audit results.



Artificial Intelligence Management System Policy

Management Review

Reviews the AIMS to ensure suitability, effectiveness, and improvement.

Management Review

Executive management will review the organization's AIMS at planned intervals to ensure the AIMS continues to be suitable, adequate, and effective.

Management Review Inputs

Management reviews will include the following:

- the status of actions from previous management reviews;
- changes in external/internal issues relevant to the AIMS;
- changes in needs/expectations of interested parties relevant to the AIMS;
- information on the AIMS performance, including trends in:
 - o nonconformities and corrective actions;
 - o monitoring and measurement results;
 - o audit results; and
 - o opportunities for continual improvement.

Management Review Results

The results of the management review will include decisions related to continual improvement opportunities along with any need for changes to the AIMS. Documentation will be made available as evidence of the results of management reviews.



Artificial Intelligence Management System Policy

Improvement

Addresses nonconformities and drives continual AIMS improvement.

Improvement

Continual Improvement

The organization will continually improve the suitability, adequacy, and effectiveness of the AIMS

Nonconformity and Corrective Action

When a nonconformity occurs, the organization will:

- *react to the nonconformity and as applicable: take action to control and correct it and/or deal with the consequences;
- evaluate the need for action to eliminate the cause(s) of the nonconformity to ensure it does not recur (or occur elsewhere), by:
 - o reviewing the nonconformity;
 - o determining the causes of the nonconformity;
 - o determining if similar nonconformities exist (or can potentially occur);
 - o implement any action needed;
 - o review the effectiveness of any corrective action taken; and
 - o make changes to the AIMS, if necessary.

Corrective actions will be appropriate to the effects of the nonconformities encountered. Documentation will be made available as evidence of the nature of the nonconformities (and any subsequent actions taken) along with the results of any corrective action.



Artificial Intelligence Management System Policy

Source

Lists applicable standards, regulations, and reference documents.

Sources:

EU AI Act

ISO 9001: QMS

ISO 27001: ISMS

ISO 27701: PIMS

ISO/IEC 22989:2022, Information technology — Artificial intelligence — Artificial intelligence concepts and terminology

ISO 42001: AIMS



Secure Your Compliance.
Secure the Contract.

Get Audit Ready for your next big deal.

We don't just provide templates; our team of experienced experts and auditors brings the deep regulatory knowledge needed to turn these pages into a passing audit score and your next big contract.

www.elevateconsult.com cmmc@elevateconsult.com +1 888 601 5351