ISO 42001 Artificial intelligence — Management system

Approval List

If the document is approved in an electronic system, indicate “Signed in <system>” in the Signature field and “NA” in the date field.

Department / Function	**Name**	**Signature**	**Date**
AI Governance Manager			YYYY-MM-DD
AI Chief Technical Officer			YYYY-MM-DD

Revision History

Rev	Description of Change	Author	Revision Date
1	Initial Release.		YYYY-MM-DD

Table of Contents

1 SCOPE

This document specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving an AI (artificial intelligence) management system within the context of an organization.

This document is intended for use by an organization providing or using products or services that utilize AI systems. This document is intended to help the organization develop, provide or use AI systems responsibly in pursuing its objectives and meet applicable requirements, obligations related to interested parties and expectations from them.

This document is applicable to any organization, regardless of size, type and nature, that provides or uses products or services that utilize AI systems.

2 NORMATIVE REFERENCES

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 TERMS AND DEFINITIONS

For the purposes of this document, the terms and definitions given in ISO/IEC 22989 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1 organization

person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (3.6)

Note 1 to entry: The concept of organization includes, but is not limited to, sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution or part or combination thereof, whether incorporated or not, public or private.

Note 2 to entry: If the organization is part of a larger entity, the term “organization” refers only to the part of the larger entity that is within the scope of the AI management system (3.4).

3.2 interested party

person or organization (3.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity

Note 1 to entry: An overview of interested parties in AI is provided in ISO/IEC 22989:2022, 5.19.

3.3 top management
person or group of people who directs and controls an organization (3.1) at the highest level

Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization.

Note 2 to entry: If the scope of the management system (3.4) covers only part of an organization, then top management refers to those who direct and control that part of the organization.

3.4 management system
set of interrelated or interacting elements of an organization (3.1) to establish policies (3.5) and

objectives (3.6), as well as processes (3.8) to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines.

Note 2 to entry: The management system elements include the organization's structure, roles and responsibilities, planning and operation.

3.5 policy
intentions and direction of an organization (3.1) as formally expressed by its top management (3.3)

3.6 objective
result to be achieved

Note 1 to entry: An objective can be strategic, tactical, or operational.

Note 2 to entry: Objectives can relate to different disciplines (such as finance, health and safety, and environment). They can be, for example, organization-wide or specific to a project, product or process (3.8).

Note 3 to entry: An objective can be expressed in other ways, e.g. as an intended result, as a purpose, as an operational criterion, as an AI objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

Note 4 to entry: In the context of AI management systems (3.4), AI objectives are set by the organization (3.1), consistent with the AI policy (3.5), to achieve specific results.

3.7 risk
effect of uncertainty

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

The organization shall implement the controls determined according to 6.1.3 that are related to the operation of the AI management system (e.g. AI system development and usage life cycle related controls).

The effectiveness of these controls shall be monitored and corrective actions shall be considered if the intended results are not achieved. Annex A lists reference controls and Annex B provides implementation guidance for them.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the AI management system are controlled.

8.2 AI risk assessment

The organization shall perform AI risk assessments in accordance with 6.1.2 at planned intervals or when significant changes are proposed or occur.

The organization shall retain documented information of the results of all AI risk assessments.

8.3 AI risk treatment

The organization shall implement the AI risk treatment plan according to 6.1.3 and verify its effectiveness.

When risk assessments identify new risks that require treatment, a risk treatment process in accordance with 6.1.3 shall be performed for these risks.

When risk treatment options as defined by the risk treatment plan are not effective, these treatment options shall be reviewed and revalidated following the risk treatment process according to 6.1.3 and the risk treatment plan shall be updated.

The organization shall retain documented information of the results of all AI risk treatments.

8.4 AI system impact assessment

The organization shall perform AI system impact assessments according to 6.1.4 at planned intervals or when significant changes are proposed to occur.

The organization shall retain documented information of the results of all AI system impact assessments.

9 PERFORMANCE EVALUATION

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

— what needs to be monitored and measured;

— the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

— when the monitoring and measuring shall be performed;

— when the results from monitoring and measurement shall be analysed and evaluated.

Documented information shall be available as evidence of the results.

The organization shall evaluate the performance and the effectiveness of the AI management system.

9.2 Internal audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the AI management system:

a) conforms to:

1) the organization’s own requirements for its AI management system;

2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

The organization shall:

a) define the audit objectives, criteria and scope for each audit;

b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

c) ensure that the results of audits are reported to relevant managers.

a) react to the nonconformity and as applicable:

1) take action to control and correct it;

2) deal with the consequences;

b) evaluate the need for action to eliminate the cause(s) of the nonconformity, so that it does not recur or occur elsewhere, by:

1) reviewing the nonconformity;

2) determining the causes of the nonconformity;

3) determining if similar nonconformities exist or can potentially occur;

c) implement any action needed;

d) review the effectiveness of any corrective action taken;

e) make changes to the AI management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered. Documented information shall be available as evidence of:

— the nature of the nonconformities and any subsequent actions taken;

— the results of any corrective action.

Form AI Machine Learning

1. Purpose

To establish a standardized procedure for managing machine learning frameworks in compliance with ISO/IEC 23053. This procedure ensures AI/ML systems are developed, validated, deployed, and maintained using structured framework processes that address transparency, robustness, reproducibility, and accountability.

2. Scope

This procedure applies to all AI/ML projects, including supervised, unsupervised, and reinforcement learning models, where standardized frameworks and lifecycle management processes are required.

3. Responsibilities

- ML Framework Architect: Defines the ML framework architecture and ensures alignment with ISO/IEC 23053.

- Data Science Team: Implements ML pipelines in accordance with framework requirements.

- Quality Assurance (QA): Ensures reproducibility, traceability, and compliance testing of ML workflows.

- IT Operations: Supports deployment environments, resource allocation, and monitoring.

- Regulatory Affairs: Ensures framework use complies with applicable laws, standards, and regulations.

4. Procedure Steps

Step No.	Activity	Description	Responsible	Frequency	Records
1	Framework Definition	Define ML framework components (data pipeline, model training, evaluation, deployment).	ML Framework Architect	Initial + Updates	Framework Definition Document

2	Pipeline Standardization	Standardize ML workflows for data preparation, model training, validation, and deployment.	Data Science Team	Per Project	Pipeline Specification Document
3	Reproducibility Assurance	Ensure reproducibility of experiments through version control, configuration management, and logging.	QA	Continuous	Reproducibility Reports
4	Validation & Testing	Perform framework-based validation, testing for accuracy, fairness, robustness, and safety.	QA + Data Science Team	Per Release	Validation Reports
5	Deployment Compliance	Ensure framework integrates with secure, monitored production environments.	IT Ops	Per Deployment	Deployment Records

6	Monitoring & Feedback	Continuously monitor ML system performance and log anomalies for retraining or corrective action.	IT Ops + Data Science	Real-time	Monitoring Logs
7	Corrective / Preventive Actions (CAPA)	If framework deficiencies are found, initiate CAPA according to QMS.	QA	As Needed	CAPA Records
8	Approval & Release	Document framework compliance review and authorize continued use.	Regulatory Affairs + QA	As Needed	Approval Record

5. Records & Forms

- Framework Definition Document
- Pipeline Specification Document
- Reproducibility Reports
- Validation Reports
- Deployment Records
- Monitoring Logs
- CAPA Records
- Approval Sign-Off Sheet

6. References

ISO/IEC 23053:2022 – Framework for AI Systems Using Machine Learning

ISO/IEC 22989:2022 – AI Concepts and Terminology

ISO/IEC 5338:2023 – AI System Life Cycle Processes

ISO/IEC 23894:2023 – AI Risk Management

Form <Name>

Approval List

If the document is approved in an electronic system, indicate “Signed in <system>” in the Signature field and “NA” in the date field.

Department / Function	Name	Signature	Date
Quality Assurance Manager			YYYY-MM-DD
Management Representative			YYYY-MM-DD

Revision History

Rev	Description of Change	Author	Revision Date
1	Initial Release.		YYYY-MM-DD

Delete this page as content is added to the document.

Form AI Data Bias & Data Integrity Checks (ISO24027)

1. Purpose

To ensure that AI/ML systems maintain data integrity and minimize risks of bias in compliance with ISO/IEC 24027. This procedure defines controls for identifying, monitoring, and mitigating data-related risks to safeguard fairness, safety, and reliability.

2. Scope

Applies to all datasets used in the training, testing, validation, and monitoring of AI/ML-enabled products. This includes supervised, unsupervised, and reinforcement learning applications where data quality and fairness are critical.

3. Responsibilities

- Data Science Team: Conducts data integrity checks and bias assessments.

- Quality Assurance (QA): Ensures adherence to ISO/IEC 24027 requirements and maintains audit records.

- AI Ethics Officer: Reviews data bias findings, recommends corrective measures.

- IT Operations: Implements secure data storage, access control, and logging mechanisms.

- Regulatory Affairs: Ensures compliance with data governance, legal, and ethical standards.

4. Procedure Steps

Step No.	Activity	Description	Responsible	Frequency	Records
1	Data Collection Integrity	Verify authenticity, traceability, and secure sourcing of all data collected.	Data Science Team	Per Dataset	Data Source Integrity Report
2	Bias Identification	Apply statistical and algorithmic fairness metrics to detect bias	Data Science Team	Quarterly	Bias Detection Report

		across sensitive attributes.			
3	Bias Mitigation	Implement re-sampling, re-weighting, or algorithmic adjustments to reduce detected bias.	AI Ethics Officer	As Needed	Bias Mitigation Log
4	Data Integrity Validation	Check datasets for missing values, anomalies, and adversarial manipulations.	QA	Per Update	Data Integrity Validation Report
5	Monitoring in Production	Continuously monitor model outputs for evidence of bias or data drift.	IT Ops + Data Science	Real-time	Monitoring Logs
6	Corrective / Preventive Actions (CAPA)	Initiate CAPA process if data integrity or bias issues exceed acceptable thresholds.	QA	As Needed	CAPA Records
7	Approval & Release	Document review of findings, approve continued data usage, or reject compromised data.	Regulatory Affairs + QA	As Needed	Approval Record

5. Records & Forms

- Data Source Integrity Report

- Bias Detection Report

- Bias Mitigation Log

- Data Integrity Validation Report

- Monitoring Logs

- CAPA Records

- Approval Sign-Off Sheet

6. References

ISO/IEC 24027:2021 – Assessment of the Robustness of Neural Networks

ISO/IEC 22989:2022 – AI Concepts and Terminology

ISO/IEC 5338:2023 – AI System Life Cycle Processes

ISO/IEC 23894:2023 – AI Risk Management

Form <Name>

Approval List

If the document is approved in an electronic system, indicate “Signed in <system>” in the Signature field and “NA” in the date field.

Department / Function	Name	Signature	Date
Quality Assurance Manager			YYYY-MM-DD
Management Representative			YYYY-MM-DD

Revision History

Rev	Description of Change	Author	Revision Date
1	Initial Release.		YYYY-MM-DD

Delete this page as content is added to the document.

Form AI Continuous Validation (ISO 5338)

1. Purpose

To ensure continuous validation of AI/ML systems throughout their operational lifecycle in compliance with ISO/IEC 5338. This procedure ensures that system performance, fairness, safety, robustness, and compliance requirements are maintained after deployment.

2. Scope

Applies to all AI/ML-enabled products, including supervised, unsupervised, reinforcement learning, and continuously learning systems that are deployed in production.

3. Responsibilities

- AI Validation Lead: Oversees execution of continuous validation.

- Quality Assurance (QA): Ensures compliance with regulatory and ISO standards.

- Data Science Team: Performs re-validation tests, monitors performance drift.

- IT Operations: Ensures system logging, monitoring, and alerting.

- Ethics & Compliance Officer: Reviews validation outcomes for fairness and bias.

4. Procedure Steps

Step No.	Activity	Description	Responsible	Frequency	Records
1	Define Validation Metrics	Identify KPIs (accuracy, robustness, fairness, safety, latency) aligned with business and regulatory objectives.	AI Validation Lead	Initial + Annual Review	Validation Plan
2	Establish Baseline	Use pre-deployment	Data Science Team	Pre-deployment	Baseline Report

		validation data to set benchmark thresholds.			
3	Continuous Monitoring	Implement monitoring pipeline for accuracy drift, bias, error rates, hardware faults, and network latency.	IT Ops	Real-time	Monitoring Dashboard
4	Trigger Conditions	Define conditions that trigger re-validation (e.g., performance drop >5%, fairness violations, anomaly detection).	QA	Continuous	Trigger Criteria Log
5	Re-Validation Testing	Conduct validation tests using updated datasets and real-world production data.	Data Science Team	Monthly or Triggered	Validation Test Report
6	Documentation & Review	Document validation results, deviations, corrective actions. Escalate high-risk issues.	QA	Monthly	Validation Report
7	Corrective / Preventive Actions (CAPA)	If validation fails, initiate CAPA per ISO 13485 QMS.	QA	As Needed	CAPA Records
8	Approval & Release	Approve continued operation or rollback/patch system if	Ethics Officer + QA Manager	As Needed	Approval Record

		unacceptable risks remain.			

5. Records & Forms

- Continuous Validation Plan (CVP)

- Validation Test Reports

- Monitoring Logs

- Trigger Criteria Log

- CAPA Records

- Approval Sign-Off Sheet

6. References

ISO/IEC 5338:2023 – AI System Life Cycle Processes

ISO 13485:2016 – Medical Devices Quality Management Systems

ISO/IEC 22989:2022 – AI Concepts and Terminology

Form <Name>

Approval List

If the document is approved in an electronic system, indicate “Signed in <system>” in the Signature field and “NA” in the date field.

Department / Function	Name	Signature	Date
Quality Assurance Manager			YYYY-MM-DD
Management Representative			YYYY-MM-DD

Revision History

Rev	Description of Change	Author	Revision Date
1	Initial Release.		YYYY-MM-DD

Delete this page as content is added to the document.