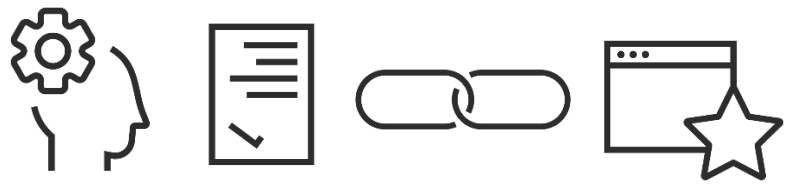
code4thought ®

ISO 42001 Advisory Form

A self-assessment tool to gauge your organization's readiness for ISO 42001 alignment or certification.



About code4thought: code4thought is a technology company focused on rendering AI and large-scale software systems trustworthy and thoughtful. Through our proprietary AI Quality Testing platform, **iQ4AI** and expert advisory **Trustworthy AI services**, we provide comprehensive quality testing and assessment solutions for AI systems across the entire lifecycle. We empower organizations with the tools and insights needed to ensure performance, compliance and responsible AI development and adoption.

Contents

Note: This guide provides a general overview of ISO 42001 and its application. Organizations should seek expert advice to determine the most appropriate course of action for their specific needs and circumstances.

1. Understanding the needs and expectations of interested parties

1) Information to be reported to interested parties can include, for example:
Mark all that apply.

- ☐ technical system documentation, including, but not limited, to datasets for training, validation and testing as well as algorithmic choices justifications and verification and validation records;
- ☐ risks related to the system;
- ☐ results of impact assessments;
- ☐ logs and other system records. *1.2.5.*

2. AI Policy

1) The AI policy can be informed by:
Mark all that apply.

- ☐ business strategy;
- ☐ organisational values and culture and the amount of risk the organisation is willing to pursue or retain;
- ☐ the level of risk posed by the AI systems;
- ☐ legal requirements, including contracts;
- ☐ the risk environment of the organisation;
- ☐ impact to relevant interested parties. *2.2.4*

2) The AI policy can include:
Mark all that apply.

- ☐ principles that guide all activities of the organisation related to AI;
- ☐ process for handling deviations and exceptions to policy. *2.2.5*

Topics that may require additional guidance:

- ⇒ AI resources and assets;
- ⇒ AI system impact assessments;
- ⇒ AI system development.

3. Roles, responsibilities and authorities

1) Have you defined roles and responsibilities for any of these areas:
Mark all that apply.

- ☐ risk management;
- ☐ AI system impact assessments;
- ☐ asset and resource management;
- ☐ security;
- ☐ safety;
- ☐ privacy;
- ☐ development;
- ☐ performance;
- ☐ human oversight;
- ☐ supplier relationships;
- ☐ demonstrate its ability to consistently fulfil legal requirements;
- ☐ data quality management (during the whole life cycle);
- ☐ the development, review and evaluation of the AI policy. *2.3.3*

4. Reporting of concerns

1) The reporting mechanism fulfils the functions below (advisory list):
Mark all that apply.

- ☐ options for confidentiality or anonymity or both;
- ☐ available and promoted to employed and contracted persons;
- ☐ staffed with qualified persons;
- ☐ stipulates appropriate investigation and resolution powers for the persons referred to in c);
- ☐ provides for mechanisms to report and to escalate to management in a timely manner;
- ☐ provides for effective protection from reprisals for both the persons concerned with reporting and investigation (by anonymity and confidentiality);
- ☐ provides reports according to the AI management system;
- ☐ provides response mechanisms within an appropriate time frame. *2.4.2*

5. AI Objectives

1) A non-exclusive AI objective list that may be checked against your organisation's AI objectives:

Mark all that apply.

- ☐ **Accountability and accessibility** Existing accountability frameworks should be reviewed. Actions of natural persons can now be supported by or based on the use of an AI system.
- ☐ **AI expertise** Dedicated specialists with expertise in assessing, developing and deploying AI systems is needed.
- ☐ **Availability and quality of training and test data** AI systems based on ML need training, validation and test data in order to train and verify the systems for the intended behaviour.
- ☐ **Environmental impact** The use of AI can have positive and negative impacts on the environment
- ☐ **Fairness** The inappropriate application of AI systems for automated decision-making can be unfair to specific persons or groups of persons.
- ☐ **Maintainability** The ability of the organisation to handle modifications of the AI system in order to correct defects or adjust to new requirements.
- ☐ **Privacy** The misuse or disclosure of sensitive and personal data (e.g., health records) can have harmful effects on data subjects.
- ☐ **Robustness and reliability** Demonstrate the ability (or inability) of the system to have comparable performance on new data as on the data on which it was trained or the data of typical operations.
- ☐ **Safety** The expectation that a system does not, under defined conditions, lead to a state in which human life, health, property or the environment is endangered.
- ☐ **Security** New security issues should be considered beyond classical information and system security concerns, with regard to AI systems based on ML approaches.
- ☐ **Transparency and explainability** Transparency relates both to characteristics of the organisation operating AI systems and to those systems themselves. Explainability relates to explanations of important factors influencing the AI system results that are provided to interested parties in a way understandable to humans. *3.1.2*

2) Does the organisation provide requirements and guidelines as necessary to ensure that measures are integrated into the various stages (e.g., the requirement to use a specific

testing tool or method to address unfairness or unwanted bias) to achieve such objectives?

- ☐ Yes
- ☐ No *3.1.4*

6. Actions to address risks and opportunities

1) Has the organisation defined 'risk' adapted to its business context?
Consider the definitions used in sectors where the AI system is developed for and used.

- ☐ Yes
- ☐ No *3.2.1.1*

7. AI System Impact Assessment

1) Does the organisation include in its AI system impact assessment procedure:
Mark all that apply.

- ☐ circumstances under which an AI system impact assessment should be performed which can include, but are not limited to:
  - ☐ criticality of the intended purpose and context in which the AI system is used or any significant changes to these;
  - ☐ complexity of AI technology and the level of automation of AI systems or any significant changes to that;
  - ☐ sensitivity of data types and sources processed by the AI system or any significant changes to that;
- ☐ elements that are part of the AI system impact assessment process, which can include:
  - ☐ identification (e.g., sources, events and outcomes);
  - ☐ analysis (e.g., consequences and likelihood);
  - ☐ evaluation (e.g., acceptance decisions and prioritization);
  - ☐ treatment (e.g., mitigation measures);
  - ☐ documentation, reporting and communication;

- ☐ who is responsible from performing the AI system impact assessment;
- ☐ how the AI system impact assessment can inform the design or use of the system, whether it can trigger reviews and approvals;
- ☐ individuals and societies that are potentially impacted based on the system's intended purpose, use and characteristics (e.g., assessment for individual, groups of individuals or societies);
- ☐ other (data used for the development of the AI system, the AI technologies, the functionality of the overall system. *3.2.4.4*

2) Does the organisation document:
Mark all that apply.

- ☐ the intended use of the AI system and any reasonably foreseeable misuse of the AI system;
- ☐ positive and negative impacts of the AI system to the relevant individuals or groups of individuals, or both, and societies;
- ☐ predictable failures, their potential impacts and measures taken to mitigate them;
- ☐ relevant demographic groups the system is applicable to;
- ☐ complexity of the system;
- ☐ the role of humans in relationships with system, including human oversight capabilities, processes and tools available to avoid negative impacts;
- ☐ employment and staff skilling. *3.2.4.5*

8. Resources

1) Documentation on data should include, but is not limited to:
Mark all that apply.

- ☐ the provenance of the data;
- ☐ the date that the data were last updated or modified (e.g., date tag in metadata);
- ☐ for machine learning, the categories of data (e.g., training, validation, test and production data);
- ☐ categories of data;
- ☐ process for labelling data;
- ☐ intended use of the data;

- ☐ quality of data;
- ☐ applicable data retention and disposal policies;
- ☐ known or potential bias issues in the data;
- ☐ data preparation. *4.1.5*

9. Management guidance for AI system development

1) Responsible development of AI system processes should include consideration of, without limitation, the following:

- ☐ life cycle stages;
- ☐ testing requirements and planned means for testing;
- ☐ human oversight requirements, including processes and tools, especially when the AI system can impact natural persons;
- ☐ at what stages AI system impact assessments should be performed;
- ☐ training data expectations and rules (e.g., what data can be used, approved data suppliers and labelling);
- ☐ expertise (subject matter domain or other) required or training for developers of AI systems or both;
- ☐ release criteria*;
- ☐ management approvals and sign-offs necessary at various stages;
- ☐ change control;
- ☐ usability and controllability;
- ☐ engagement of interested parties. *8.1.2*

*Set of requirements to be met prior to release and deployment.

10. AI system requirements and specifications

1) Some of the factors that can be considered and documented:

- ☐ why the AI system is to be developed (e.g., business case, customer request, government policy);
- ☐ how the model can be trained and how the data requirements can be achieved. *8.2.2*

11. Documentation of AI system design and development

1) For the design and development of the AI system, the organisation can document, including, but not limited to:

- ☐ machine learning approach (e.g., supervised vs. unsupervised);
- ☐ learning algorithm and type of machine learning model utilized;
- ☐ how the model is intended to be trained and which data quality;
- ☐ evaluation and refinement of models;
- ☐ hardware and software components;
- ☐ security threats considered throughout the AI system life cycle; security threats specific to AI system include data poisoning, model stealing or model inversion attacks;
- ☐ interface and presentation of outputs;
- ☐ how humans can interact with the system;
- ☐ interoperability and portability considerations. *8.3.1*

12. AI system verification and validation

1) These measures can include, but are not limited to:

- ☐ testing methodologies and tools;
- ☐ selection of test data and their representation of the intended domain of use;
- ☐ release criteria requirements. *8.4.2*

2) *The AI system should be evaluated against the documented criteria for evaluation.* The organisation should define and document evaluation criteria such as, but not limited to:

- ☐ a plan to evaluate the AI system components and the whole AI system for risks related to impacts on individuals or groups of individuals, or both, and societies;
- ☐ the evaluation plan can be based on, for example:

  (a) reliability and safety requirements of the AI system, including acceptable error rates for the AI system performance;
  (b) responsible AI system development and use objectives such as those in 3.1, question 2;

(c) operational factors such as quality of data, intended use, including acceptable ranges of each operational factor;
(d) any intended uses which can require more rigorous operational factors to be defined, including different acceptable ranges for operational factors or lower error rates;

- ☐ the methods, guidance or metrics to be used to evaluate whether relevant interested parties who make decisions or are subject to decisions based on the AI system outputs can adequately interpret the AI system outputs. The frequency of evaluation should be determined and can be based upon results from an AI system impact assessment;
- ☐ any acceptable factors that can account for an inability to meet a target minimum performance level, especially when the AI system is evaluated for impacts on individuals or groups of individuals, or both, and societies (e.g., poor image resolution for computer vision systems or background noise affecting speech recognition systems). Mechanisms to deal with poor AI system performance as a result of these factors should also be documented. *8.4.3*

13. AI System Deployment

1) A deployment plan should take into account such as, but not limited to:

- ☐ the environment AI system developed and deployed (developed on premises and deployed using cloud computing);
- ☐ how the components are deployed (e.g., software and model can be deployed separately);
- ☐ release criteria;
  (a) verification and validation measures;
  (b) performance metrics;
  (c) user testing;
  (d) management approvals and sign-offs;
- ☐ the perspectives of and impacts to relevant interested parties. *8.5.2*

14. AI System Operation and Monitoring

1) Monitoring, repairs, updates and support can include, but not limited to:

Monitoring:

- ☐ general errors and failures;
- ☐ whether the system is performing as expected with production data;
- ☐ success rates in resolving problems or in achieving task, or confidence rates;
- ☐ meeting commitment or expectation and needs of interested parties, including;
  - (a) ensuring compliance with customer requirements or applicable legal requirements;
  - (b) where machine learning is used, ensuring that it continues to meet its design goals and operates on production data as intended;
  - (c) where concept or data drift in production data is possible, identifying the need for retraining to ensure that the AI system continues to meet its design goals and operates on production data as intended;
- ☐ repairing responses to errors and failures;
- ☐ updating the system including components affected, update schedule, information to users on what is included in the update;
- ☐ changes in the system operations, new or modified intended uses, changes in system functionality;
- ☐ procedures in place to address operational changes, including communication to users;
- ☐ support processes for;
  - ☐ how users can contact the appropriate help;
  - ☐ how issues and incidents are reported;
  - ☐ support service level agreements and metrics;
- ☐ to be considered;
  - ☐ unanticipated uses of the AI system;
  - ☐ AI-specific information security threats (e.g., data poisoning, model stealing, model inversion attacks). *8.6.2*

15. AI System Technical Documentation

1) Does your AI system technical documentation include the following elements? (non-exhaustive list)

- ☐ a general description of the AI system, including its intended purpose;
- ☐ usage instructions;
- ☐ technical assumptions about its deployment and operation (run-time environment, related software and hardware capabilities, assumptions made on data, etc.);
- ☐ technical limitations (acceptable error rates, accuracy, reliability, robustness);
- ☐ monitoring capabilities and functions that allow users or operators to influence the system operation. *8.7.2*

2) *The organisation should have procedures in place to address operational changes including communication to users and internal evaluations on the type of change. The organisation should document the technical information related to the responsible operation of the AI system. Documentation should be up-to-date, accurate and approved by the relevant management within the organisation.* The documentation can include, but is not limited to:

- ☐ a plan for managing failures;
- ☐ processes for monitoring the health of the AI system and for addressing AI system failures;
- ☐ standard operating procedures for the AI system, including events monitoring, events logging, investigating and prevention of failures;
- ☐ the roles of personnel responsible from various stages of AI system life cycle;
- ☐ system updates. *8.7.3*

An exemplary list of documentation elements related to all AI system life cycle stages:

- ⇒ design and system architecture specification;
- ⇒ design choices made and quality measures taken during the system development process;
- ⇒ information about the data used during system development;
- ⇒ assumptions made and quality measures taken on data quality (e.g., assumed statistical distributions);

⇒ management activities (e.g., risk management) taken during development or operation of the AI system;

⇒ verification and validation records;

⇒ changes made to the AI **system** when it is in operation;

⇒ impact assessment documentation.

16. AI system recording of event logs

1) The organisation ensures logging for AI system it deploys:

(a) automatically collects and records event logs including;

(b) traceability of the AI system's functionality to ensure that the AI system is operating as intended;

(c) detection of the AI system's performance outside of the AI system's intended operating conditions that can result in undesirable performance on production data or impacts to relevant interested parties through monitoring of the operation of the AI system;

(d) the date and time the AI system is used;

(e) the production data on which the AI system operates on;

(f) the outputs that fall out of the range of the intended operation of the AI system. *8.8.2*

2) *Event logs should be kept as long as required for the intended use of the AI system and within data retention policies of the organisation.* Has the organisation determined a retention period in accordance with applicable legal requirements?

☐ Yes

☐ No *8.8.3*

**The requirement of the EU AI Act is to retain the event logs for six months pursuant to Art.19, unless provided otherwise in the applicable law.*

17. Data for AI systems

1) Does data management include the topics below (non-exhaustive):

- ☐ privacy and security implications due to the use of data, some of which can be sensitive in nature;
- ☐ security and safety threats that can arise from data dependent AI system development;
- ☐ transparency and explainability aspects including data provenance and the ability to provide an explanation of how data are used for determining an AI system's output if the system requires transparency and explainability;
- ☐ representativeness of training data compared to operational domain of use;
- ☐ accuracy and integrity of the data. *9.1.2*

18. Acquisition of data

1) Has the organisation determined any details for data acquisition such as:

- ☐ categories of data needed for the AI system;
- ☐ quantity of data needed;
- ☐ data sources (e.g., internal, purchased, shared, open data, synthetic);
- ☐ characteristics of the data source (e.g., static, streamed, gathered, machine generated);
- ☐ data subject demographics and characteristics (e.g., known or potential biases or other synthetic errors);
- ☐ prior handling of the data (e.g., previous uses, conformity with privacy and security requirements);
- ☐ data rights (e.g., PII, copyright);
- ☐ associated meta data (e.g., details of data labelling and enhancing);
- ☐ provenance of the data. *9.2.2*

19. Quality of data for AI systems

1) Where the organisation uses supervised or semi-supervised machine learning, the quality of training, validation, test and production data should be:

- ☐ defined, measured and improved to the extent possible;
- ☐ suitable for the organisation's intended purpose. *9.3.2*

*It is also advised that the organisation considers the impact of bias in system performance and system fairness and make adjustments as necessary to the model and data used to improve performance and fairness

20. Data provenance

1) *Depending on factors such as the source of the data, its content and the context of its use, organisations should consider whether measures to verify the provenance of the data are needed.* The record can include information about:

- ☐ the creation, update, transcription, abstraction, validation and transferring of the control of data;
- ☐ data sharing (without transfer of control);
- ☐ data transformations. *9.4.2*

21. Data preparation

1) *For a given AI task, the organisation should document its criteria for selecting specific data preparation methods and transforms as well as the specific methods and transforms used in the AI task.* Do you use any of these common preparation methods and transformations for data used in the AI system?

- ☐ statistical exploration of the data (e.g., distribution, mean, median, standard deviation, range, stratification, sampling) and statistical metadata (e.g., data documentation initiative (DDI) specification);
- ☐ cleaning (i.e., correcting entries, dealing with missing entries)
- ☐ imputation (i.e., methods for filling in missing entries);
- ☐ normalisation;
- ☐ scaling;

- ☐ labelling of the target variables;
- ☐ encoding (e.g., converting categorical variables to numbers). *9.5.2*

22. System documentation and information for users

1) Do you provide any of this information to users (non-exhaustive list):

- ☐ purpose of the system;
- ☐ that the user is interacting with an AI system;
- ☐ how to interact with the system;
- ☐ how and when to override the system;
- ☐ technical requirements for system operation, including the computational resources needed, and limitations of the system as well as its expected lifetime;
- ☐ needs for human oversight;
- ☐ information about accuracy and performance;
- ☐ relevant information from the impact assessment, including potential benefits and harms particularly if they are applicable in specific contexts or certain demographic groups;
- ☐ revisions to claims about the system's benefits;
- ☐ updates and changes in how the system works, as well as any necessary maintenance measures, including their frequency;
- ☐ contact information;
- ☐ educational materials for system use. *10.1.2.*

2) Do you document whether and what information* is to be provided to users?

- ☐ Yes
- ☐ No *10.1.3*

*Relevant criteria include but are not limited to the intended use and reasonably foreseeable misuse of the AI system, the expertise of the user and specific impact of the AI system.

23. Communication of incidents

1) Have the organisation determined any of the below, by legal (such as contracts) or regulatory requirements:

- ☐ types of incidents that must be communicated;
- ☐ the timeline for notification;
- ☐ whether and which authorities must be notified;
- ☐ the details required to be communicated. *10.3.2*

24. Processes for responsible use of AI systems

1) Some of the policies to be considered by the organisation to determine whether to use a particular AI system:

- ☐ whether the AI system is developed internally or by a third party;
- ☐ required approvals;
- ☐ cost (including for ongoing monitoring and maintenance);
- ☐ approved sourcing requirements;
- ☐ legal requirements applicable to the organisation.

25. Objectives for responsible use of AI systems

1) At which stages of the AI system life cycle meaningful human oversight objectives are incorporated?

Mark all that apply

- ☐ Checking the outputs of the AI system;
  - ☐ including having authority to override decisions made by the AI system.
- ☐ Ensuring that human oversight is included if required for acceptable use of the AI system according to instructions or other documentation associated with the intended deployment of the AI system.
- ☐ Monitoring the performance of the AI system;
  - ☐ including the accuracy of the AI system outputs.

- ☐ Reporting concerns related to the outputs of the AI system and their impact to relevant interested parties.
- ☐ Reporting concerns with changes in the performance or ability of the AI system to make correct outputs on the production data.
- ☐ Considering whether automated decision-making is appropriate for a responsible approach to the use of an AI system and the intended use of the AI system.
- ☐ Other
- ☐ None *11.2.1*

2) Are the personnel involved in human oversight activities related to the AI system informed of, trained and understand the instructions and other documentation to the AI system and the duties they carry out to satisfy human oversight objectives?

- ☐ Yes
- ☐ No *11.2.2*

26. Intended use of the AI system

1) Does the organisation take necessary actions, when deploying the AI system to ensure that:

- ☐ human oversight is applied as required (informed by the AI system impact assessment)
- ☐ the data that the AI system is used on aligns with the documentation associated with the AI system;
- ☐ the operation of the AI system is monitored;
- ☐ the organisation communicates its concerns to the relevant personnel inside the organisation and any third-party suppliers of the AI system;
- ☐ event logs are kept as long as required by the intended use or organisation's retention policy or regulatory data retention obligations. *11.3.1*

27. Third-party and customer relationships

27.1. Allocating responsibilities

1) *In order to establish the responsibility and accountability of the organisation, risks should be appropriately apportioned when third parties are involved at any stage of the AI system life cycle.* Does the organisation document all parties intervening in the AI system life cycle and their roles and determine their responsibilities?

- ☐ Yes
- ☐ No *12.1.1*

2) Does the organisation:

- ☐ provide the necessary documentation for the AI system to relevant interested parties and to the third party that the organisation is supplying the AI system to;
- ☐ ensure that the responsibilities are split between PII processors and controllers based on the data processing activities of involved parties and AI system. *12.1.2*

27.2. Suppliers

1) *Organisations developing or using an AI system can utilize suppliers by sourcing datasets, machine learning algorithms or models, or other components of a system such as software libraries, to an entire AI system itself for use on its own or as part of another product. Selection of suppliers can pose varying level of risk to the system and organisation.* Does the organisation consider:

- ☐ different types of suppliers;
- ☐ what they supply;
- ☐ the requirement placed on those suppliers;
- ☐ the levels of ongoing monitoring and evaluation needed for the suppliers. 12.2.1

2) Does the organisation require the supplier to take corrective actions when the AI system or its components from a supplier do not perform as intended or can result in impacts to individuals or groups of individuals, or both, and societies that are not aligned with the responsible approach to AI systems taken by the organisation?

- ☐ Yes
- ☐ No 12.2.2

3) Does the organisation document how the AI system and AI system components are integrated into AI systems developed or used by the organisation?

- ☐ Yes
- ☐ No 12.2.3

27.3. Customers

1) *The organisation should understand customer expectations and needs* when it is supplying a product or a service related to the AI system (i.e., when it is itself a supplier).* Does the organisation fulfil the customer's needs and expectations in any of the following forms?

- ☐ requirements for the product or service itself during a design or engineering phase;
- ☐ contractual requirements;
- ☐ general usage agreements. 12.3.1

*An example, the organisation can identify risks related to the use of its AI products and services by the customer and can decide to treat the identified risks by giving appropriate information to its customer, so that the customer can then treat the corresponding risks. Appropriate information such as the AI system is only valid for a certain domain of use.

Take the Next Step Toward Responsible AI Governance

At code4thought, we believe that trustworthy AI starts with structured, transparent, and ethical practices—exactly what ISO 42001 aims to establish. As the first global standard for AI Management Systems, ISO 42001 provides organizations with the foundation to govern AI responsibly, mitigate risk, and foster innovation with integrity.

You can find more info about ISO 42001 and other AI Governance Standards in our Ultimate Guide here

We are your partner in building AI systems that are not only compliant but also trustworthy, reliable, and innovative through our **Trustworthy AI services.** Our specialized **AI Governance Advisory**, along with our **360° AI Assessment** and **AI Quality Testing & Audit**, support organizations at every stage of their compliance journey—from readiness evaluation to full implementation. Whether you're just beginning to explore ISO 42001 alignment or preparing for certification, we're here to guide you with expertise and actionable insights.

Ready to transform how you govern and manage AI? Contact our team today to discover how code4thought and iQ4AI can help you implement world-class AI governance solutions tailored to your unique business needs. Together, we'll unlock the full potential of AI while ensuring it serves as a force for good in your organization and beyond.

Visit code4thought.eu to learn more or schedule a consultation today!