EU AI Act Technical Documentation Guide

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 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.

In the present **Guide**, you will find all the necessary steps regarding drawing up the technical documentation required by the EU AI Act.

Should you need any further assistance, our EU AI Act Assurance service aims at enabling organizations to adhere to the regulatory requirements set forth by the EU AI Act in a timely and cost-efficient manner. It offers a pragmatic implementation of the EU AI Act's risk management approach for businesses. We assess your AI systems, models, algorithms and respective processes, identify gaps and provide recommendations for remediation, including for the technology itself.

FURTHER READING

The EU AI Act: Your Roadmap to Trustworthy AI and Business Value Maximization

In the Driver's Seat: Short Handbook on AI Auditing & Testing for Business and IT Leaders

World Summit AI 2024 Amsterdam – USE CASE: AI legislation: A regulatory hurdle or an opportunity for strategic growth?

AI Regulation: Deus Ex Machina?
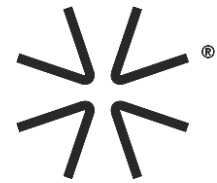
ISO/IEC TR 29119-11: A Technical Report Providing Guidelines for Testing AI-Based Systems

ISO 42001: Understanding the First AI Management System Standard

Navigating the AI Ecosystem Securely: An Introduction to the NIST AI Risk Management Framework (AI RMF)

OECD AI Principles: Guardrails to Responsible AI Adoption
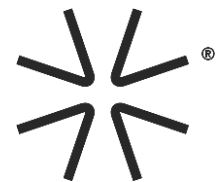
More in our Knowledge Hub

Technical Documentation, mentioned in Article 11 of the Act, is mandatory for high-risk AI systems under the EU AI Act.

The technical documentation of a high-risk AI system shall be drawn up before that system is placed on the market or put into service and shall be kept up-to date.

The technical documentation shall be drawn up in such a way as to demonstrate that the high-risk AI system complies with the requirements set out in Chapter III, Section 2 of the Act and to provide national competent authorities and notified bodies with the necessary information in a clear and comprehensive form to assess the compliance of the AI system with those requirements. It shall contain, at a minimum, the elements set out in Annex IV. SMEs, including start-ups, may provide the elements of the technical documentation specified in Annex IV in a simplified manner.
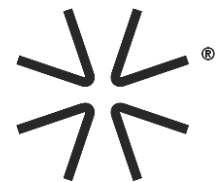
Please answer all the questions marked with a green asterisk *****.

Throughout the Guide, the terms 'AI system' and 'high-risk AI system' are used interchangeably pursuant to the EU AI Act text.

Contents

Technical Documentation

1. Description of the AI system

1) * Technical documentation should contain a description of the AI system. In this regard, please provide:

- the intended purpose* of the AI system:

- the name of the provider**:

* '**intended purpose**' means the use for which an AI system is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation.
** '**provider**' means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.
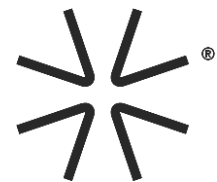
1.1 Versions of the AI system

1) * Please give a description of the version of the AI system and its relation to previous versions.

2) * Please specify the versions of relevant software or firmware, and any requirements related to version updates.

- Software:

- Firmware:

- Requirements:

3) * Please describe all the forms in which the AI system is placed on the market or put into service (e.g. software packages embedded into hardware, downloads, or APIs).

1.2 System components

1) * Please describe the hardware on which the AI system is intended to run.

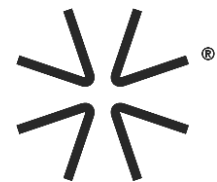**2)** Where applicable, please provide a report on how the AI system interacts with other;

- hardware:

- software:

- other AI systems that are not part of the AI system itself:

3) * Is your AI system a component of products?

- ☐ Yes *Skip to question 4*
- ☐ No *Skip to question 5*

4) Please provide photographs or illustrations showing external features, the marking and internal layout of those products.

5) *Please answer only one item of the bullet list below.

- a basic description of the user-interface provided to the deployer:

- where applicable, instructions for use* for the deployer and a basic description of the user-interface provided to the deployer

* '**instructions for use**' means the information provided by the provider to inform the deployer of, in particular, an AI system's intended purpose and proper use.

2. Elements of the AI system and of the process

Answer the questions in this section for the purposes of providing a detailed description of the elements of the AI system and of the processes for its development.

1) * Please provide a detailed description of;

a) the methods and steps performed for the development of the AI system:

i. Please add, where relevant, recourse to pretrained systems and tools provided by third parties and how those were used, integrated or modified by the provider:

2.1 Design specifications

1) * Please provide a detailed description of;

a) the design specifications of the system, namely the general logic of the system and of the algorithms:
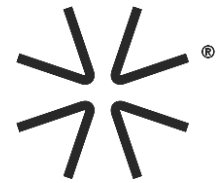
i.   the key design choices including the rationale and assumptions made, including with regard to persons or groups of persons in respect of who, the system is intended to be used:

ii.   the main classification choices:
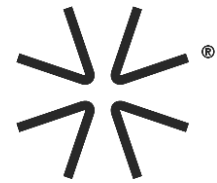
iii.   what the system is designed to optimise for, and the relevance of the different parameters:

iv.   the description of the expected output and output quality of the system:

v.   the decisions about any possible trade-off made regarding the technical solutions adopted to comply with the requirements set out in Chapter III, Section2:, (Requirements for High-Risk AI Systems)

2.2   Description of the system architecture

1) * Please provide a detailed answer of;

a) the description of the system architecture explaining the way software is designed and developed, how software components build on or feed into each other and integrate into the overall processing:

i. the computational resources used to develop, train, test and validate the AI system (i.e., processing power (CPU/GPU), memory (RAM), storage, network bandwidth, energy and power supply etc.):

2.3   Data requirements

1) Where relevant, please explain the data requirements in terms of;

a) datasheets describing the training methodologies:

i. training techniques (e.g., 'supervised learning', 'unsupervised learning', 'reinforcement learning' etc.):

ii. training data* sets used;

- general description of these datasets:

- provenance of the datasets:

- scope and main characteristics:

iii. how the data was obtained and selected:

iv. labelling procedures (e.g. for supervised learning):

v. data cleaning methodologies (e.g. outliers detection):

* '**training data**' means data used for training an AI system through fitting its learnable parameters;

2.4   Human oversight

1) * 'High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overse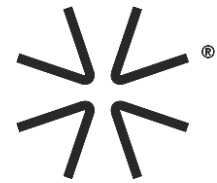en by natural persons during the period in which they are in use. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.'
Provide the human oversight measures needed in accordance with Article 14, including;

a) Human oversight report consisting of:
   i. all personnel involved in human oversight of the high-risk AI system:
   ii. each person's role and responsibility:
   iii. relevant risks:
   iv. criteria for efficacy of human oversight:

   1) data and model choices:
   2) choice of personnel
   3) handling of outcomes:
   4) human limitations in accomplishing such roles:
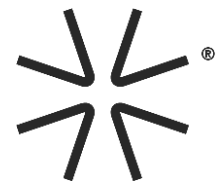
      5) context of the human oversight (e.g., the field, geography where high-risk AI system is used):

      6) omission, annulling or revoking outputs by personnel in charge of human oversight:

    v. Human oversight log to track the following;

      1) the interaction of the personnel with the system:

      2) an influence on the output of the system or an impact to a user:

      3) any error in pause or stop button functions:

      4) any delay:

        (b) in information flow from the system for human intervention:

        (c) in personnel intervention:

b) whether the measures prevent or minimize the risks to health, safety or fundamental rights that may emerge when the AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse:

c) Are the measures commensurate with the risks, level of autonomy and context of use of the high-risk AI system:

d) Are the measures identified and built into the AI system (when technically feasible) by the provider, or the measures are identified by the provider and are appropriate to be implemented by the deployer?

2) * Is your high-risk AI system a remote biometric identification system? (Please answer as 'No' if the sole purpose of your system is to confirm that a specific natural person is the person he or she claims to be.)

    ☐ Yes *Skip to question 3*
    ☐ No *Skip to question 4*

3) Do you ensure that the identification resulting from the system is separately verified and confirmed by at least two natural persons with necessary competence, training and authority? (This extra measure shall be disregarded for the high-risk AI systems which are used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.)

    ☐ Yes
    ☐ No

4) *Do you ensure the high-risk AI system is provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate:

☐ to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance;

☐ to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;

☐ to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available;

☐ to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system;

☐ to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state.

    i. Please explain how you ensure the above points:

    ii. Please provide the technical measures needed to facilitate the interpretation of the outputs of the AI system by the deployers:
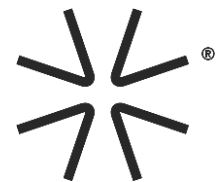
2.5   Predetermined changes

1) Where applicable, please provide;

    a. a detailed description of predetermined changes to the AI system and its performance:

Please add;

    b. all the technical solutions adopted related to the predetermined changes to the AI system, to ensure

continuous compliance with the relevant requirements set out in Chapter III, Section 2:
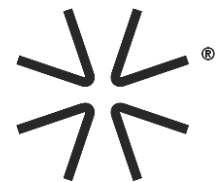
2.6   Validation and testing procedures

1) *Please provide detailed information about;

a. the validation and testing procedures used:

- information about the validation* and testing data** used and their main characteristics:

- metrics used to measure accuracy, robustness and compliance with other relevant requirements set out in Chapter III, Section 2:

1) Please add potentially discriminatory impacts:

- test logs and all test reports dated and signed by the responsible persons, including with regard to pre-determined changes:

* '**validation data**' means data used for providing an evaluation of the trained AI system and for tuning its non-learnable parameters and its learning process in order, inter alia, to prevent underfitting or overfitting;
** '**testing data**' means data used for providing an independent evaluation of the AI system in order to confirm the expected performance of that system before its placing on the market or putting into service;

2.7 Cybersecurity

1) * 'The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (data poisoning), or pre-trained components used in training (model poisoning), inputs designed

to cause the AI model to make a mistake (adversarial examples or model evasion), confidentiality attacks or model flaws.'

Please explain the cybersecurity measures put in place for the high-risk AI system:

3. Monitoring, functioning and control of the AI system

1) *Please provide detailed information about the monitoring, functioning and control of the AI system, in particular with regard to:

    a) its capabilities and limitations in performance*:

        i. the degrees of accuracy for specific persons or groups of persons on which the system is intended to be used and the overall expected accuracy in relation to its intended purpose:

    b) in view of the intended purpose of the AI system,

        i. the foreseeable unintended outcomes and sources of risks to health and safety:

        ii. fundamental rights:

        iii. discrimination:

    c) the human oversight measures needed in accordance with Article 14:

    d) the technical measures put in place to facilitate the interpretation of the outputs of the AI system by the deployers:

    e) specifications on input data**, as appropriate:
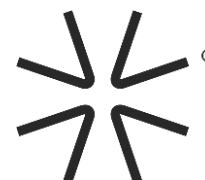
* '**performance of an AI system**' means the ability of an AI system to achieve its intended purpose
** '**input data**' means data provided to or directly acquired by an AI system on the basis of which the system produces an output;

4. Risk Management System

1) *Do you have a risk* management system in place in relation to your AI system?

☐ Yes *Skip to question 2*
☐ No *Check the questions below and answer all that apply, regardless of having a risk management system in place.*
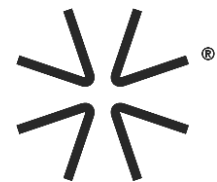
* '**risk**' means the combination of the probability of an occurrence of harm** and the severity of that harm.
** depending on the circumstances regarding its specific application, use, and level of technological development, AI may generate risks and cause harm to public interests and fundamental rights that are protected by Union law. Such harm might be material or immaterial, including physical, psychological, societal or economic harm.

2) * 'A risk management system* shall be established, implemented, documented and maintained in relation to high-risk AI systems. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system. The risk management system may be combined with a risk management process established pursuant to other Union law. '

Please provide a detailed description of the risk management system including:

* Risks referred to in this Section shall concern only those which may be reasonably mitigated or eliminated through the development and design of the high-risk AI system or the provision of adequate technical information.

a) *How frequently do you document, review and update the risk management system?

b) *Does the system cover the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system used in accordance with its intended purpose?

☐ Yes
☐ No

i.   Please share the results:

c)   *Does the system cover the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose;

☐ Yes
☐ No

i.   and under conditions of reasonably foreseeable misuse?

☐ Yes
☐ No

ii.   Please share the results:

d)   *Does the system cover the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system*?

☐ Yes
☐ No

i.   Please share the results:

e)   *Does the system contain the adoption of appropriate and targeted risk management measures* designed to address the risks identified pursuant to the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system used in accordance with its intended purpose?

☐ Yes
☐ No
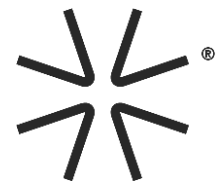
* The risk management measures referred above, shall give due consideration to the effects and possible interaction resulting from the combined application of the requirements set out in Chapter III, Section 2 of the EU AI Act with a view to minimising risks more effectively while achieving an appropriate balance in implementing the measures to fulfil those requirements.

The measures shall ensure elimination or reduction of risks identified and evaluated pursuant to the points (b), (c), (d) in as far as technically feasible through adequate design and development of the high-risk AI system.

The measures shall be such that the relevant residual risks associated with each hazard, as well as the overall residual risk of the high-risk AI system is judged to be acceptable.

  i. Please share all the above-mentioned measures:

3) * What are the residual risks, relevant to the above-mentioned measures, if any?

4) Where appropriate, do you implement adequate mitigation and control measures addressing risks that cannot be eliminated?
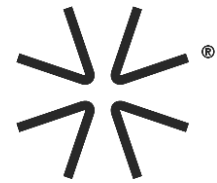
  ☐ Yes
  ☐ No

  a) Please share all the above-mentioned measures:

5) *Do you provide a document in the nature of 'instructions for use' along with the AI system, which shall contain at least the following information:

Check all that apply.

  ☐ the identity and the contact details of the provider and, where applicable, of its authorised representative;

  ☐ the characteristics, capabilities and limitations of performance of the high-risk AI system, including:

    ☐ (i) its intended purpose;

☐ (ii) the level of accuracy, including its metrics, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;

☐ (iii) any known or foreseeable circumstance, related to the use of the high-risk AI system in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to risks to the health and safety or fundamental rights referred to in Article 9(2);

☐ (iv) where applicable, the technical capabilities and characteristics of the high-risk AI system to provide information that is relevant to explain its output;

☐ (v) when appropriate, its performance regarding specific persons or groups of persons on which the system is intended to be used;

☐ (vi) when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the high-risk AI system;

☐ (vii) where applicable, information to enable deployers to interpret the output of the high-risk AI system and use it appropriately;

☐ the changes to the high-risk AI system and its performance which have been pre- determined by the provider at the moment of the initial conformity assessment, if any;

☐ the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of the high-risk AI system by the deployers;

☐ the computational and hardware resources needed, the expected lifetime of the high-risk AI system and any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of that AI system, including as regards software updates;

☐ where relevant, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret the logs in accordance with Article 12.

☐ No
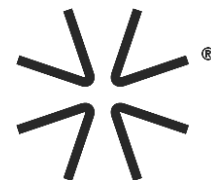
6) Where appropriate, do you offer training* to deployers?

☐ Yes
☐ No

* With a view to eliminating or reducing risks related to the use of the high-risk AI system, due consideration shall be given to the technical knowledge, experience, education, the training to be expected by the deployer, and the presumable context in which the system is intended to be used.

a) Please describe the training in details:

7) *Does the risk management system encapsulate inspection of whether in view of its intended purpose the high-risk AI system is likely to have an adverse impact on;

a. persons under the age of 18:

b. other vulnerable groups:

c. Please share the results.

5. Testing procedure

1) * 'High-risk AI systems shall be tested for the purpose of identifying the most appropriate and targeted risk management measures. Testing shall ensure that high-risk AI systems perform consistently for their intended purpose and that they are in compliance with the requirements set out in Chapter III, Section 2.'

Please provide detailed information about testing procedure, including;

a) How frequent do you conduct testing? (e.g. 'throughout the development process', 'prior to being placed in the market' or 'prior to being put into service')
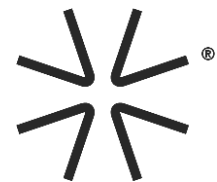
b) Please provide detailed information about testing in real-world
conditions*, if any?

* **'testing in real-world conditions'** means the temporary testing of an AI system for its intended purpose in
real-world conditions outside a laboratory or otherwise simulated environment, with a view to gathering
reliable and robust data and to assessing and verifying the conformity of the AI system with the requirements
of this Regulation and it does not qualify as placing the AI system on the market or putting it into service
within the meaning of this Regulation, provided that all the conditions laid down in Article 57 or 60 are fulfilled.

c) Please give some examples of the metrics the AI system is tested
against and probabilistic thresholds (if any).

6. Changes to the system

1) *Please provide a description of all the relevant changes the AI system
has undergone through its lifecycle.

7. EU Standards and Conformity

1) *Please provide a list of the harmonised standards applied in full or in
part the references of which have been published in the *Official Journal
of the European Union*; where no such harmonised standards have been
applied, a detailed description of the solutions adopted to meet the
requirements set out in Chapter III, Section 2 of the EU AI Act, including a
list of other relevant standards and technical specifications applied.

2) *Please provide a copy of the EU declaration of conformity referred to in
Article 47 of the EU AI Act.
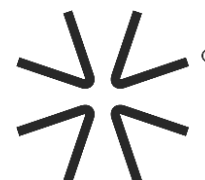
8. Post-Market Monitoring

1) * Does your AI system fall in any of the following categories?

- Machinery
- Safety of toys
- Recreational craft and personal watercraft
- Lifts and safety component for lifts
- Equipment and protective systems intended for use in potentially explosive atmospheres
- Radio equipment
- Pressure equipment
- Cableway equipment
- Personal protective equipment
- Appliances burning gaseous fuels
- Medical devices
- In vitro diagnostic medical devices
  or,
- Point 5 of Annex III placed on the market or put into service by financial institutions that are subject to requirements under Union financial services law

Mark only one box

☐ Yes *Skip to question 2*
☐ No *Skip to question 3*

2) Is your post-market monitoring system* integrated as appropriate within an already established post-market monitoring system under the Union harmonization legislation listed in Section A of Annex I (i.e. the list above)?

☐ Yes *(You may integrate the required post-market monitoring system by AIA to your already existing post-market monitoring system provided that it includes all the elements requested in the questions 3 and 4.)*
☐ No *Skip to question 3*

* '**post-market monitoring system**' means all activities carried out by providers of AI systems to collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;

3) * 'EU AI Act requires keeping records and the availability of technical documentation, containing information which is necessary to assess the
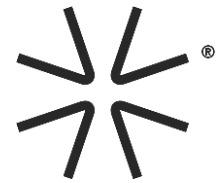
compliance of the AI system with the relevant requirements and facilitate post market monitoring. Such information should include the general characteristics, capabilities and limitations of the system, algorithms, data, training, testing and validation processes used as well as documentation on the relevant risk-management system, the automatic recording of events, by means of logs, over the duration of the lifetime of the system and drawn in a clear and comprehensive form.'

Please give a detailed description of the Post-Market Monitoring System referred to in Article 72 including;

a) * Do you actively and systematically collect, document and analyze relevant data* on the performance of the high-risk AI system throughout its lifetime?

b) *Does the data allow the provider to evaluate the continuous compliance of AI systems with the requirements set out in Chapter III, Section 2?

c) Does post-market monitoring include an analysis of the interaction with other AI systems, where relevant?

*Data may be provided by deployers or which may be collected through other sources, except for the deployers which are law enforcement authorities.

4) * 'Post-Market Monitoring Plan should encapsulate how the provider plans to realize the post-market monitoring system, as well as if the monitoring will be performed by deployers or users, and the necessary instructions to be accompanied with the high-risk AI system.'

Please provide the Post-Market Monitoring Plan referred to in Article 72(3).
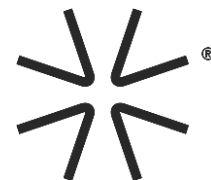
Important Note

The information provided in this Guide is intended for educational and informational purposes only. The content is not intended to be a substitute for professional advice or any other legal advisory, service, etc. The site's administrators and contributors make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the information, products, services, or related graphics contained in the Guide for any purpose. Any reliance you place on such information is therefore strictly at your own risk.

The site's administrators and contributors of the Guide are not liable for any loss or damage, including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from loss of data or profits arising out of, or in connection with, the use of this Guide.

The Guide may contain links to other websites which are not under the control of the administrators and contributors. We have no control over the nature, content, and availability of those sites. The inclusion of any links does not necessarily imply a recommendation or endorsement of the views expressed within them.

Every effort is made to keep the website up and running smoothly. However, the administrators and contributors take no responsibility for, and will not be liable for, the website being temporarily unavailable due to technical issues beyond our control.