4

Companies developing compliance with requirements

Guide 4. Quality Management

European Artificial Intelligence Act

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

This guide has been developed within the framework of the development of the Spanish pilot for the regulatory AI Sandbox, through collaboration among participants, technical assistance providers, potential competent national authorities, and the sandbox's expert advisory group.

The aim of the guide is to serve as an introductory support to the European Regulation on Artificial Intelligence and its applicable obligations. Although it is not legally binding and does not replace or develop the applicable legislation, it provides practical recommendations aligned with regulatory requirements, pending the approval of the harmonised implementing standards for all Member States.

This document is subject to an ongoing process of evaluation and review, with periodic updates in line with the development of standards and the various guidelines published by the European Commission, and it will be updated once the Digital Omnibus amending the Artificial Intelligence Act is approved.

Among the relevant technical references currently under development, particular note should be made of **prEN 18228, *"Artificial Intelligence – Quality Management System for EU AI Act Regulatory Purposes,"*** which will establish the quality management framework applicable to AI systems in the context of compliance with the European Regulation on Artificial Intelligence

Revision date: 10 December 2025

General content

Detailed Index

1. Preamble

1.1 Purpose of the document

This guide presents the organisational and technical measures that will help providers and deployers to comply with the article ***"Quality Management System"*** of the European Regulation on Artificial Intelligence. This article sets out the quality management requirements that must be incorporated by any high-risk AI system (HRAIS) and certain general-purpose AI systems (article "*Requirements for providers of general-purpose AI models*"). In this sense, throughout the guide we will generally refer to these systems as "AI system" with the aim of simplifying the discourse.

1.2 How to Read This Guide

This section has been prepared to **accompany the reader** in reading the guide and help them to achieve a more **agile and effective** understanding **of the contents.**

To this end, we present a brief explanation of the content and relevance of each of the sections:

1. **Preamble**
   1.1. **Objective of the document**: brief introduction to the contents and objective of the guide.
   1.2. **How to read this guide:** section that makes it easier for the reader to understand the guide.
   1.3. **Who is it for?** Explanation of the obligations of the provider and deployer.
   1.4. **Use cases:** preliminary explanation of the examples with which we will accompany the guide
2. **Introduction:** section of the guide detailing and describing what a quality management system is in general context and in the specific context of the European Regulation on Artificial Intelligence**.**
3. **European Regulation on Artificial Intelligence**: analysis is carried out of the articles around which this guide has been written and the relationship between the sections of these articles and those of the guide where they are addressed.
4. **What elements should I implement and how should I do it to develop an adequate quality management system?** the main section of the guide in which the elements of the article are analysed, and it is specified how each of them should be addressed for their proper compliance.
5. **Other elements to consider**: In this section we address the rest of the specific elements of the article (such as the analysis of the implementation of the quality management system proportional to the size of the provider's organization).
6. **References, standards and norms**: documentation referenced throughout the guide.

1.3 Who is it for?

The requirements described in the article "*Quality Management System*" are primarily geared towards the development of the system, carried out by the provider. In this article, no requirements are specified for the person who makes use of the system, that is, the deployer. In the event that the deployer, in a given situation, participates in the development of the system, he or she should implement the measures developed for the provider.

In this context, the measures detailed throughout this guide are measures intended to serve as a guide for the provider. These measures are both organisational and technical in nature.

1.4 Use cases and examples throughout the guide

In order to facilitate the understanding of the guide, a series of examples are incorporated throughout it that aim to serve as a reference for the adaptation of HRAIS for the management of quality systems in accordance with the requirements of the regulation.

These examples are developed based on the use cases described in the **Guide 2. Practical guide and examples to understand the AI Act.**

Finally, it should be noted that whenever an example is given, it will be done in an illustrative way. Provider and deployer should consider implementing all measures outlined in this guide, as appropriate. Each AI system, following the guidelines in this guide, should identify and implement the most appropriate measures according to the characteristics of its AI system and its specific purpose. In addition, the examples presented are specific to the use cases.

To this end and given the cross-cutting nature of the subject matter, the implications of the regulation of a fictitious company will be analysed point by point of the regulation in the company.

2. Introduction

2.1 What is a quality management system?

A quality management system in general terms, as understood according to the ISO 9001 reference standard, consists of a set of processes designed to enable an organization to continuously improve its overall performance, as well as provide it with a basis for sustainable development.

In the context of the European Regulation on Artificial Intelligence, where the general purpose is to ensure **the health, safety and fundamental rights of individuals** in the context of the use of AI systems, the quality management system (as set out in the article "Quality management system") is one that will contain the elements specified in that article (*Some of them are: a strategy for regulatory compliance, the risks management system in accordance with what is specified in the corresponding article, data management systems and procedures*) and whose documentation will be reflected in policies, procedures and written instructions.

This guide facilitates the understanding of the article "Quality Management System" and helps the reader in the implementation of the appropriate measures that allow him to comply with what is specified in said article. In this way, in the next section we will analyse each of the elements specified in the article and try to explain in detail how they should be addressed and documented.

Before entering the next section, it is important to note that, as can be seen, the vast majority of the elements that a quality management system must contain have already been developed in one of the technical guides developed. In this context, these elements will be referenced from this guide to the appropriate guide where they have been developed, incorporating the additional content necessary to facilitate compliance with the element in question. Thus, for example, subparagraph (g) specifies that the quality management system shall include *"the risks management system referred to in Article 9"*. In this case, we will incorporate in the corresponding section of this guide (next section) an explanation of how this element should be completed by linking it to the corresponding content, in this case, of the guide developed to facilitate compliance with the article "Risks management system".

The article establishes that the system must be documented in a systematic manner trough written policies, procedures and instructions.

This guide does not prescribe a specific format, leaving the choice to each organization (e.g., internal policies, technical procedures, annexes, etc).

3. European Regulation on Artificial Intelligence

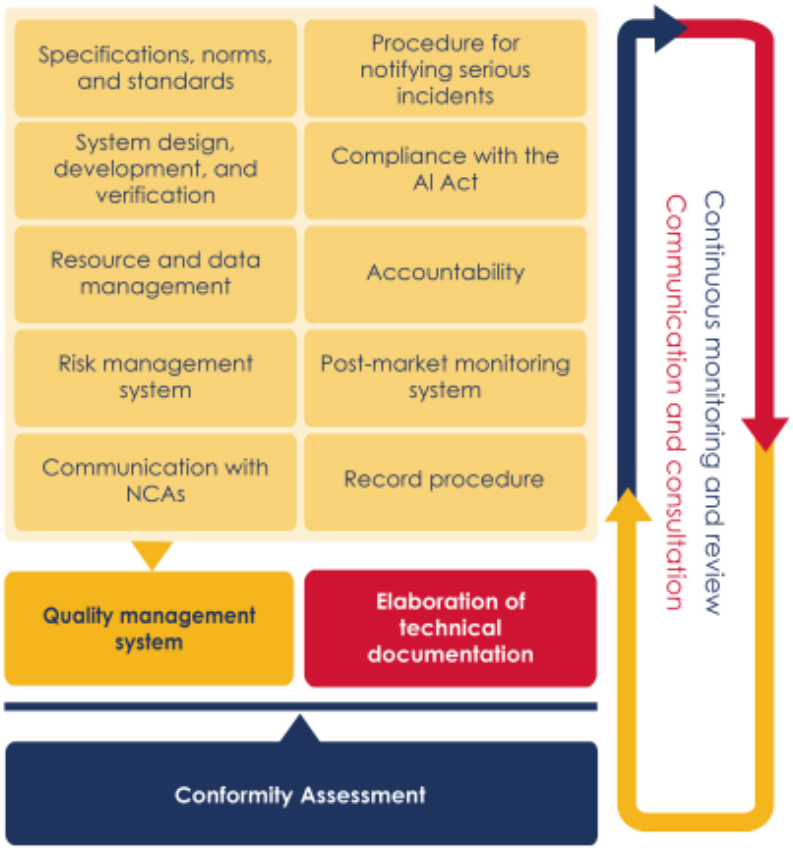
3.1 Preliminary analysis and relationship of the articles

The obligations on quality management systems are mainly found in the article of the European Regulation on Artificial Intelligence, Article 17 *"Quality Management System"*.

In this sense:

- **Article Quality Management System** → sets out the obligations of providers of high-risk AI systems to implement a documented quality management system that ensures regulatory compliance. This system should include compliance strategies, risks management, design and development control, testing, post-market surveillance, incident reporting, and communication with authorities and stakeholders. Its scope should be proportional to the size of the provider and can be integrated with existing systems if it complies with EU industry regulations.

A summarized and visual way to look at it is:



3.2 Content of the articles in the AI Act

AI Act

Art.17 – Quality Management System

1. **Providers** of high-risk AI systems shall **put a quality management system in place** that ensures **compliance with this Regulation**. That system shall be documented in a systematic and orderly manner in the form of written **policies, procedures and instructions**, and shall include at least the following aspects:

(a) a **strategy for regulatory compliance**, including compliance with **conformity assessment** procedures and procedures for the **management of modifications** to the high-risk AI system;

(b) techniques, procedures and systematic actions to be used for the **design, design and verification** of the high-risk AI system;

(c) techniques, procedures and systematic actions to be used for the **development**, **quality control and quality assurance** of the high-risk AI system;

(d) **examination, test and validation** procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;

e) **technical specifications**, including **standards**, to be **applied** and, where the relevant **harmonised standards** are **not applied** in full or do not cover all of the relevant requirements set out in Section 2, the **means** to be used to **ensure** that the high-risk AI system **complies with those requirements**;

(f) **systems and procedures for data management**, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems;

(g) the **risk management system** referred to in Article 9;

(h) the setting-up, implementation and maintenance of a **post-market monitoring system**, in accordance with Article 72;

(i) **procedures** related to the **reporting** of a **serious incident** in accordance with Article 73;

(j) the handling of **communication** with **national competent authorities**, other relevant authorities, including those providing or supporting the access to data, notified bodies, other **operators, customers** or other **interested parties;**

(k) **systems and procedures** for **record-keeping** of **all relevant documentation and information;**

(l) **resource management**, including security-of-supply related **measures**;

(m) an **accountability framework** setting out the responsibilities of the management and other staff with regard to all the aspects listed in this paragraph.

2. The implementation of the aspects referred to in paragraph **1 shall be proportionate to the size of the provider's organization**. Providers shall, in any event, respect the degree of rigor and the level of protection required to ensure the compliance of their high-risk AI systems with this Regulation.

3. Providers of high-risk AI systems that are subject to obligations regarding quality management systems or an equivalent function under relevant sectoral Union law may include the aspects listed in paragraph 1 as part of the quality management systems pursuant to that law.

4. For providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the obligation to put in place a quality management system, with the exception of paragraph 1, points (g), (h) and (i) of this Article, shall be deemed to be fulfilled by complying with the rules on internal governance arrangements or processes pursuant to the relevant Union financial services law. To that end, any harmonised standards referred to in Article 40 shall be taken into account.

3.3 Correspondence of the articles with the sections of the guide

The following table details the sections of this guide that address the different elements of this article:

Article	Regulation requirement	Guide Section
17.1.a	Regulatory compliance, conformity assessment and change management	Section 4.1
17.1.b	Design, Control and Verification	Section 4.2
17.1.c	Development, control and quality assurance	Section 4.3
17.1.d	Examination, testing and validation	Section 4.4
17.1.e	Technical specifications, standards and harmonised standards	Section 4.5

17.1.f	Data management systems and procedures.	Section 4.6
17.1.g	Risks management system	Section 4.7
17.1.h	Post-market monitoring system	Section 4.8
17.1.i	Serious Incident Reporting	Section 4.9
17.1.j	Communication	Section 4.10
17.1.k	Documentation	Section 4.11
17.1.l	Resource management	Section 4.12
17.1.m	Accountability framework	Section 4.13
17.2	Implementation of the quality management system proportional to the size of the provider's organization	Section 5.1
17.3	Financial institutions and providers subjects to sectoral legislation	Section 5.2
17.4	Financial institutions and providers subjects to sectoral legislation	Section 5.2

This mapping does not replace other requirements of the Regulation (technical documentation, conformity assessment, obligations under Chapter III, Section 2). Each of these must be addressed in its own dedicated technical guide.

4. What elements should I implement and how should I do it to develop an adequate quality management system?

The **first section** of the article consists **of a list of the elements** that, as a minimum, **our** quality management system **must contain**. This documentation will be reflected in **policies**, **procedures** and **written instructions**.

In the following subsections (4.1 to 4.13) **each of the elements set out in this list** will be fragmented, analysed and described and **facilitate the understanding** of the **requirements** described.

The rest of the sections of the article (2, 3 and 4) include a series of additional considerations that we will analyse in subsections 5.1 and 5.2.

4.1 Regulatory compliance, conformity assessment and change management

AI Act

Art.17.1a – Quality Management System

A **strategy for regulatory compliance**, including compliance with **conformity assessment** procedures and procedures for the **management of modifications** to the high-risk AI system.

The **conformity assessment** procedure consists of a whole series of processes and phases through which it is verified that a product complies with the requirements of harmonisation legislation required so that such a product can be placed on the market with certain guarantees.

The conformity assessment process has been developed in the "Conformity assessment Guide". This guide describes the two conformity assessment procedures applicable to AI systems, which are described in Annexes VI and VII of the AI Act. These procedures are:

- The internal self-assessment carried out by the provider itself
- External control carried out by a notified body.
- Each of these procedures in turn contemplates a series of phases that must be reached in order to understand that the conformity assessment has been passed.

- The choice of one or the other conformity assessment procedure is linked to the type of AI system developed by the provider in accordance with the provisions of Article "Conformity assessment" of the AI Act.

The quality management system should contain at least one indication of the conformity assessment procedure that is applicable to its high-risk AI system by reference to point 3(B) of the Conformity Assessment Guide.

The **Technical Documentation** guide establishes how to document the management of the modifications of the AI system in the following aspects:

- On the one hand, it is indicated that a list of both software and firmware, related to the AI system, must be maintained. This includes information on the versions of libraries, software components, or third-party elements. The information updates must be kept up to date and maintain a history of versions.
- Those predetermined changes that are established in the life cycle of the product must be contemplated within the quality management system. The technical documentation guide sets out the data that needs to be collected in the documentation in order to make the default changes.
- The documentation of each change made to the AI system must contain the same sections as the general documentation of the AI system. There must be records of having successfully passed the verification and validation procedures of the same, to ensure that the AI system retains the defined parameters of accuracy, robustness and cybersecurity.
- A distinction must be made between substantial changes, non-substantial changes and predefined changes, as set out it the article on modifications. Substantial changes may require repeating all or part of the community assessment procedure.

In section 4.2 Design, Control and Verification of Design and in section 4.4 Examination, testing and validation, aspects related to the verification and validation aspects respectively that must be taken into account when managing updates of the AI system are addressed.

The provider should consider that each change made to the AI system should, in itself, be subject to the same types of quality controls applicable to the entire assembly. In this way, a criterion of continuity of quality is established, not only applicable to the design, implementation, and commissioning process, but also applicable once the system has been commissioned, to any modification that it may undergo.

4.2 Design, Control and Verification of Design

AI Act

Art.17.1b - Quality Management System

Techniques, procedures and systematic actions to be used for the **design, design control and design verification** of the high-risk AI system.

The provider is responsible, during the design process of the AI system, for the systematic procedure that will allow the verification of said design. This design has to arise, not only from the technical and functional requirements of the system itself, but also from the mechanisms for mitigating the risks identified in the risks management plan.

A fundamental aspect that the provider must consider for the control and verification of the design is the relationship between the risks and the design, this implies having a follow-up by the teams involved on a regular basis.

There are three broad sets of AI system design aspects specifically addressed by the accompanying guides related to AI system cybersecurity, accuracy, and robustness.

Cybersecurity

The cybersecurity guide establishes the concept of AI system inventory so that cybersecurity is applied by design. In the design phase, the necessary security controls must be established, applied to the inventory of assets and threats. Specifically, it should be considered during the design and related to cybersecurity (see section Cybersecurity for the high-risk artificial intelligence system in the organization, of the cybersecurity guide):

- Involve the data protection officer (DPO), from the design of the AI system and for cybersecurity planning, as an interlocutor within the established working group to develop the planning and be present in decision-making.
- The relationship of cybersecurity as an establishment of security controls is directly related to the risks management system (see risks management guide).
- Within the design process, those responsible for monitoring the cybersecurity measures applied to the AI system must be established. Define a dashboard for monitoring the operation.

As indicated in section 3 of the cybersecurity guide, inventories of actors and assets must be carried out (see the section for details). The provider must keep the inventories updated and establish a person responsible for ensuring that the information they reflect is in accordance with the definitions established in the design of the AI system.

Accuracy

During the design of the high-risk AI system, the criteria that define the appropriate accuracy for the model are established, with the aim of covering the requirements established in the article "Accuracy, robustness and cybersecurity" of the European Regulation on Artificial Intelligence (see section Ensuring accuracy, in the accuracy guide). The control and verification of these design criteria must be carried out by the provider, guaranteeing the following aspects:

- The selected metrics are appropriate for measuring the accuracy of the model, according to its intended purpose and the mitigation of the risks detected for the model in the risks analysis.
- In the same way, the objective function will be verified to be adequate for the purpose and risks.
- The design includes the necessary mechanisms to ensure accuracy throughout the model's lifecycle.

The accuracy guide contains the technical measures that must be evaluated in the criteria described therein to ensure their quality.

Robustness

The robustness of an AI system must be verified and analysed throughout the life cycle, but its definition is established in the design phase. Recognized characteristics of the system must be identified and in which it must show robustness. These characteristics must be established in the design phase and must come directly from two main points:

- They must be aligned with the risks plan.
- They must be motivated by the intended purpose.

During the design, evidence must be available that the design of the robustness criteria is aligned with the points indicated.

From the design of the AI system, the provider must establish a series of properties to establish the quality control of the robustness. These properties are **reliability, stability, sensitivity, relevance and achievability**. Part of the systematic process of quality control for robustness is directly related to the design of the experiments, the implementation of which will be addressed in the following sections.

The robustness guide establishes the selection criteria for the proposed metrics (which can be consulted in Annex I of the same document). These metrics are set by design for the AI system and will need to be taken into account during the quality management process for the design phase.

4.3 Development, control and quality assurance

AI Act

Art.17.1c - Quality Management System

Techniques, procedures and systematic actions to be used for the **development**, **quality control and quality assurance** of the high-risk AI system.

In the same way that the design proposes systematic procedures for the three aspects related to the technical requirements related to cybersecurity, accuracy and robustness, it is the responsibility of the provider to extend these procedures to the development process of the AI system.

To this end, in general, the provider must **monitor** the specifications established in the design, their layout and compliance, according to the requirements that must be covered, in relation to cybersecurity, accuracy and robustness. This monitoring can be carried out with various market tools (*open source* or commercial) that allow defining an ML-OPS operation that can follow the trace of the actions carried out from the design and its implementation during the development of the solution.

The actions described here must be included within the ML-OPS processes of the AI system, iteratively in each step of the development process and ensuring that the specifications established in the system design are met.

Specific to each of the elements that we have considered in previous sections, the following should be considered.

Cybersecurity

The cybersecurity guide establishes that, during the implementation of the AI system, the implementation of security controls according to the identified vulnerabilities must be addressed.

These security controls are aimed at establishing safeguards on data vulnerabilities, adversarial attacks, and the exploitation of flaws in the AI system.

As quality assurance measures for cybersecurity during the development process in the cybersecurity guide, the following actions are proposed to the provider, among others: red/blue team mechanics, specific tests with automatic tests, continuous SAST and DAST, analysis of known CVE/VWE vulnerabilities and generic and specific penetration tests for the AI system on AI vulnerability vectors (adversarial or penetration attacks)

Quality during the development of the system requires an analysis of the cybersecurity indicators established in the scorecard to ensure that they remain correct throughout the

development. The evidence of the monitoring of cybersecurity indicators and their guarantee of maintenance is a way of illustrating **how** quality actions are demonstrated.

Accuracy

Accuracy quality assurance during AI system development is based on the execution of automated tests designed to validate, at each stage of model development, its relationship with the accuracy defined in the design. Therefore, these automated tests must take into account the following points:

- The preprocessing of the data (in the accuracy guide).
- During the development process, overlearning should be avoided, as detailed in the accuracy guide).
- The selected baseline models, with which a comparison is established to monitor the development and ensure their quality control (see section 4.1.3 of the accuracy guide).

The main objective of quality control during development is to ensure that the metrics and their values defined in the design remain within the specified ranges, and that the system, at this stage, performs as intended or progressively achieves the expected behaviour. Therefore, it is necessary to keep evidence of all validations performed.

Robustness

Robustness quality control is set out in a two-step procedure that is performed throughout the development of the AI system:

- Verification: Understood as the confirmation, with the provision of evidence, that the requirements specified in the design are met as they were established.
- Validation: Understood as the confirmation of the requirements established on the intended purpose, and in relation to the criteria for robustness that have been established in the design phase.

Additionally, in this verification and validation process, two additional parameters must be taken into consideration as metrics associated with those already selected, whose values must be established in design and guaranteed in development:

- Efficiency: during development, evidence of the efficiency of the system must be generated in validation and verification, as detailed in the robustness guide.
- Performance: In the Performance in AI systems section, you can dive deeper into performance related to robustness.

In the Validation and Verification section of the robustness guide, these two aspects are addressed. The provider during the development of the system must ensure that the system is verified and validated, and that evidence of the process is recorded.

4.4 Examination, testing and validation

AI Act

Art.17.1d - Quality Management System

The **examination, test and validation** procedures to be carried out **before**, **during** and **after the development** of the high-risk AI system, and the **frequency** with which they have to be carried out;

Throughout the related sandbox guidelines on cybersecurity, accuracy and robustness that accompany the sandbox, the examination, testing and validation measures that apply to AI systems have been specified, in accordance with compliance with the requirements set out in the European Regulation on Artificial Intelligence

Quality assurance of security controls applied to mitigate system vulnerabilities are in themselves adequate testing procedures to validate that such quality is achieved. In this sense, all the tests carried out in the previous section, with the aim of guaranteeing quality during development, should record at least:

- The version of the data with which they were made, along with the version of the model.
- The expected results
- The results obtained
- Whether the test allows validation of the validated aspect or not
- If it is not validated, indicate the criticality

In the event that previous unsuccessful tests are being corrected, it should include at least:

- The reference of the previous test battery in which the error was logged

The solution applied to correct it. **Not all systems will require the same level of testing complexity. The scope of testing must be proportionate to the risk and the design of the system, in accordance with Article 17(2).**

Cybersecurity

In the case of cybersecurity, its assurance is in itself a process of examination, testing and validation, since quality in cybersecurity cannot be understood without it being constantly *stressed* and tested. For this reason, the methods described in the previous section are considered as examination and proof mechanisms. To ensure that cybersecurity is properly validated, the testing process described in this section will be followed.

Accuracy

The procedures for examining and testing accuracy are somewhat more specific given their formal nature, although they should be recorded and reviewed as indicated in this section. These procedures can be established in two large groups:

- Statistical significance test (see section 4.3.2 accuracy guide). This type of test allows the validation of the selected accuracy metric to be statistically validated. The details of the typology of possible types and their implementation can be seen in the accuracy guide.
- Database and model benchmarks (see section 4.3.3 of the accuracy guide). Benchmarks depend on the task and the state of the art of the field; therefore, they will need **to be updated** as time goes by and models and databases **evolve**.

Robustness

These tests are used to quantify that the system achieves the robustness established by design, in all steps of the life cycle, but especially for the implementation of a system or the distribution of an application. These experiments must be in addition to the verification and validation operations carried out during development.

The steps in the robustness experimentation process involve planning (see Annexes to the robustness guide), conducting the experiments, analysing the results, interpreting them, and deciding on the outcome and the action to be taken. During all these steps, the necessary evidence of their action must be left, which justifies the next step, and the decisions made.

Section 7.1.2 deals in detail with the process indicated here, for carrying out tests aimed at guaranteeing the robustness of the system in accordance with the established requirements and the mentioned design procedure. It is a quality control for the robustness of the system that the provider must implement. As indicated, the results of the experiments must be properly recorded.

4.5 Technical specifications, standards and harmonised standards

AI Act

Art.17.1e - Quality Management System

The **technical specifications**, including **standards**, to be **applied** and, where the relevant **harmonised standards** are **not applied** in full or do not cover all of the relevant requirements set out in Section 2, the **means** to be used to **ensure** that the high-risk AI system **complies with those requirements**;

The defined quality management system must incorporate some of the following elements in its documentation:

- Where available and used by the provider, **a list of harmonised standards** applied together with the requirements of the Regulation that they cover.

- Where they exist and have been used by the provider, **a list of common specifications** applied together with the requirements of the Regulation that they cover.
- **Technical specifications applied** together with the requirements of the Regulation that they cover. In the event that the provider has covered all the requirements of the Regulation with the application of harmonised standards or common technical specifications, it shall not be necessary to indicate other national and international technical specifications and standards.

To **document** this section, we recommend **the following:** the quality management system could incorporate the harmonised standards that cover some or part of the requirements for AI systems and in turn another set of international standards and standards that cover the rest of the remaining requirements.

There are currently no harmonised standards approved by the European standardisation bodies or common specifications approved by the European Commission covering the requirements placed on AI systems by the Regulation.

For the sandbox, and as long as there are no harmonised standards and common specifications that do not exist or are not applied by the provider, **the quality management system** must contain those technical specifications that have been applied by the provider to meet the requirements of the Regulation, in this case:

- **The Technical Guides** that have been provided together with the requirements covered by the Regulation.
- For those cases in which the providers have gone beyond the Technical Guides provided, the **technical specifications based on the national or international standards** that may have been used together with the requirements covered by the Regulation.

The way to document this information could be based on the following table (non-real **example**):

Article	Harmonised standard/common specification/standard
Article 12.2	National Standard X
Articles 14. Paragraphs 1 and 2	Harmonised standard X
Article 15. Paragraphs 1, 2 and 3.	ISO X Standard

The table is indicative: not all requirements of the Regulation necessarily need to be linked to a standard or norm.

For more information , please refer to the Conformity Assessment Guide and the Technical Documentation Guide.

4.6 Data management systems and procedures

AI Act

Art.17.1f – Quality Management System

Systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems;

The defined quality management system must incorporate in its documentation the data management systems and procedures described in this section. The AI Act's article "Data and Data Governance" contains a broader list of requirements that every high-risk AI system must meet. In summary, the training data, validation, and testing will be subject to the following data governance and management practices:

- Choosing a **suitable design**.
- **Data collection processes**.
- **Processing operations** for data **preparation** (*annotation, labelling, cleansing, enrichment, and aggregation*).
- **Formulation of the relevant assumptions** with respect to the **information of the data they measure and represent.**
- **Pre-assessment of the availability, quantity and adequacy** of the required datasets:
  - They will be relevant and representative.
  - They will be complete.
  - They will have the appropriate statistical properties.
  - They shall take into account, depending on their intended purpose, the particular characteristics or elements of the geographical, behavioural or functional context in which the HRAIS is intended to be used.
- **Analysis of biases** (*taking into account those that may affect the health and safety of people or give rise to some type of discrimination prohibited by Union law).*
- **Detection and remediation** of **gaps or deficiencies** in data:
  - They will be error-free.

The provider must document in its Quality Management System how these processes are implemented, specifying responsibilities, tools, evidence and review criteria. These requirements shall apply without prejudice to the principles and obligations of the GDPR including data minimization, purpose limitation and impact assessments where applicable.

In addition, to the extent strictly **necessary** to ensure the **monitoring, detection and correction of bias,** special categories of personal data may be processed, always providing appropriate safeguards **for the fundamental** rights and freedoms **of individuals.**

For the proper fulfilment of these requirements, the "Data and Data Governance Guide" has been developed. This guide presents the measures that will be used by providers and deployers to comply with the article "***Data and data governance***". The "Technical documentation" section of this guide details how the documentation of each measure should be addressed.

4.7 Risks management system

AI Act

Art.17.1g – Quality management system.

The **risks management system** referred to in Article 9.

A **risks management system** aims to **identify and analyse risks** and implement **mitigating measures**. By risk, we mean any factor with a probability of happening and an impact in case it happens. In fact, risk is calculated as the product of such factors, probability and impact.

In the context of the European Regulation on Artificial Intelligence, the risks management system to be developed should pay particular attention to **risks that may affect the health, safety and fundamental rights of individuals.** In this sense, the focus should be on the identification and analysis of any risk that may have a special impact on the mentioned elements. Therefore, appropriate measures must be implemented to mitigate the risks identified and assessed.

For the proper compliance with these requirements, the "Risks Management Guide" has been developed. This guide presents the measures that will be used by providers and deployers to comply with the article "***Risks management system***". The "Technical documentation" section of this guide details how the documentation of each measure should be addressed.

4.8 Post-market monitoring system

AI Act

Art.17.1h – Quality management system

The setting-up, implementation and maintenance of a **post-market monitoring system**, in accordance with Article 72;

A post-market monitoring system for high-risk AI systems is conceived as a **set of processes and tools** aimed at collecting data from a system to transform it into a series of indicators about its activity with the aim of monitoring artificial intelligence (AI) **systems after its**

market launch, placing into service, as applicable. The objective is for the provider to be able to assess whether the AI systems meet the requirements set out in Chapter III, Section 2, throughout the entire life cycle of the intelligent system.

For the adequate compliance with these requirements, the "Guide to post-market monitoring system" has been developed. This guide presents the measures that will help providers and deployers to comply with the article "*Post-market surveillance*". The monitoring system is primarily structured around the provider, without prejudice to the obligations relating to use, oversight and notification that fall upon the deployer. The "Technical documentation" section of this guide details how the documentation of each measure should be addressed.

4.9 Reporting of Serious Incidents

AI Act

Art.17.1i – Quality Management System

The **procedures** related to the **reporting** of a **serious incident** in accordance with Article 73;

The incident management guide establishes in section 4.1.1, how to address the reporting requirements of serious incidents according to the European Regulation on Artificial Intelligence. This section describes the procedure for reporting serious incidents, and the measures that allow this procedure to be addressed. An important aspect of incident reporting procedures is that they also involve the deployer, since they are responsible for notifying the provider of the AI system through the channel established for this purpose. Special attention is required by section 4.1.1 of the mentioned guide, which visually summarises the procedure for reporting serious incidents, which must be included in the quality management system.

The quality management system must have clearly documented at least:

- The chain of responsibility for the notification of the incident, which includes the figure of the DPO, as well as other figures of relevance at the level of compliance that are applicable.
- The mechanism for recording incidents that is used, as well as the mechanism for generating and preserving evidence.
- The incident resolution chain, with those responsible for its application.
- In the case of the provider, and that the incident affects several (potentially all) AI system deployment managers, the chain of responsibility for communication, channel, and format, where clear instructions must be provided to the deployer how to proceed for that particular incident and whether deployers should, in any case, in turn notify the authorities, natural persons affected by the incident in their own systems.

- The notification of the incident during the use of the system is an aspect that may also be the responsibility of the deployer of the AI system, so the aspects indicated apply to it as well.

4.10 Communication

AI Act

Art.17.1j – Quality Management System

The handling of **communication** with **national competent authorities**, other relevant authorities, including those providing or supporting the access to data, notified bodies, other **operators, customers** or other **interested parties;**

The Regulation establishes throughout its articles a set of obligations that are required of providers and deployers of AI systems in relation to the communications that they have to deploy with the national competent authorities, notified bodies, customers, etc.

The list of communications can be consulted in the Guide to concepts and transversal information.

The defined quality management system must incorporate in its documentation the different communication procedures derived from the previously indicated obligations, among others, these procedures may include:

- The communication channel or channels **that will be used for each of the communications arising from the different obligations described** must be indicated and described.
- The **format or formats** in which the documents that are required must be provided.
- The person or persons responsible **for managing the different communications** must be appointed.
- The tools that allow access to the data, records, source code and other actions that derive from these obligations must be **implemented and described**. Some of these tools are mentioned in the Technical Documentation Guide.

For further information, please note that the obligations arising from Annex VII of the AI Act on the assessment by a notified body of the quality management system and technical documentation are also discussed in the Technical Documentation Guide and the Conformity Assessment Guide.

4.11 Documentation

AI Act

Art.17.1k – Quality Management System

Systems and procedures for **record-keeping** of **all relevant documentation and information;**

The documentation of the AI system has been articulated throughout the guides that accompany it and related to the sandbox in two aspects.

On the one hand, each guide, especially those that have a more technical and less procedural aspect, establish the documentation criteria necessary for the correct application of the measures. This is the case, among others, with the cybersecurity, accuracy, robustness and records guides.

On the other hand, specifically, the Technical Documentation guide provides the structure of the content of the technical documentation of the high-risk AI system and the criteria for its conservation.

The provider shall establish a number of technical measures to maintain a record of relevant documentation and information. The documentation must be maintained throughout the entire lifecycle of the system, from its design to its withdrawal and must be also retained for the periods required by the Regulation after the system has been withdrawn to this end, in order to keep the documentation up to date and to maintain a record of it the provider must least:

- Establish, within the management processes of the artificial intelligence system, a **procedure for monitoring changes** that are reflected in the updating of documentation.
- Generate a **chain of responsibility** or establish a person responsible for managing the change in the system, who is responsible for updating the documentation according to the changes.
- The documentation of **changes to the** AI system should be at the **level of completeness of the rest** of the technical documentation described in this guide.
- **Establish, define and size** according to a document management system, an equivalent technical solution, which allows you to guarantee its conservation and changes. The system must ensure that documentation is retained and accessible by notified bodies for evaluation. Likewise, any technical documentation that aims to serve as instructions to the deployer must be accessible to him.

4.12 Resource management

AI Act

Art.17.1l – Quality management system

Resource management, including security-of-supply related **measures**.

Before addressing this section, the reader is recommended to revisit section 1.2 where the relationship between a quality management system as understood in the ISO 9001 reference standard and the one developed in the European Regulation on Artificial Intelligence is explained in detail.

Taking into account what is indicated in section 1.2, it should be noted that the management of resources has been linked more directly to what is set out in ISO 9001. Thus, in this section, we are going to try to guide the reader by detailing the main elements that must be considered in the management of resources:

People:

- **According to ISO 9001:** *"The organization must determine and provide the necessary people for the effective implementation of a quality management system and for the operation and control of its processes."*
- **How to approach it:** What we must do in this case is to analyse in detail the people and profiles that we will need to be able to address all the elements established in the quality management system of the AI Act. To do this, we must assess these elements and the information provided for each of them throughout this guide in order to be able to make the most appropriate estimate possible.

Infrastructure:

- **According to ISO 9001:** *"The organization must determine, provide, and maintain the infrastructure necessary for the operation of its processes and achieve compliance of products and services."*
- **How to approach it:** ISO 9001 includes some elements in the infrastructure section such as software and hardware resources or information and communication technologies. In the context of the development of the quality management system of the European Regulation on Artificial Intelligence that has been analysed throughout this guide, the elements related to the infrastructure would be all those technical and technological resources necessary for the development of said system. For example, for the development of the examination, testing and validation procedures of section "d)", as indicated in section 4.4 and as detailed in the guides referenced there on topics such as cybersecurity, accuracy and robustness, the necessary infrastructure must be in place for the development of these tests.

Environment for the operation of the processes:

- **According to ISO 9001**: *"The organization must determine, provide, and maintain the environment necessary for the operation of its processes and to achieve the conformity of products and services."*
- **How to approach it:** ISO 9001 includes in this section some elements such as human, physical, social or psychological factors. In this context, the organization must determine what are the ideal factors in each scenario (temperature, lighting, air circulation, noise, stress prevention, etc.) for the adequate development of the quality management system.

Tracking and measurement resources:

- **According to ISO 9001**: *"The organization must determine and provide the necessary resources to ensure the validity and reliability of the results when monitoring or measurement is carried out to verify the conformity of products and services with the requirements. The organization must ensure that the resources provided are appropriate for the specific type of monitoring and measurement activities undertaken and that they are maintained to ensure continued suitability for their purpose. In addition, the organization must retain appropriate documented information as evidence that monitoring and measurement resources are fit for purpose."*
- **How to approach it:** AI systems are software artifacts with a very special nature, which means that their behaviour over time can vary, not only in those cases in which the system continues to learn over time, but in general in all scenarios. The appearance of unexpected domain spaces in the input data, or even the existence of undetected errors or failures that can affect accuracy, robustness, cybersecurity (see corresponding guides) or even the intended purpose causing harm to people or affecting rights and freedoms, are aspects that cannot be ruled out. This type of monitoring fits into the scenario of post-marketing monitoring (see this guide), in which the parameters, metrics and technical controls that were established in the design are monitored and with the aim of covering the risks found in the risks plan, especially those related to guaranteeing the health, safety and fundamental rights of people.

Knowledge of the organization:

- **According to ISO 9001**: *"The organization must determine the knowledge necessary for the operation of its processes and to achieve the conformity of products and services. This knowledge should be maintained and made available to the extent that it is needed. When addressing changing needs and trends, the organization must consider its current knowledge and determine how to acquire or access the additional knowledge needed and the required updates."*
- **How to approach it:** ISO 9001 includes in this section knowledge gained from experience (e.g. lessons learned from projects or results of process improvements), by consulting internal sources (e.g. intellectual property or internal documentation generated from previous projects and experiences) and by consulting external sources (e.g. consultation of norms and standards or collection of knowledge from

clients or providers). In this context, in order to develop the quality management system of the European Regulation on Artificial Intelligence, the organisation must ensure that it has the necessary and sufficient knowledge to address each of the aspects required by the Regulation and analysed throughout this guide.

4.13 Accountability framework

AI Act

Art.17.1m – Quality Management System

An **accountability framework** setting out the responsibilities of the management and other staff with regard to all the aspects listed in this paragraph.

The objective of this accountability framework is to establish the responsibilities and authorizations around the different elements that make up the quality management system. Responsibilities should be assigned to all personnel involved in any of these processes and should be reflected and documented in job descriptions and similar statements, where appropriate. In addition, the responsibilities assigned must be well documented and reflected in the document developed to include the quality management system.

Thus, in this section we will collect all the elements that have been addressed throughout this guide and provide some examples of how responsibilities could be assigned for each of them, reviewing each of the sections of the article:

Example – Visual summary of responsibility assignment

Below, a table can be found as a visual summary of the following responsibilities within the accountability framework, which will be analysed by section.

Requirements	Proposed responsible entity
Strategy for regulatory compliance	Legal profile
Systematic techniques to be used in the design	Desing team member
Systematic techniques to be used in development	Desing team member
Examination, Testing, and Validation Procedures	Red/Blue Team Member or QA Team Member
Technical specifications, including the rules, that will be applied	Legal profile + technical profile

Data management systems and procedures	CDO or AI System Owner
The risk management system	CDO or AI System Owner
Post-market monitoring system	QA team member
Procedures associated with the notification of serious incidents	Quality manager
Communication with the NCAs	DPO or Legal department member
Documentation record	Compliance team member
Resource management	RRHH team member

AI Act

Art.17.1a – Quality Management System

A **strategy for regulatory compliance**, including compliance with **conformity assessment** procedures and procedures for the **management of modifications** to the high-risk AI system;

Example – Assignment of Responsibility

As a general rule, those responsible for this section should have a legal profile. However, given the close relationship between the conformity assessment process and the AI system design process, it is recommended that members of the team responsible for system design are also present, as well as those assigned post-market surveillance tasks.

AI Act

Art.17.1b – Quality Management System

The techniques, procedures and systematic actions to be used for the **design, design and verification** of the high-risk AI system;

Example – Assignment of Responsibility

Those responsible for this section are identified within the team that carries out the design, which is responsible for monitoring the quality in the design process, whose work is supervised and validated by the technical managers of the provider. Thus, in an SME or a newly created company, they can be identified within the product managers, and in larger companies they can be directly related to or to the CTO's office.

AI Act

Art.17.1c – Quality Management System

The techniques, procedures and systematic actions to be used for the **development**, **quality control and quality assurance** of the high-risk AI system;

Example – Assignment of Responsibility

As in the previous section, the structure of the development team will be responsible to the full extent of quality assurance during the development process. This assignment of responsibility should be directed from the equivalent figures project manager, team leaders to those associated with the development team. In the same way as in the previous case, they must report depending on the structure of the provider to the corresponding internal figure and in larger companies again related to the CTO.

AI Act

Art.17.1d – Quality Management System

The **examination, test and validation** procedures to be carried out before, during and after the development of the high-risk AI system, and the frequency with which they have to be carried out;

Example – Assignment of Responsibility

The assignment of responsibility for examination, testing, and validation procedures is related to the structure that the quality assurance team has within the provider structure. For all associated procedures, there must be a team responsible for their performance, generation of evidence and validation of results. Depending on the size of the provider's organization, this team may have different sizes and structures: from small teams in red/blue team format, to large QA and validation teams. Regardless of size, it is

recommended to the provider that the design and development teams be different from the testing teams.

AI Act

Art.17.1e – Quality Management System

The **technical specifications**, including **standards**, to be **applied** and, where the relevant **harmonised standards** are **not applied** in full or do not cover all of the relevant requirements set out in Section 2, the **means** to be used to **ensure** that the high-risk AI system **complies with those requirements**;

Example – Assignment of Responsibility

The profile of those responsible for this section will include people with legal knowledge of the subject, as well as more technical profiles related to the different harmonised standards and, where appropriate, international standards that are intended to be applied. The distinction between these profiles is due to the very nature of the technical specifications and harmonised standards. Thus, the legal profile will, above all, assess the legal consequences of the non-application/partial application/full application of harmonised standards/common specifications/international standards for the AI Act. For their part, those responsible for having a markedly technical profile will focus on assessing which harmonised standards/common specifications/international standards apply to the specific AI system and how these should be implemented.

AI Act

Art.17.1f – Quality Management System

Systems and procedures for data management, including data acquisition, data collection, data analysis, data labelling, data storage, data filtration, data mining, data aggregation, data retention and any other operation regarding the data that is performed before and for the purpose of the placing on the market or the putting into service of high-risk AI systems;

Example – Assignment of Responsibility

Data management systems and procedures, as described in the data and data governance guidance developed to comply with the "Data and Data Governance" article of the Regulation, should ideally be coordinated and managed by a cross-organizational figure (such as a CDO in those organizations that have one). This controller will be responsible for ensuring that all the elements described in the mentioned guide are addressed for the adequate compliance with data and data governance requirements. As well as coordinating the rest of the possible figures involved, for example, it will be necessary to have the support of the DPO for adequate compliance with the regulations

on the protection of personal data when applicable. In a smaller organization, such as an SME, this role may be held by the AI system manager, if, for example, in this case the person responsible is in charge of complying with all the requirements of the European AI Act.

AI Act

Art.17.1g – Quality Management System

The **risks management system** referred to in Article 9.

Example – Assignment of Responsibility

The risks management system, as described in the risks management guide developed to comply with the article "Risks management system" of the AI Act, should ideally be coordinated and managed by a figure who crosses the entire organization (such as a CRO in those organizations that have one). This person will be responsible for ensuring that all the elements described in the mentioned guide are addressed for the adequate compliance with the requirements related to risks management. In a smaller organization, such as an SME, this role may be held by the AI system manager, if, for example, in this case the person responsible is in charge of complying with all the requirements of the European Regulation on Artificial Intelligence.

AI Act

Art.17.1h – Quality management system

The setting-up, implementation and maintenance of a **post-market monitoring system**, in accordance with Article 72;

Example – Assignment of Responsibility

As detailed in the guide developed for the implementation of a post-market monitoring system, the requirements described in the mentioned article are focused on the measures that the service provider must take once the intelligent system is in production. Therefore, it is the responsibility of the provider to assess that the requirements set out in this article are met throughout the life cycle. The responsibility for defining and coordinating this system, in a large organization, could fall on the teams in charge of quality assurance. As mentioned in section b), for all associated procedures, there must be a team responsible for their performance, generation of evidence and validation of results. Depending on the size of the provider's organization, this team may have different size and structure. Regardless of size, it is recommended to the provider that the design and development teams be different from the testing teams.

AI Act

Art.17.1i – Quality Management System

The **procedures** related to the **reporting** of a **serious incident** in accordance with Article 73;

Example – Assignment of Responsibility

In the same section, the chains of responsibility that must be taken into account have been indicated, and their structure, which according to the size of the company must be adapted to have a clear responsibility. It is very important that the provider has a communication channel with the deployer for the incident reporting mechanism. Reference is made to the mentioned section for details.

AI Act

Art.17.1j – Quality Management System

The handling of **communication** with **national competent authorities**, other relevant authorities, including those providing or supporting the access to data, notified bodies, other **operators, customers** or other **interested parties;**

Example – Assignment of Responsibility

Depending on the type of communication that is contemplated, it will be advisable to identify different responsible parties. It may be interesting that there is a central person in charge that brings together each and every one of the possible communications mentioned in the Regulation and, in turn, there are specific lower levels for the management of each of the communications. For example, providers are obliged to provide the documentation required by the authorities in terms of the protection of fundamental rights. This precept enabled data protection authorities to request certain documentation generated as a result of compliance with the AI Act, this communication, although it may be centralized in a general manager, the specific management of it could be carried out by a specific unit, in this case, the Data Protection Officer (if any) or corresponding legal department.

AI Act

Art.17.1k – Quality Management System

Systems and procedures for **record-keeping** of **all relevant documentation and information;**

Example – Assignment of Responsibility

The technical documentation guide establishes a series of contents that must be recorded and incorporated for the AI system. This type of information is very vertical and extensive throughout the company, and as mentioned in the mentioned guide, depending on the size of the provider's organization, it can be carried out by different teams, or by more multidisciplinary teams (in the case of SMEs and start-ups). Given this vertical nature, it is necessary that there is a figure responsible for the coordination and general aspects of the process (format, repository), which in large companies may be related to compliance teams, and in SMEs or newly created companies, depend on the management structure of the latter.

AI Act

Art.17.1l – Quality management system

Resource management, including security-of-supply-related **measures**.

Example – Assignment of Responsibility

The management of resources, addressed in this same guide, could be coordinated by a figure transversal to the entire organization as a department in charge of quality assurance. In any case, each of the pillars described within the management of resources is probably supported by different departments. Thus, for example, the management of resources related to people and profiles and the necessary knowledge would be the responsibility of the human resources department.

5. Other elements to consider

5.1 Implementation of the quality management system proportional to the size of the provider's organization

This section will deal with the provisions of section 2 of the article:

AI Act

Art.17.2 – Quality management system

The implementation of the aspects referred to in paragraph **1 shall be proportionate to the size of the provider's organization**.

Additionally, we collect in this section what is indicated in **Recital 146**:

AI Act

Recital 146

Moreover, in light of the very small size of some operators and in order to ensure proportionality regarding costs of innovation, it is appropriate to allow microenterprises to fulfil one of the most costly obligations, namely to establish a quality management system, in a simplified manner which would reduce the administrative burden and the costs for those enterprises without affecting the level of protection and the need for compliance with the requirements for high-risk AI systems. The Commission should develop guidelines to specify the elements of the quality management system to be fulfilled in this simplified manner by microenterprises.

This text deals with the need to **ensure proportionality** in the application of the Regulation considering the **size** of the operators and the **costs** of innovation. It is proposed **to scale the** most expensive obligations to **the size of the company**, minimizing the associated costs for microenterprises when establishing the quality management system discussed in this guide, to **reduce administrative burden and costs**. In doing so, it seeks to protect micro-enterprises without compromising the level of AI protection or the need to comply with the requirements applicable to high-risk AI systems.

Overall, the aim of this text is to find a balance between the application of the Regulation and the need to protect micro-enterprises that might have difficulties in complying with all regulatory obligations. The purpose is to promote innovation and growth of companies, while ensuring the protection of deployers. Proportionality is a key principle in the

Regulation and this text emphasises the need to apply it correctly in order to achieve these objectives.

5.2 Financial institutions and providers subjects to sectoral legislation

This section will deal with the provisions of paragraphs 3 and 4 of the article that establishes:

AI Act

Art.17.3 – Quality Management System

Providers of high-risk AI systems that are subject to obligations regarding quality management systems or an equivalent function under relevant sectoral Union law may include the aspects listed in paragraph 1 as part of the quality management systems pursuant to that law.

This section refers to the regulation of providers of high-risk artificial intelligence systems and how they can comply with the obligations related to quality management systems. Specifically, it is established that in the case of those providers that are already subjects to obligations related to quality management systems according to the relevant sectoral legislation of the European Union, the aspects described in paragraph 1 may form part of the existing quality management systems under that legislation.

In other words, the text suggests that in some cases specific regulatory requirements for high-risk AI could be integrated into existing quality management systems that apply to providers of high-risk AI systems, as long as such systems comply with applicable European Union sectoral regulations.

The purpose of this text is to provide clarity and consistency in the regulation of high-risk AI, while avoiding duplication of requirements and facilitating compliance. This can also help improve the effectiveness and efficiency in the regulation of high-risk AI, as existing quality management systems are leveraged to meet new regulatory requirements. In summary, the aim of the text is to ensure the regulation of high-risk AI in the EU, reducing the administrative and cost burden for providers, while ensuring the safety and security of the person responsible for the final deployer.

AI Act

Art.17.4 – Quality Management System

For providers that are financial institutions subject to requirements regarding their internal governance, arrangements or processes under Union financial services law, the obligation to put in place a quality management system, with the exception of paragraph 1, points (g), (h) and (i) of this Article, shall be deemed to be fulfilled by complying with the rules on internal governance arrangements or processes pursuant to the relevant Union financial services law. To that end, any harmonised standards referred to in Article 40 shall be taken into account.

This text refers to the regulation of providers that are financial institutions and how they can comply with the obligations to establish a quality management system within the framework of European Union legislation on financial services. In particular, it provides that, if financial institutions already comply with the requirements relating to their internal governance systems or processes under EU financial services legislation, they will be considered to have complied with the obligation to establish a quality management system. However, it is specified that in any case the provisions of subsections g) h) and i) must be complied with.

This text suggests that standards relating to internal governance systems or processes can meet the obligations to establish a quality management system. In addition, it is mentioned that all the harmonised standards mentioned in the article "Harmonised standards and standardization deliverables" of the Regulation will be taken into account in this context.

The purpose of this text is to promote efficiency and simplification in the regulation of providers that are financial institutions and that are already subjects to specific internal governance requirements under EU financial services law. This means that they will not have to comply with additional requirements in relation to the quality management system if they already comply with internal governance requirements (with the exception of subparagraphs (g), (h) and (i)). The aim of this approach is to avoid duplication of requirements and reduce the administrative burden for financial institutions. In summary, the text seeks to improve the effectiveness and efficiency of the regulation of providers that are financial institutions, while guaranteeing the protection of deployers.

This guide takes as a reference Regulation (EU) 2024/1689 of the European Parliament and of the Council, of 13 June 2024 (Artificial Intelligence Act).

6. Self-assessment questionnaire

To carry out a self-assessment of compliance with the requirements of the Artificial Intelligence Act referred to in this guide, a global self-assessment questionnaire has been generated with a series of questions with the key points to be taken into account regarding the obligations dictated by the articles of the AI Act mentioned in this guide.

It will be necessary to refer to this document in order to carry out the section of the self-assessment questionnaire corresponding to this guide.

7. References, Standards, and Norms

For the development of this guide, the following norms and standards have been consulted and used:

[1] ISO-IEC 38505-1 - Information technology - Governance of IT - Governance of data. Part 1: Application of ISO/IEC 38500 to the governance of data

[2] ISO-IEC 38507 - Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations

[3] ISO-IEC 5338 - Information technology - Artificial intelligence - AI system life cycle processes

[4] ISO-IEC 24027 - AI Algorithmic bias - Information technology - Artificial Intelligence (AI) - Bias in AI systems and AI-aided decision making

[5] ISO-IEC 5259-1 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 1: Overview, terminology, and examples

[6] ISO-IEC 5259-2 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 2: Data quality measures

[7] ISO-IEC 5259-3 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 3: Data quality management requirements and guidelines

[8] ISO-IEC 5259-4 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 4: Data quality process framework

[9] ISO-IEC 5259-5 - Artificial intelligence - Data quality for analytics and machine learning (ML) - Part 5: Data quality governance

[10] ISO-IEC 8183 - Information technology — Artificial intelligence — Data life cycle framework

[11] ISO-IEC 42001 - Information technology - Artificial intelligence - Management system

[12] ISO-IEC 22989 - Information technology - Artificial intelligence - Artificial intelligence concepts and terminology

[13] prEN 18286 Artificial intelligence - Quality management system for EU AI Act regulatory purposes

[14] VERMA, Sahil and RUBIN, Julia, 2018. Fairness definitions explained. In: Proceedings of the International Workshop on Software Fairness - FairWare '18 [online]. Gothenburg, Sweden: ACM Press. 2018. p. 1–7. [Accessed 6 May 2019]. Fairness definitions explained | Proceedings of the International Workshop on Software Fairness (acm.org)

[15] MITCHELL, Shira, POTASH, Eric, BAROCAS, Solon, D'AMOUR, Alexander and LUM, Kristian, 2020. Prediction-Based Decisions and Fairness: A Catalogue of Choices, Assumptions, and Definitions. arXiv:1811.07867 [stat] [online]. 24 April 2020. [1811.07867] Prediction-Based Decisions and Fairness: A Catalogue of Choices, Assumptions, and Definitions (arxiv.org)

[16] GAJANE, Pratik and PECHENIZKIY, Mykola, 2018. On Formalizing Fairness in Prediction with Machine Learning. arXiv:1710.03184 [cs, stat] [online]. 28 May 2018. [Accessed 30 October 2020]. [1710.03184] On Formalizing Fairness in Prediction with Machine Learning (arxiv.org)

[17] AGARWAL, Alekh, DUDÍK, Miroslav and WU, Zhiwei Steven, 2019. Fair Regression: Quantitative Definitions and Reduction-based Algorithms. arXiv:1905.12843 [cs, stat] [online]. 29 May 2019. [Accessed 30 October 2020]. [1905.12843] Fair Regression: Quantitative Definitions and Reduction-based Algorithms (arxiv.org)

[18] Confusion matrix, 2020. Wikipedia [online]. [Accessed 30 October 2020].

Financiado por
la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de
Recuperación,
Transformación
y Resiliencia

España | digital 2026