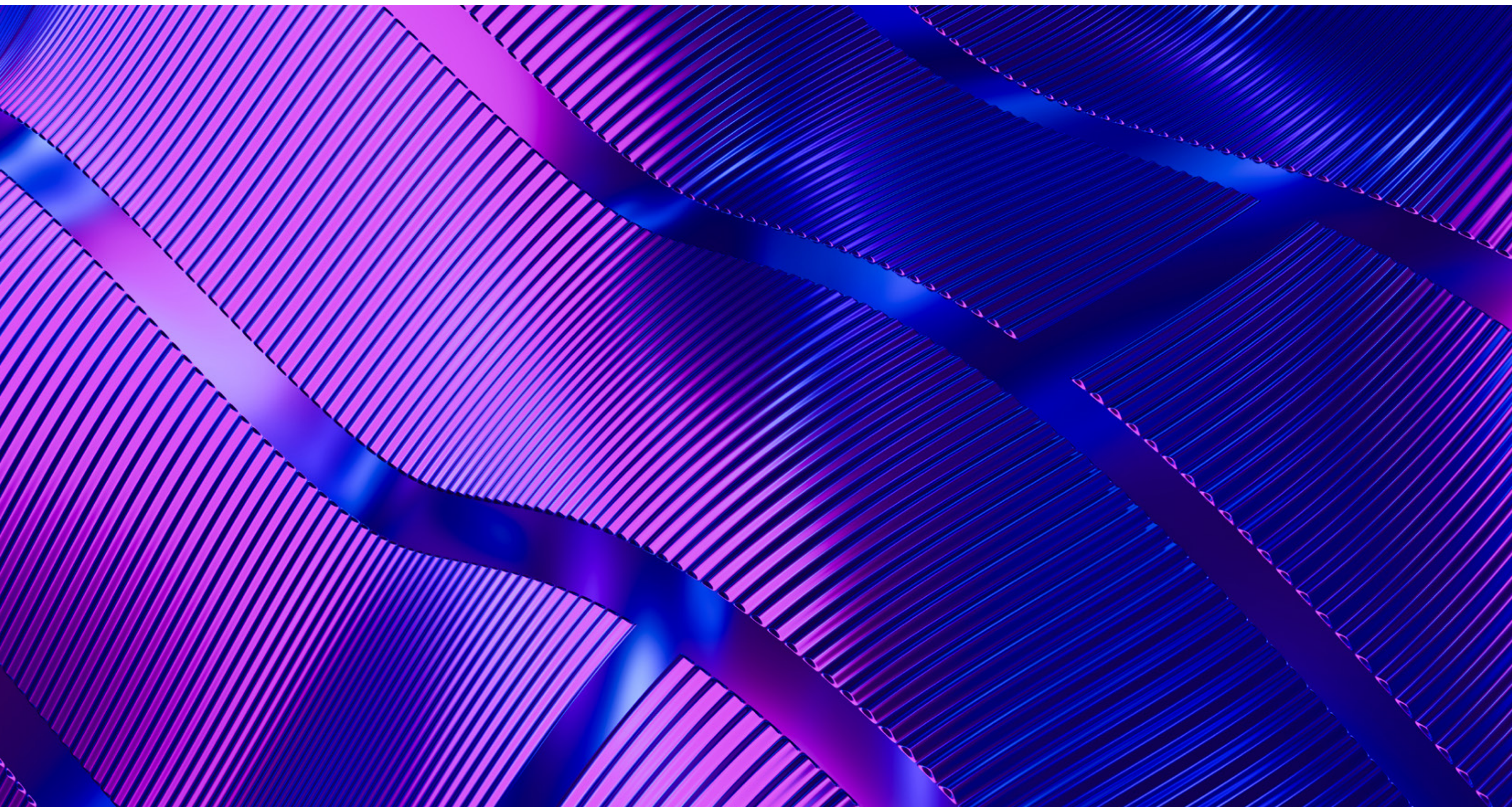
HERBERT SMITH FREEHILLS KRAMER

NEW AESIA GUIDELINES TO SUPPORT COMPLIANCE WITH THE EUROPEAN ARTIFICIAL INTELLIGENCE ACT (AI ACT)

2026



Contents

Introduction

New AESIA Guidelines to support compliance with the AI Act

The Spanish Artificial Intelligence Supervisory Agency (*Agencia Española de Supervisión de la Inteligencia Artificial*, or **AESIA**) has released 16 guides to support compliance with the European Artificial Intelligence Act (**AI Act**).

The guides have been developed as part of Spain's pilot AI Regulatory Sandbox, an initiative designed to facilitate implementation of and compliance with the AI Act by offering practical, non-binding recommendations aligned with the AI Act's requirements, pending approval of the harmonised rules applicable across all Member States.

The 16 guides are structured into three groups:

1. **Introductory guides (Guides 1 and 2)**: These documents provide a general and practical overview of the AI Act to facilitate an initial understanding via supporting materials and hypothetical use cases to illustrate the application of the rules;
2. **Specialised technical guides (Guides 3 to 15)**: These guides address specific legal and technical requirements applicable to high-risk AI systems. They include critical aspects such as conformity assessment procedures, quality and risk management systems, data governance, transparency, human oversight, accuracy, system robustness and cybersecurity, as well as technical documentation; and
3. **Checklist User Manual (procedural support) (Guide 16)**: This guide provides a structured methodology in checklist form, enabling organisations to easily assess their degree of compliance, identify deficiencies and design a structured conformity plan.

AESIA has pointed out that these documents do not replace existing regulations and will be reviewed as European standards and guidelines are issued or developed further. It is expected that they will be updated as legislative amendments to the "Digital Omnibus Package" are adopted.

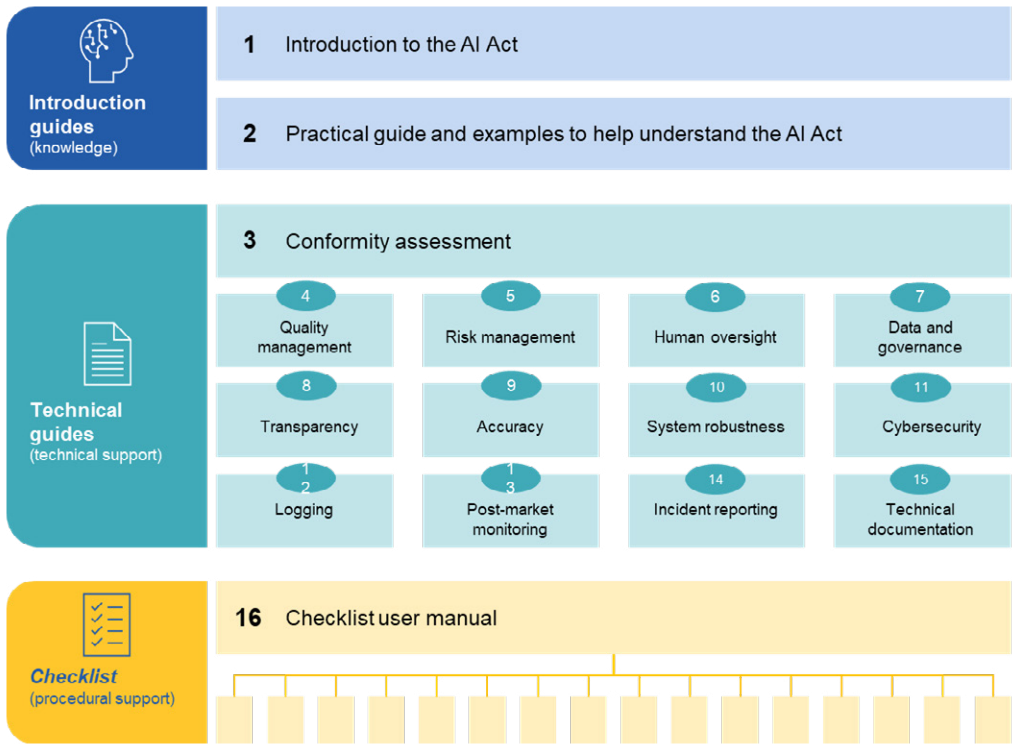


Illustration. *'Relation of the AI Act's guides'. Source: Guide no. 1, p. 4.*

Introductory guides (1-2)

These documents provide a general and practical overview of the AI Act to facilitate an initial understanding via supporting materials and hypothetical use cases to illustrate the application of the rules.

The key aspects of the guides are set out below:

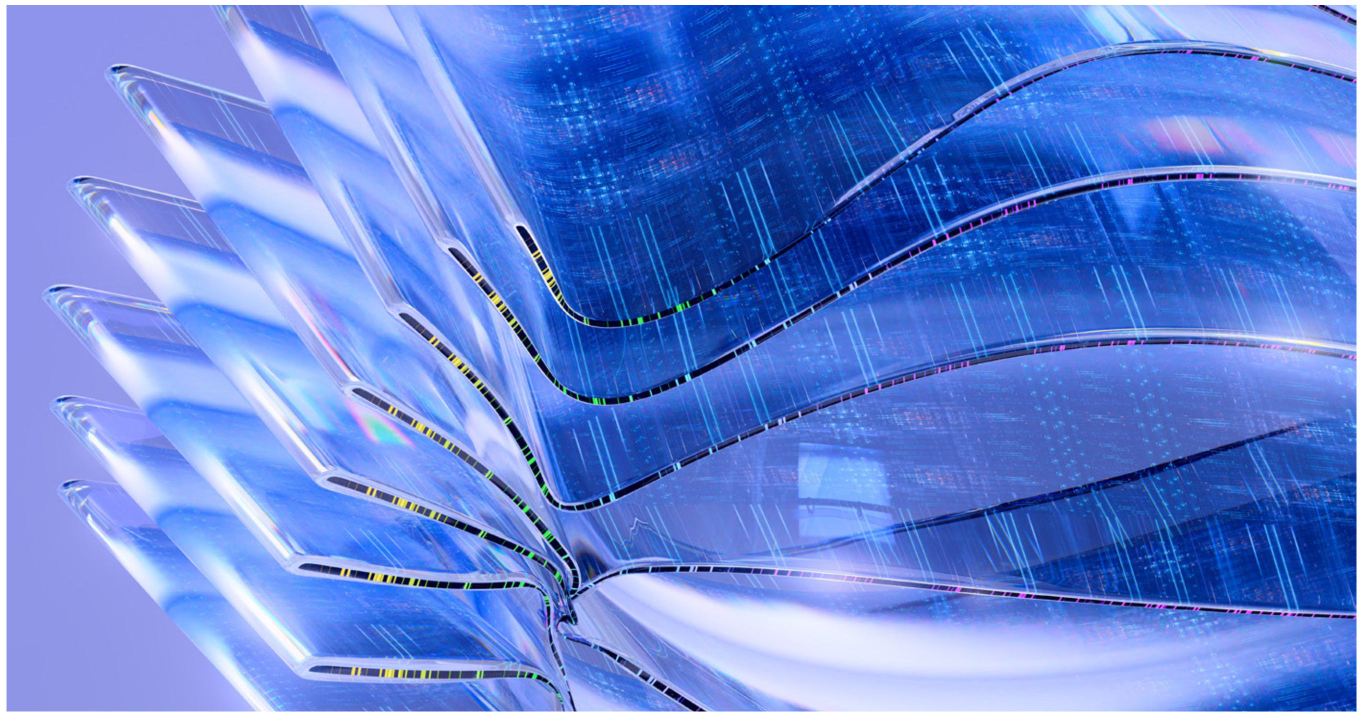
Guide 1

Guide 1 "Introduction to the AI Act" provides a structured overview of the regulatory framework and addresses the following key points, among others:

- Objectives of the AI Act;
- Scope of application and exclusions: it sets out the main areas of exclusion under Article 2 AI Act, such as that the AI Act does not apply to AI systems or models developed exclusively for scientific research and development, for military, defence-related or national security purposes, nor for non-professional personal use by individuals;
- Risk: it explains the governance system based on the level of risk associated with each technology, including systems prohibited due to their unacceptable degree of risk, high-risk systems, and other systems – the bulk of the obligations fall on the first two categories;
- Operators: the main obligations imposed by the AI Act on the different operators, such as suppliers, deployers, importers and distributors; and
- Fostering Innovation: in order to encourage responsible innovation, the guide highlights the role of regulatory sandboxes and offers bespoke conditions to facilitate the integration of small and medium-sized enterprises (SMEs) into the ecosystem.

Guide 2

Guide 2 "Practical guide and examples to help understand the AI Act" aims to help understand the AI Act by means of practical examples. This guide, in particular, provides examples that focus on "high-risk systems" such as work-based biometric identification AI systems, AI systems used in personnel management (promotion), or in the detection of false reporting. In addition, the guide highlights several general concepts and terms described in Article 3 AI Act, which are crucial for a better understanding of the act as they are used throughout the other sandbox guides and materials. Most of these concepts and terms are accompanied by examples applicable to AI systems. Finally, the guide provides a summary of the obligations and roles imposed by the AI Act on providers and deployers, linking them directly to the **specialised technical guides** (Guides 3 to 15) that elaborate on each specific requirement under the AI Act.



Specialised technical guides (3-15)

These guides address specific legal and technical requirements applicable to high-risk AI systems. They include critical aspects such as conformity assessment procedures, quality and risk management systems, data governance, transparency, human oversight, accuracy, system robustness and cybersecurity, as well as technical documentation.

The key aspects of the guides are set out below:

Guide 3

Guide 3, titled **"Conformity Assessment"**, provides a detailed and indicative overview of the mandatory conformity assessment process that high-risk Artificial Intelligence (**AI**) systems must undergo under the AI Act (Article 43) before being placed on the market or put into service in the European Union. Its **purpose** is to provide a practical roadmap for **providers** (the party legally responsible for the process) to demonstrate that its system complies with the AI Act's essential security, transparency and data governance requirements.

Guide 3 clarifies the **two main procedures** for conducting a conformity assessment:

- **Internal control (self-assessment):** This is the rule-of-thumb for most high-risk systems (points 2 to 8 of Annex III), such as systems connected to employment, education, and financial services. Under this framework, the provider is able to verify internally that its Quality Management System (QMS) and technical documentation comply with the AI Act; or
- **Third-party intervention (notified body):** Mandatory in the case of biometric identification systems (Annex III, point 1) when the provider has not implemented or has only partially implemented the available harmonised standards or common specifications. In these cases, an independent body must audit and certify the system.

Guide 3 sets out the **technical and documentary requirements** that must be met to accredit compliance with the AI Act, integrating aspects such as QMS implementation, the development of technical documentation, and the design of post-market monitoring plans. It also provides examples and methodologies to facilitate implementation of these requirements by means of instruments such as harmonised standards and common specifications (respectively, technical standards created by standardisation bodies at the request of the Commission, and technical rules issued directly by the Commission itself when the former do not exist or are insufficient).

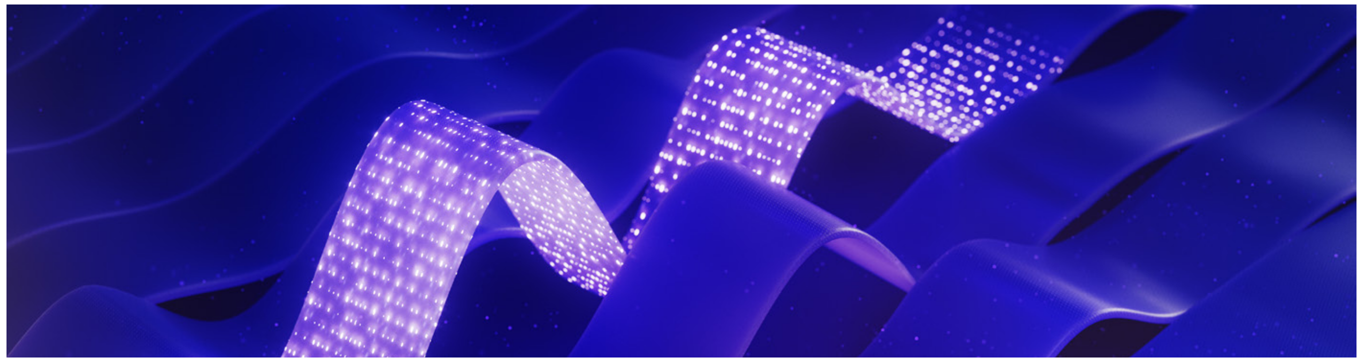
Process success will culminate with the drawing up of an **EU Declaration of Conformity** and the affixing of the **CE mark** (a key indicator, but not in itself absolute proof, of a product's compliance with EU legislation).

Guide 4

Guide 4, titled **"Quality Management System"**, articulates all of the AI Act's operational obligations within an organisation. Its **purpose** is to analyse the organisational and technical measures that will serve providers (and, in specific cases of joint development, deployers) to comply with Article 17 of the AI Act. The purpose of the QMS is to ensure that high-risk AI systems are secure, reliable, auditable throughout their life cycle.

Guide 4 sets out the key elements that an entity must integrate to adequately comply with the AI Act through policies, procedures and instructions. The following should be highlighted from among the 13 mandatory sections in Article 17: the development of a clear accountability and governance framework that defines the responsibilities of management and technical staff; documented processes for the design, development, testing and validation of systems; and cybersecurity and accuracy measures integrated from the design stage.

One fundamental aspect is that QMS implementation should be **proportional to the size of the provider's organisation**.
This principle is designed to balance the administrative burden with the company's capacity.



Guide 5

Guide 5, titled "**Risk Management**", supports compliance with article 9 of the AI Act from an operational perspective under the heading "Risk management system". This article establishes an obligation to implement an iterative and continuous process throughout a high-risk AI system's life cycle to identify and mitigate potential risks. The onus for complying with this obligation is primarily on the provider, as the system's developer. However, Guide 5 clarifies that, if a deployer plays a role in system development, it must implement the measures established by the provider. The system should be geared towards protection of individuals' health, safety and fundamental rights.

With a view to devising a suitable risk management system, Guide 5 sets out a roadmap composed of **eight interconnected phases**.

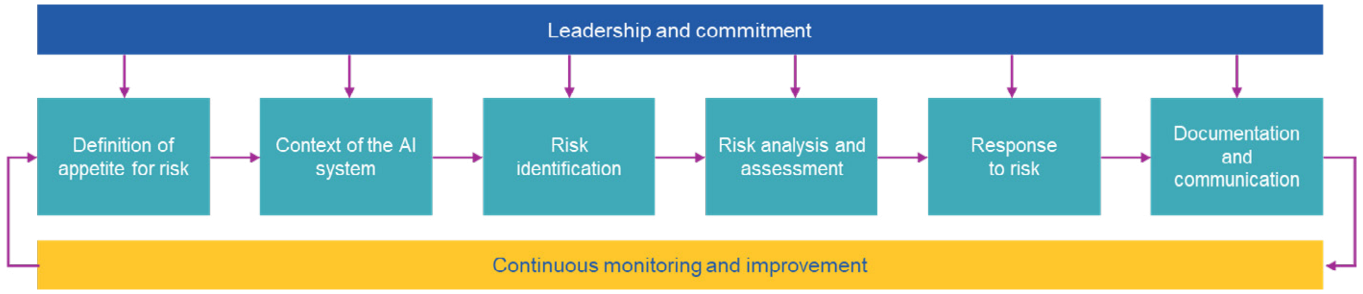


Illustration. *Phases of the risk management system. Source: Guide 5, p. 15*

A **key aspect of the guide** is determining appetite for risk, defined as the degree of risk that an organisation is prepared to tolerate to achieve its goals. This assessment is made on a scale of 1 to 15. If a system has a critical impact, such as the administration of insulin in the medical field, appetite for risk should be very low; conversely, in low-impact systems such as taste-based movie recommendations, tolerance may be much higher.

Finally, the guide warns of **critical dangers** such as algorithmic discrimination and the negative impact of biometric systems. Using case studies, it illustrates how data biases can unfairly penalise groups based on race or gender in access to health or employment.

Guide 6

Guide 6, titled "**Human Oversight**", focuses on the operational implementation of the obligations defined in Article 14 of the AI Act. Its main objective is to ensure that high-risk AI systems are designed in such a way that they can be effectively monitored by natural persons during use.

Human oversight is not merely a technical requirement; it is a governance mechanism aimed at preventing AI from undermining human autonomy or causing harm to health, safety or fundamental rights. The guide stresses that human oversight enables accountability for the system's actions. Specifically, in order for humans to truly understand how a system works, the guide lists a number of measures that the design should incorporate, including:

- **"Counterfactual reasoning":** the system should not simply describe why it made a decision but also explain what changes to the input data would have altered the outcome. This is essential for a supervisor or a data subject to understand, for example, under what conditions a rejected application would have been accepted.
- **Hierarchical breakdown:** The interface should allow information to be navigated in a structured manner, from the most global (the model's general reasoning mechanism) to the most specific (the logic behind a specific individual decision).
- The guide also explains the three fundamental approaches to gauge how much autonomy is given to the system:
- *Human-in-the-loop* (HITL): There is human involvement in every decision cycle. This is the recommended level for high-risk cases where each action must be validated individually.
- *Human-on-the-loop* (HOTL): Monitoring is performed after the fact or during operation, allowing intervention if an anomaly is detected.
- *Human-in-command* (HIC): Humans retain overall command and ultimate responsibility for critical decisions and safe operation of the system.

One **key element** is emphasis on the need for appropriate interfaces. The provider must provide the deployer with tools that allow the AI results and reasoning to be interpreted simply, visually and in normal language.

Finally, the guide addresses a **critical psychological risk**: human tendency to blindly trust machine decisions. To combat this, it proposes measures such as implementing a 'forced error' mode, ie introducing deliberate failures in sandbox environments to test whether the supervisor maintains critical judgement, and ensuring awareness by training supervisors to understand the system's typical limitations and shortcomings.

Guide 7

Guide 7, titled **"Data and Data governance"**, develops the operational requirements set out in Article 10 of the AI Act. Its fundamental aim is to ensure that **training, validation and test data sets** used in high-risk AI systems are adequate, relevant and sufficiently representative and that they meet quality requirements to **avoid bias and discriminatory results**.

Data governance is defined as a set of elements (policies, processes and standards) integrated into a management model that encompasses **five critical phases of the data life cycle**, explained in detail in the guide:

1. **Information requirements:** Defining what information we need to feed into the AI system to achieve the intended purpose.
2. **Data collection:** Obtaining the data, ensuring its adequacy and representativeness. It is advisable that data are obtained from different sources.
3. **Preparation:** Labelling, cleaning, enrichment and transformation operations.
4. **Availability:** Making the data available for system development using appropriate technical tools.
5. **Deletion:** secure deletion of data once they have fulfilled their intended purpose.

In the case of data preparation, the guide points out that it is important to decide at what stage of the life cycle quality controls are defined and implemented. AESIA recommends assessing quality directly at the source repositories and focusing subsequent checks on the quality of the process (checking that data are copied, ingested or transferred correctly). This avoids redundant checks at different layers and simplifies management and remediation.

A key point addressed by the guide is the **processing of special categories of personal data** (such as ethnic origin, health or religion). Article 10.5 of the AI Act exceptionally allows the processing of data of this kind exclusively for the purpose of detecting and correcting bias, subject to a series of conditions. The guide specifies that anonymisation should always be the default premise; only if anonymisation "significantly" impacts the accuracy of bias detection would pseudonymisation be justified.

Finally, the importance of technical documentation is another key aspect highlighted under the guide. In addition to including the data governance elements listed in Annex IV of the AI Act, AESIA recommends the good practice of expanding documentation by including and justifying the life cycle stages mentioned above. Each measure implemented should be specified and detail included of how implementation took place, as well as identifying the person responsible for that implementation.

Guide 8

Guide 8, titled **"Transparency and Information available to users"**, elaborates on the requirements of Article 13 of the AI Act from an operational perspective. Its main aim is to ensure that high-risk AI systems are designed and developed in such a way that their operation is sufficiently transparent to enable those responsible for deployment and users to interpret the results and use them correctly.

This guide translates the legal obligation to "be transparent" into a set of technical and documentary measures to be complied with by providers and deployers of high-risk AI systems. The **ultimate aim** is to remove system opacity so that the human responsible for oversight can exercise real and effective control over the technology.

We highlight below some **key points** set out by AESIA in the guide to achieve transparency:

- **Clear and complete instructions for use:** The guide details the minimum content that manuals should contain to ensure that users understand the system's capabilities and limitations, as well as its level of accuracy and foreseeable risks to fundamental rights.
- **Design geared towards understanding:** It emphasises that information should not only be technical, but also understandable by the profile of user who will operate the system. This includes the use of interfaces that allow a hierarchical breakdown of information (from general to specific) and explain the counterfactual (why the system did not make a different decision).
- **Visibility of data samples:** The aim is for users to be able to understand and assess for themselves whether the training sample is fair and representative for their specific business objective or use case. It is important to list the data sources used and to perform an exploratory data analysis to ascertain their essence, associated meta-information, or critical values or outliers.
- **Risk management for unintended uses:** It is necessary not only to document intended use, but to identify and warn of reasonably foreseeable misuses, providing the necessary metrics for users to detect performance failures in real time.

- **External transparency channels:** As a best practice to facilitate ongoing understanding, the guide suggests using resources external to the system, such as webpages, wikis or doc pages, to compile in an easily accessible way all information on the technology's capabilities and limitations.

Finally, Guide 8 sets out a series of specific steps for providers and deployers to document compliance with transparency requirements.

Guide 9

Guide 9, entitled "**Accuracy**", offers guidance on the accuracy required by high-risk AI systems under Article 15 of the AI Act. Accuracy plays a crucial role in AI systems to **mitigate, as much as possible, potential risks to health, safety and fundamental rights** that may arise from the use of high-risk AI systems.

We highlight below some key points set out by AESIA in Guide 9 for ensuring compliance with the accuracy requirement:

- **Life cycle-based approach to accuracy.** Assessing aspects of an AI system's life cycle is essential because they can influence its overall accuracy – the primary aim is to ensure that an AI system's accuracy remains stable and constant over time. To achieve this, **data pre-processing should be performed** (among other things, assessing that model training data is free of sampling bias and using identical data processing methodology to compare accuracy among various models); and **measures should be taken commensurate with the type of model and intended purpose to avoid overfitting** (eg, that hyperparameters are reported during model training/testing and validation processes, as well as their values for each model, or that no information from the test dataset is used when fitting hyperparameters).
- **Suitable metric selection to measure accuracy.** Annex 7.1 of the guide provides a non-exhaustive list of accuracy metrics that can be used to measure accuracy, as well as the types of models to which they relate. Two key elements should be considered when selecting an appropriate accuracy metric for a system: (i) the system's intended purpose; and (ii) the risks encountered in the risk management system, as well as selecting a target function that can achieve the intended purpose. In this section, the guide highlights the importance of **having a centralised repository** where all metrics information associated with a model at any point in its life cycle is managed.
- **Measures necessary for the provider to ensure consistent accuracy throughout the life cycle.** Providers should, among other elements, implement technical measures related to inventories of accuracy metrics and target functions (eg. system output is accompanied by a measure of uncertainty associated with the accuracy of that output); and use specific metrics accompanied by statistical evaluations that are suitable for determining data distribution, data dependence and other assumptions so as to achieve a meaningful evaluation.
- **Suitable documentation.** The accuracy assurance and selection process should be properly documented in accordance with all remaining technical documentation provided in Guide 15, entitled "Technical Documentation". This process includes documentation such as model cards and database cards, which offer a better overview of the accuracy metrics that have been provided and the source of the data used to train the model.

Guide 10

Guide 10, entitled "**System Robustness**", elaborates on Article 15 of the AI Act, focusing on the robustness of high-risk AI systems. This guide identifies **cybersecurity** as a cornerstone of robustness because it safeguards against attacks that could manipulate an AI system's response and, therefore, undermine its accuracy. It also points out that robustness mechanisms must be designed to ensure that cybersecurity measures do not deteriorate over time.

In order to properly assess an AI system's robustness, AESIA highlights several key considerations, including:

- **Responsibility lies with the AI system provider to establish appropriate robustness metrics.** To properly assess a model's robustness, the provider should take the following steps:
  - set robustness requirements or objectives and associated metrics.
  - design experiments to test and demonstrate robustness.
  - conduct experiments according to the established plan – results, data used and all output values are then recorded so that metrics are calculated in a more aggregated manner.
  - interpret the results to inform decision-making.
  - determine whether the system meets robustness requirements based on the criteria and interpretation identified above.
- To ensure adequate robustness, providers must implement **verification procedures** to confirm that the design requirements have been met, as well as a **validation** process to confirm that the AI system fulfils its intended purpose when tested with **real-world data sets** and executed code.
- The metrics chosen to validate robustness features should be tested and verified in **hardware environments** that mirror the computational resources available to the deployed system (memory, CPU, processing speed, etc.). Hardware-related robustness metrics should be described in the AI system documentation before accuracy and performance tests are designed for the system's operational stage; similarly, robustness should be monitored through statistics, data distribution and changes in business usage.

The guide further underlines the importance of both providers and, where appropriate, deployers **having sufficient technical robustness** to ensure that failures, errors or inconsistencies do not seriously compromise system security or adversely affect fundamental rights. To this end, the guide emphasises the need for providers to:

- establish strategies and measures to predict potential failures, unintended consequences that could adversely impact on or that affect individuals' security or fundamental rights.
- address shortcomings in AI system robustness against errors, failures or inconsistencies – to do so, providers should:
  - **From an organisational standpoint**, among other measures: implement techniques for alerting the responsible parties or, if no response is received from them in a timely manner, implement a function that allows automatic system shutdown and introduce failsafe protocols to allow humans to anticipate catastrophic events.
  - **From a technical standpoint** recommended measures include promoting multi-stakeholder engagement to maximise diversity and the inclusion of different domain profiles during system design, development, maintenance, implementation, monitoring and use; and setting up model design evaluation committees to predict inconsistencies in system design or implementation that may lead to unintended outcomes.
- **Redundancy mechanisms** should be in place to ensure system robustness, including back-up systems or failover plans.

Finally, the guide stresses the importance of AI systems that continue to learn after deployment, as learning can increase the risk of new biases emerging over time. Providers and deployers should therefore ensure that continued training of an AI system over time does not erode the robustness achieved prior to deployment, and should adopt mitigation strategies to address any changes that negatively affect a system's accuracy and robustness and/or its underlying data.

Guide 11

Guide 11, entitled "**Cybersecurity**", develops the measures that ought to be implemented in AI systems to mitigate the risks and attacks they may face throughout their life cycle.

The guide stresses that, to effectively implement these measures, it is essential to first identify the types of potential threats and attacks that exist. To this end, it provides an outline that connects the different phases of a system's life cycle to the possible attacks in each of them:

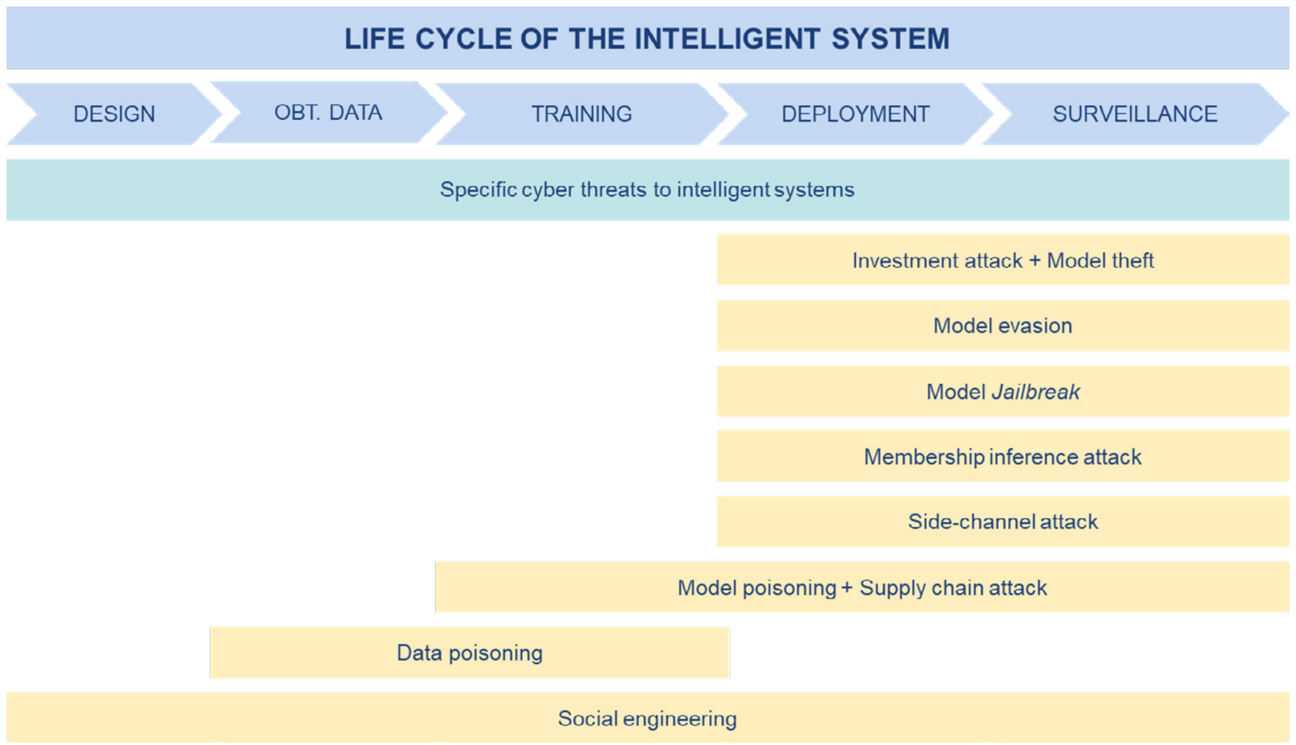


Illustration. *'Life cycle of the Intelligent System'. Source: Guide no. 11.*

This approach offers providers and deployers greater awareness of potential risks and the ability to adjust safeguards accordingly. The main cybersecurity measures are grouped into the following blocks:

1. **Organisational cybersecurity measures**, which must be guaranteed and maintained throughout the system's life cycle:
   - The provider shall take actions including: plan, on a global level, the degree of cybersecurity applied to the AI system during the design and development process; involve the Data Protection Officer from inception of the AI system; accompany the instructions for use of the AI system with high-level recommendations on cybersecurity applied to AI; designate persons responsible for monitoring; if the AI system is delivered to the deployer in an on-premise or in-cloud format managed by the deployer, the provider must provide adequate instructions to protect it.
   - Organisational measures should be aligned with technical measures. Thus, during the system's installation and/or configuration processes and in the instruction manual, the provider must include information regarding all system-specific cybersecurity risks and how it is protected. In addition, tools should be implemented throughout the life cycle to automate security testing and ensure that updates maintain a consistent and non-degraded level of cybersecurity.
2. **Measures to bolster system resilience against unauthorised attempts** to alter its use, output or operation. These measures should be supported by inventories of system assets and actors throughout the system's life cycle. These measures include, but are not limited to, the following:
   - The supplier must implement measures including: inventory of all the actors involved in the process; establish access and permission levels for each of them; definition of the roles involved in the use of the tool; planning and performance of an inventory of assets including tools, data, processes and models.

     From the perspective of technical support, these inventories must have adequate IT systems, mechanisms that allow application of the access policies and a centralised, updated and accessible documentary system.
   - The person responsible for deployment should be aware of the actors and assets that are applicable to them. At an organisational level, it should integrate the supplier's documentation with its internal organisational chart and, where the system is its own asset, treat it as such for cybersecurity purposes.
3. **Measures to identify and mitigate vulnerabilities associated with training data**, which should establish security controls to prevent tampering or manipulation:
   - The provider shall, among other measures, implement security controls depending on the vulnerability identified. For example, expanding datasets through augmentation techniques when they are insufficient or establishing appropriate access control policies if vulnerabilities are detected in permissions management.
   - In the case of the deployer, its primary action on an organisational level to protect systems against poisoning attacks will be to read and understand the instruction manual.
4. **Measures to safeguard against adversarial attacks**, via specific security controls:
   - The provider shall, for example, avoid the use of widely known models where there is a risk of adversarial transferability, and integrate specific AI system security into its awareness strategies.
   - The deployer should be aware of and analyse all vulnerabilities and controls that fall under its responsibility and allocate human and technical resources to mitigate them.
5. **Measures against attacks aimed at discovering and exploiting AI system flaws**, whether intrinsic to the model or arising from its integration into the software environment:
   - The supplier shall identify and inventory the defects of the selected model, document them in the threat model and implement measures to mitigate their exploitation.
   - The deployer shall understand the manual developed by the provider on intrinsic system defects and **the configuration mechanisms applicable to the AI system within the scope of the intended purpose**.

Guide 12

Guide 12, entitled "**Automatically generated records and log files**", details the measures that must be implemented by providers and deployers to comply with the requirements of the AI Act in relation to the generation and keeping of logs in AI systems.

The guide stresses the importance of adhering to the following core principles for effective records management in AI systems: confidentiality, integrity, availability, authenticity, accessibility and traceability, accountability, and retention and deletion practices. It also identifies several key considerations, including:

- The type of actor responsible for record-keeping should be taken into account. Providers/deployers should be responsible for retaining system-generated records provided that they are under their control for at least six months, unless otherwise provided for in applicable Union or national law. In the case of financial institutions, records shall be retained as part of their mandatory documentation obligations.
- Logs must reflect the information identified as necessary following the assessment process.

- Logs for remote biometric identification systems must include at least the following specific elements: the period of each system use (the start date and time and the end date and time of each use); the reference database against which the system has matched the input data; the input data with which the search has produced a match; and the identification of the natural persons involved in verifying the results.

However, the following processes must be addressed in a scaled manner to ensure that the logs are developed and managed properly:

1. **Log assessment and design:** this process involves analysing and determining the need to generate the log, defining the specific objectives for generating the log and establishing a scope. In this phase, the log is designed by identifying fields and categories to collect information. Within the process of assessing and designing the logs, it is necessary to: identify the need, identify the objectives, define the scope, design the log and identify those responsible for it. This process should be supported by:
   - The **risk-management measures** set out in Guide 5 – it will be determined from the inventory which events should be logged.
   - The **post-market monitoring framework** described in Guide 13, which identifies the information required once the system has been placed on the market.
   - The **human oversight measures** in Guide 6, to identify the required information that the system should provide for this purpose.

   This process should be reviewed on an ongoing basis, especially where changes to the system affect the underlying risk analysis.

2. **Capture, storage and access control:** this involves capturing, storing and retaining the records defined in the assessment and design phase to ensure protection against unauthorised access, alteration, loss or destruction. To this end, records should be stored in a manner that ensures protection against the above, including: collecting information in accordance with the criteria set out in step (i); selecting appropriate storage media and protection materials; implementing appropriate cybersecurity and access control measures; developing and defining roles and responsibilities for risk management; etc.

3. **Log retention and deletion:** this process establishes the requirements for retaining and deletion of logs that have been created, captured and stored. This is determined by two factors: on the one hand, the need for retaining the records identified in process (i); and, on the other hand, taking into account applicable regulatory requirements (for example, the Spanish Law on Data Protection and the Guarantee of Digital Rights and the GDPR if the logs include personal data).

   Deletion of a log must be authorised and documented and must, at all times, comply with the security and access measures that have been implemented. Logs subject to legal proceedings must not be deleted until appropriate authorisation has been obtained.

4. **Monitoring and continuous improvement:** the objective is to ensure and improve the quality and effectiveness of the risk management system; it is also necessary to monitor and establish specific periods for reviewing and updating the log management system. The following phases should be established as part of the process: monitoring and identification of potential errors, analysis of the logged data, implementation of improvements, evaluation of the improvements, and continuous improvement cycle.

Finally, the guide highlights the importance of establishing responsibilities and authorisations for each of the above processes. Responsibilities should be assigned to all personnel involved in any of the processes and should be reflected and documented in job descriptions and equivalent documentation where appropriate. All responsibilities must be documented and set out in written form.

Guide 13

Guide 13, entitled "**Post-market monitoring plan**", explains what post-market monitoring systems entail and why they are important in high-risk AI systems. These systems consist of a set of processes and tools that collect data from an AI system and translate them into a series of indicators that reflect how the system is operating, enabling monitoring after the system has been placed on the market. In practice, this allows providers to assess whether an AI system adequately meets the requirements applicable to high-risk systems. These systems operate through subsystems, including indicator capture systems, indicator logging systems, automated alert systems, and different analysis interfaces for those responsible for surveillance.

To help build an appropriate post-market monitoring framework, the guide outlines the main phases involved in developing these systems as well as the components that must be included:

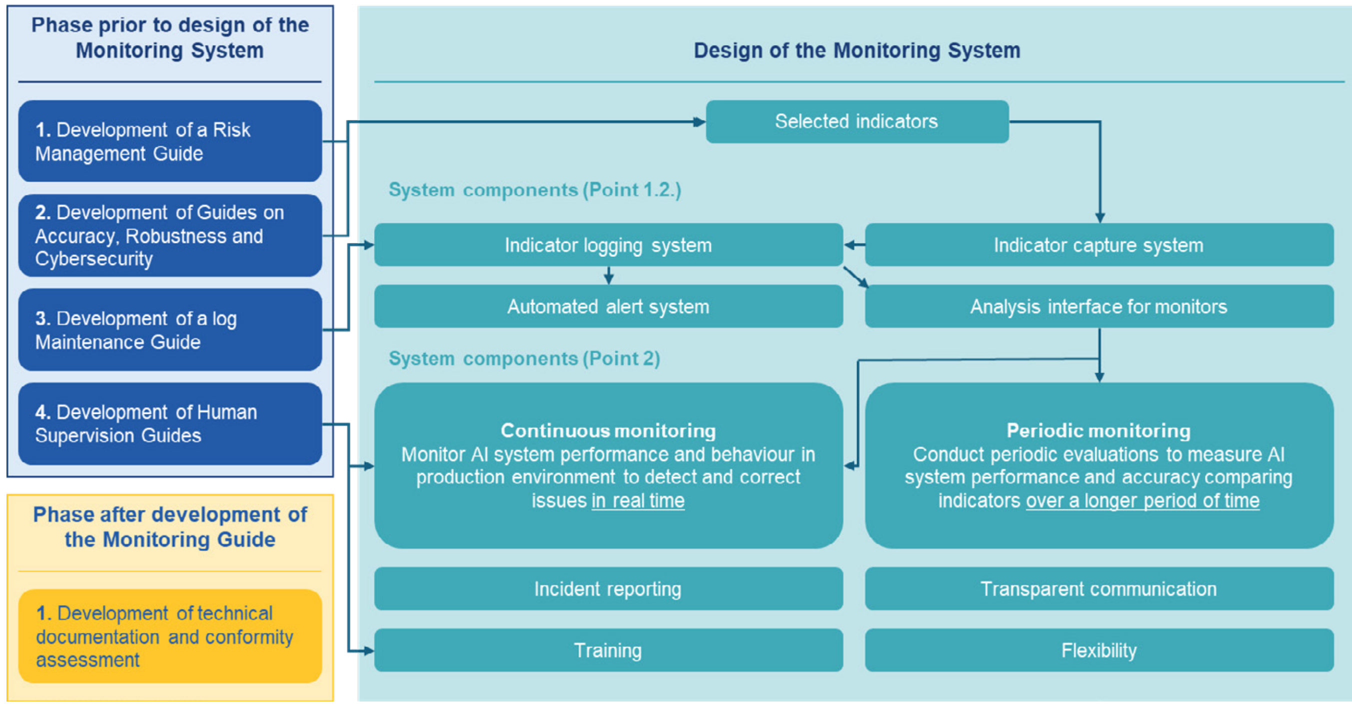


Illustration. *'Post-market monitoring plan'. Source: Guide no. 13.*

Accordingly, the following measures/actions must be implemented to develop an effective post-market monitoring plan:

- **Continuous monitoring of high-risk AI systems** to ensure that the system continues to operate safely and effectively once placed on the market. The guide notes that continuous monitoring – through monitoring system indicators, safety indicators, and by monitoring indicator variations via alerts, etc – is key to remain prepared for sudden changes to a system's behaviour and for performance issues emerging from a range of factors, such as ageing training data or inadequate training.
- **Regular evaluation** (periodic monitoring) to measure an AI system's performance and accuracy, which will make it possible to detect issues quickly and to take remedial action to correct them. Some of the measures used to assess a system's performance and accuracy include: performance tests (which measure a system's response time and its ability to handle large volumes of data (and accuracy tests (which measure a system's accuracy when performing specific tasks, such as image object recognition or language translation).
- **Transparent communication** to the recipient of the information (eg, the provider, deployer, etc.) as to the system's characteristics, its performance and the consequences of its use in production, so as to support a proper understanding of all use-case implications.
- **Training for supervisors**, providing them with basic training on how the AI system works and how it is used.

- **Flexibility** through a flexible and scalable plan to enhance system monitoring, ie, adapting the system to internal and external changes that may impact operation. Measures to achieve this include identifying applicable regulations, assessing the system's performance and security, identifying performance and security risks, monitoring compliance with existing regulations, establishing a contingency plan, etc.

Finally, the guide notes that the other AESIA guides must be taken into account when implementing a robust post-marketing monitoring system. This is why the final section of the guide maps post-marketing monitoring systems against other AESIA guides and explains the links between them.

Guide 14

Guide 14, entitled "**Reporting of serious incidents**", sets out the procedural framework and operational measures that providers and, in certain cases, deployers must implement to comply with Article 73 of the AI Act.

The guide highlights the following key operational aspects:

- **Obliged parties:** Providers bear primary responsibility for reporting incidents, regardless of geographical origin, provided that the system operates in the EU market. Deployers must notify the authorities if they detect the incident and are unable to contact the provider.
- **Hierarchy of deadlines:** An incident must be reported immediately after establishing a causal link between the system and the incident, according to the following deadlines:
  - **2 days:** In the event of a widespread breach or an incident relating to critical infrastructure.
  - **10 days:** If a fatality has occurred.
  - **15 days:** In the case of all other serious incidents.
- **Incremental reporting:** To ensure prompt reporting, an initial incident report may be submitted even if it is incomplete, followed by a complete report once all the information has been gleaned.
- **Exceptions for equivalent regimes:** Where systems are subject to EU sector legislation with equivalent reporting obligations (including safety components of medical devices regulated by Regulations 2017/745 and 2017/746), reporting will be limited exclusively to incidents affecting fundamental rights. If the system operates in several Member States, the incident report must be addressed to all market surveillance authorities (MSAs), -*Autoridades de Vigilancia de Mercado (AVM)*- in the Member States concerned.

The guide also identifies the following processes with a view to appropriate management:

- **Technical assessment and investigation:** Once an incident has been reported, the provider must conduct a risk assessment without delay and implement corrective measures. The provider may not modify the system in a way that could affect the evaluation of the causes without first informing the pertinent authorities. The MSA then has 7 days to adopt appropriate measures, which may include the withdrawal or banning of the system, and must immediately notify the European Commission. If the incident affects fundamental rights, the MSA shall also inform the relevant national authorities.
- **Integration within governance and QMS:** The procedure must be formalised within the provider's Quality Management System (QMS). Key operational measures include: maintaining contact with the AVM; establishing a communication channel with the deployer (Article 13.3.a); having an understanding of the system's categorisation to determine whether exceptions apply; and understanding what constitutes fundamental rights under EU law so as to identify when a deviation amounts to a reportable breach.

Guide 15

Guide 15, entitled "**Technical Documentation**", explains what post-market monitoring systems entail and why they are important in high-risk AI systems. These systems consist of a set of processes and tools that collect data from an AI system and translate them into a series of indicators that reflect how the system is operating, enabling monitoring after the system has been placed on the market. In practice, this allows providers to assess whether an AI system adequately meets the requirements applicable to high-risk systems. These systems operate through subsystems, including indicator capture systems, indicator logging systems, automated alert systems, and different analysis interfaces for those responsible for surveillance.

To help build an appropriate post-market monitoring framework, the guide outlines the main phases involved in developing these systems as well as the components that must be included:

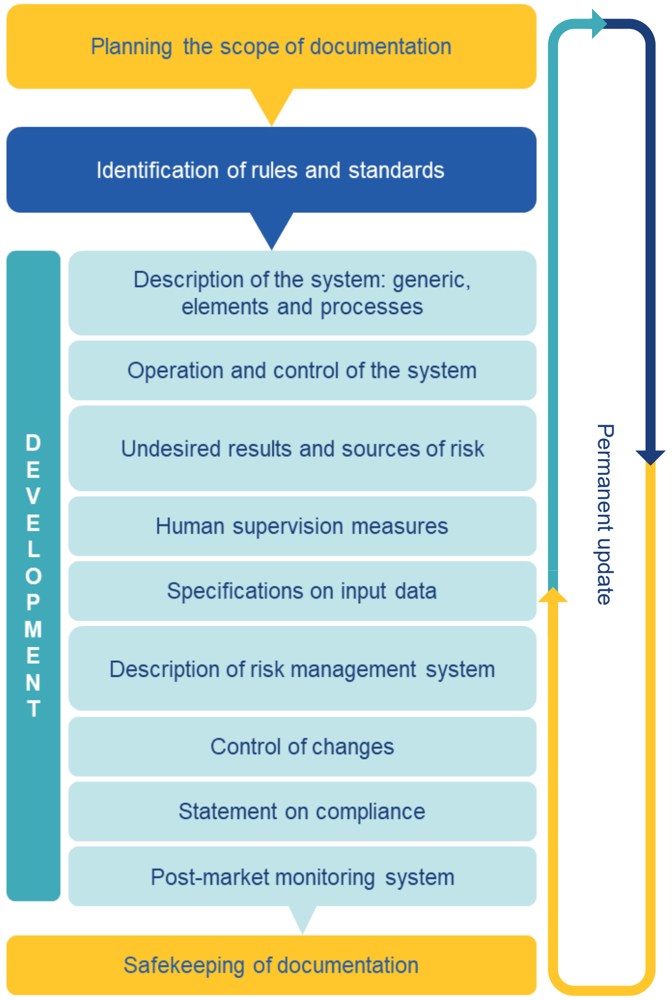


Illustration. *'Technical documentation'. Source: Guide no. 15.*

The following must be taken into account throughout the technical documentation process:

- The technical documentation must be complete before the AI system is placed on the market and put into service.
- To ensure the documentation remains up to date throughout the AI system's life cycle, the provider must take measures such as: within the AI system's management processes, establishing a procedure for tracking changes that triggers updates of the documentation; establishing a chain of responsibility (or appointing a person responsible for managing changes to the system who is tasked with updating the documentation accordingly); or establishing, defining and scaling a document management system or equivalent technical solution, enabling the provider to ensure custody and updating of the documentation.
- The documentation must be retained for a period of 10 years from the date on which the AI system is placed on the market. The provider must have the technical measures in place to keep this documentation and ensure there is no risk of it being lost.

Thus, to assist AI system providers, the guide sets out the structure that the technical documentation must follow to comply with the minimum content requirements set out in Annex IV of the AI Act. Among other things, it must include the following: a general description of the AI system, including the intended purpose (description of the use for which it has been designed, context of use of the system, and terms and conditions of use), the name of the provider and the version of the system; the manner in which the AI system interacts or can be used to interact with hardware or software, as well as with other AI systems, which are not part of the AI system itself; or general-purpose user guides intended for the deployer and installation instructions.

Checklist user manual

This guide provides a structured methodology in checklist form, enabling organisations to easily assess their degree of compliance, identify deficiencies and design a structured conformity plan.

Guide 16

Guide 16, entitled "**Checklist User Manual**", is intended to enable companies to conduct a self-assessment on their compliance with all the requirements set out in the AI Act for high-risk AI systems and to design a plan to adapt their systems to the requirements established in it.

This tool is an Excel document composed of nine tabs, of which: five are informative tabs containing instructions for use and contextual information, and four are operational tabs requiring information to be entered.

The five informative tabs are:

- **"Cover"**: containing a mandatory confidentiality reminder.
- **"Introduction":** providing a summary of steps and what the tool can do.
- **"AI Act Article":** identifying the sections of the article of the AI Act regarding which the organisation will conduct a self-assessment.
- **"Guide Measures (GM)":** setting out the detailed explanatory measures as contained in each one of the guides. In addition, a set of guidance questions is included per measure with the aim of providing context so that the answers to the questions can offer an idea of whether or not the system already complies with the measure in question.
- **"GM-Section relationship":** summarises the potential application of the measures set out in the "Guide Measures" tab to each of the sections of the article.

The four operational tabs are:

- **"GM Self-Assessment":** this allows the user to identify both the maturity level of the proposed measure's implementation within the system and the perceived level of difficulty in carrying it out. Once the tab has been completed, an Adaptation Plan is generated. If the company considers that a measure could be applied to an additional section, this may be indicated at the end of the pre-populated rows, with two columns to be completed regarding the perceived level of difficulty and maturity level.
- **"Additional Measures (AM)":** the assessment included in this tab, together with the following two, consists of information from organisations regarding the measures they themselves propose as possible means of complying with the AI Act; the suitability of those measures is assessed by AESIA. The company must indicate the measures which, in its experience, enable compliance with sections of the article. To this end, it must add a row per measure, providing a brief description of the measure and the file name.
- **"AM-Section Relationship":** provides a concise summary of the potential application of the measures reported in the previous tab to each of the sections of the article.
- **"AM Self-Assessment":** this tab appears automatically, pre-populated with a row for each of the relationships described in the previous tab.

Contacts

Pablo García Mexía
Head of digital law
T +34 91 423 4010
pablo.garciamexia@hsfkramer.com

Iria Calviño
Partner, regulated sectors
T +34 91 423 4022
iria.calvino@hsfkramer.com

Jaime Bofill
Partner, Insurance/FSR/Fintech
T +34 91 423 4008
jaime.bofill@hsfkramer.com

Authors

Elena Valín
Associate
T +34 91 423 4181
elena.valin@hsfkramer.com

Rebeca Oriol
Junior associate
T +34 91 423 4152
rebeca.oriol@hsfkramer.com

For a full list of our global offices visit **HSFKRAMER.COM**