THE IMPACT OF THE EU AI ACT IN 6 SIX STEPS

Step 1: Is the system prohibited under the AI Act?

The first step in the process is to determine whether the AI system could qualify as a **prohibited practice**, as listed in article 5 AI Act. This requires careful attention to what the regulation considers to be unacceptable practices. These systems are considered to fundamentally conflict with EU values and pose a threat to people's safety, livelihoods, or fundamental rights. Therefore, it is forbidden to place them on the EU market, put them into service or use them. The EU AI Office has issued guidelines to help identify what qualifies as a prohibited AI system.

Certain sectors or contexts will not be discussed within this tool; **the context of national security, defence and military purposes, or judicial and law enforcement** (to a certain extent).

We advise to first map whether a system may a prohibited system, a high-risk AI system or a system to which transparency requirements apply. Only if the answer is (maybe) positive, we believe it to be useful to consider whether the system in question qualifies as an "AI system" under the AI Act.

This sequence has a practical benefit: the definition of an AI system under the Act is not fully clear and requires substantial effort. This effort can be avoided if the system is already out of scope because it does not fall into one of the mentioned categories.

Knowledge Centre Data & Society

Artificial Intelligence Flanders

MANIPULATIVE SYSTEMS

(i) Subliminal techniques beyond a person's consciousness or **purposefully manipulative or deceptive techniques**, aiming to or having the effect of materially **distorting behaviour** by appreciably impairing informed decision making leading to decisions the person would otherwise not make OR a system that **exploits vulnerabilities** (e.g. age, disability, specific social or economic situation) aiming or having the effect to materially **distort behaviour AND (ii)** this (reasonably likely) causes someone **significant harm**.

SOCIAL SCORING

Evaluation or classification of persons **(social scoring) – over a period of time** - , based on social behaviour OR known, inferred and predicted personal or personality characteristics;

AND which leads to **detrimental or unfavourable treatment**;

- In social contexts unrelated to the context in which the data was originally generated or collected; OR
- That is unjustified or disproportionate to their social behaviour or its gravity.

FACIAL RECOGNITION DATABASES

Creating or expanding **facial recognition databases** through the **untargeted scraping** of facial images from the internet or CCTV footage.

RISK ASSESSMENT OF CRIMINAL OFFENCE

Risk assessments to **assess or predict the risk of a person committing a criminal offence**, based solely on the **profiling** of a natural person **OR on assessing their personality traits and characteristics**.

Not prohibited when it merely supports a human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity.

EMOTIONS IN THE WORKPLACE AND EDUCATION INSTITUTIONS

Infer **emotions** in the workplace or in an education institution based on biometric data.

Not prohibited when intended to be used for medical or safety reasons.

BIOMETRIC CATEGORISATION

Systems that categorise individual natural persons **based on biometric data to deduce or infer** race, political opinions, trade union membership, religious or philosophical beliefs, sex life or orientation.

Not prohibited when used for labelling, filtering or categorizing biometric data in the area of law enforcement.

'REAL-TIME' BIOMETRIC IDENTIFICATION

'Real-Time' remote biometric identification systems in **publicly accessible places** for the purposes of law enforcement. Significant exceptions apply and are described in the AI Office guidelines.

'Real-time' refers to instant, near-instant or without significant delay.

EXCEPTIONS FOR RESEARCH

The prohibitions only apply when systems are **put on the market or put into service**. Preceding development and research activities are not in scope (article 2(8) AI Act).

Additionally, a general exception for **AI systems specifically developed and put into service for the sole purpose of scientific research and development** is included in article 2(6) AI Act.

However, once an AI system is marketed or used beyond (scientific) research & development, it must fully comply with the AI Act. Practically, it is wise to consider the prohibitions and other obligations already in the research & development stage.

Research must still follow recognised ethical and professional standards, existing regulations and relevant laws such as the GDPR.

EXCEPTIONS FOR PERSONAL USE

The AI Act is not applicable when the system is used for purely non-professional purposes by natural persons.

THE IMPACT OF THE EU AI ACT IN 6 SIX STEPS

Step 2: Is the system a high-risk system (type 1)?

If the AI system is not a prohibited AI system under article 5 AI Act, attention must be given to the high-risk AI systems listed in **article 6 AI Act**. These systems could pose a serious risk to the health or safety of individuals or their fundamental rights.

The high-risk AI systems can be divided in **two types**.

- The first type relates to **products to which sectoral, European product legislation already applies**. If an organization is already involved with products or safety components for these kind of products, they may already be aware that specific legislation applies and that conformity assessments must be done.
- The second type of high-risk AI systems are systems used for a **specific purpose in a specific context or sector**. If both the purpose and context are present, the system is high-risk.

Type 1 – Relevant products under specific legislation (Annex I)


Machinery


Toys


Recreational craft and personal watercraft


Lifts


Pressure equipment


Cableway installations


Personal protective equipment


Appliances burning gaseous fuels


Medical devices


Radio equipment (e.g. WiFi)


In vitro diagnostic medical devices


Equipment and protective systems intended for use in potentially explosive atmospheres

The system is high-risk when it is (part of) a product that falls within one of the specified legislation (or is a safety component of such a product) in Annex I **and requires a third-party conformity assessment** by a third party under said legislation. A safety component is a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property.

Be aware: the product categories may be broader than anticipated. For instance—radio equipment does not only include radios. It includes TVs, radio receivers, devices that connect to public telecom networks, cordless phones, mobile phones, and more. Therefore, in case of doubt about whether the AI system is a (safety component of a) product in one of the categories, it is recommended to look further into the respective definitions.

EXCEPTIONS

Civil aviation, two- or three-wheel vehicles or quadricycles, agricultural and forestry vehicles, marine equipment, rail systems, motor vehicles and their trailers, drones. These are not subject to the obligations for high-risk AI systems in the AI Act.

Knowledge Centre Data & Society

Artificial Intelligence Flanders

THE IMPACT OF THE EU AI ACT IN 6 SIX STEPS

Step 2: Is the system a high-risk system (type 2)?

Knowledge Centre Data & Society

Artificial Intelligence Flanders

The Type 2 high-risk AI systems are explained on this page. In the titles you can find the sectors or contexts in which specific purposes are deemed to be high-risk. First identify whether the AI system is used in the one of the mentioned sectors/contexts, then also determine whether the purpose or objective of the AI systems is one of the uses described under the title. If this is the case, the AI system will most likely be qualified as a high-risk AI system under the AI Act.

CRITICAL INFRASTRUCTURE

Safety components in the management and operation of **critical (digital) infrastructure, road traffic, or in the supply of water, gas, heating or electricity**. (e.g. AI-based smart traffic lights).

EDUCATION AND VOCATIONAL TRAINING

AI systems used in educational and vocational training institutions, at all levels, will be considered high-risk for the following purposes:

- To determine **access or admission or to assign natural persons to institutions**;
- To **evaluate learning outcomes**;
- Assessing the **appropriate level of education** that an individual will receive or will be able to access;
- Monitoring and detecting prohibited **behaviour of students during tests**.

ESSENTIAL PRIVATE AND PUBLIC SERVICES AND BENEFITS

AI systems used to determine **access to and enjoyment of essential private services and essential public services and benefits** will be considered high-risk for the following uses:

- Used by public authorities or on their behalf --> To evaluate the **eligibility** of natural persons for essential public assistance benefits and services, incl. healthcare services, as well as **to grant, reduce, revoke, or reclaim** such benefits and services;
- To evaluate the **creditworthiness** of natural persons or establish their **credit score** (not high-risk for detecting financial fraud);
- For risk assessment and pricing in relation to natural persons in the case of **life and health insurance**;
- To **evaluate and classify emergency calls** by natural persons or to be used **to dispatch, or to establish priority** in the dispatching of, emergency **first response services**, as well as of **emergency healthcare patient triage systems**.

BIOMETRICS

Biometrics (if permitted by Union or national law):

- **Remote biometric identification systems**.
  - Remote = the ability of biometric systems to identify individuals without their active involvement, typically at a distance through the comparison of a person's biometric data with biometric data contained in a reference database.
- Used for **biometric categorisation**, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics.
- Used for **emotion recognition**.

N.B.: conditions and safeguards of article 5(2) to (7) AI Act must be met for law enforcement (see step 1).

EMPLOYMENT

AI systems used **on the workfloor** and for **access to self-employment** are high-risk when:

- Used for the **recruitment or selection** of natural persons, in particular to place targeted job advertisements, to analyse and filter job applications, and to evaluate candidates;
- The AI systems **make decisions** affecting:
  - **Terms** of work-related relationships, the **promotion or termination** of work-related contractual relationships,
  - The **allocation of tasks** based on individual behaviour or personal traits or characteristics;
  - The **monitoring and evaluation** of the performance and behaviour of persons in such relationships.

OTHER

In addition to the AI systems described in this tool, other sectors are also regulated. This is the area of **law enforcement** (e.g. AI systems that function as polygraph), **migration, asylum and border control management, and the administration of justice and democratic processes**. For the purposes of this tool we have left them out of scope.

EXCEPTIONS

A general exception applies to these type 2 AI systems: they are not considered high-risk when they **do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons**, including by not materially influencing the outcome of their decision-making.

The EU AI Act lists 4 conditions, under any of which this exception is fulfilled. This is case of the AI system **is intended to**:

1. Perform a **narrow procedural task**
2. Improve the result of a previously completed **human activity**
3. Detect **decision-making patterns** or deviations from such prior patterns and not meant to replace or influence previously completed assessments without human review
4. Perform a **preparatory task** to an assessment relevant for the purposes of the use cases listed in Annex III

The above exception does not apply if the AI system performs profiling, in which case it is still considered high-risk.

THE IMPACT OF THE EU AI ACT IN 6 SIX STEPS

Step 3: Do any additional transparency requirements apply?

Regardless of whether the system can be classified as high-risk (or not), it may also fall within the scope of the additional transparency requirements contained in article 50 AI Act. The required **information must always be given in a clear and distinguishable manner** at the latest **at the time of the first interaction or exposure** to the AI system. Moreover, such information provision must apply the relevant **accessibility** requirements. Each of the transparency requirements is subject to law enforcement exceptions which will not be discussed in detail in this tool.

Knowledge Centre Data & Society

Artificial Intelligence Flanders

If...	Then...	Unless..
The AI system is intended to **interact directly with natural persons**. For example, a chatbot.	The provider shall ensure that the system is developed and designed in such a way that the natural persons are **informed** that they are interacting with an AI system.	Unless this is obvious from the point of view of a natural person who is reasonably well-informed, observant and circumspect, taking into account the circumstances and the context of use.
The AI system **generates synthetic audio, image or video or text content** (incl. GPAIM). Not for AI systems that perform an assistive function for standard editing or do not substantially alter the input data provided by the deployer or the semantics thereof.	The provider shall ensure that the **system's output are marked in a machine-readable format and detectable** as artificially generated or manipulated. This must happen effectively, interoperable, robustly and reliably as far as this is technically feasible, taking into account the specificities and limitations of various types of content, the costs of implementation and the generally acknowledged state of the art.	
The AI system is an **emotion recognition system or a biometric categorisation system**.	The deployer shall **inform the natural persons** exposed to the (operation of the) system, and shall take the applicable data protection legislation into account.	
The AI system generates or manipulates image, audio or video content constituting a **deep fake**.	The deployer shall **disclose** that the content has been artificially generated or manipulated.	Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, this obligation can be done in an appropriate manner that does not hamper the display or enjoyment of the work.
The AI system generates or manipulates **text** which is published **with the purpose of informing the public on matters of public interest**.	The deployer shall **disclose** that the content has been artificially generated or manipulated.	Not when the AI-generated content has undergone a process of human reviews or editorial control and where a natural or legal person holds editorial responsibility for the publication of the content (e.g. news agency).

THE IMPACT OF THE EU AI ACT IN 6 SIX STEPS

Step 4: Is it an AI system/model or GPAIM?

If a system falls under one of the prohibited practices or high-risk categories, or is subject to increased transparency, the organization should now verify whether the system is also qualified as an AI system/model in the AI Act. Since this definition is not fully clarified, it is preferable to first establish whether the AI system is within the scope of application by looking at the prohibited, increased transparency and high-risk AI systems, as was done in steps 1 to 3.

Knowledge Centre Data & Society

Artificial Intelligence Flanders

AI SYSTEM - WHAT?

The EU AI Act applies to "AI systems". It is crucial to understand what this term encompasses. To this end, the EU AI Office released its first set of guidelines, providing insights into which systems qualify as AI systems under article 3(1) AI Act. As many of these terms can be ambiguous, we include short explanations below.

> "A **machine-based** system that is designed to operate on **varying levels of autonomy** and that may exhibit **adaptiveness** after deployment, and that, for explicit or implicit **objectives, infers**, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can **influence physical or virtual environments**."

Machine-based: the term "machine" can include both hardware or software components. This terms covers a wide variety of computational systems – even those that are biological or organic – as long as they possess computational capacity.

Autonomy: the system must exhibit some reasonable degree of independence from human intervention. Systems that require full manual control and constant human input are excluded.

Adaptiveness: the system may have self-learning capabilities. This element is optional, and not a defining requirement.

AI system objectives: the objectives are internal to the system, focusing on the goals of the tasks and desired outcomes. They can be explicitly encoded by developers or implicitly derived from system behaviour or underlying assumptions of the system. These can differ from the intended purpose (which is external) in a specific context.

Inferencing how to generate outputs using AI techniques: can be understood as the process of obtaining outputs from inputs or data and to the capability of the system to derive models or algorithms from inputs or data using AI techniques (e.g. machine learning approaches and logic- and knowledge-based). This means that simpler traditional software systems or programming approaches (e.g. basic data processing) should not be included.

Generation of outputs that can influence physical or virtual environments and interaction with the environment: the AI system should actively impact the environments in which they are deployed.

AI MODEL - WHAT?

An AI model is not explicitly defined in the AI Act. It can be understood as the underlying computational function or algorithm that processes input data to produce outputs such as predictions, content, recommendations, or decisions. This model can be a component of an AI system and is responsible for the system's ability to perform tasks.

GENERAL-PURPOSE AI MODEL - WHAT?

It is an **AI model** (see above), which displays **significant generality** and is capable of competently performing a **wide range of distinct tasks**. It can also be integrated into a variety of downstream systems or applications. How the model is placed on the market is irrelevant.

Exception: GPAIM used for research, development or prototyping activities before they are placed on the market are not subject to the requirements.

Providers of all GPAIM must adhere to the obligations of article 53 AI Act. When these GPAIM also have a **systemic risk**, the obligations from article 55 are also applicable.

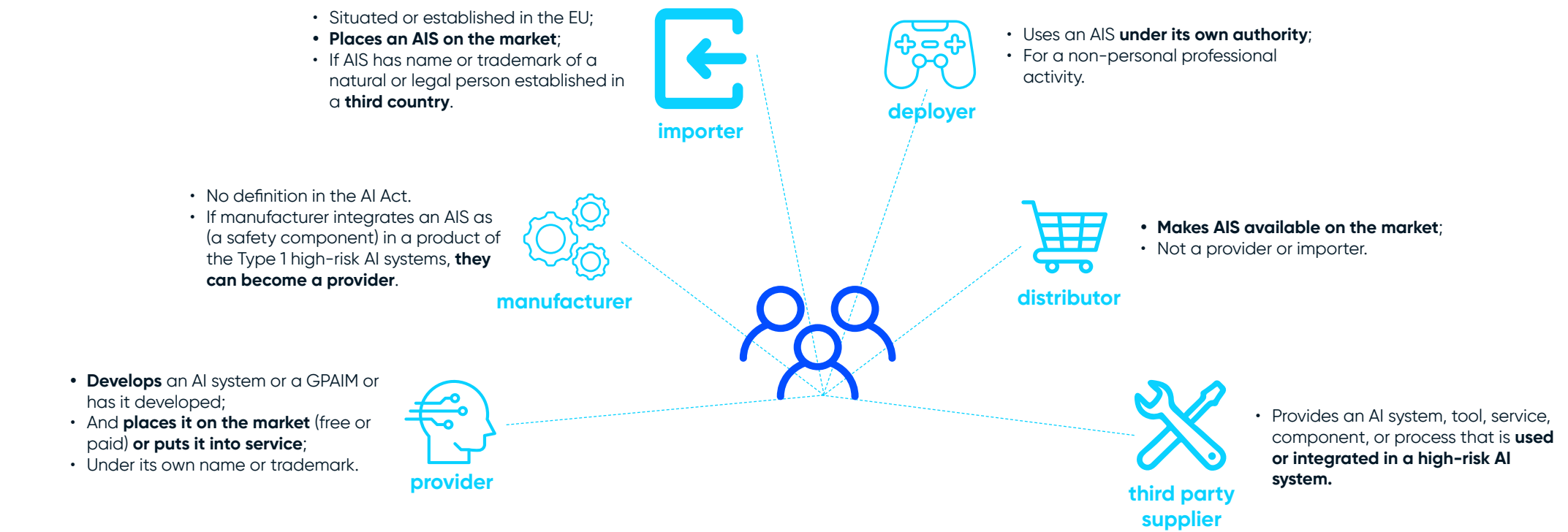
Systemic risks are risks that are specific to the high-impact capabilities of GPAIM. A model has a systemic risk if it has **high-impact capabilities** based on an evaluation or if it is designated as having systemic risk following a decision by the EU Commission. A model is presumed to have high-impact capabilities if its training is greater than 10^25 floating points operations.

THE IMPACT OF THE EU AI ACT IN 6 SIX STEPS

Step 5: Who is who in the EU AI Act?

Knowledge Centre Data & Society

Artificial Intelligence Flanders



- Situated or established in the EU;
- **Places an AIS on the market**;
- If AIS has name or trademark of a natural or legal person established in a **third country**.

- Uses an AIS **under its own authority**;
- For a non-personal professional activity.

- No definition in the AI Act.
- If manufacturer integrates an AIS as (a safety component) in a product of the Type 1 high-risk AI systems, **they can become a provider**.

- **Makes AIS available on the market**;
- Not a provider or importer.

- **Develops** an AI system or a GPAIM or has it developed;
- And **places it on the market** (free or paid) **or puts it into service**;
- Under its own name or trademark.

- Provides an AI system, tool, service, component, or process that is **used or integrated in a high-risk AI system.**

OTHER RELEVANT DEFINITIONS (ARTICLE 2 AI ACT)

Placing on the marke: first making available of an AIS or a GPAIM on the Union market.

Making available on the market: the supply of an AIS or a GPAIM for distribution or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge.

Putting into service: the supply of an AIS for first use directly to the deployer or for own use in the Union for its intended purpose.

Intended purpose: the use for which an AIS is intended by the provider, including the specific context and conditions of use, as specified in the information supplied by the provider in the instructions for use, promotional or sales materials and statements, as well as in the technical documentation.

Substantial modification: a change to an AIS after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider and as a result of which the compliance of the AIS with the requirements set out in Chapter III, Section 2 AI Act is affected or results in a modification to the intended purpose for which the AIS has been assessed. An importer, distributor, deployer or third-party can be consider a provider if they make such a modification to an existing AI-system.

THE IMPACT OF THE EU AI ACT IN 6 SIX STEPS

Step 6: What corresponding obligations apply?

After establishing which actor an organization qualifies as under in the AI Act, the final step is to consider the corresponding obligations when developing, using and selling high-risk AI systems. Some obligations are applicable to all actors. Others are distributed to specific actors. Below we included a brief checklist of obligations. Note that this is not exhaustive. Obligations applicable to providers are indicated with "(P)", obligations applicable to deployer with "(D)".

HUMAN OVERSIGHT

- √ **Effective oversight (P):** design and develop mechanisms for effective human oversight on, intervention in, and interpretation of high-risk AI systems.
- √ **Training and competence (D):** train personnel overseeing high-risk AI systems and provide them necessary competence and authority.
- √ **User rights (D):** ensure affected persons can exercise their rights to explanations of individual decision-making using Type 2 high-risk AI systems.

DATA GOVERNANCE & PRIVACY

- √ **Data governance (P):** ensure data used in AI systems meets quality criteria for the purpose such as relevance, accuracy, completeness, and appropriate governance practices.
- √ **Correct input data (D):** ensure the input data used is relevant for the high-risk AI system and sufficiently representative.
- √ **Data privacy compliance (P & D):** align data processing activities with GDPR and other relevant data protection regulations.

RISK MANAGEMENT SYSTEM

- √ **Risk assessment (P):** conduct a thorough risk analysis for the AI system, identifying potential risks to fundamental rights, safety, and privacy when used.
- √ **Mitigation strategies (P & D):** develop and implement measures to mitigate identified risks and, as deployer, take technical and organisational measures to follow instructions for use.
- √ **Ongoing monitoring (P):** establish processes for post-market monitoring and evaluation of AI system performance and risk.

ACCURACY, TESTING AND VALIDATION

- √ **Accuracy, robustness and security (P):** Design and develop the system to achieve appropriate level of accuracy, robustness and cybersecurity throughout its lifecycle.
- √ **Pre-deployment testing and validation (P):** conduct testing of AI systems before deployment to identify appropriate risk management measures and its accuracy metrics, robustness and security.

INCIDENT RESPONSE AND REPORTING

- √ **Incident management plan (P & D):** develop and maintain a serious incident response plan for addressing and reporting serious incidents to the relevant authorities and, for the deployer, to the provider of the AI system.
- √ **Remediation actions (P):** establish protocols for taking corrective actions to address and mitigate non-compliance and serious incidents.

Knowledge Centre Data & Society

Artificial Intelligence Flanders

TRANSPARENCY AND ACCOUNTABILITY

- √ **Transparent design (P):** design and develop AI system to enable appropriate interpretation of the output by the deployer.
- √ **Instructions for use (P & D):** Draft the required instructions for use so that deployers can appropriately use the AI system or, as deployer, use the AI system in accordance with them.
- √ **Documentation (P):** maintain technical and other documentation for each high-risk AI system, including development processes, changes, and risk management systems to demonstrate compliance with requirements.
- √ **Record-keeping (P & D):** Design the system to keep automatic logging of events and keep generated logs for an appropriate time, at least 6 months.
- √ **Register (P):** Type 2 high-risk AI systems must be registered in an EU database.
- √ **Inform workers' representatives (D):** when putting into service a high-risk AI system in the workplace.

CONFORMITY ASSESSMENT AND MARKING

- √ **Conformity assessment process (P):** the system must undergo relevant conformity assessment procedures before being placed on the market or put into service
- √ **Declaration of conformity (P):** after placing the system on the market or putting it into service, draft appropriate EU declaration of conformity.
- √ **Add CE markings (P):** a CE marking must be affixed to the high-risk AI system.

GOVERNANCE FRAMEWORK

- √ **Quality management system (P):** develop and implement internal policies and procedures to ensure ongoing compliance with the EU AI Act.
- √ **Third-party management: (P):** specify required information, technical details and access, or other assistance in contracts with third-party suppliers of components for high-risk AI systems.