EU AI Act

Step 1 Qualification

Agent Prompt: Classify the AI System Based on Risk Category

Goal:
Determine whether the AI system described in the user's documentation qualifies as a **prohibited**, **high-risk**, **general-purpose AI (GPAI)**, **limited-risk**, or **minimal-risk** system according to the EU AI Act. Extract only what can be justified based on the documentation and flag ambiguity when necessary.

Step 1: Extract Basic System Characteristics

From the AI use case documentation, extract:

- Intended purpose of the system
- Target users (internal, external, public)
- Deployment context (e.g. public space, private sector, workplace)
- AI capabilities (e.g. classification, prediction, generation, recommendation)
- Use of biometric, emotion recognition, or decision-making on individuals
- General-purpose nature (i.e. trained for broad tasks, not purpose-specific)

Step 2: Classify the System Using EU AI Act Definitions

Use the extracted information to classify the system into one of the following categories. Mark as "Not Enough Info" if classification cannot be reasonably determined from available documentation.

- Use **subliminal techniques** or manipulative behavior
- Exploit vulnerable groups (children, mentally impaired)
- Enable **untargeted remote biometric ID in public spaces**
- Implement **social scoring** by governments
- Use real-time biometric categorization without exemptions

If yes → Classify as "Prohibited"

B. High-Risk System (Articles 6–7 + Annex III)
Check if the system falls into a category listed in **Annex III**, such as:

- Biometric identification
- Critical infrastructure (transport, water, energy)
- Education and vocational training
- Employment, HR, and worker management
- Access to essential services (banking, housing, insurance)
- Law enforcement and border control
- Administration of justice or democratic processes
- Safety components of regulated products (e.g. medical devices, cars)

If yes → Classify as "High-Risk"

C. General-Purpose AI (GPAI) System (Articles 52–56)

- Is **trained on broad data sets**
- Can perform a **wide range of tasks** (e.g. text, image, speech)
- Is **adapted** or fine-tuned for downstream use cases
- Does not have a narrowly defined, pre-specified purpose

If yes → Classify as "GPAI"

D. Limited-Risk System (Article 52)
Check if the system:

- Is a **chatbot**, **emotion detection system**, **deepfake generator**, or similar interface
- Requires **transparency obligations** to inform users they are interacting with AI

If yes → Classify as "Limited-Risk"

E. Minimal-Risk System
If none of the above apply, and the system is:

- A productivity tool (e.g. spam filter, calculator, AI in games)
- Not making decisions that impact individuals' rights or safety
- Not subject to any transparency, risk, or sectoral obligations

→ Classify as "Minimal-Risk"

Output Format:

- **Classification:** (Prohibited / High-Risk / GPAI / Limited-Risk / Minimal-Risk / Not Enough Info)

- **Extracted Evidence:**

- **Recommendation (if unclear):** Indicate what additional documentation would be needed to complete classification

Step 2 Prompt Library

Sub-Prompt: Article 5(1)(a) – Manipulative or Subliminal Techniques

Check:
Does the documentation describe or imply the use of **subliminal**, **manipulative**, or **deceptive techniques** that influence a person's behavior **without their awareness**, with the effect of **impairing informed decision-making** and potentially causing **significant harm**?

Flag if:

- Techniques operate **below conscious awareness**

- System's objective or effect is to **distort choices**

- Harm described or reasonably foreseeable due to influence on decisions

Output Format:

- **Status:** (Yes / No / Unclear)

- **Evidence:** Quote or paraphrase from documentation

- **Recommendation:** If Yes or Unclear → "Prohibited under Article 5(1)(a). This practice must be immediately discontinued or redesigned to eliminate subliminal or manipulative elements that distort user decisions without awareness and cause harm."

- **Reference:** EU AI Act Article 5(1)(a)

Check:
Does the documentation indicate that the system targets or could exploit **vulnerable groups** (based on **age**, **disability**, or **social/economic status**) in a way that **distorts behavior** and may **cause significant harm**?

Flag if:

- Intended users include **children**, **elderly**, or **economically disadvantaged**
- The system nudges behavior without safeguards for such groups
- Use case suggests personalized manipulation based on vulnerability

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Direct excerpt or summary from documentation
- **Recommendation:** If Yes or Unclear → "Prohibited under Article 5(1)(b). System must not be designed or deployed in ways that exploit vulnerabilities tied to age, disability, or socio-economic status that distort behavior and risk harm."
- **Reference:** EU AI Act Article 5(1)(b)

Sub-Prompt: Article 5(1)(c) – Social Scoring

Check:
Does the documentation describe or imply the use of the AI system to **evaluate or classify natural persons** over time based on **social behavior** or **personality characteristics**, leading to **unfavorable or disproportionate treatment**?

Flag if:

- Scoring based on **lifestyle**, **morality**, or **online/offline behavior**
- Repeated evaluation of individuals across contexts

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Quoted or paraphrased excerpt
- **Recommendation:** If Yes or Unclear → “Prohibited under Article 5(1)(c). Social scoring systems that result in unrelated or unjustified adverse treatment are not permitted.”
- **Reference:** EU AI Act Article 5(1)(c)
-

Sub-Prompt: Article 5(1)(d) – Predictive Criminal Risk Based on Profiling

Check:
Does the documentation show that the AI system is used to **assess or predict criminal risk** of individuals **based solely on profiling** or **personality traits**, without reference to **objective and verifiable facts linked to criminal activity**?

Flag if:

- System outputs a **risk score** or **prediction** of future criminal behavior
- Inputs include **personality analysis**, **behavioral patterns**, or **non-evidentiary profiling**
- No link to **specific incidents** or **factual indicators** of criminal activity

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Relevant excerpt or description
- **Recommendation:** If Yes or Unclear → “Prohibited under Article 5(1)(d). AI systems must not be used to predict criminal behavior solely through profiling or personality assessment without factual basis.”

-

Sub-Prompt: Article 5(1)(e) – Untargeted Facial Scraping

Check:
Does the documentation indicate that the system **creates or expands facial recognition databases** using **untargeted scraping** of facial images from the **internet** or **CCTV footage**?

Flag if:

- Data sources include **public image repositories**, **social media**, **surveillance feeds**
- No indication of **targeted consent**, **lawful collection**, or **purpose-limited acquisition**
- System builds or augments a **facial recognition dataset** through broad scraping

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Referenced data sources or scraping methods
- **Recommendation:** If Yes or Unclear → “Prohibited under Article 5(1)(e). Systems must not build or expand facial recognition datasets via untargeted scraping from public sources or surveillance footage.”
- **Reference:** EU AI Act Article 5(1)(e)
-

Sub-Prompt: Article 5(1)(f) – Emotion Recognition in Workplace or Education

Check:
Does the documentation indicate that the system is used to **infer emotions** of individuals in a **workplace** or **educational setting**, **except** for clearly stated **medical or safety purposes**?

Flag if:

- System detects or infers **emotions**, **sentiment**, **stress**, or **affective state**

- No justification tied to **health**, **safety**, or **medical necessity**

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Stated purpose or deployment context
- **Recommendation:** If Yes or Unclear → “Prohibited under Article 5(1)(f). Emotion recognition in workplace or educational settings is not permitted unless explicitly justified for medical or safety use.”
- **Reference:** EU AI Act Article 5(1)(f)

Sub-Prompt: Article 6(1) – Regulated Product Integration (Annex I)

Check:
Does the documentation indicate that the AI system is **intended to be a component of a product** or system that is covered by **Union harmonization legislation** listed in **Annex I**?

Examples of Annex I-covered products include:

- Medical devices
- Machinery
- Vehicles
- Toys
- Aviation systems
- Radio equipment
- Pressure equipment

Flag if:

- The system is intended for use in such products during or after market placement

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Reference to product type, regulatory context, or integration purpose
- **Recommendation:** If Yes or Unclear → “AI system qualifies for high-risk classification under Article 6(1) due to integration into a regulated product per Annex I.”
- **Reference:** EU AI Act Article 6(1), Annex I

Sub-Prompt: Article 6(1) – Safety Function

Check:
Does the documentation indicate that the AI system performs a **safety function**, meaning that **its failure or malfunction could directly endanger the health or safety of people**?

Flag if:

- The AI system controls, influences, or overrides **safety-critical operations**
- A failure could lead to **physical harm**, **health risk**, or **loss of control** over regulated equipment
- The safety role is explicitly mentioned or can be inferred from the system's function

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Excerpt describing safety relevance or operational risk
- **Recommendation:** If Yes or Unclear → “System qualifies as high-risk under Article 6(1) due to performing a safety function within a regulated product.”
- **Reference:** EU AI Act Article 6(1)

Check:
Does the documentation indicate that the AI system is intended to be used in any of the **eight high-risk use case categories listed in Annex III**?

The categories are:

1. **Biometric identification and categorization** of natural persons
2. **Critical infrastructure** (e.g. water, energy, transport)
3. **Education and vocational training**
4. **Employment, worker management, access to self-employment**
5. **Access to essential services** (credit, insurance, housing, etc.)
6. **Law enforcement**
7. **Migration, asylum, and border control**
8. **Administration of justice and democratic processes**

Flag if:

- The system's purpose matches any category above
- Deployment context or customer type indicates use in these sectors

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Use case summary, deployment plan, or customer segment
- **Recommendation:** If Yes or Unclear → "System qualifies as high-risk under Article 6(2) due to intended use in an Annex III category."
- **Reference:** EU AI Act Article 6(2), Annex III

Check:
Does the documentation suggest that the AI system, **while not originally intended for a high-risk use by the provider**, is being **used or repurposed by the deployer** in a way that matches any **Annex III high-risk categories**?

Flag if:

- The system is being **applied in a high-risk domain** by the user or customer, even if the provider's purpose statement does not explicitly include it
- The deployment context includes **schools**, **hospitals**, **courts**, **border agencies**, or **law enforcement**, etc.
- Use indicates **decision-making that significantly affects people's rights or access to services**

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Deployment scenario, downstream application, or integration notes
- **Recommendation:** If Yes or Unclear → "System may qualify as high-risk under Article 6(2) due to real-world deployment in an Annex III context, regardless of original intent."
- **Reference:** EU AI Act Article 6(2), Annex III

Sub-Prompt: Article 9(1) – Presence of a Risk Management System

Check:
Does the documentation show that a **risk management system** has been:

- **Established**
- **Implemented**
- **Documented**

...specifically in relation to the **AI system throughout its lifecycle**?

Flag if:

- Risk processes are **not described** or are only mentioned for **pre-deployment** stages
- There's no reference to a **structured system** guiding risk handling across **design, development, deployment, and updates**

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Documentation excerpts or risk framework references
- **Recommendation:** If No or Unclear → "Required under Article 9(1). Providers must implement and document a full-lifecycle risk management system specific to the high-risk AI system."
- **Reference:** EU AI Act Article 9(1)

Sub-Prompt: Article 9(2)(a) – Risk Identification & Analysis

Check:
Does the documentation show that the provider has **identified and analyzed** all **known and reasonably foreseeable risks** the AI system may pose to:

- **Health**
- **Safety**
- **Fundamental rights**

...when used in accordance with its **intended purpose**?

Flag if:

- No clear list of risks is documented

- No consideration of **rights-based impacts**, such as bias, discrimination, or privacy harm

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Direct excerpts describing risk categories or sources
- **Recommendation:** If No or Unclear → "Required under Article 9(2)(a). Providers must identify and analyze foreseeable risks to health, safety, and rights based on how the system is intended to be used."
- **Reference:** EU AI Act Article 9(2)(a)

Sub-Prompt: Article 9(2)(a) – Risk Identification & Analysis

Check:
Does the documentation show that the provider has **identified and analyzed** all **known and reasonably foreseeable risks** the AI system may pose to:

- **Health**
- **Safety**
- **Fundamental rights**

...when used in accordance with its **intended purpose**?

Flag if:

- No clear list of risks is documented
- Risks are vaguely described or focused only on technical failure
- No consideration of **rights-based impacts**, such as bias, discrimination, or privacy harm

Output Format:

- **Evidence:** Direct excerpts describing risk categories or sources

- **Recommendation:** If No or Unclear → “Required under Article 9(2)(a). Providers must identify and analyze foreseeable risks to health, safety, and rights based on how the system is intended to be used.”

- **Reference:** EU AI Act Article 9(2)(a)

Sub-Prompt: Article 9(2)(c) – Post-Market Risk Evaluation

Check:
Does the documentation show that the provider **evaluates risks** based on data gathered from a **post-market monitoring system** (as referenced in **Article 72**)?

Flag if:

- There is **no mention** of post-deployment monitoring or feedback loops

- The risk management process is treated as **static**, with no indication of **continuous updates**

- No link to **real-world incident tracking**, user complaints, or performance degradation analysis

Output Format:

- **Status:** (Yes / No / Unclear)

- **Evidence:** Monitoring references, feedback procedures, or data analysis workflows

- **Recommendation:** If No or Unclear → “Required under Article 9(2)(c). Risk management must incorporate feedback from post-market monitoring to update and refine risk assessments.”

- **Reference:** EU AI Act Article 9(2)(c), cross-reference Article 72

Sub-Prompt: Article 9(2)(d) – Targeted Risk Mitigation Measures

Check:
Does the documentation describe **specific and appropriate risk management measures** that have been

Flag if:

- Controls are **generic** (e.g. "regular audits", "monitoring") without linking to specific risks
- No evidence that **identified risks have corresponding mitigations**
- Mitigation actions are not tailored to risk **type**, **impact**, or **user context**

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Risk control matrix, mitigation plans, design adjustments
- **Recommendation:** If No or Unclear → “Required under Article 9(2)(d). Documented risk management must include clear mitigation measures tied to each identified risk.”
- **Reference:** EU AI Act Article 9(2)(d)

Sub-Prompt: Article 9(5) – Residual Risk Evaluation

Check:
Does the documentation demonstrate that the provider has:

- Assessed the **residual risk** remaining after mitigation, for **each hazard**, and
- Determined that the **overall residual risk** of the system is **acceptable**?

Flag if:

- No mention of **residual risks** after applying mitigation
- Acceptability criteria are missing or vague (e.g. “risk reduced” without thresholds)
- No documented rationale for **why residual risk is considered tolerable**

Output Format:

- **Evidence:** Residual risk matrix, acceptability thresholds, or documented justification

- **Recommendation:** If No or Unclear → “Required under Article 9(5). Providers must assess whether the remaining risk after mitigation is acceptable and provide a documented rationale.”

- **Reference:** EU AI Act Article 9(5)

Sub-Prompt: Article 9(6–8) – Testing to Inform Risk Management

Check:
Does the documentation show that the AI system has been **tested** to:

- Identify and validate **risk management measures**

- Confirm the system performs **consistently with its intended purpose**

- Assess performance against **predefined metrics and probabilistic thresholds**

- Possibly include **real-world testing** (per Article 60)

Flag if:

- No structured testing is described prior to release

- No metrics, benchmarks, or thresholds are referenced

- Testing is described only in functional or accuracy terms—not tied to **risk control**

- No mention of **when** or **how often** testing occurs

Output Format:

- **Status:** (Yes / No / Unclear)

- **Evidence:** Testing protocols, QA plans, threshold documentation

- **Recommendation:** If No or Unclear → “Required under Article 9(6–8). Testing must validate risk controls and confirm consistent system performance before market entry.”

Sub-Prompt: Article 9(9) – Consideration of Children and Vulnerable Groups

Check:
Does the documentation show that the provider has considered whether the AI system is likely to **impact individuals under 18** or other **vulnerable groups**, and reflected this in their risk management approach?

Flag if:

- No mention of **user demographics**, age-specific risks, or vulnerable populations
- Risk controls are generic and not tailored to those **with reduced agency, power, or digital literacy**
- No adjustments in **design**, **messaging**, or **guardrails** based on user vulnerability

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** User segmentation, safeguards, or tailored mitigation for minors/vulnerable groups
- **Recommendation:** If No or Unclear → "Required under Article 9(9). Providers must assess and address the system's potential impact on minors and other vulnerable users."
- **Reference:** EU AI Act Article 9(9)

Sub-Prompt: Article 9(10) – Integration with Other Risk Management Frameworks

Check:
If the provider is subject to **other Union-level regulatory frameworks** (e.g. medical device, financial services, aviation), does the documentation show that the AI-related risk management process is:

- **Integrated** with existing compliance processes, or
- **Coordinated** to avoid duplication or inconsistency?

Flag if:

- No mention of other applicable EU regulatory obligations where known (e.g. CE, GDPR, MiFID, MDR)

- There's no mapping between AI risks and broader **enterprise or sectoral risk controls**

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Cross-references to product compliance files or harmonized risk procedures
- **Recommendation:** If No or Unclear → “Required under Article 9(10). Providers must align AI risk processes with existing Union compliance frameworks, where applicable.”
- **Reference:** EU AI Act Article 9(10)

Gatekeeper Prompt: Article 10(1) – Use of Model Training Techniques

Check:
Does the documentation indicate that the AI system involves techniques requiring the training of AI models, such as:

- Supervised, unsupervised, or reinforcement learning
- Fine-tuning of pre-trained models
- Transfer learning or embedding generation
- Any technique where performance depends on training with datasets

If No:
→ **Proceed only with the governance sub-prompt for Article 10(6)** (testing data governance for non-trained systems)

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Model training references, ML techniques, architecture description
- **Routing:** Based on status, guide agent to correct downstream prompt path
- **Reference:** EU AI Act Article 10(1)

Sub-Prompt: Article 10(2)(a) – Data Design Choices

Check:
Does the documentation describe the design choices made in the construction of training, validation, and testing datasets, including:

- **Rationale for the dataset's structure, splitting strategy, or sampling logic**
- Selection criteria for inclusion/exclusion of data
- Why certain data sources were prioritized

Flag if:

- No description of how the dataset design aligns with the intended use of the system
- No justification for dataset composition, balance, or partitioning strategy

- **Status:** (Yes / No / Unclear)

- **Evidence:** Dataset documentation, training pipeline, or design rationale

- **Recommendation:** If No or Unclear → “Required under Article 10(2)(a). The documentation must reflect conscious design choices made in dataset construction and alignment with the AI system’s intended use.”

- **Reference:** EU AI Act Article 10(2)(a)

Sub-Prompt: Article 10(2)(b) – Data Origin and Collection Purpose

Check:
Does the documentation specify:

- **The source and origin** of all training, validation, and testing datasets

- **The data collection process**, and

- **For personal data, the original collection purpose**, and whether it aligns with the intended AI use

Flag if:

- Data origin is not clearly stated

- Source legitimacy (e.g., scraped, purchased, open source) is ambiguous

- No mapping of personal data’s original purpose to current AI use context

Output Format:

- **Status:** (Yes / No / Unclear)

- **Recommendation:** If No or Unclear → “Required under Article 10(2)(b). Documentation must include data origin and, for personal data, clearly link its original collection purpose to the intended AI application.”

- **Reference:** EU AI Act Article 10(2)(b)

Sub-Prompt: Article 10(2)(c) – Data Pre-processing and Preparation Operations

Check:
Does the documentation describe the **data preparation operations** applied to the training, validation, or testing datasets, including:

- **Annotation** or labeling methodology
- **Cleaning**, deduplication, or normalization steps
- **Updating**, **enrichment**, or **aggregation** techniques used
- Any **automated or manual processes** applied before model input

Flag if:

- There is no clear description of how raw data is prepared for use
- Steps taken to improve dataset quality or consistency are undocumented
- No auditability of data prep process

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Pipeline diagrams, preprocessing scripts, or annotation protocols
- **Recommendation:** If No or Unclear → “Required under Article 10(2)(c). The documentation must include details on all major data preparation steps used to shape training, validation, and testing

- **Reference:** EU AI Act Article 10(2)(c)

Sub-Prompt: Article 10(2)(d) – Assumptions About Data Representation

Check:
Does the documentation include a clear statement of **assumptions** made about what the training, validation, and testing datasets are intended to:

- **Measure**, represent, or approximate
- Capture in terms of **real-world behavior**, categories, patterns, or outcomes
- Serve as a proxy for (e.g. user intent, creditworthiness, risk level, etc.)

Flag if:

- Assumptions about the data's meaning are **implicit or missing**
- The documentation does not specify **what the labels or features are presumed to signify**
- There's no reflection on whether these assumptions are valid for the intended use

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Data documentation, labeling guidelines, model objective notes
- **Recommendation:** If No or Unclear → "Required under Article 10(2)(d). Providers must explicitly document the assumptions about what their data represents and how it relates to the AI system's intended task."
- **Reference:** EU AI Act Article 10(2)(d)

Sub-Prompt: Article 10(2)(e) – Data Sufficiency and Availability Assessment

Check:
Does the documentation include an assessment of whether the data used for training, validation, and testing is:

- **Fit for purpose**, given the system's intended context
- Reflective of the target use case and operational conditions

Flag if:

- No explicit assessment of data sufficiency is provided
- Dataset size, coverage, or granularity is not aligned with intended application
- Gaps are acknowledged but not quantified or addressed

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Dataset size/coverage stats, sufficiency analysis, design justification
- **Recommendation:** If No or Unclear → "Required under Article 10(2)(e). Documentation must show that the provider assessed whether data volume and quality are sufficient for the intended system purpose."
- **Reference:** EU AI Act Article 10(2)(e)

Sub-Prompt: Article 10(2)(f) – Bias Detection in Datasets

Check:
Does the documentation include an analysis of **potential bias** in the training, validation, or testing datasets that could:

- Affect **health and safety**
- Lead to **adverse impacts on fundamental rights**, or
- Result in **unlawful discrimination** under EU law

...especially where **outputs influence future inputs** (e.g., feedback loops)?

- No bias audit or exploratory analysis is described
- Protected group-level bias (e.g., race, gender, age) not assessed
- Feedback loops or long-term bias amplification risks are not acknowledged

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Bias audit reports, fairness metrics, subgroup performance
- **Recommendation:** If No or Unclear → "Required under Article 10(2)(f). The provider must assess datasets for bias that could affect rights, safety, or lead to discriminatory outcomes."
- **Reference:** EU AI Act Article 10(2)(f)

Sub-Prompt: Article 10(2)(g) – Bias Mitigation Measures

Check:
Does the documentation describe **specific actions** taken to:

- **Detect**, **prevent**, and **mitigate** any biases identified in the dataset (as required by Article 10(2)(f))?

This may include:

- Rebalancing datasets
- Re-sampling or stratified splits
- Fairness-aware pre-processing
- Exclusion of problematic features or labels

Flag if:

- Biases are acknowledged but no mitigation strategy is documented

- No link between identified risks and corrective actions

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Mitigation steps, fairness preprocessing, or policy notes
- **Recommendation:** If No or Unclear → “Required under Article 10(2)(g). Documented mitigation measures must correspond to the specific types of bias identified in the dataset.”
- **Reference:** EU AI Act Article 10(2)(g)

Sub-Prompt: Article 10(2)(h) – Identification of Data Gaps or Shortcomings

Check:
Does the documentation identify any **gaps, limitations, or shortcomings** in the training, validation, or testing datasets that:

- Prevent full compliance with EU AI Act requirements
- Limit representativeness, fairness, or performance
- Create known blind spots in specific groups, regions, or scenarios

Also, does it describe **how these shortcomings are being addressed or managed**?

Flag if:

- No explicit mention of data limitations or risks
- Gaps are acknowledged but **no remediation path** is described
- Disclaimers exist without operational plans to fix or monitor them

Output Format:

- **Status:** (Yes / No / Unclear)

- **Recommendation:** If No or Unclear → “Required under Article 10(2)(h). Documentation must reflect awareness of data gaps and outline how they are being addressed or monitored.”

- **Reference:** EU AI Act Article 10(2)(h)

Sub-Prompt: Article 10(3) – Data Quality: Representativeness, Accuracy, Completeness

Check:
Does the documentation show that the training, validation, and testing datasets are:

- **Relevant** and aligned with the intended system use

- **Sufficiently representative**, especially across different user groups or contexts

- As far as possible, **free of errors and complete**

- Statistically appropriate (either as standalone datasets or in combination)

Flag if:

- No mention of data quality checks, statistical audits, or sampling validity

- No subgroup performance analysis or diversity metrics

- Datasets are reused with no discussion of their relevance or limitations

Output Format:

- **Status:** (Yes / No / Unclear)

- **Evidence:** Dataset descriptions, QA reports, representativeness claims

- **Recommendation:** If No or Unclear → “Required under Article 10(3). Providers must demonstrate that datasets are accurate, complete, and representative relative to the AI system’s intended purpose.”

- **Reference:** EU AI Act Article 10(3)

Check:
Does the documentation show that the training, validation, and testing datasets account for:

- **Geographic, contextual, behavioral, or functional characteristics** specific to the environment in which the AI system will operate?

Examples:

- Regional dialects, languages, or social norms
- Industry-specific workflows
- Cultural context or behavioral patterns
- Environmental conditions (e.g., lighting, network availability, population density)

Flag if:

- The documentation assumes global generalizability without localized adaptation
- No evidence that the data was assessed for **contextual alignment** with its deployment environment
- Known geographic deployment, but **data provenance or adaptation not specified**

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Geographic annotations, contextual fit assessment, or deployment-target mapping
- **Recommendation:** If No or Unclear → “Required under Article 10(4). Datasets must reflect the actual context in which the AI system will operate.”
- **Reference:** EU AI Act Article 10(4)

Check:
Does the documentation indicate that the provider is using **special categories of personal data** (e.g., racial origin, political opinions, biometric data, etc.) for the purpose of **bias detection and correction**?

If so, does it demonstrate compliance with **all six conditions** below?

1. **Necessity:** Bias cannot be corrected using other data
2. **Security Measures:** Technical limitations on re-use, pseudonymization applied
3. **Access Controls:** Strict access restrictions and confidentiality in place
4. **No Data Sharing:** Data is not transmitted, shared, or accessed externally
5. **Deletion:** Data is deleted once bias correction is complete or retention ends
6. **Documentation:** Reasons for necessity are recorded in processing activity logs

Flag if:

- Sensitive data is used but justification is vague
- Not all safeguards are described
- Retention and access policies are unclear or missing

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Use case rationale, security architecture, compliance logs
- **Recommendation:** If No or Unclear → “Required under Article 10(5). Use of sensitive personal data for bias correction must be strictly necessary and meet all defined safeguards.”
- **Reference:** EU AI Act Article 10(5), GDPR Articles 9, 35

Trigger Condition:
This prompt applies **only** if the AI system does **not involve model training** (e.g., rule-based systems, symbolic AI).

Check:
Does the documentation describe appropriate data governance measures for the **testing dataset**, including:

- **Data origin, quality, and preparation**
- Alignment with the **intended purpose** of the system
- **Bias detection and mitigation**, if applicable
- Evidence that testing data is **representative and complete**

Flag if:

- No documentation for testing data governance is provided
- Data quality, coverage, or context relevance are unclear
- No effort is made to detect or reduce potential bias in evaluation

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Testing data protocols, evaluation design, QA documentation
- **Recommendation:** If No or Unclear → “Required under Article 10(6). Even non-trained systems must apply governance and quality controls to testing datasets.”
- **Reference:** EU AI Act Article 10(6)

Sub-Prompt: Article 11(1) – Technical Documentation for High-Risk AI Systems

Check:
Does the documentation show that a **technical file** has been prepared **before market placement or deployment**, and that it includes content aligned with **Annex IV** of the EU AI Act?

The technical file should demonstrate:

- **Compliance** with all applicable requirements from Articles 8–15
- Presentation of information in a **clear, structured format**
- Ability to support **assessment by national authorities or notified bodies**
- Regular **updates** as the system evolves

Flag if:

- No technical documentation is referenced or attached
- Structure of documentation does not align with Annex IV elements
- Documentation is outdated or lacks version control
- SMEs/startups: simplified form not used if claimed

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** System architecture, compliance mapping, risk controls, update logs
- **Recommendation:** If No or Unclear → “Required under Article 11(1). Providers must prepare up-to-date technical documentation demonstrating compliance, aligned with Annex IV.”
- **Reference:** EU AI Act Article 11(1), Annex IV

Trigger Condition:
This prompt applies **only if** the AI system is also subject to other **Union harmonization legislation**, such as:

- Medical Device Regulation (MDR)
- Machinery Directive
- General Product Safety Regulation
- Other product-specific compliance laws listed in **Annex I, Section A**

Check:
If applicable, does the documentation include a **single, integrated technical file** that:

- Covers both **AI-specific requirements** under the EU AI Act (Annex IV), and
- Requirements of the other **relevant EU regulatory framework(s)**?

Flag if:

- There are **separate files** with no clear integration
- The AI-related risks and conformity information are **not mapped or cross-referenced**
- There's no documentation to show how the combined set meets both sets of obligations

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Technical file references, compliance checklists, harmonization alignment
- **Recommendation:** If No or Unclear → “Required under Article 11(2). Where applicable, providers must maintain a single, unified technical file demonstrating compliance with both the EU AI Act and other relevant Union legislation.”
- **Reference:** EU AI Act Article 11(2), Annex I

Check:
Does the documentation confirm that the high-risk AI system includes **automatic logging capabilities** over its lifetime?

Specifically, does it enable logging of events relevant to:

- **(a)** Identifying risks under Article 79(1) or detecting substantial system modifications
- **(b)** Supporting **post-market monitoring** (Article 72)
- **(c)** Monitoring system operation per **Article 26(5)** (e.g., provider-deployer feedback loop)

Flag if:

- No mention of a **technical logging mechanism**
- Logging is **manual only** or not tied to specific regulatory requirements
- Logged events are not aligned with **risk tracking**, **usage monitoring**, or **compliance auditing**

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Logging architecture, audit trail capability, monitoring integrations
- **Recommendation:** If No or Unclear → "Required under Article 12(1)–(2). High-risk AI systems must enable automatic event logging that supports traceability, risk identification, and post-market compliance."
- **Reference:** EU AI Act Article 12(1)–(2)

Sub-Prompt: Article 12(3) – Logging for Remote Biometric Identification Systems

Trigger Condition:
Activate only if the user documentation describes a system used for **remote biometric identification** in **publicly accessible spaces** for **law enforcement or surveillance purposes**.

Check:

- **(a)** Start and end timestamps for each use session
- **(b)** The **reference database** used during operation (e.g., biometric watchlist)
- **(c)** The **input data** that led to a match (e.g., captured image or video frame)
- **(d)** Identification of the **human verifier** involved, as required under Article 14(5)

Flag if:

- These elements are **partially or entirely missing**
- Logging is enabled but does not meet the **traceability requirements**
- There is no clear link to **law enforcement procedures or human-in-the-loop review**

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Log schema, biometric system audit config, operational logs
- **Recommendation:** If No or Unclear → “Required under Article 12(3) for systems under Annex III(1)(a). Logging must include session timeframes, match data, database used, and human verifier identification.”
- **Reference:** EU AI Act Article 12(3)

Sub-Prompt: Article 13(1)–(2) – Transparency & Instructions for Use

Check:
Does the documentation demonstrate that the high-risk AI system:

- Has been designed and developed to ensure **sufficient transparency**, so that deployers can **interpret outputs and use them appropriately**

- In an **appropriate format** (digital or otherwise)
- **Concise, complete, correct, and clear**
- **Relevant, accessible, and comprehensible** to deployers

Flag if:

- Output interpretability features are missing or unclear
- No instructions are provided, or they are overly technical, incomplete, or not adapted to the deployer context
- Instructions lack usability, readability, or access considerations

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Output explanation features, attached instruction manuals, training resources
- **Recommendation:** If No or Unclear → "Required under Article 13(1)–(2). Providers must ensure output interpretability and deliver high-quality, accessible instructions for deployers."
- **Reference:** EU AI Act Article 13(1)–(2)

Sub-Prompt: Article 13(3)(a) – Provider Identification and Contact Information

Check:
Do the instructions for use explicitly include the following:

- **Name or legal identity** of the provider
- **Contact details**, such as physical address, email, or support channel
- If applicable, the same information for the provider's **authorized representative**

Flag if:

- No reliable method of contact is listed
- Authorized representative is mentioned but not detailed

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Extracted section from documentation
- **Recommendation:** If No or Unclear → “Required under Article 13(3)(a). The provider’s name and contact information must be clearly included in the instructions for use.”
- **Reference:** EU AI Act Article 13(3)(a)

Sub-Prompt: Article 13(3)(b)(i) – Intended Purpose of the High-Risk AI System

Check:
Do the instructions for use clearly state the **intended purpose** of the AI system, including:

- The **task** the system is designed to perform
- The **context** or environment in which it is intended to be deployed
- The **user group** or stakeholder(s) it is designed to support

Flag if:

- Purpose is described vaguely or inconsistently
- No clear indication of deployment context or intended function
- Multiple use cases are listed without clarification of which is primary

Output Format:

- **Status:** (Yes / No / Unclear)

- **Recommendation:** If No or Unclear → “Required under Article 13(3)(b)(i). Instructions must clearly define the system’s intended purpose, context of use, and target users.”

- **Reference:** EU AI Act Article 13(3)(b)(i)

Sub-Prompt: Article 13(3)(b)(ii) – Accuracy, Robustness, and Cybersecurity Metrics

Check:
Do the instructions for use include clear, measurable information about the system’s:

- **Accuracy** metrics (e.g. precision, recall, F1 score, error rate)

- **Robustness** against input variation, adversarial examples, or operational noise

- **Cybersecurity** posture, including tested safeguards and vulnerabilities

Also check for:

- Known or foreseeable conditions that could affect performance

- Limits of system reliability in those scenarios

Flag if:

- No performance metrics are listed or are unquantified

- No mention of robustness or cybersecurity testing

- Risks to performance under certain conditions are not disclosed

Output Format:

- **Status:** (Yes / No / Unclear)

- **Evidence:** Metrics tables, validation reports, system behavior documentation

- **Recommendation:** If No or Unclear → “Required under Article 13(3)(b)(ii). Providers must specify tested accuracy, robustness, and cybersecurity metrics, and any known limitations.”

Sub-Prompt: Article 13(3)(b)(ii) – Accuracy, Robustness, and Cybersecurity Metrics

Check:
Do the instructions for use include clear, measurable information about the system's:

- **Accuracy** metrics (e.g. precision, recall, F1 score, error rate)
- **Robustness** against input variation, adversarial examples, or operational noise
- **Cybersecurity** posture, including tested safeguards and vulnerabilities

Also check for:

- Known or foreseeable conditions that could affect performance
- Limits of system reliability in those scenarios

Flag if:

- No performance metrics are listed or are unquantified
- No mention of robustness or cybersecurity testing
- Risks to performance under certain conditions are not disclosed

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Metrics tables, validation reports, system behavior documentation
- **Recommendation:** If No or Unclear → "Required under Article 13(3)(b)(ii). Providers must specify tested accuracy, robustness, and cybersecurity metrics, and any known limitations."
- **Reference:** EU AI Act Article 13(3)(b)(ii)

Check:
Do the instructions for use include information about the system's ability to provide **output explanations**, specifically:

- Whether the system includes **technical features** or components that support **interpretability**
- What types of **explanations** are available (e.g., decision scores, feature importance, rationale summaries)
- In what form explanations are provided (e.g., visual, textual, dashboard-based)
- Any limitations of these explanations

Flag if:

- No explanation capability is described
- Output is presented as a black box with no rationale or traceability
- No indication of how deployers can interpret or question decisions

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** System UI examples, logs, LIME/SHAP/Fairlearn references, toolkits
- **Recommendation:** If No or Unclear → "Required under Article 13(3)(b)(iv). Providers must specify how the system enables deployers to interpret its outputs and any known limits of explainability."
- **Reference:** EU AI Act Article 13(3)(b)(iv)

Sub-Prompt: Article 13(3)(b)(v) – Group-Specific Performance Metrics

Check:
Do the instructions for use provide information about the system's **performance across specific groups of persons**, such as:

- Demographic groups (e.g., age, gender, ethnicity)

- Any groups **intended to be affected** by the system

Also check whether:

- Performance metrics vary across these groups
- Any **disparities, gaps, or limitations** are documented
- There is evidence of **bias mitigation** or fairness audits

Flag if:

- No group-based performance is mentioned
- Only general accuracy is provided with no disaggregation
- System is likely to affect distinct groups but this isn't addressed

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Validation results by subgroup, fairness audits, disclaimers
- **Recommendation:** If No or Unclear → "Required under Article 13(3)(b)(v). Providers must describe system performance across groups of persons it is intended to be used on, especially if disparities exist."
- **Reference:** EU AI Act Article 13(3)(b)(v)

Sub-Prompt: Article 13(3)(b)(vi) – Specifications on Data Used for Model Development

Check:
Do the instructions for use include relevant information about **training, validation, or testing data sets**, including:

- **Specifications for input data** (e.g., formats, schema, sampling characteristics)

- Data relevance for the intended purpose
- Known **limitations or gaps** in the data
- Whether the data reflects the context or group on which the system will be used

Flag if:

- No data specifications are provided
- Only general terms like “data-driven” or “trained on historical records”
- The description omits dataset composition or representativeness

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Data description section, input specs, dataset audit summary
- **Recommendation:** If No or Unclear → “Required under Article 13(3)(b)(vi). Providers must disclose specifications or relevant information about the data used to train, validate, and test the system.”
- **Reference:** EU AI Act Article 13(3)(b)(vi)

Sub-Prompt: Article 13(3)(b)(vii) – Output Interpretation Support for Deployers

Check:
Do the instructions for use include guidance or tools that help **deployers interpret the system’s output** in context?

Specifically, verify whether:

- The documentation provides **clarity on how to read and apply the system’s output**
- There are **examples, confidence scores, or thresholds** explained
- Guidance is given on how to handle **ambiguous or low-confidence results**

Flag if:

- No deployer guidance is provided for output usage
- Explanations are overly technical or insufficiently detailed
- No mention of interpretability or downstream decision-making support

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Output interpretation guide, confidence interval explanations, usage instructions
- **Recommendation:** If No or Unclear → "Required under Article 13(3)(b)(vii). Providers must equip deployers with sufficient information to properly interpret and act on the system's output."
- **Reference:** EU AI Act Article 13(3)(b)(vii)

Sub-Prompt: Article 13(3)(c) – Disclosure of Pre-Determined System Changes

Check:
Do the instructions for use describe any **predefined changes** to the AI system that have been:

- Planned by the provider at the time of **initial conformity assessment**
- Related to future updates that may impact performance, purpose, or compliance
- Considered part of the **system's expected evolution** (e.g., retraining schedules, feature rollouts)

Assess whether the documentation:

- Explicitly states what changes are pre-approved
- Clarifies whether re-certification will be required if changes exceed predefined boundaries

Flag if:

- Lack of clarity on boundaries for acceptable system updates
- Changes are occurring in practice but were not declared in initial documentation

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** System change log, versioning plan, conformity scope
- **Recommendation:** If No or Unclear → "Required under Article 13(3)(c). Any pre-determined changes to system functionality or performance must be disclosed in the documentation."
- **Reference:** EU AI Act Article 13(3)(c)

Sub-Prompt: Article 13(3)(c) – Disclosure of Pre-Determined System Changes

Check:
Do the instructions for use describe any **predefined changes** to the AI system that have been:

- Planned by the provider at the time of **initial conformity assessment**
- Related to future updates that may impact performance, purpose, or compliance
- Considered part of the **system's expected evolution** (e.g., retraining schedules, feature rollouts)

Assess whether the documentation:

- Explicitly states what changes are pre-approved
- Clarifies whether re-certification will be required if changes exceed predefined boundaries

Flag if:

- No mention of future system changes
- Lack of clarity on boundaries for acceptable system updates

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** System change log, versioning plan, conformity scope
- **Recommendation:** If No or Unclear → “Required under Article 13(3)(c). Any pre-determined changes to system functionality or performance must be disclosed in the documentation.”
- **Reference:** EU AI Act Article 13(3)(c)

Sub-Prompt: Article 13(3)(d) – Human Oversight Measures

Check:
Do the instructions for use clearly describe the **human oversight measures** established for the AI system, including:

- **Who** is responsible for oversight (roles or qualifications)
- **What tools or interfaces** are provided to enable oversight
- How oversight helps **detect, intervene, or override** incorrect or harmful outputs
- Any **technical supports** in place (e.g., flags, alerts, thresholds) to assist human review
- **References to Article 14** implementation

Flag if:

- No human-in-the-loop process is defined
- Oversight is implied but not operationalized
- System lacks mechanisms for human intervention or monitoring

Output Format:

- **Status:** (Yes / No / Unclear)

● **Recommendation:** If No or Unclear → “Required under Article 13(3)(d). Providers must describe oversight responsibilities and technical measures enabling effective human interpretation and control.”

● **Reference:** EU AI Act Article 13(3)(d)

Sub-Prompt: Article 13(3)(e) – Maintenance, Resources, and System Lifetime

Check:
Do the instructions for use specify the following operational and maintenance details:

● **Expected lifetime** of the high-risk AI system

● Required **computational and hardware resources** for operation

● Any **scheduled or conditional maintenance tasks** (e.g., frequency of updates, model retraining, performance recalibration)

● **Instructions for proper care**, including security patches, software dependencies, or expiration warnings

Flag if:

● No mention of system lifetime or maintenance needs

● Resource requirements are unclear or unspecified

● Documentation fails to guide deployers on upkeep necessary for safe and compliant use

Output Format:

● **Status:** (Yes / No / Unclear)

● **Evidence:** System lifecycle chart, update policies, hardware/software requirements

● **Recommendation:** If No or Unclear → “Required under Article 13(3)(e). Providers must define expected system lifetime and detail maintenance and resource needs to ensure sustained compliance and performance.”

● **Reference:** EU AI Act Article 13(3)(e)

Check:
Do the instructions for use describe how deployers can:

- **Access and manage logs** generated by the high-risk AI system
- **Collect, store, and interpret** those logs properly
- Ensure that logs align with the requirements of **Article 12** (e.g., traceability, incident detection, monitoring use)

Confirm whether:

- Logging functions are documented clearly
- Technical instructions or UI references are included
- Guidance includes **retention**, **format**, or **security** considerations (where relevant)

Flag if:

- Logging is mentioned but deployer access/usage is unclear
- No mention of logs despite system being high-risk
- Deployers are expected to monitor use but lack instructions to do so

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Log handling section in user guide, interface screenshots, retention policies
- **Recommendation:** If No or Unclear → “Required under Article 13(3)(f). Providers must describe how deployers should collect, store, and interpret logs to support monitoring and compliance.”
- **Reference:** EU AI Act Article 13(3)(f)

Check:
Does the AI system's design include features or interfaces that enable **natural persons to effectively oversee the system while it is in use**?

Look for:

- Clear human-machine interfaces
- Monitoring dashboards, override controls, audit tools
- Description of how the design supports real-time or periodic human intervention
- Any reference to built-in observability features

Flag if:

- No mention of human-machine interface tools
- No clarity on how a person can oversee the system during its operational phase
- Oversight mechanisms are passive or unclear

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** UI screenshots, interface design documentation, operational controls
- **Recommendation:** If No or Unclear → "Required under Article 14(1). System must be designed with explicit interface tools to enable effective human oversight throughout its use."
- **Reference:** EU AI Act Article 14(1)

Sub-Prompt: Article 14(2) – Oversight for Risk Mitigation

Check:
Does the documentation show that **human oversight is intentionally designed** to:

- Address risks that may still exist **despite compliance** with other requirements
- Function effectively under **intended use and reasonably foreseeable misuse**

Assess whether:

- Risk mitigation through oversight is explicitly discussed
- Risk scenarios are tied to specific oversight mechanisms
- The system anticipates and documents limits of technical safeguards

Flag if:

- Oversight is discussed only in generic terms
- No explicit link between oversight and residual risk mitigation
- Misuse scenarios are unacknowledged

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Risk mitigation section, human-in-the-loop design rationale
- **Recommendation:** If No or Unclear → “Required under Article 14(2). Human oversight must be demonstrably aimed at mitigating risks that persist even after applying technical safeguards.”
- **Reference:** EU AI Act Article 14(2)

Sub-Prompt: Article 14(3) – Allocation of Oversight Responsibilities

Check:
Does the documentation specify whether **human oversight is ensured through**:

- (a) Measures **built into the system** by the provider (e.g., default monitoring tools, stop functionality, auto alerts),

- or **both**?

Ensure that:

- The party responsible for oversight is **explicitly identified**
- The measures are **commensurate** with the system's level of autonomy, context, and risk profile

Flag if:

- No clarity on who ensures oversight
- Measures are mentioned but not attributed to provider or deployer
- The system context suggests risk, but no proportionate oversight mechanism is defined

Output Format:

- **Status:** (Provider / Deployer / Both / Unclear)
- **Evidence:** Design documentation, SOPs, integration guides
- **Recommendation:** If Unclear → "Required under Article 14(3). Provider must define whether oversight is embedded in the system, expected from deployer, or both, and justify the allocation based on system risk and context."
- **Reference:** EU AI Act Article 14(3)

Sub-Prompt: Article 14(4)(a) – Understanding and Monitoring Capabilities

Check:
Does the documentation support natural persons assigned to oversight in:

- **Understanding the system's capacities and limitations**
- Monitoring operation for **anomalies, dysfunctions, or unexpected performance**

- Documentation or training materials about known system behaviors and limits
- Diagnostic tools, alerts, or dashboards that facilitate ongoing monitoring
- Instructions on how to detect deviations from expected behavior

Flag if:

- No reference to training or documentation that explains system behavior
- Monitoring functions are missing or unclear
- Oversight personnel are expected to intervene without meaningful system insight

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Monitoring instructions, training resources, failure mode guides
- **Recommendation:** If No or Unclear → "Required under Article 14(4)(a). Oversight personnel must be supported with documentation and tools that enable effective understanding and monitoring of the AI system's operation."
- **Reference:** EU AI Act Article 14(4)(a)

Sub-Prompt: Article 14(4)(b) – Awareness of Automation Bias

Check:
Does the system or its accompanying documentation help oversight personnel remain aware of the risk of **automation bias**, i.e., the tendency to:

- Automatically rely on or over-rely on AI system output
- Accept AI suggestions without critical evaluation

Evaluate whether:

- Training or instructions include **scenarios where AI output may be misleading**

- There are built-in mechanisms (e.g. confidence scores, explainability cues, manual override reminders) to **encourage critical review**

Flag if:

- No mention of automation bias or risks of blind reliance

- System is treated as authoritative with no instruction to challenge outputs

- Interface design encourages passive acceptance

Output Format:

- **Status:** (Yes / No / Unclear)

- **Evidence:** Warning labels, user training guides, interface cues

- **Recommendation:** If No or Unclear → "Required under Article 14(4)(b). Oversight guidance must address the risk of automation bias and promote active, critical review of system outputs."

- **Reference:** EU AI Act Article 14(4)(b)

Sub-Prompt: Article 14(4)(c) – Ability to Interpret System Output

Check:
Does the system provide tools or guidance that enable oversight personnel to **correctly interpret the output**?

Specifically, check for:

- Instructions or explanations accompanying outputs (e.g., visualizations, scoring methods, logic flows)

- Use of **interpretability methods** (e.g., LIME, SHAP, saliency maps) if the model is complex

- Clear labeling of outputs, especially in high-stakes decisions (e.g., risk scores, classifications)

Flag if:

- Outputs are provided without explanation or structure
- Oversight personnel receive results without tools to interpret or contextualize them
- No mention of how to assess confidence, limitations, or variability in output

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Output guides, explainability tools, documented interpretation procedures
- **Recommendation:** If No or Unclear → "Required under Article 14(4)(c). Oversight personnel must be equipped with tools or instructions to interpret AI outputs appropriately."
- **Reference:** EU AI Act Article 14(4)(c)

Sub-Prompt: Article 14(4)(d) – Authority to Override or Disregard Outputs

Check:
Does the system allow human overseers to:

- Make an explicit decision to **disregard** or **override** the system's output in specific situations
- Exercise judgment and **opt out** of relying on AI recommendations
- Follow a documented process or UI option for overriding AI results

Verify whether:

- The documentation clearly states that humans may **choose not to use** the system in a given situation
- The system allows **manual decision-making**, even if the AI has provided an outcome
- Oversight roles are empowered to reverse or skip AI suggestions

- No explicit mention of human authority to override
- System design does not allow output to be bypassed
- Human decision-making is undermined or made impractical

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Override protocol, user interface options, documented authority boundaries
- **Recommendation:** If No or Unclear → "Required under Article 14(4)(d). Human oversight must include the ability to disregard or override AI outputs in specific scenarios."
- **Reference:** EU AI Act Article 14(4)(d)

Sub-Prompt: Article 14(4)(e) – Ability to Safely Interrupt the System

Check:
Does the system include a mechanism that enables human overseers to **intervene or halt its operation** safely?

Look for:

- A clearly defined **'stop' function** or interrupt control
- Procedures to bring the system into a **safe state** upon shutdown
- Documentation describing when and how to activate the halt mechanism
- Role-based access or controls to ensure **authorized intervention**

Flag if:

- No mention of interrupt or shutdown functionality
- Intervention process is ambiguous or unsafe

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** UI controls, shutdown protocols, safety design features
- **Recommendation:** If No or Unclear → “Required under Article 14(4)(e). High-risk AI systems must allow human overseers to interrupt operation and bring the system to a safe state.”
- **Reference:** EU AI Act Article 14(4)(e)

Sub-Prompt: Article 14(5) – Dual Human Verification for Biometric Identification

Check:
If the AI system is used for biometric identification as specified in **Annex III, point 1(a)**, does the system documentation show that:

- Any **identification result** from the AI is subject to **independent verification by at least two qualified humans**
- These individuals have **the necessary competence, training, and authority** to validate the result
- This process is **not bypassed**, unless the use case falls under the stated exception for law enforcement, migration, border control, or asylum under applicable law

Ensure that:

- The verification step is explicitly described and assigned
- Verification logs or audit records are mentioned
- Exceptions are documented with legal basis, if claimed

Flag if:

- No verification protocol is described
- Fewer than two humans are involved in result confirmation (and no legal exception applies)

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Verification SOPs, role descriptions, exception claims
- **Recommendation:** If No or Unclear → "Required under Article 14(5). Biometric identification results must be verified by at least two qualified individuals unless a legally justified exception applies."
- **Reference:** EU AI Act Article 14(5)

Sub-Prompt: Article 15(1) – Accuracy Aligned with Intended Use

Check:
Does the AI system documentation show that the model is **designed and tested** to achieve an **appropriate level of accuracy** given:

- The system's **intended use**
- The **context in which it operates**
- Any **risk associated with inaccuracy**

Look for:

- Description of model accuracy in relation to use case goals
- Design or training decisions intended to optimize for accuracy
- Discussion of tolerances, thresholds, or performance ranges

Flag if:

- No clear mapping between accuracy and purpose
- Claims about accuracy are generic or unsupported

Output Format:

- **Status:** (Yes / No / Unclear)
- **Evidence:** Accuracy claims in use case summary, model documentation, validation results
- **Recommendation:** If No or Unclear → "Required under Article 15(1). Accuracy must be defined and justified relative to the AI system's intended purpose and documented risk profile."
- **Reference:** EU AI Act Article 15(1)

Sub-Prompt: Article 15(3) – Declared Accuracy Metrics in Instructions for Use

Check:
Do the **instructions for use** provided with the AI system include:

- **Specific accuracy metrics** (e.g., precision, recall, F1 score, MAE, AUC)
- Expected performance levels **under normal and foreseeable conditions**
- Any **limitations or variability** based on input characteristics, data quality, or deployment context

Ensure that:

- Metrics are clearly defined, not just broad terms like "high accuracy"
- Metrics are **relevant to the AI system's function** (e.g., diagnostic, classification, forecasting)
- The source of these metrics (e.g., test results) is documented

Flag if:

- No metrics are included in the user instructions
- Metrics are present but not tied to intended use
- Accuracy claims lack context or empirical support

- **Status:** (Yes / No / Unclear)
- **Evidence:** Accuracy section of user guide, validation test summaries
- **Recommendation:** If No or Unclear → “Required under Article 15(3). Providers must declare relevant accuracy metrics in the system’s instructions for use.”
- **Reference:** EU AI Act Article 15(3)

Sub-Prompt: Article 15(4) – Robustness Against Errors and Fault Conditions

Check:
Does the documentation show that the AI system is **designed to remain robust** under conditions such as:

- **Internal faults**, system bugs, or hardware failures
- **External inconsistencies**, including unpredictable inputs or user behavior
- Interaction with **natural persons or other systems** that may impact performance

Look for:

- Mention of **redundancy mechanisms**, fail-safe design, fallback procedures
- Testing protocols for **unexpected operating conditions**
- Specific mitigation for known fragilities in similar systems

Flag if:

- No reference to how the system behaves under fault or stress
- Fail-safe or error-handling mechanisms are absent or weakly defined
- No robustness testing documented

Output Format:

- **Evidence:** Architecture diagrams, robustness testing results, mitigation plans

- **Recommendation:** If No or Unclear → “Required under Article 15(4). System design must account for internal and environmental errors and remain resilient throughout deployment.”

- **Reference:** EU AI Act Article 15(4)

Sub-Prompt: Article 15(4) – Feedback Loop Control for Post-Deployment Learning

Check:
If the AI system continues to learn **after deployment**, does the documentation describe:

- Risks of **biased outputs reinforcing future inputs** (feedback loops)

- Mechanisms in place to **detect, limit, or reset** learned behaviors that degrade system integrity

- Any **human review steps** involved in monitoring post-deployment learning outcomes

Look for:

- Explicit mention of **post-deployment adaptation or continuous learning**

- Monitoring tools or alert systems tied to output drift or anomalous behavior

- Training hygiene protocols (e.g. exclusion of self-generated data)

Flag if:

- System learns from its own outputs without safeguards

- Feedback loops are possible but unacknowledged

- No plans to prevent cumulative bias or performance erosion

Output Format:

- **Status:** (Yes / No / Unclear)

- **Recommendation:** If No or Unclear → “Required under Article 15(4). Post-deployment learning must be monitored to prevent biased feedback loops and ensure stability over time.”

- **Reference:** EU AI Act Article 15(4)

Sub-Prompt: Article 15(4) – Feedback Loop Control for Post-Deployment Learning

Check:
If the AI system continues to learn **after deployment**, does the documentation describe:

- Risks of **biased outputs reinforcing future inputs** (feedback loops)

- Mechanisms in place to **detect, limit, or reset** learned behaviors that degrade system integrity

- Any **human review steps** involved in monitoring post-deployment learning outcomes

Look for:

- Explicit mention of **post-deployment adaptation or continuous learning**

- Monitoring tools or alert systems tied to output drift or anomalous behavior

- Training hygiene protocols (e.g. exclusion of self-generated data)

Flag if:

- System learns from its own outputs without safeguards

- Feedback loops are possible but unacknowledged

- No plans to prevent cumulative bias or performance erosion

Output Format:

- **Status:** (Yes / No / Unclear)

- **Evidence:** Lifecycle documentation, retraining policy, human-in-the-loop steps

- **Reference:** EU AI Act Article 15(4)

Sub-Prompt: Article 16(a) – Compliance with Section 2 Requirements (Articles 8–15)

Check:
Review the user's documentation and determine whether the provider demonstrates that the **AI system meets all applicable requirements under Articles 8 through 15**, which include:

- Article 8 – General compliance and harmonization
- Article 9 – Risk management system
- Article 10 – Data and data governance
- Article 11 – Technical documentation
- Article 12 – Record-keeping and logging
- Article 13 – Transparency and instructions for use
- Article 14 – Human oversight
- Article 15 – Accuracy, robustness, and cybersecurity

Focus on whether there is:

- Explicit alignment to each requirement
- Traceable documentation or evidence per requirement
- Any gaps, omissions, or vague claims of compliance without supporting artifacts

Flag if:

- Requirements are mentioned without supporting documentation

- Documentation fails to address core EU AI Act requirements for high-risk systems

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear – Needs Review)

- **Evidence:** Summarize supporting references or absence thereof (e.g., “risk management process described in page 5, but no human oversight measures found”)

- **Recommendation:** If Not Compliant or Unclear → “Provider must demonstrate compliance across all Articles 8–15 with referenced documentation per EU AI Act Article 16(a).”

- **Reference:** EU AI Act Article 16(a)

Sub-Prompt: Article 16(b) – Provider Identification and Contact Information

Check:
Review the documentation for evidence that the provider has included:

- **Name** (legal entity)

- **Registered trade name** or **trademark**

- **Contact address**

- Placement of this information on:

    - the AI system, or

    - the packaging, or

    - accompanying documentation

This is required even if the AI system is not a physical product — digital equivalents (e.g., metadata, file headers, PDF cover pages) are acceptable.

Flag if:

- Information is incomplete (e.g., name present but no contact details)
- Contact info is present but not tied to the provider entity

Output Format:

- **Status:** (Present / Missing / Incomplete)
- **Evidence:** Copy of provider identity block or statement of absence
- **Recommendation:** If Missing or Incomplete → "Provider must declare their name, trade name/trademark, and contact address in system documentation per Article 16(b)."
- **Reference:** EU AI Act Article 16(b)

Sub-Prompt: Article 16(c) – Quality Management System (QMS)

Check:
Determine whether the documentation provides evidence that the provider has implemented a **Quality Management System (QMS)** aligned with Article 17, including:

- **Procedures** to ensure compliance with EU AI Act requirements
- **Governance structure** for quality control
- Inclusion of **design, testing, risk management, traceability, data governance, monitoring, and incident response** processes
- Internal audits, roles, and responsibilities tied to AI governance

This sub-prompt should also verify that the QMS is **documented**, **up-to-date**, and **applies to the specific high-risk AI system** being evaluated.

Flag if:

- No QMS is mentioned
- A generic QMS is referenced without mapping to AI-specific obligations

Output Format:

- **Status:** (Present / Missing / Incomplete)
- **Evidence:** Section in QMS, document title, page number, or lack thereof
- **Recommendation:** If Missing or Incomplete → “Per Article 16(c) and Article 17, providers must maintain a quality management system that documents governance, design, testing, and risk processes for the high-risk AI system.”
- **Reference:** EU AI Act Articles 16(c) and 17

Sub-Prompt: Article 16(d) – Retention of Technical Documentation (per Article 18)

Check:
Review whether the provider has:

- Prepared **technical documentation** as required under Article 11
- Retained the documentation for **10 years** after the AI system has been placed on the market or put into service
- Included evidence that this documentation is **available upon request** by competent authorities

Documentation should cover:

- System architecture and design
- Compliance with requirements (Articles 8–15)
- Testing protocols and results
- Risk management procedures
- Instructions for use

Flag if:

- Documentation is partial or missing critical components
- No indication of ability to retrieve and provide the documentation when requested

Output Format:

- **Status:** (Present / Missing / Unclear)
- **Evidence:** Reference to version-controlled documentation, retention policy, or file repository
- **Recommendation:** If Missing or Unclear → “Provider must retain full technical documentation for at least 10 years and ensure it is accessible for compliance verification, per Articles 16(d) and 18.”
- **Reference:** EU AI Act Articles 16(d) and 18

Sub-Prompt: Article 16(d) – Retention of Technical Documentation (per Article 18)

Check:
Review whether the provider has:

- Prepared **technical documentation** as required under Article 11
- Retained the documentation for **10 years** after the AI system has been placed on the market or put into service
- Included evidence that this documentation is **available upon request** by competent authorities

Documentation should cover:

- System architecture and design
- Compliance with requirements (Articles 8–15)
- Testing protocols and results
- Risk management procedures
- Instructions for use

- No retention period is mentioned
- Documentation is partial or missing critical components
- No indication of ability to retrieve and provide the documentation when requested

Output Format:

- **Status:** (Present / Missing / Unclear)
- **Evidence:** Reference to version-controlled documentation, retention policy, or file repository
- **Recommendation:** If Missing or Unclear → “Provider must retain full technical documentation for at least 10 years and ensure it is accessible for compliance verification, per Articles 16(d) and 18.”
- **Reference:** EU AI Act Articles 16(d) and 18

Sub-Prompt: Article 16(f) – Conformity Assessment Prior to Market Launch (per Article 43)

Check:
Determine whether the provider has documented evidence that the **high-risk AI system has undergone the appropriate conformity assessment procedure** under Article 43, including:

- Selection of the applicable assessment route (e.g. internal control, third-party audit)
- Supporting records of the conformity assessment activities (e.g. checklists, validation protocols, test results)
- Assessment was completed **before** the system was placed on the market or put into service
- If applicable: involvement of a **notified body** and issuance of a certificate of conformity

Flag if:

- No conformity assessment is mentioned
- No indication that the assessment was completed **prior to deployment**

Output Format:

- **Status:** (Completed / Not Completed / Unclear)
- **Evidence:** Type of conformity procedure used, references to Article 43 compliance documentation
- **Recommendation:** If Not Completed or Unclear → "A conformity assessment must be completed and documented before placing the system on the market or into service, as required under Articles 16(f) and 43."
- **Reference:** EU AI Act Articles 16(f) and 43

Sub-Prompt: Article 16(g) – EU Declaration of Conformity (per Article 47)

Check:
Verify that the provider has drawn up a formal **EU Declaration of Conformity** for the high-risk AI system, which:

- States compliance with **all applicable EU AI Act requirements**
- References the system's identification and intended purpose
- Includes the name and signature of the responsible person
- Is dated and matches the version of the system placed on the market
- Aligns with the format and content required under **Article 47 and Annex V**

This document must be prepared and available **before** the system is marketed or put into service.

Flag if:

- Declaration is missing, outdated, unsigned, or incomplete
- Declaration only refers to partial compliance
- Document is referenced but not included or accessible

- **Status:** (Present / Missing / Incomplete)

- **Evidence:** Document name, date, signatory, or note of absence

- **Recommendation:** If Missing or Incomplete → “Provider must draw up and sign a Declaration of Conformity stating full compliance with EU AI Act, as required by Articles 16(g) and 47.”

- **Reference:** EU AI Act Articles 16(g) and 47

Sub-Prompt: Article 16(h) – CE Marking (per Article 48)

Check:
Review whether the provider has affixed the **CE marking** to indicate conformity with the EU AI Act. Confirm that:

- The CE mark is present on the **AI system**, or if not feasible, on its **packaging** or **accompanying documentation**

- The CE marking complies with the **design and visibility requirements** outlined in Article 48

- The placement of the mark is **documented and traceable** to the specific system being evaluated

Digital products may display the CE mark in:

- Splash screens

- About/Info sections

- PDF reports or downloadable components

Flag if:

- CE marking is absent or only mentioned without visual evidence

- CE marking is used but doesn’t correspond to a completed conformity process

- CE is used prematurely or inappropriately

- **Status:** (Marked / Not Marked / Incomplete)

- **Evidence:** Screenshot, file reference, or notation confirming location or absence of CE mark

- **Recommendation:** If Not Marked or Incomplete → “System must carry the CE mark once conformity assessment is complete, as mandated in Articles 16(h) and 48. Improper use may indicate regulatory violation.”

- **Reference:** EU AI Act Articles 16(h) and 48

Sub-Prompt: Article 16(i) – Registration in the EU Database (per Article 49(1))

Check:
Determine whether the provider has complied with the **registration obligation** by submitting required information about the high-risk AI system to the **EU database referred to in Article 71**. Specifically verify:

- The system has been registered **prior to being placed on the market or put into service**

- Registration includes all required data fields:

    - Provider identity

    - System purpose

    - Conformity assessment route

    - Risk category and use case

- A **registration reference or identifier** is included in the documentation

Flag if:

- There is no indication of registration or database entry

- System is marked as “under review,” “pending,” or “planned” but already deployed

- Information is referenced vaguely without supporting documentation

- **Status:** (Registered / Not Registered / Unclear)

- **Evidence:** Registration ID, system entry record, or lack thereof

- **Recommendation:** If Not Registered → “Provider must register the high-risk AI system in the EU database prior to deployment, per Articles 16(i) and 49(1). Non-compliance may prevent lawful market entry.”

- **Reference:** EU AI Act Articles 16(i) and 49(1)

Sub-Prompt: Article 16(j) – Corrective Actions and Notifications (per Article 20)

Check:
Review whether the provider has documented procedures for:

- **Identifying non-compliance** with any EU AI Act requirements (e.g., from monitoring, audits, or reports)

- **Taking corrective actions** such as halting distribution, modifying the system, or issuing updates

- **Notifying** relevant market surveillance authorities, as well as importers/distributors, in a timely manner when:

    - A high-risk AI system presents a risk (per Article 79(1))

    - A system is withdrawn or recalled

- Tracking **corrective action status and resolution**

Flag if:

- No procedures are described for managing non-compliance

- There is no mention of notification responsibilities or regulatory engagement

- Corrective actions are implied but not linked to Article 20 obligations

Output Format:

- **Evidence:** Incident response policies, recall workflows, notification protocols, or absence thereof

- **Recommendation:** If Not Compliant → “Provider must implement documented processes to act upon system non-compliance and notify authorities, per Articles 16(j) and 20.”

- **Reference:** EU AI Act Articles 16(j) and 20

Sub-Prompt: Article 16(k) – Ability to Demonstrate Conformity Upon Request

Check:
Determine whether the provider has processes and documentation in place to **demonstrate the conformity** of the high-risk AI system **upon a reasoned request** from a national competent authority. Specifically:

- Can the provider present **evidence of compliance** with the requirements in **Section 2** (Articles 8–15)?

- Is there a documented process for retrieving and presenting:

    - Technical documentation (Article 11)

    - Test and validation reports

    - Risk management records

    - Instructions for use

- Has the provider **designated personnel** responsible for regulatory interactions?

Flag if:

- No procedure exists to respond to regulatory requests

- System documentation is dispersed or not versioned

- No individual or team is assigned responsibility for compliance disclosures

Output Format:

- **Evidence:** Existence of a compliance file, designated contact, or ability to respond to regulatory requests

- **Recommendation:** If Not Demonstrable → “Provider must be able to demonstrate compliance with Section 2 upon request from authorities. Ensure a centralized, version-controlled repository is maintained.”

- **Reference:** EU AI Act Article 16(k)

Sub-Prompt: Article 16(l) – Accessibility Compliance (Directives 2016/2102 and 2019/882)

Check:
Assess whether the provider has ensured that the high-risk AI system complies with **accessibility requirements** under:

- **Directive (EU) 2016/2102** — Accessibility of public sector websites and mobile applications

- **Directive (EU) 2019/882** — European Accessibility Act (applicable to products and services offered to consumers)

Focus on whether the system's interface, outputs, and documentation are:

- **Perceivable, operable, understandable, and robust** for users with disabilities

- Available in accessible formats (e.g., screen reader compatible text, alternative formats, keyboard navigation)

- Accompanied by instructions for use that are compliant with accessibility standards

Flag if:

- Accessibility is not mentioned or is deferred to third parties

- User interface or documentation is not designed to accommodate individuals with disabilities

- System is intended for public use or consumer services but lacks accessibility evidence

Output Format:

- **Evidence:** WCAG references, accessible formats, inclusive design practices

- **Recommendation:** If Not Compliant → "Provider must ensure the system meets applicable EU accessibility requirements as outlined in Directives 2016/2102 and 2019/882."

- **Reference:** EU AI Act Article 16(l); Directives 2016/2102 and 2019/882

Sub-Prompt: Article 17.1(a) – Compliance Strategy and Procedures

Check:
Review the user-provided documentation to determine whether the provider has described a formal strategy or set of procedures to ensure regulatory compliance, including:

- **A documented plan to comply with the EU AI Act**

- **Steps for conducting or supporting conformity assessments** (Article 43)

- **Processes for managing substantial modifications** to the AI system

- **Any mention of post-market monitoring or regulatory maintenance**

Flag if:

- No compliance strategy or mention of conformity processes is documented

- Documentation is silent on modification controls or regulatory upkeep

- There is no reference to risk or audit readiness practices tied to the EU AI Act

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Extracted summary of relevant compliance or GRC procedures

change control, and post-market obligations."

- **Reference:** EU AI Act Article 17(1)(a)

Sub-Prompt: Article 17.1(b) – Design, Development, and Validation Procedures

Check:
Review the user-provided documentation to assess whether it includes clear procedures for:

- The **design process** of the AI system (e.g. design inputs, objectives, constraints)
- **Development steps**, tools, or workflows used to build and test the system
- **Validation procedures** that ensure the system performs according to its intended purpose
- How design decisions are justified and whether iterative validation is documented

Flag if:

- The AI system documentation lacks structure or traceability in design or development steps
- There are no references to internal validations or performance verification methods
- No distinction between development and deployment/testing phases

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Design documents, model architecture descriptions, validation reports
- **Recommendation:** If Not Compliant → "Provider should implement and document a structured design-development-validation workflow aligned with Article 17(1)(b), ensuring the system is validated for its intended use."

Sub-Prompt: Article 17.1(c) – Development QA/QC Procedures

Check:
Examine user-provided documentation to determine whether the provider has described procedures for:

- **Quality assurance (QA)** activities during AI system development
- **Quality control (QC)** methods to verify that system components meet requirements before deployment
- Processes that support defect detection, issue tracking, and adherence to internal development standards
- Evidence of peer review, code audits, or documented test passes during development

Flag if:

- There is no evidence of structured QA/QC practices during model development
- Testing appears ad hoc with no described controls or standards
- No record of defect prevention, review checkpoints, or formal acceptance criteria

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** QA frameworks, development review checklists, tracked issues or test logs
- **Recommendation:** If Not Compliant → “Provider should implement and document structured quality assurance and control procedures during development in alignment with Article 17(1)(c). This ensures reproducibility, traceability, and alignment with regulatory expectations.”
- **Reference:** EU AI Act Article 17(1)(c)

Check:
Review the user documentation to determine whether it includes:

- Clear descriptions of **testing procedures** conducted before, during, or after development
- Information on **how frequently** these tests are run and under what conditions
- Reference to validation against intended purpose and performance requirements
- Coverage of both **functional** and **non-functional** testing (e.g., fairness, robustness, security)

Flag if:

- Testing is mentioned without detail or tied to specific stages
- Frequency of testing is undefined or not aligned with lifecycle checkpoints
- No indication of metrics or criteria used to evaluate test outcomes

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Testing reports, validation logs, test plans, evaluation dashboards
- **Recommendation:** If Not Compliant → "Provider should document testing procedures across the AI lifecycle and define frequency and evaluation criteria in accordance with Article 17(1)(d)."
- **Reference:** EU AI Act Article 17(1)(d)

Sub-Prompt: Article 17.1(e) – Technical Standards and Alternatives

Check:
Review the user documentation to determine whether the provider has:

- Identified any **technical standards** (e.g. ISO/IEC, IEEE, CEN/CENELEC) used to guide the design, development, or evaluation of the AI system

- If **no standards were used**, explained the **alternative methods or controls** used to demonstrate compliance with EU AI Act Section 2 requirements

Flag if:

- No mention of technical standards or equivalent alternatives
- Documentation lists standards without explaining how they were applied
- No alignment between standards and system testing, validation, or assurance

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** List of standards used, justification for alternative controls, alignment references
- **Recommendation:** If Not Compliant → "Provider should identify applicable technical standards or explicitly justify the alternative methods used to demonstrate compliance, as required under Article 17(1)(e)."
- **Reference:** EU AI Act Article 17(1)(e)

Sub-Prompt: Article 17.1(f) – Data Governance Procedures Before Release

Check:
Review the user-provided documentation to determine whether it describes procedures followed **before release** to ensure:

- Data used in training, validation, and testing complies with governance practices outlined in **Article 10**
- Any **bias detection, mitigation, or quality control measures** were completed
- There is documentation of **data preparation workflows** (e.g., annotation, cleaning, validation)
- Procedures for verifying data representativeness and relevance to intended use

- No mention of pre-release data review or controls
- No link to prior assessments under Article 10 (data quality, bias, coverage)
- No indication that datasets were validated prior to system deployment

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Data preparation logs, governance workflows, sign-off documents
- **Recommendation:** If Not Compliant → "Provider should implement and document pre-release data governance procedures to ensure the system meets the requirements under Articles 10 and 17(1)(f), including checks for quality, relevance, and fairness."
- **Reference:** EU AI Act Article 17(1)(f)

Sub-Prompt: Article 18.1(a) – Retention of Technical Documentation

Check:
Review the user documentation to confirm whether the provider has committed to retaining the technical documentation described in **Article 11** for a minimum of **10 years** after the high-risk AI system is placed on the market or put into service. Look for:

- A statement of retention period
- Procedures or policies that describe **how and where** technical documentation will be stored
- Evidence that the documentation is complete and aligns with Article 11 requirements

Flag if:

- No mention of long-term retention
- Retention period is shorter than 10 years
- No reference to documentation storage or maintenance policy

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Document control policies, retention schedules, reference to technical file repository

- **Recommendation:** If Not Compliant → “Provider should commit to retaining the full technical documentation as specified in Article 11 for at least 10 years post-deployment, in line with Article 18.1(a).”

- **Reference:** EU AI Act Article 18.1(a)

Sub-Prompt: Article 18.1(b) – Retention of QMS Documentation

Check:
Examine the user-provided documentation to determine whether the provider has stated or demonstrated that:

- The **Quality Management System (QMS)** documentation, as required under Article 17, will be retained for **at least 10 years** after the AI system is placed on the market or put into service

- The QMS documentation includes version control, internal audits, procedural manuals, and change logs

- Storage processes ensure accessibility by national competent authorities if requested during this retention period

Flag if:

- No reference to QMS document retention

- Retention is less than 10 years

- QMS documentation is referenced but not described or organized for review

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Quality manual, retention policies, document register or audit logs

- **Recommendation:** If Not Compliant → “Provider should document a plan to retain Quality Management System records for at least 10 years, per Article 18.1(b), ensuring they are accessible to

- **Reference:** EU AI Act Article 18.1(b)

Sub-Prompt: Article 18.1(c) – Documentation of Notified Body–Approved Changes

Check:
Review the user's AI system documentation to verify whether the provider has retained or committed to retaining, for a minimum of **10 years**, any documentation related to **changes that were reviewed or approved by a notified body**. Look for:

- Change logs or version histories specifically marked as **notified body–reviewed**
- Official approval records, change control forms, or correspondence from the notified body
- Internal procedures for recording and storing such regulatory changes

Flag if:

- AI system is subject to notified body oversight but no such records are mentioned
- Change documentation exists but lacks confirmation of notified body approval
- No indication of long-term retention policy

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Approval logs, version control documents, notified body correspondence
- **Recommendation:** If Not Compliant → "Provider should ensure that all documentation related to notified body–approved changes is retained and organized for at least 10 years post-deployment, as required by Article 18.1(c)."
- **Reference:** EU AI Act Article 18.1(c)

Sub-Prompt: Article 18.1(d) – Retention of Notified Body Decisions and Documents

Check:
Assess whether the provider has committed to retaining, for **at least 10 years**, any **decisions, certifications,**

- References to third-party conformity assessment outcomes
- Copies of **certificates, conformity decisions, or audit reports** issued by a notified body
- A documented process for **filing and maintaining** these materials

Flag if:

- The AI system underwent third-party conformity assessment but records are missing
- No mention of retention period or storage responsibility
- Materials referenced but not stored or made accessible

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Notified body reports, audit files, regulatory folders
- **Recommendation:** If Not Compliant → "Provider should ensure that all decisions and documents issued by notified bodies are securely stored and accessible for at least 10 years, in line with Article 18.1(d)."
- **Reference:** EU AI Act Article 18.1(d)

Sub-Prompt: Article 18.1(e) – EU Declaration of Conformity Retention

Check:
Examine the user's documentation to determine whether the **EU Declaration of Conformity**, prepared in accordance with **Article 47**, has been:

- Properly issued and signed
- Retained for at least **10 years** after the AI system is placed on the market or put into service
- Stored in a way that ensures accessibility to **national competent authorities** upon request

Flag if:

- No declaration found
- Declaration exists but lacks a retention policy
- The declaration is incomplete or not aligned with Article 47 requirements

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** EU Declaration of Conformity file, location within compliance documentation
- **Recommendation:** If Not Compliant → "Provider should ensure that a complete EU Declaration of Conformity is issued and retained for at least 10 years, per Article 18.1(e), and made available to competent authorities when requested."
- **Reference:** EU AI Act Article 18.1(e)

Sub-Prompt: Article 19(1) – Retention of Automatically Generated Logs

Check:
Review the user documentation to determine whether the provider:

- Acknowledges that the AI system **automatically generates logs**
- Retains these logs for **at least 6 months**, or longer if required by the system's **intended purpose**
- Has implemented a **log management process** that addresses access, format, and traceability
- Accounts for **Union or national data protection laws** (e.g., GDPR) that may impact retention period or scope

Focus only on logs **under the provider's control**, not deployer-managed environments.

Flag if:

- Retention period is undefined or <6 months
- Log practices don't match the intended purpose or compliance requirements

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Logging policy, retention period in documentation, references to GDPR compliance
- **Recommendation:** If Not Compliant → "Provider should retain system-generated logs for at least 6 months, aligned with the system's intended purpose, unless otherwise specified by data protection laws. Logging practices must ensure accessibility for traceability and compliance checks."
- **Reference:** EU AI Act Article 19(1)

Sub-Prompt: Article 19(2) – Financial Institution Log Retention

Check:
If the provider is a **financial institution**, determine whether the documentation shows that:

- Automatically generated logs from the high-risk AI system are being **retained**
- Logs are maintained **as part of internal governance or risk documentation**, required under **EU financial services law** (e.g., MiFID II, Solvency II, PSD2)
- Retention and access procedures are integrated into the organization's broader **compliance framework**

Flag if:

- The provider is a financial institution but has no mention of logs or governance documentation
- Log retention is separated from existing regulatory documentation, with no mapping to financial compliance requirements
- No clear indication of alignment with financial services law

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Governance or audit policies, integration of AI system logs into financial regulatory documentation

- **Recommendation:** If Not Compliant → “Provider should ensure that all logs generated by high-risk AI systems are maintained as part of its regulatory documentation under applicable financial services law, in accordance with Article 19(2).”

- **Reference:** EU AI Act Article 19(2)

Sub-Prompt: Article 20(1) – Corrective Action Process for Non-Conforming High-Risk AI Systems

Check:
Review the documentation to determine whether the provider has clearly documented procedures for handling **non-conforming high-risk AI systems**, specifically:

- A mechanism to detect or be alerted to non-conformities with the EU AI Act

- A process to take one or more of the following actions:

    - Bring the system into compliance

    - Withdraw the system

    - Disable the system

    - Recall the system

- A communication plan to **inform relevant parties** (e.g., distributors, deployers, authorized representatives, importers) when such actions are initiated

Flag if:

- No corrective action process is mentioned

- The process does not specify possible outcomes (withdrawal, disablement, etc.)

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Extract from compliance or operational risk documents referencing non-conformance response
- **Recommendation:** If Not Compliant → "Provider should document and implement a formal corrective action process for non-conforming high-risk AI systems, including the potential for withdrawal, disablement, or recall, and notify all relevant parties as required by Article 20(1)."
- **Reference:** EU AI Act Article 20(1)

Sub-Prompt: Article 20(2) – Notification and Investigation of Risk

Check:
Review the documentation to confirm whether the provider has a defined process in place to:

- **Identify and assess** if the AI system presents a risk within the meaning of **Article 79(1)** (i.e., a risk to health, safety, or fundamental rights)
- **Investigate the cause** of the risk, ideally in collaboration with the **reporting deployer**
- **Inform** the following parties without delay:
  - **Market surveillance authorities** responsible for the system
  - **Notified bodies** that issued conformity certificates (if applicable)

Flag if:

- No risk response protocol is described
- No process for collaborating with deployers on investigations
- No procedure to inform external authorities

Output Format:

- **Evidence:** Risk response procedures, deployment of Article 79 risk definitions, escalation protocols

- **Recommendation:** If Not Compliant → "Provider must establish a formal process for risk notification under Article 20(2), including investigation of the root cause in collaboration with deployers and timely communication with market surveillance authorities and notified bodies."

- **Reference:** EU AI Act Article 20(2)

Sub-Prompt: Article 21(1) – Documentation Submission to Competent Authorities

Check:
Review the user's documentation to confirm whether the provider has a defined process for responding to **reasoned requests from competent authorities** that includes:

- A commitment to provide all required technical and compliance documentation demonstrating conformity with **Section 2** of the EU AI Act

- Confirmation that such documentation can be provided in one of the **official EU languages** as requested by the Member State's competent authority

- Internal designation of responsibility for handling such requests (e.g. legal, compliance, risk team)

Flag if:

- No documented process exists

- No mention of language availability or translation

- No role or department is designated for external authority engagement

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Relevant section in compliance manual, legal SOPs, or risk policy

- **Recommendation:** If Not Compliant → "Provider must establish a documented protocol to respond to reasoned requests from competent authorities, including supplying required conformity documentation in a recognized EU language, as per Article 21(1)."

Sub-Prompt: Article 21(2) – Log Access for Competent Authorities

Check:
Review the provider's documentation to determine whether it includes a procedure for:

- Granting **access to logs** referred to in **Article 12(1)** upon a reasoned request from a competent authority
- Identifying **which logs are under the provider's control**
- Ensuring that logs are securely stored and can be retrieved in a timely and structured format
- Logging and tracking such requests and responses internally for audit purposes

Flag if:

- No mention of log access protocols
- Unclear who controls the logs
- No mechanism to comply with a formal request for logs

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Logging procedures, role assignments, data access policies
- **Recommendation:** If Not Compliant → "Provider should document how automatically generated logs (under their control) will be made accessible to competent authorities upon request, in alignment with Article 21(2). This should include internal controls, responsible roles, and delivery process."
- **Reference:** EU AI Act Article 21(2)

Sub-Prompt: Article 22(1) – Appointment of EU-Based Authorized Representative

Check:
Review the provider's documentation to determine whether it includes:

- Evidence of a **written mandate** designating an **authorized representative** established within the EU
- Confirmation that this mandate was established **prior to placing the system on the EU market**
- Contact details and authority delegated to the representative

Flag if:

- The provider is non-EU and no authorized representative is identified
- The mandate lacks clarity on scope or timing
- The representative is not EU-based

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Mandate document, representative's contact info, jurisdictional declarations
- **Recommendation:** If Not Compliant → "Providers established outside the EU must designate an authorized representative located in the EU via a written mandate prior to market availability, in accordance with Article 22(1)."
- **Reference:** EU AI Act Article 22(1)

Sub-Prompt: Article 22(3) – Responsibilities of the Authorised Representative

Check:
Review the provider's documentation to determine whether the mandate for the authorised representative includes the following delegated tasks:

- Verifying that the **EU Declaration of Conformity** and **technical documentation** (Article 11) are complete
- Keeping at the disposal of authorities for **10 years**:
    - Contact details of the provider

- Technical documentation
- Certificate issued by the notified body (if applicable)

● Providing competent authorities, upon **reasoned request**, with all relevant compliance documentation and access to **logs** under provider's control

● Cooperating with competent authorities in **risk mitigation actions**

● Ensuring compliance with **registration obligations** under Article 49(1), if applicable

Flag if:

● Mandate is missing or doesn't explicitly include these responsibilities

● No reference to documentation retention or access provisions

● No role for log access coordination is mentioned

Output Format:

● **Status:** (Compliant / Not Compliant / Unclear)

● **Evidence:** Mandate content, documentation retention plan, log access policy

● **Recommendation:** If Not Compliant → "The provider must ensure the authorised representative's mandate explicitly includes the responsibilities in Article 22(3), including documentation retention, log access, and cooperation with authorities."

● **Reference:** EU AI Act Article 22(3)

Sub-Prompt: Article 22(4) – Mandate Termination and Notification

Check: Review the provider's documentation and any referenced agreement with the authorised representative to determine whether it includes:

● A defined process for mandate termination by the authorised representative if the provider is found to be non-compliant

    - The relevant market surveillance authority
    - The notified body (if applicable)

- Documentation or procedures showing how such termination events are handled, logged, and communicated

Flag if:

- No termination clause exists in the mandate
- No instructions for notification to authorities
- No responsibility defined for informing relevant bodies

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Clauses in the mandate agreement; termination protocol; authority communication plan
- **Recommendation:** If Not Compliant →
"The provider should ensure that its mandate agreement with the authorised representative includes a termination clause per Article 22(4), with a protocol for immediate notification to the relevant market surveillance authority and notified body in cases of non-compliance."
- **Reference:** EU AI Act Article 22(4)

Sub-Prompt: Article 23(1) – Pre-Market Verification by Importers

Check:
Review the documentation to determine whether the importer has verified, **prior to market placement**, that:

- A conformity assessment has been carried out by the provider (per Article 43)
- The provider has created technical documentation in line with Article 11 and Annex IV
- The high-risk AI system bears the CE marking and includes:

    - Instructions for use

- The provider has appointed an authorised representative (Article 22(1))

Flag if:

- Any of the four verification checks are missing or undocumented
- Importer does not describe their pre-market due diligence process
- Evidence of falsified or missing conformity artifacts

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Documentation of importer's verification steps; references to conformity assessment, CE label, declaration of conformity, and authorised rep
- **Recommendation:**
  "Importer must establish a documented procedure to verify the provider's conformity assessment, technical documentation, CE marking, and the appointment of an authorised representative, before placing the AI system on the market."
- **Reference:** EU AI Act – Article 23(1)

Sub-Prompt: Article 23(2) – Handling Non-Conforming or Risky AI Systems

Check:
Review the importer's documentation to confirm whether it includes a procedure for:

- **Identifying** when a high-risk AI system is suspected to be:
    - Not in conformity with the EU AI Act
    - Falsified

- **Preventing** the system from being placed on the market until it is brought into conformity
- **Notifying** the provider, authorised representative, and market surveillance authorities if:
    - A non-conforming system presents a risk under Article 79(1)

Flag if:

- No process exists for identifying and handling non-conforming or falsified systems
- There's no escalation protocol for informing relevant parties when risk is identified
- Lack of clarity on importer's role in conformity assessment workflow

---

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Non-conformance handling policy, risk identification protocols, notification workflows
- **Recommendation:**
  "Importer should formalize and document a risk management protocol for identifying non-compliant or falsified AI systems and outline clear steps for delaying market placement and notifying all relevant parties, as per Article 23(2)."
- **Reference:** EU AI Act – Article 23(2)

Sub-Prompt: Article 23(3) – Importer Identification and Contact Information

Check:
Review documentation and product packaging guidelines to confirm whether the importer:

- Includes their:
    - **Name**

    - **Contact address**

- Ensures this information is affixed to:

    - The high-risk AI system itself

    - Its **packaging** or **accompanying documentation**, where applicable

Flag if:

- Importer information is missing or incomplete

- No evidence of policy or process to affix importer identity details

- No procedure to verify compliance for each shipment or product unit

---

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Packaging guidelines, product labeling policy, importer information template

- **Recommendation:**
"Importer must ensure that complete and accurate identification and contact details are consistently affixed to each high-risk AI system or its accompanying materials, as required under Article 23(3)."

- **Reference:** EU AI Act – Article 23(3)

Sub-Prompt: Article 23(4) – Storage and Transport Conditions

Check:
Examine the importer's documentation and internal protocols to determine whether they have measures in place to:

- Maintain **storage conditions** that preserve system integrity

- Prevent damage, degradation, or environmental exposure that could affect the AI system's performance or conformity

Flag if:

- No reference to environmental or physical storage/transport conditions
- No documented procedure for handling during shipping
- No verification step to ensure AI systems remain compliant after arrival

---

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Shipping SOPs, storage specifications, logistics partner agreements
- **Recommendation:**
  "Importer should document and implement appropriate safeguards to ensure that storage and transportation of high-risk AI systems do not compromise their compliance with Section 2 of the Regulation."
- **Reference:** EU AI Act – Article 23(4)

Sub-Prompt: Article 23(5) – Retention of Documentation by Importers

Check:
Review the importer's compliance documentation and processes to determine whether they:

- Retain the following for **10 years** after the high-risk AI system is placed on the market or put into service:
  - The **certificate issued by the notified body** (if applicable)
  - The **instructions for use**

Flag if:

- There is no reference to documentation retention practices
- The retention period is shorter than 10 years
- No clear assignment of responsibility for long-term document management

---

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Retention policy, document archive system, version control protocols
- **Recommendation:**
  "Importer must establish and maintain a document retention policy ensuring the certificate (if any), instructions for use, and EU declaration of conformity are retained for at least 10 years, as required under Article 23(5)."
- **Reference:** EU AI Act – Article 23(5)

Sub-Prompt: Article 23(6) – Documentation Access for Competent Authorities

Check:
Review the importer's procedures to determine whether they ensure the ability to:

- Provide competent authorities, upon a reasoned request, with:
  - All necessary information and documentation required to demonstrate conformity with Section 2
  - The documentation listed in **Article 23(5)**
- Deliver documentation in a **language easily understood** by the requesting authority
- Guarantee that **technical documentation** can also be made available when needed

- No procedure exists for responding to competent authority requests
- Documentation is not available in appropriate languages
- No access to or control over the technical documentation

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Process map, designated contact roles, response procedures
- **Recommendation:**
  "Importer must document a process to fulfill competent authority requests for conformity documentation in an accessible format and language. This includes maintaining access to technical documentation, even if developed by another party."
- **Reference:** EU AI Act – Article 23(6)

Sub-Prompt: Article 23(6) – Documentation Access for Competent Authorities

Check:
Review the importer's procedures to determine whether they ensure the ability to:

- Provide competent authorities, upon a reasoned request, with:
  - All necessary information and documentation required to demonstrate conformity with Section 2
  - The documentation listed in **Article 23(5)**
- Deliver documentation in a **language easily understood** by the requesting authority
- Guarantee that **technical documentation** can also be made available when needed

Flag if:

- Documentation is not available in appropriate languages
- No access to or control over the technical documentation

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Process map, designated contact roles, response procedures
- **Recommendation:**
  "Importer must document a process to fulfill competent authority requests for conformity documentation in an accessible format and language. This includes maintaining access to technical documentation, even if developed by another party."
- **Reference:** EU AI Act – Article 23(6)

Sub-Prompt: Article 24(1) – Pre-Market Verification by Distributors

Check:
Review documentation provided by or about the distributor to determine whether it includes procedures for verifying, **prior to making the AI system available on the market**, that:

- The AI system bears the required **CE marking**
- It is accompanied by:
  - A copy of the **EU Declaration of Conformity** (Article 47)
  - **Instructions for use**
- The **provider** has complied with:
  - **Article 16(b)** – Provider contact information is on system/packaging/docs
  - **Article 16(c)** – A quality management system is in place

- **Article 23(3)** – Their contact info is on the system/packaging/docs

Flag if:

- No evidence of CE marking verification process
- EU Declaration of Conformity or instructions for use not mentioned
- Distributor does not check provider/importer obligations

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** List documents reviewed and relevant content
- **Recommendation:**
  If Not Compliant → "Distributor should implement a documented process to verify CE marking, EU Declaration of Conformity, and that the provider/importer have fulfilled their obligations under Articles 16(b)(c) and 23(3) before the AI system is made available on the market."
- **Reference:** EU AI Act Article 24(1)

Sub-Prompt: Article 24(2) – Withholding Non-Compliant Systems from Market

Check:
Review distributor documentation or processes to determine if it includes:

- A protocol for evaluating whether an AI system is **non-compliant** based on available information
- A decision-making process to **withhold the AI system from market** until compliance is ensured
- Procedures to **notify the provider or importer** if a system presents a **risk** under Article 79(1)

Flag if:

- No mention of pre-distribution compliance check

- No documented escalation or notification process

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Compliance policy, incident escalation procedure
- **Recommendation:**
  If Not Compliant → "Distributor should define a process for withholding systems from market if there are signs of non-compliance and clearly outline responsibilities for notifying providers or importers in case of risk."
- **Reference:** EU AI Act Article 24(2)

Sub-Prompt: Article 24(2) – Withholding Non-Compliant Systems from Market

Check:
Review distributor documentation or processes to determine if it includes:

- A protocol for evaluating whether an AI system is **non-compliant** based on available information
- A decision-making process to **withhold the AI system from market** until compliance is ensured
- Procedures to **notify the provider or importer** if a system presents a **risk** under Article 79(1)

Flag if:

- No mention of pre-distribution compliance check
- No defined trigger for withholding the system
- No documented escalation or notification process

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)

- **Recommendation:**
  If Not Compliant → "Distributor should define a process for withholding systems from market if there are signs of non-compliance and clearly outline responsibilities for notifying providers or importers in case of risk."

- **Reference:** EU AI Act Article 24(2)

Sub-Prompt: Article 24(3) – Storage and Transport Conditions Under Distributor Responsibility

Check:
Examine distributor procedures or contractual obligations to verify:

- Whether there are **controls or guidelines** in place to ensure that **storage and transport conditions** do not jeopardize compliance with Section 2 of the EU AI Act

- If any **risk mitigation measures** (e.g. climate control, handling instructions, packaging standards) are defined to preserve AI system integrity

Flag if:

- No mention of specific storage or transport controls

- No reference to Section 2 compliance during logistics

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Distribution agreements, internal SOPs, compliance checklists

- **Recommendation:**
  If Not Compliant → "Distributor should ensure documented procedures are in place to maintain appropriate storage and transport conditions aligned with AI system compliance requirements under Section 2."

- **Reference:** EU AI Act Article 24(3)

Check:
Review distributor documentation and procedures to determine if they outline:

- How the distributor identifies and handles **non-conformity** in AI systems they've placed on the market
- Specific actions taken to **withdraw, recall, or bring the system into compliance**
- Protocols for **informing providers, importers, and competent authorities** when risks (as defined in Article 79(1)) are identified
- Internal escalation or notification processes for such events

Flag if:

- No reference to any **corrective action protocol**
- No mention of **communication with providers or authorities**
- No traceability on **non-compliance events**

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Corrective action logs, distributor SOPs, communication templates
- **Recommendation:**
  If Not Compliant → "Distributor must establish a formal process to initiate corrective actions—including withdrawal or recall—if a system is found non-compliant or poses risk under Article 79(1). This process should include timely notifications to the provider, importer, and relevant authorities."
- **Reference:** EU AI Act Article 24(4)

Sub-Prompt: Article 24(5) – Documentation Provided by Distributors to Authorities

Check:
Review distributor documentation to verify whether it includes procedures for:

- Providing all relevant **information and documentation** related to their actions under Article 24(1)–(4)
- Demonstrating **conformity of the AI system** with Section 2 requirements
- Maintaining access to such documentation in a **retrievable and structured format**

Flag if:

- No procedures for handling authority requests
- Unclear documentation retention strategy
- No reference to Article 24(1)–(4) activities being tracked

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Internal response protocols, document access systems, request handling logs
- **Recommendation:**
  If Not Compliant → "Distributor should implement procedures to respond to requests from competent authorities under Article 24(5), including maintaining documentation of all relevant actions and ensuring retrievability for audit or investigation."
- **Reference:** EU AI Act Article 24(5)

Sub-Prompt: Article 24(6) – Distributor Cooperation with Authorities

Check:
Review distributor documentation to assess whether it outlines:

- A defined **process for cooperating** with relevant competent authorities
- Procedures for **mitigating or reducing risks** posed by high-risk AI systems
- Role assignments and escalation paths for regulatory inquiries or enforcement actions

Flag if:

- No mention of cooperation protocols with authorities
- Lack of clarity on roles responsible for handling authority interactions
- Absence of risk mitigation coordination plans

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)
- **Evidence:** Protocols for authority interaction, team assignments, regulatory risk response plans
- **Recommendation:**
  If Not Compliant → "Distributor should document procedures for cooperating with competent authorities as per Article 24(6), including defined responsibilities and coordination plans for addressing system risks."
- **Reference:** EU AI Act Article 24(6)

Sub-Prompt: Article 25(1)(a) – Branding or White-Labeling High-Risk AI Systems

Check:

- Review the provided AI system documentation and assess if the AI system has been branded or white-labeled by the user or another party.
- Verify whether the system is marketed or put into service under the name or trademark of the distributor, importer, deployer, or third-party involved.
- Confirm whether the system complies with the necessary provider obligations under **Article 16** despite the labeling or rebranding.

Flag if:

- There is no clear identification of the brand or name under which the AI system is marketed.
- No documentation or evidence showing the allocation of responsibilities between the original provider

● The system is marketed or put into service under an unregistered or non-compliant brand.

Output Format:

● **Status:** (Compliant / Not Compliant / Unclear)

● **Evidence:** Brand labels, product descriptions, supplier agreements

● **Recommendation:** If Not Compliant → “Ensure the system is correctly branded under the provider’s name, and responsibilities are allocated as per Article 16. Update product documentation to reflect the rebranding or white-labeling procedures."

● **Reference:** EU AI Act Article 25(1)(a)

Sub-Prompt: Article 25(1)(b) – Substantial Modification of High-Risk AI Systems

Check:

● Review the AI system documentation to determine if the AI system has undergone any substantial modifications since being placed on the market or put into service.

● Confirm whether the modified system continues to qualify as a high-risk AI system under **Article 6**.

● Verify that the modifications are clearly documented and aligned with the high-risk AI system requirements.

● Check whether the user’s documentation specifies the modifications and their impact on the system’s risk classification.

Flag if:

● Modifications to the system are not clearly documented or identified.

● The system no longer meets the high-risk AI system criteria as per **Article 6** after modification.

● No evidence of a new assessment or conformity process after modification.

Output Format:

● **Evidence:** Documentation of modifications, conformity assessments, risk assessments

● **Recommendation:** If Not Compliant → “Ensure all modifications to the high-risk AI system are documented and undergo a new risk assessment to confirm the system still meets high-risk criteria as outlined in Article 6. Reassess the conformity procedure accordingly.”

● **Reference:** EU AI Act Article 25(1)(b)

Sub-Prompt: Article 25(1)(c) – Modification of Intended Purpose of AI System

Check:

● Review the AI system documentation to determine whether the intended purpose of the AI system has been modified after it was placed on the market or put into service.

● Verify if the system, after modification, now qualifies as a high-risk AI system under **Article 6**.

● Confirm whether the modification is explicitly documented and whether the revised intended purpose aligns with high-risk criteria.

● Check if the user has documented any updates to the system’s intended purpose, including the updated risk assessment.

Flag if:

● The AI system’s intended purpose is not clearly defined after modification.

● The modified intended purpose leads the system to fall within the high-risk category under **Article 6**, but no re-assessment or conformity checks are conducted.

● There is no documentation of the modification and its impact on risk classification.

Output Format:

● **Status:** (Compliant / Not Compliant / Unclear)

● **Evidence:** Documentation of intended purpose, risk classification, updated risk assessment

● **Recommendation:** If Not Compliant → “Ensure that the modification of the intended purpose is documented and re-evaluated against the high-risk criteria under Article 6. Perform a conformity

● **Reference:** EU AI Act Article 25(1)(c)

Sub-Prompt: Article 25(2) – Cooperation Between Initial Provider and New Provider

Check:

● Review the documentation for any indication that the initial provider of the high-risk AI system has transferred the system to a new provider, and whether there is evidence of cooperation.

● Verify if the initial provider has made the necessary information and technical access available to the new provider to ensure compliance with the requirements of the EU AI Act, particularly for conformity assessment.

● Confirm if the initial provider has clearly specified whether the system is not to be changed into a high-risk AI system and therefore does not need to comply with further documentation or obligations.

● Ensure that the cooperation between the providers is documented and that the technical access provided is in line with the state of the art and relevant for compliance.

Flag if:

● The transfer of the system from the initial provider to a new provider is not documented.

● No technical or compliance-related information has been shared by the initial provider with the new provider.

● There is no indication of a clear understanding between the initial and new providers regarding the system's status and its obligation to comply with the EU AI Act.

● The system's reclassification to a high-risk AI system has not been documented.

Output Format:

● **Status:** (Compliant / Not Compliant / Unclear)

● **Evidence:** Documentation of cooperation, technical access provided, transfer of information

● **Recommendation:** If Not Compliant → "Ensure that the transfer of the system between the initial and new provider is properly documented, and that the new provider receives all relevant technical information for compliance with the EU AI Act."

Sub-Prompt: Article 25(3) – High-Risk AI Systems as Safety Components

Check:

- Review the documentation to determine if the high-risk AI system is a safety component of a product covered by Union harmonisation legislation.

- Confirm that, if the high-risk AI system is part of a product, it has been placed on the market or put into service under the name or trademark of the product manufacturer.

- Verify if the product manufacturer is considered the provider of the high-risk AI system and is complying with the obligations set out in Article 16 of the EU AI Act.

- Ensure that the high-risk AI system meets the necessary conformity assessment requirements and is compliant with the relevant Union harmonisation legislation.

Flag if:

- No documentation or confirmation that the AI system is a safety component of a product.

- The product manufacturer is not fulfilling its role as the provider of the high-risk AI system.

- The system is not placed on the market or put into service under the product manufacturer's name or trademark.

- There is no evidence of conformity assessment or compliance with the relevant Union harmonisation legislation.

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Documentation of AI system's role as a safety component, product placement details, conformity assessment evidence

- **Recommendation:** If Not Compliant → "Ensure that the AI system is correctly classified as a safety component, and that the product manufacturer assumes the provider role and meets all relevant compliance requirements under the EU AI Act."

- **Reference:** EU AI Act Article 25(3)

Check:

- Review the documentation to confirm whether the provider of the high-risk AI system and the third party (supplying AI systems, tools, services, components, or processes) have a written agreement.

- Ensure that the agreement specifies the necessary information, capabilities, technical access, and other assistance based on the generally acknowledged state of the art, required to enable the provider of the high-risk AI system to comply with the obligations set out in the EU AI Act.

- Check if the agreement includes specifications to ensure compliance with the obligations in the EU AI Act regarding the integration of third-party tools, services, or components in high-risk AI systems.

- Verify that the agreement does not apply to third parties making accessible public tools, services, or components under a free and open-source license.

Flag if:

- No written agreement between the provider and third party.

- The agreement lacks necessary specifications for compliance with the EU AI Act.

- No details regarding third-party tools or services integrated into the high-risk AI system.

- No clarification of whether the third party is providing open-source tools, services, or components.

Output Format:

- **Status:** (Compliant / Not Compliant / Unclear)

- **Evidence:** Written agreement, third-party details, specifications for compliance

- **Recommendation:** If Not Compliant → “Ensure that a written agreement is in place between the provider and the third party, specifying all necessary information and technical access to comply with the EU AI Act requirements for high-risk AI systems.”

- **Reference:** EU AI Act Article 25(4)