AI & Partners

Amsterdam - London - Singapore

EU AI Act

KYAI Action Plan

January 2025

Contents

AI & Partners
Amsterdam - London - Singapore

Executive Summary	(Slide 3)
AI System Lifecycle	(Slide 4 - 6)
Risk Pyramid	(Slide 7)
Risk Level Descriptions	(Slide 8)
Risk Classification Process	(Slide 9)
Parties	(Slide 10)
Risk Level Explanations	(Slide 11 - 14)
KYAI Process	(Slide 15)
Guidance for dealing with AI firms	(Slide 16)
KYAI Q&A	(Slide 17 – 38)
KYAI Regulatory Guide	(Slide 39 – 44)

AI Risk landscape insights

AI & Partners
Amsterdam - London - Singapore

We are pleased to present the *Know Your AI System (KYAI) Action Plan.

AI systems are those which pose a risk of harm to individuals' health, safety, and fundamental rights. They are acknowledged as a highly complex, evolving family of technologies that have general purpose application, according to the EU AI Act. In this sense, they have the capacity to affect wide swathes of society given both their functionality and risk profile.

The Risk Classification (see **Slide 9**) is a representation of the different risk categories applicable to AI systems (see **Slide 8**), in the context of the EU AI Act. Outlining what needs to be done, post-risk classification, and by whom (**a non-exhaustive list**) helps enterprises execute on their AI strategy, given the widespread application of the EU AI Act. This document aims to provide a comprehensive, non-exhaustive view of the types of action to take based on the different risk levels of an AI system following the EU AI Act's entry into force on **1st August 2024** and are based on the expert opinion of specialists and market practitioners at AI & Partners leveraging over **4.5 years** of experience.

These indicative actions have been constructed in line with reference to the EU AI Act.

All actions have been designed and created as part of brainstorming sessions together with extensive market research. All references to the EU AI Act relate to the version dated 13 June 2024.

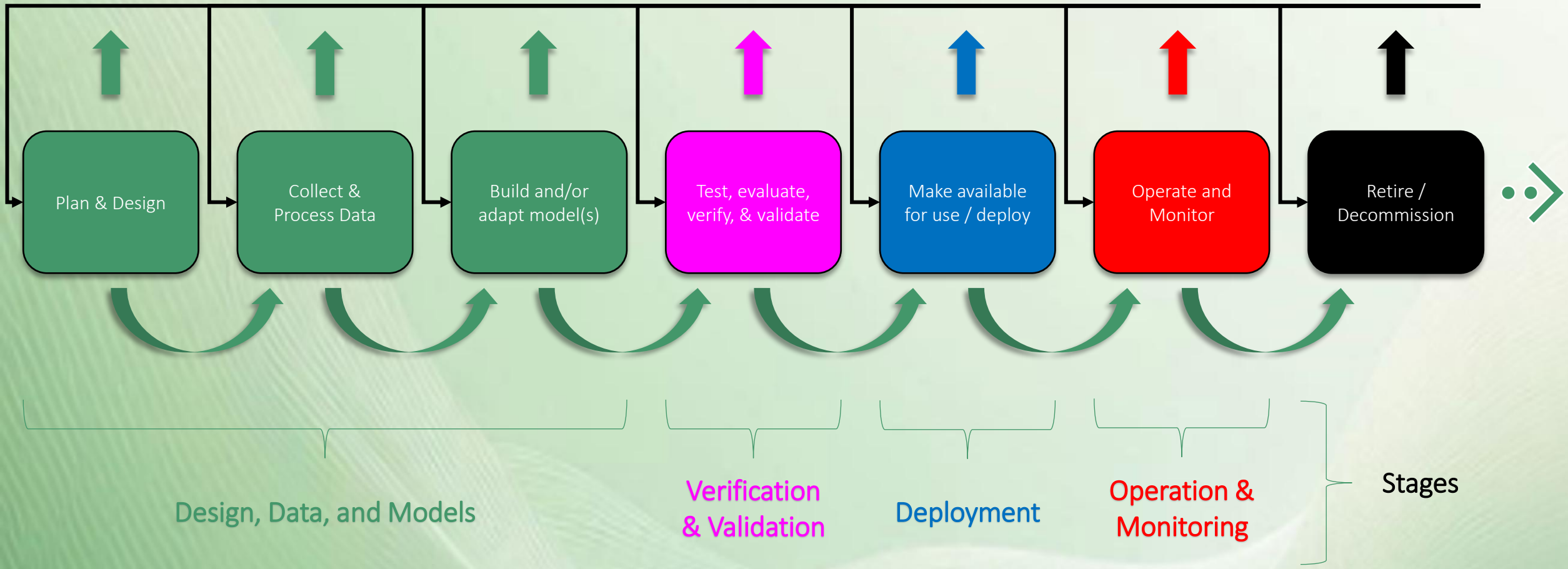
We hope you find the report useful and welcome your comments and feedback.

*This term means, "*identifying, classifying risks, and governing your AI system to ensure it is safe, compliant, and used responsibly.*" (AI equivalent of Know Your Client (KYC)).

AI System lifecycle

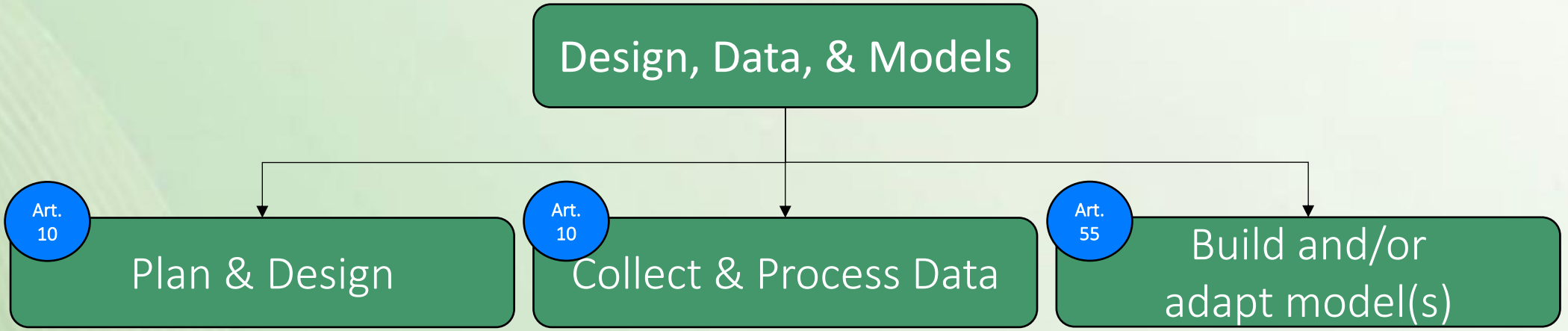
AI & Partners
Amsterdam - London - Singapore

Applies to everything from design to decommissioning



Stage 1

AI & Partners
Amsterdam - London - Singapore



This stage involves the initial conceptualization and planning of the AI system. It includes:

- **Design Specifications**: Outlining the general logic of the AI system, including the algorithms, key design choices, and the rationale behind them. It also includes assumptions made regarding the intended users and the system's optimization goals.
- **System Architecture**: A detailed explanation of how software components interact and integrate within the overall system. This includes the computational resources required for development, training, testing, and validation.
- **Regulatory Compliance Strategy**: Establishing a strategy to ensure compliance with relevant regulations, including conformity assessment procedures and management of modifications.

This phase focuses on gathering and preparing the data necessary for training, validating, and testing the AI model. Key activities include:

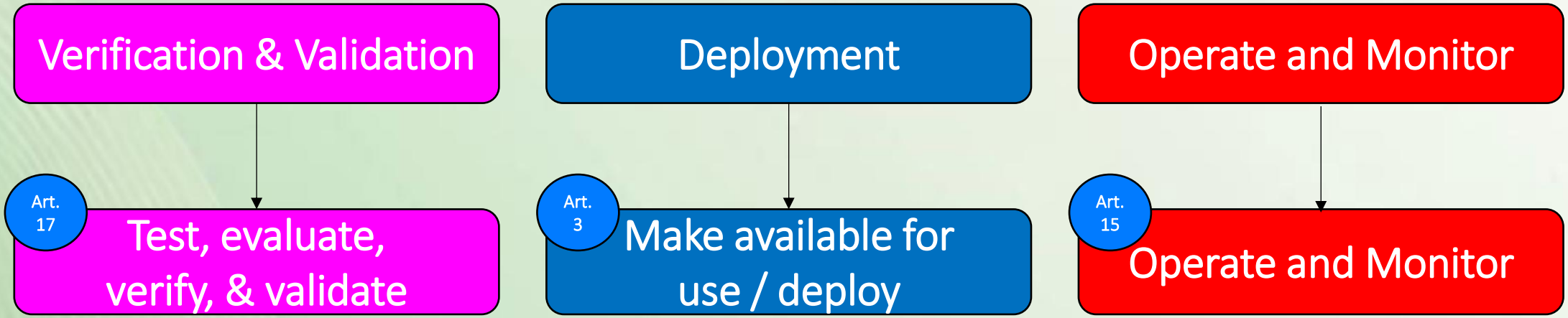
- **Data Collection**: Gathering data from various sources, ensuring it meets the quality criteria for the intended purpose of the AI system. This includes understanding the origin of the data and the processes used for its collection.
- **Data Preparation**: Involves data cleaning, annotation, labelling, updating, enrichment, and aggregation. It also includes formulating assumptions about what the data represents and assessing its availability, quantity, and suitability.
- **Bias Detection and Mitigation**: Identifying and addressing potential biases in the data that could affect the system's performance or lead to discrimination. This includes implementing measures to detect, prevent, and mitigate these biases.

This stage involves the actual development and refinement of the AI model. It includes:

- **Model Training**: Using the prepared data to train the AI model. This involves selecting appropriate training methodologies and techniques, and understanding the computational resources required, such as the number of floating-point operations and training time.
- **Model Evaluation**: Conducting evaluations to assess the model's performance, including adversarial testing to identify and mitigate systemic risks. This also involves documenting the evaluation results and any adaptations made to the model.
- **Model Adaptation**: Fine-tuning and aligning the model based on evaluation results and feedback. This may include updating the model to improve its performance or to comply with new regulatory requirements.

Stages 2 – 4

AI & Partners
Amsterdam - London - Singapore



Verification and validation are processes used to ensure that an AI system meets its design specifications and intended purpose. Key activities include:

- **Verification**: Techniques, procedures, and systematic actions to check that the AI system's design and development meet the specified requirements. It includes design control and design verification.
- **Validation**: Examination, testing, and validation procedures carried out before, during, and after the development of the AI system. It ensures that the system performs as intended in real-world conditions.

Deployment refers to the process of making the AI system available for use by the deployer or end-users. Key activities include:

- **Make Available for Use/Deploy**: The supply of the AI system for first use directly to the deployer or for own use in the Union for its intended purpose. It includes ensuring that the system is registered and complies with all regulatory requirements before being put into service.

Operation and monitoring involve the continuous use and oversight of the AI system to ensure it functions correctly and safely over its lifecycle. Key activities include:

- **Operate and Monitor**: Implementation and maintenance of a post-market monitoring system to collect and review experience gained from the use of the AI system. It involves identifying any need for corrective or preventive actions.
- **Test, Evaluate, Verify, & Validate**: During operation, the system must be regularly tested and evaluated to ensure it continues to meet the required standards of accuracy, robustness, and cybersecurity. This includes monitoring for any risks to health, safety, or fundamental rights.

Tiered-approach to risk

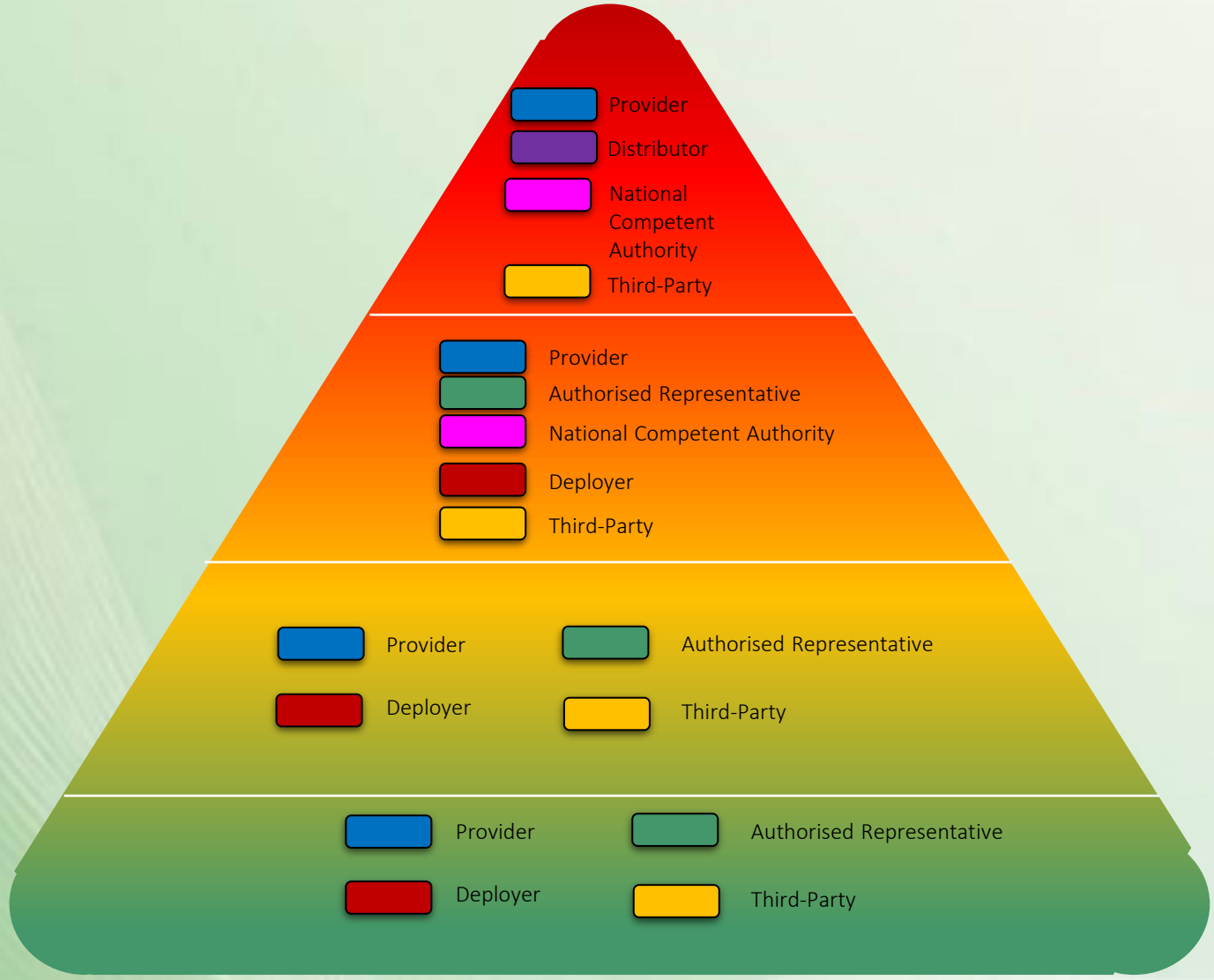
AI & Partners
Amsterdam - London - Singapore

Unacceptable

High

Limited

Minimal or No



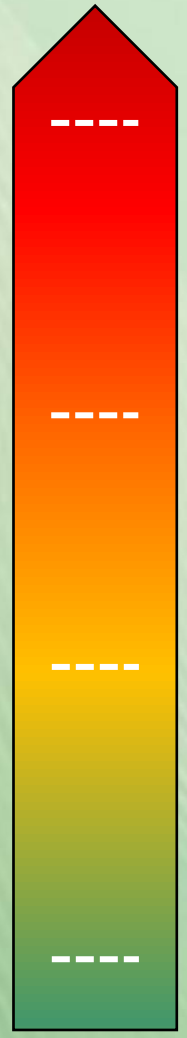
Party

- Provider
- Deployer
- Authorised Representative
- Importer
- Operator
- Third-Party
- Distributor
- National Competent Authority

*This this a non-exhaustive illustration of all risk levels for AI systems mapped against applicable parties in terms of regulatory obligations.

Risk level relative to compliance obligations

AI & Partners
Amsterdam - London - Singapore



Unacceptable

AI systems considered a clear threat to the fundamental rights of people will be banned. This includes AI systems or applications that manipulate human behaviour to circumvent users' free will, such as toys using voice assistance encouraging dangerous behaviour of minors, systems that allow 'social scoring' by governments or companies, and certain applications of predictive policing. In addition, some uses of biometric systems will be prohibited, for example emotion recognition systems used at the workplace and some systems for categorising people or real time remote biometric identification for law enforcement purposes in publicly accessible spaces (with narrow exceptions).

High

AI systems identified as high-risk will be required to comply with strict requirements, including risk-mitigation systems, high quality of data sets, logging of activity, detailed documentation, clear user information, human oversight, and a high level of robustness, accuracy, and cybersecurity. Regulatory sandboxes will facilitate responsible innovation and the development of compliant AI systems. Such high-risk AI systems include for example AI systems used for recruitment, or to assess whether somebody is entitled to get a loan, or to run autonomous robots.

Limited

AI systems like chatbots must clearly disclose to users that they are interacting with a machine. Certain AI-generated content, including deep fakes, must be labelled as such, and users need to be informed when biometric categorisation or emotion recognition systems are being used. In addition, providers will have to design systems in a way that synthetic audio, video, text and images content is marked in a machine-readable format, and detectable as artificially generated or manipulated.

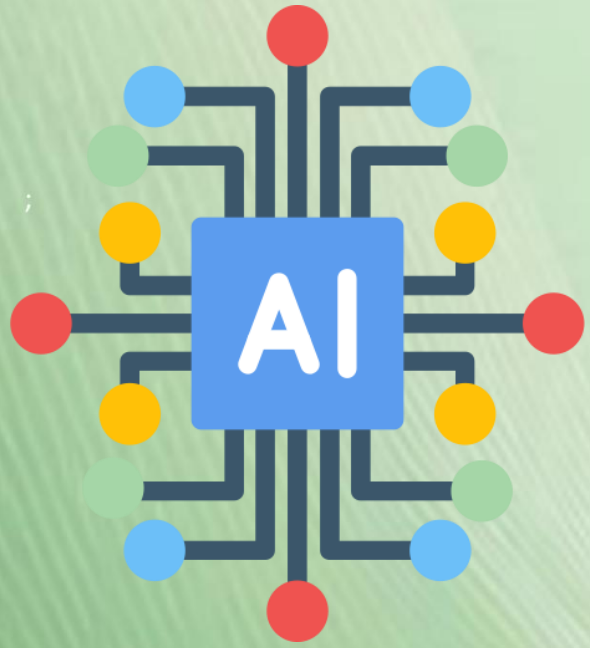
Minimal or No

Most AI systems, such as AI-enabled recommender systems and spam filters, fall into this category. These systems face no obligations under the AI Act due to their minimal risk to citizens' rights and safety. Companies can voluntarily adopt additional codes of conduct.

Know Your AI System (KYAI)

AI & Partners
Amsterdam - London - Singapore

Pre-



Submission for risk classification

Post-

RegTech

- Unacceptable
- High
- Limited
- Minimal or No

Broad network of in-scope parties

AI & Partners
Amsterdam - London - Singapore

Provider
A natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge.

Deployer
A natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity.

Authorised Representative
A natural or legal person located or established in the Union who has received and accepted a written mandate from a provider of an AI system or a general-purpose AI model to, respectively, perform and carry out on its behalf the obligations and procedures.

Importer
A natural or legal person located or established in the Union that places on the market an AI system that bears the name or trademark of a natural or legal person established in a third country.

Operator
A provider, product manufacturer, deployer, authorised representative, importer or distributor.

***Third-Party**
A person that supplies AI systems, tools and services but also components or processes that are incorporated by the provider into the AI system with various objectives, including the model training, model retraining, model testing and evaluation, integration into software, or other aspects of model development. Additionally, this also includes service providers assisting any other actors, such as a legal professional.

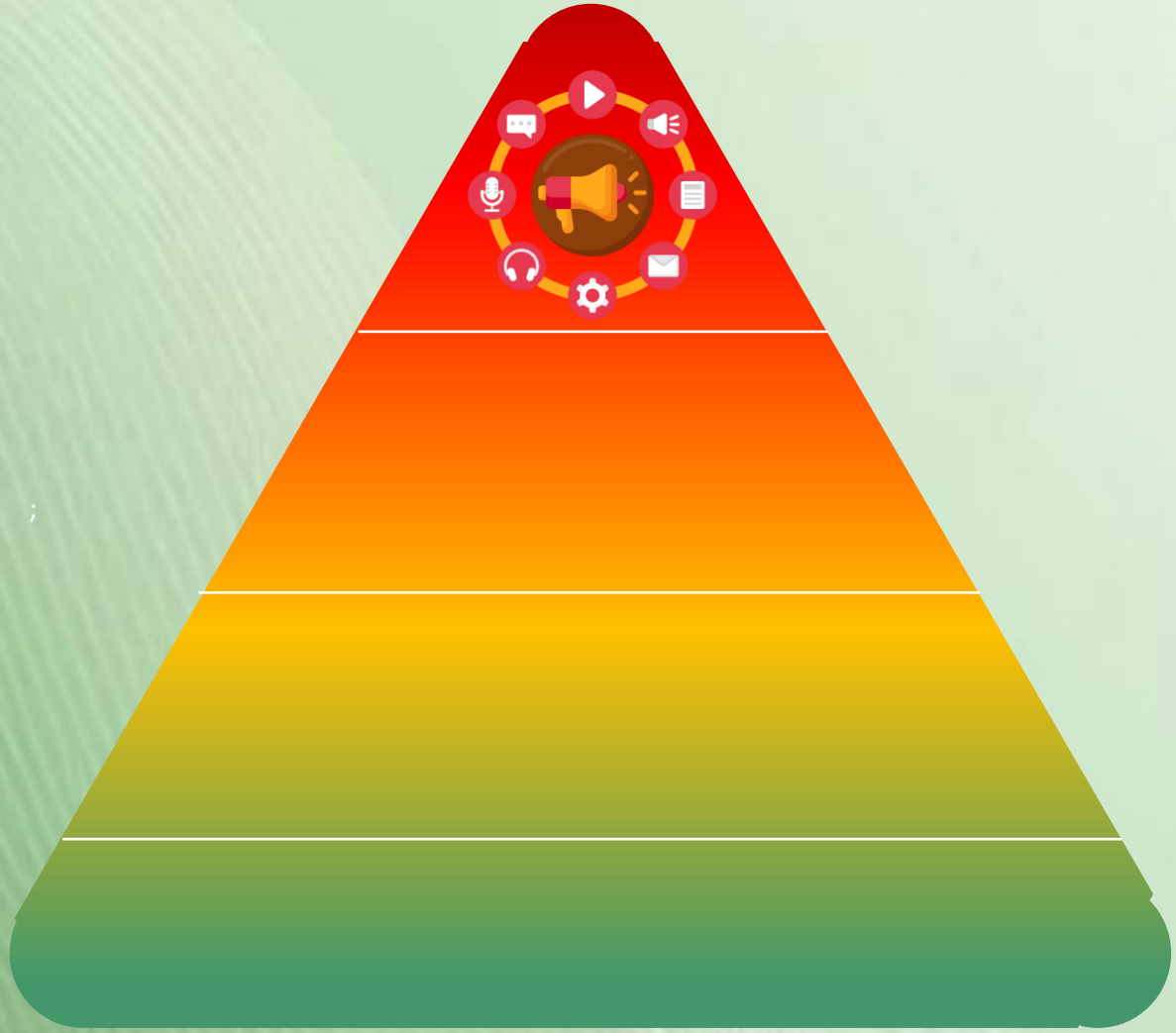
Distributor
A natural or legal person in the supply chain, other than the provider or the importer, that makes an AI system available on the Union market.

National Competent Authorities
Notifying authority or a market surveillance authority. For AI systems put into service or used by Union institutions, agencies, offices, and bodies, references to national competent authorities or market surveillance authorities in the Regulation are construed as references to the European Data Protection Supervisor.

*This term is not expressly defined under Article 3. This definition has been inferred from the provisions of Recitals 88 & 89.

Unacceptable risk

AI & Partners
Amsterdam - London - Singapore



What?

Prohibition of Use: The AI system must not be placed on the market, put into service, or used within the European Union. This is because AI systems classified as unacceptable risk are prohibited under the EU AI Act.

When?

Immediately: The prohibition applies immediately upon classification. The AI system must not be marketed, deployed, or used from the moment it is identified as an unacceptable risk.

Where?

Within the EU: The prohibition applies across all member states of the European Union. The AI system must not be placed on the market, put into service, or used anywhere within the EU.

Who?

- Provider
- Distributor
- Third Party
- Authorised Representative

Why?

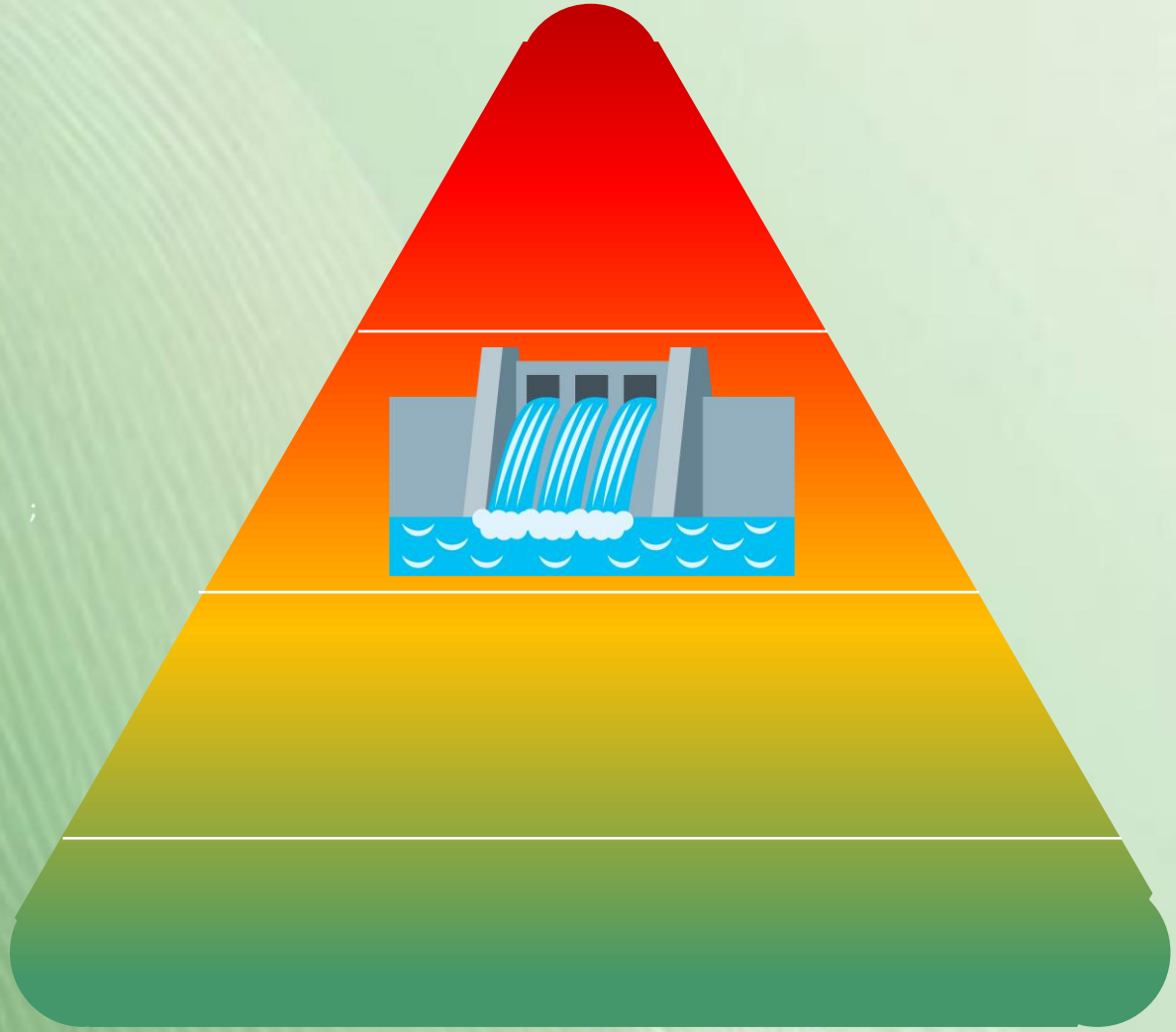
Legal Compliance: To comply with the EU AI Act, which prohibits the use of AI systems classified as unacceptable risk. Non-compliance can result in legal penalties and sanctions.
Safety and Rights Protection: To protect the health, safety, and fundamental rights of individuals. AI systems classified as unacceptable risk pose significant threats that cannot be mitigated.

How?

Market Surveillance: National competent authorities conduct market surveillance to identify and remove AI systems classified as unacceptable risk.
Compliance Measures: Providers and distributors must implement internal compliance measures to ensure that such AI systems are not placed on the market or put into service.

High risk

AI & Partners
Amsterdam - London - Singapore



What?

Compliance with Requirements: The AI system must comply with the requirements set out in Section 2 of Chapter III of the EU AI Act, including design, & development, according to the state of the art in AI technologies.

When?

Before Market Placement:
- Prepare technical documentation.

Throughout the System's Lifetime:
- Log events automatically.

Ongoing:
- Ensure human oversight measures are in place during the period the AI system is in use.

Where?

Within the EU: All actions must take place within the jurisdiction of the European Union, as the EU AI Act applies to high-risk AI systems placed on the EU market or put into service within the EU.

Who?

Provider | Deployer | Third Party | Authorised Representative

Why?

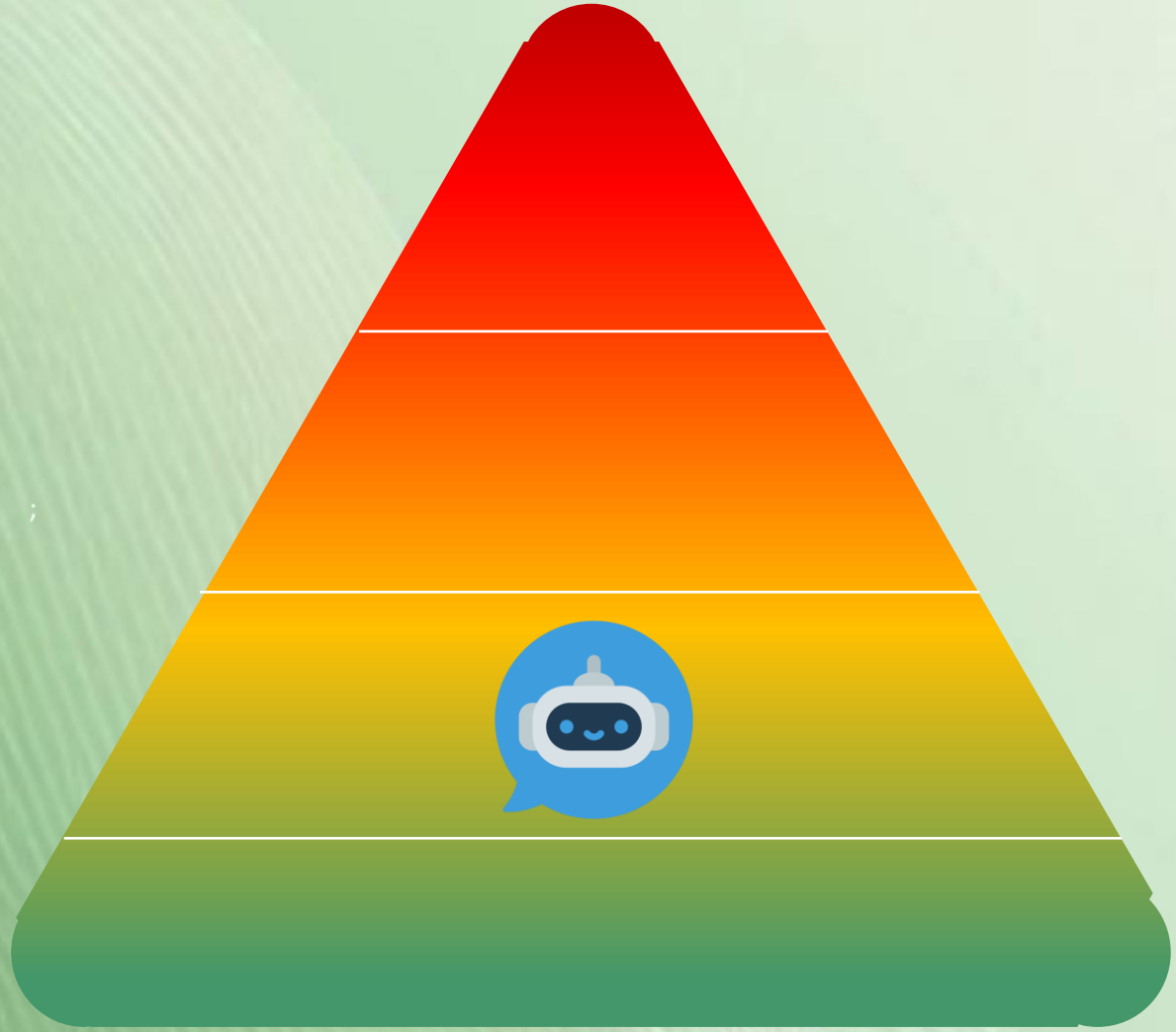
Legal Compliance: To comply with the EU AI Act and avoid penalties for non-compliance
Safety and Trust: To ensure the AI system is safe, reliable, and respects fundamental rights.
Market Access: To legally place the high-risk AI system on the EU market.

How?

Implement Systems: Establish quality and risk management systems as per the EU AI Act requirements.
Prepare Documentation: Create and maintain technical documentation that demonstrates compliance.
Data Management: Ensure data sets used for training, validation, and testing meet quality standards.

Limited

AI & Partners
Amsterdam - London - Singapore



What?

Transparency Measures: The AI system must be designed and developed to ensure that natural persons interacting with it are informed that they are dealing with an AI system, unless it is obvious to a reasonably well-informed person.

When?

At the Time of Interaction: Information must be provided to natural persons at the latest at the time of the first interaction or exposure to the AI system.
Before Market Placement: Transparency measures and disclosures must be in place before the AI system is placed on the market or put into service.

Where?

Within the EU: These actions must take place within the jurisdiction of the European Union, as the EU AI Act applies to AI systems placed on the EU market or put into service within the EU.

Who?

Why?

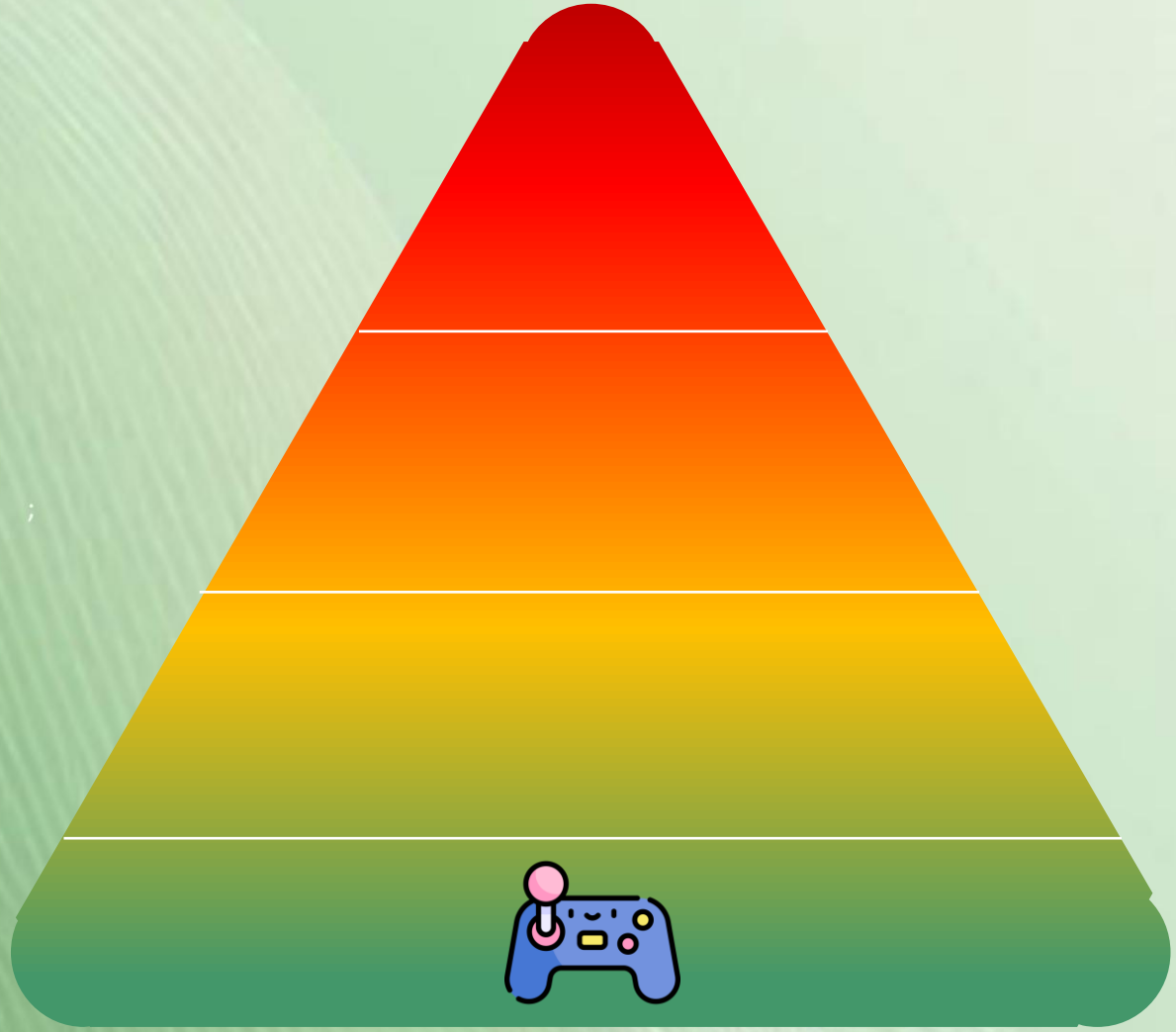
Legal Compliance: To comply with the EU AI Act and avoid penalties for non-compliance.
Public Trust and Safety: To ensure that individuals are aware when they are interacting with AI systems and to maintain transparency in AI-generated content.

How?

Design and Development: Ensure that the AI system is designed to inform users that they are interacting with an AI system.
Marking AI-Generated Content: Implement technical solutions to mark AI-generated or manipulated content in a machine-readable format.
Informing Users: Provide clear and distinguishable information to natural persons at the time of their first interaction with the AI system.

Minimal or No

AI & Partners
Amsterdam - London - Singapore



What?

Compliance with General Obligations: Ensure that the AI system complies with general obligations under the EU AI Act, which may include transparency and accountability measures, and not others.

When?

Before Market Placement: Any necessary transparency measures and general compliance obligations should be in place before the AI system is placed on the market or put into service.

Where?

Within the EU: These actions must take place within the jurisdiction of the European Union, as the EU AI Act applies to AI systems placed on the EU market or put into service within the EU.

Who?

- Provider
- Deployer
- Third Party
- Authorised Representative

Why?

Legal Compliance: To comply with the EU AI Act and avoid penalties for non-compliance.
Public Trust and Safety: To ensure that individuals are aware when they are interacting with AI systems, thereby maintaining transparency and trust in AI technologies.

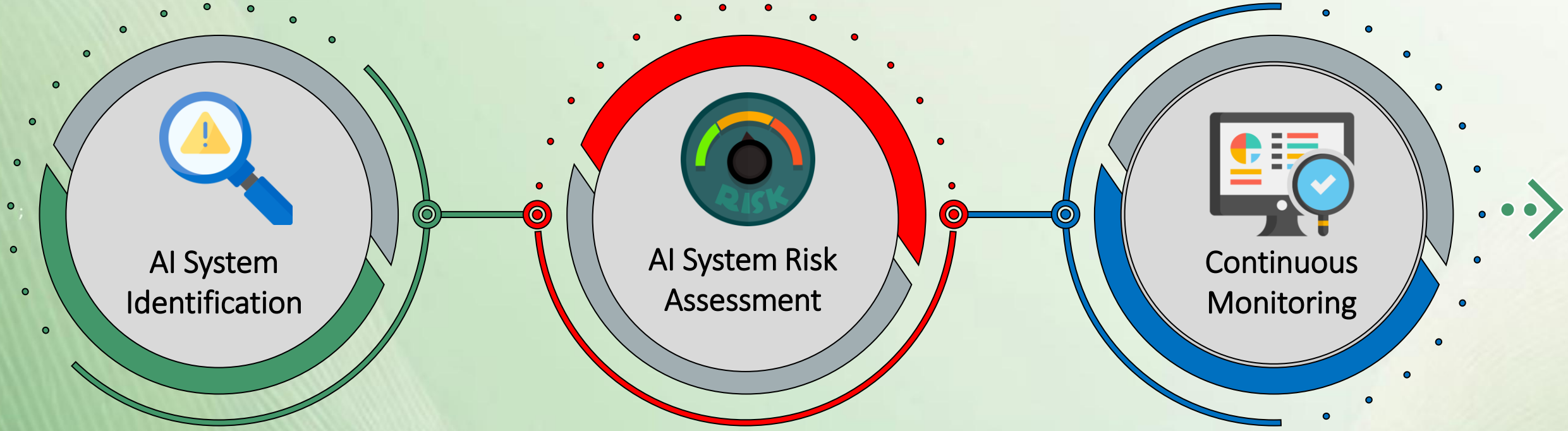
How?

Legal Compliance: To comply with the EU AI Act and avoid penalties for non-compliance.
Public Trust and Safety: To ensure that individuals are aware when they are interacting with AI systems, thereby maintaining transparency and trust in AI technologies.

End-to-end KYAI process

AI & Partners
Amsterdam - London - Singapore

Continuously reinforce the ongoing AI relationship for a frictionless experience



Verify and update the AI system information seamlessly

Evaluations by internal stakeholders and governance for onboarding

Ongoing reviews of AI systems to check for updates to risk profile

Guidance for businesses dealing with AI firms

AI & Partners
Amsterdam - London - Singapore

Overview, risks, and best practices

Risks

1. **Health & Safety Risks**: Harm from malfunctioning systems (e.g., healthcare, autonomous vehicles).
2. **Fundamental Rights Risks**: Discrimination, privacy breaches, opaque decisions.
3. **Systemic Risks**: Broader impacts on society and democracy.

Due Diligence

1. **Conduct** risk assessments of the AI system.
2. **Verify** compliance of providers/vendors.
3. **Perform** risk classification for EU AI Act.
4. **Collect** and maintain technical documentation.
5. **Test** for bias, safety, and reliability.

Monitoring

1. **Set** performance KPIs and automated systems.
2. **Schedule** regular regulatory audits.
3. **Create** feedback channels for user input.

Training

1. **Train** staff on AI functions, risks, and safeguards.
2. **Provide** end-users with clear instructions.
3. **Offer** specialized compliance training for key teams.

Reporting

1. **Set** procedures for incident reporting.
2. **Ensure** compliance with regulatory reporting.
3. **Embrace** voluntary public reporting for transparency.

General understanding

AI & Partners
Amsterdam - London - Singapore

Q.1	**What is “KYAI?”**
A.1	KYAI stands for “Know Your AI System,” a process to identify, assess risks, and govern AI systems responsibly.
Q.2	**Why is “KYAI” important?**
A.2	It ensures the AI system is safe, compliant with regulations, and aligned with ethical principles, minimizing risks to users and organizations.
Q.3	**Who is responsible for implementing “KYAI”?**
A.3	AI providers, deployers, distributors, manufacturers, importers, authorized representatives – and *users* – all share this responsibility.
Q.4	**How does “KYAI” benefit businesses?**
A.4	It enhances trust, reduces liability, ensures compliance, and mitigates risks related to AI deployment.

General understanding

AI & Partners
Amsterdam - London - Singapore

Q.5	**How does KYAI compare to Know Your Customer (KYC) practices?**
A.5	KYAI focuses on understanding and managing AI systems, while KYC is about verifying and monitoring customers to prevent risks like fraud.
Q.6	**How does KYAI align with organizational risk management?**
A.6	KYAI is part of broader risk management, addressing AI-specific risks such as bias, safety, and non-compliance.
Q.7	**Does KYAI apply to all AI systems?**
A.7	Yes, but the depth of KYAI depends on the system's risk level and regulatory requirements.
Q.8	**What is the ultimate goal of KYAI?**
A.8	To ensure AI systems are transparent, compliant, ethical, and aligned with organizational and societal values.

Identifying the AI System

AI & Partners
Amsterdam - London - Singapore

Q.1	**What is the AI system's purpose?**
A.1	The purpose defines what the AI system is designed to achieve, such as automating decisions or enhancing user experience.
Q.2	**What data does the AI system process?**
A.2	It processes structured or unstructured data, sourced internally or externally, such as personal or operational data.
Q.3	**Who developed the AI system?**
A.3	The system could be developed in-house, by a third party, or through partnerships.
Q.4	**What are the AI System's technical components?**
A.4	These include machine learning models, algorithms, datasets, APIs, and software environments.

Identifying the AI System

AI & Partners
Amsterdam - London - Singapore

Q.5	**What is the AI system's input-output process?**
A.5	It defines how input data is processed and transformed into outputs or decisions.
Q.6	**Does the system use pre-trained or custom models?**
A.6	It could use pre-trained models for efficiency or custom models for specific tasks.
Q.7	**What is the AI system's decision-making mechanism?**
A.7	It might be rule-based, statistical, or deep learning-based, depending on its purpose.
Q.8	**What is the expected lifecycle of the AI system?**
A.8	The lifecycle typically includes design, deployment, maintenance, and eventual decommissioning.

Classifying risk levels

AI & Partners
Amsterdam - London - Singapore

Q.1	**What health and safety risks does the AI system pose?**
A.1	Risks include malfunctions in critical areas like healthcare or transportation, potentially causing harm.
Q.2	**What privacy risks exist?**
A.2	These include unauthorized data access, processing sensitive data, or lack of transparency.
Q.3	**Is the AI system categorised as “high-risk”?**
A.3	Yes, if it impacts critical sectors like healthcare, law enforcement, or infrastructure, as defined by the EU AI Act.
Q.4	**Does the AI system impact fundamental rights?**
A.4	Yes, risks include violating privacy, freedom of expression, or non-discrimination rights.

Classifying risk levels

AI & Partners
Amsterdam - London - Singapore

Q.5	**How are risks assessed during development?**
A.5	Risks are assessed through scenario testing, stakeholder analysis, and compliance reviews.
Q.6	**Are ethical risks included in the classification?**
A.6	Yes, ethical risks like fairness, discrimination, and autonomy are critical components.
Q.7	**What happens if the system malfunctions?**
A.7	A response plan should address detection, mitigation, and resolution of malfunctions.
Q.8	**How do risks change over time?**
A.8	Risks evolve as the system operates in dynamic environments or integrates new features.

Governance

AI & Partners
Amsterdam - London - Singapore

Q.1	**What is the governance framework for the AI system?**
A.1	It includes policies, procedures, and accountability structures to ensure compliance and ethical use.
Q.2	**Who oversees the AI system's compliance?**
A.2	A designated team or officer, such as a Chief AI Ethics Officer or compliance manager, handles oversight.
Q.3	**Are risk management protocols in place?**
A.3	Yes, risk management involves identifying, mitigating, and monitoring risks associated with the AI system.
Q.4	**What ethical principles guide the AI system's development?**
A.4	Principles like fairness, transparency, accountability, and safety govern the AI's design and deployment.

Governance

AI & Partners
Amsterdam - London - Singapore

Q.5	**How is AI governance implemented in the organization?**
A.5	Governance involves policies, oversight structures, and accountability measures.
Q.6	**What is the role of the compliance team in governance?**
A.6	The compliance team ensures that AI systems align with regulations and internal policies.
Q.7	**How are governance processes documented?**
A.7	Processes are recorded in manuals, risk registers, and governance frameworks.
Q.8	**How is cross-functional collaboration achieved in governance?**
A.8	Collaboration involves regular meetings and shared tools for legal, technical, and business teams.

Compliance

AI & Partners
Amsterdam - London - Singapore

Q.1	**Does the AI system comply with relevant standards?**
A.1	Compliance is evaluated based on standards like the EU AI Act, GDPR, or ISO 42001.
Q.2	**Are there technical documentation requirements?**
A.2	Yes, documentation must cover design, training data, risk assessments, and testing results.
Q.3	**How often is compliance reviewed?**
A.3	Regular audits and assessments ensure ongoing adherence to regulations.
Q.4	**Is user content required for data use?**
A.4	Yes, under laws like GDPR, user consent is often mandatory for processing personal data.

Compliance

AI & Partners
Amsterdam - London - Singapore

Q.5	**How are high-risk systems identified?**
A.5	High-risk systems are flagged using criteria from regulations like the EU AI Act.
Q.6	**Are there mandatory certifications for compliance?**
A.6	Some systems may require certifications, such as ISO 42001 or similar standards.
Q.7	**How are compliance features escalated?**
A.7	Failures are reported to senior management, legal teams, or regulators as needed.
Q.8	**Is there a process for fundamental rights impact assessments (FRIAs)?**
A.8	Yes, FRIAs evaluate risks to fundamental rights under Article 27 of the EU AI Act.

Monitoring

AI & Partners
Amsterdam - London - Singapore

Q.1	**How is AI system performance monitored?**
A.1	Performance is tracked using key metrics like accuracy, reliability, and user feedback.
Q.2	**Are there processes to detect anomalies?**
A.2	Yes, anomaly detection tools and real-time monitoring systems can flag issues.
Q.3	**How are user complaints handled?**
A.3	A structured process ensures that complaints are logged, investigated, and resolved promptly.
Q.4	**How often is the AI system updated?**
A.4	Updates occur as needed to address bugs, enhance features, or respond to regulatory changes.

Monitoring

AI & Partners
Amsterdam - London - Singapore

Q.5	**What metrics are used to monitor the AI system?**
A.5	Metrics include accuracy, fairness, reliability, and user satisfaction.
Q.6	**How often is the system's performance reviewed?**
A.6	Reviews occur on a defined schedule, such as monthly or quarterly.
Q.7	**Can monitoring detect biases?**
A.7	Yes, monitoring should include bias detection mechanisms.
Q.8	**Are external audits part of monitoring?**
A.8	Yes, external audits provide independent verification of system performance.

Reporting

AI & Partners
Amsterdam - London - Singapore

Q.1	**Are incident reports required?**
A.1	Yes, incidents such as malfunctions or rights violations must be reported internally and to regulators.
Q.2	**How is transparency ensured?**
A.2	Transparency involves publishing relevant information about the system's purpose, risks, and governance.
Q.3	**What incidents must be reported?**
A.3	Incidents include malfunctions, bias, data breaches, and compliance failures.
Q.4	**Who receives internal reports on the AI system?**
A.4	Reports are shared with management, compliance teams, and system developers.

Reporting

AI & Partners
Amsterdam - London - Singapore

Q.5	**What format is used for incident reporting?**
A.5	Reports typically follow a structured template, including details of the issue and mitigation steps.
Q.6	**How are external stakeholders notified of incidents?**
A.6	Notifications are sent via formal communication channels, adhering to legal requirements.
Q.7	**Are there public reporting requirements?**
A.7	Yes, the EU AI Act requires public disclosures for high-risk AI systems.
Q.8	**How is transparency ensured in reporting?**
A.8	Transparency involves clear, concise, and accurate communication about system performance and risks.

Stakeholder Engagement

AI & Partners
Amsterdam - London - Singapore

Q.1	**Who are the internal stakeholders involved in the AI system?**
A.1	Developers, compliance officers, risk managers, executives, and end-users.
Q.2	**How are external stakeholders identified?**
A.2	External stakeholders include customers, regulators, vendors, and advocacy groups.
Q.3	**How do you communicate system risks to stakeholders?**
A.3	Risks are communicated through reports, training sessions, and updates.
Q.4	**Are stakeholders aware of their roles and responsibilities?**
A.4	Yes, roles are clarified through stakeholder agreements and onboarding.

Stakeholder Engagement

AI & Partners
Amsterdam - London - Singapore

Q.5	**How is feedback from stakeholders collected?**
A.5	Through surveys, focus groups, and feedback forms.
Q.6	**Are stakeholders trained on system use and governance?**
A.6	Yes, training ensures all stakeholders understand how to interact with the system.
Q.7	**How are stakeholder concerns addressed?**
A.7	Concerns are documented, reviewed, and resolved through predefined escalation processes.
Q.8	**Are stakeholders involved in system audits or reviews?**
A.8	Yes, key stakeholders often participate in risk assessments and audits.

Auditing

AI & Partners
Amsterdam - London - Singapore

Q.1	**Is there a regular audit schedule for the AI system?**
A.1	Yes, audits occur periodically based on system risk and regulatory requirements.
Q.2	**What is the scope of an AI system audit?**
A.2	It includes technical performance, compliance, risk management, and ethical adherence.
Q.3	**Who conducts the audits?**
A.3	Internal compliance teams or external third-party auditors.
Q.4	**What documentation is required for audits?**
A.4	Documentation includes system specifications, training data, risk assessments, and monitoring logs.

Auditing

AI & Partners
Amsterdam - London - Singapore

Q.5	**How are audit findings documented?**
A.5	Findings are recorded in structured reports, highlighting issues and recommendations.
Q.6	**Are audit results shared with stakeholders?**
A.6	Yes, results are shared with management, compliance officers, and relevant teams.
Q.7	**How are issues identified in audits addressed?**
A.7	Through corrective actions, such as updating models, retraining data, or revising governance policies.
Q.8	**Are audit results used to improve system transparency?**
A.8	Yes, findings enhance transparency by highlighting areas for improvement.

AI System Improvement

AI & Partners
Amsterdam - London - Singapore

Q.1	**How are system updates planned?**
A.1	Updates are planned based on monitoring data, feedback, and regulatory changes.
Q.2	**Is there a process for retraining AI models?**
A.2	Yes, models are retrained periodically to improve accuracy and reduce bias.
Q.3	**How is improvement prioritized?**
A.3	Improvements are prioritized based on risks, user feedback, and performance metrics.
Q.4	**What triggers the need for system improvement?**
A.4	Triggers include audit findings, regulatory changes, and performance deviations.

AI System Improvement

AI & Partners
Amsterdam - London - Singapore

Q.5	**Are updates tested before deployment?**
A.5	Yes, updates undergo rigorous testing to ensure they meet performance and safety standards.
Q.6	**How is user feedback incorporated into system improvement?**
A.6	Feedback informs enhancements in usability, functionality, and reliability.
Q.7	**Are system improvements documented?**
A.7	Yes, all changes are recorded in version control and technical documentation.
Q.8	**How is system scalability addressed during improvements?**
A.8	Updates are designed to accommodate future growth in data, users, or functionalities.

Ethical Considerations

AI & Partners
Amsterdam - London - Singapore

Q.1	**How is fairness ensured in the AI system?**
A.1	By testing for bias and incorporating diverse training datasets.
Q.2	**Are there mechanisms to mitigate discriminatory outcomes?**
A.2	Yes, algorithms are tested and adjusted to prevent discrimination.
Q.3	**How is transparency achieved in decision-making?**
A.3	By providing explanations of how the system reaches its decisions.
Q.4	**Does the system respect user privacy?**
A.4	Yes, through robust data protection measures and consent management.

Ethical Considerations

AI & Partners
Amsterdam - London - Singapore

Q.5	**How are ethical dilemmas addressed in AI design?**
A.5	Dilemmas are resolved by consulting ethical guidelines and engaging stakeholders.
Q.6	**Are the ethical implications of AI use documented?**
A.6	Yes, they are recorded in an ethics impact assessment.
Q.7	**How is societal impact evaluated?**
A.7	Through studies assessing the AI's influence on individuals, communities, and institutions.
Q.8	**Is there an ethics committee overseeing the AI system?**
A.8	Yes, many organizations establish committees to ensure ethical compliance.

Governance

AI & Partners
Amsterdam - London - Singapore

We expect senior management to take clear responsibility for managing AI governance risks, which should be treated with the same priority as other business-critical risks. Senior management must demonstrate active engagement in addressing these risks, ensuring alignment with ethical AI principles and regulatory requirements. Firms should consider their arrangements in light of frameworks like the EU AI Act and any sector-specific governance obligations.

Self-Assessment Questions

- When did senior management last review AI governance issues, including ethical concerns and compliance risks? What actions followed?
- How is senior management kept informed about emerging AI risks (e.g., reports on AI system performance or risks like bias, transparency, or security)?
- Is there evidence that critical issues, such as the misuse of AI, have been escalated appropriately?

Good Practice

- ✓ Senior management sets the right tone and demonstrates leadership on AI governance and ethical AI practices.
- ✓ Proactive steps are taken to ensure AI systems do not perpetuate harm, discrimination, or unfair outcomes.
- ✓ AI governance strategies are implemented for continuous improvement and compliance.

Bad Practice

- × Senior staff involvement in AI governance is minimal or absent.
- × Focus is on meeting minimum regulatory standards without engagement in broader ethical issues.
- × AI risks are managed reactively rather than with a strategic, proactive approach.

Management Information (MI)

AI & Partners
Amsterdam - London - Singapore

AI governance MI should provide senior management with comprehensive insights into the risks associated with AI systems. This includes regular updates and ad hoc reports to ensure alignment with risk appetite and regulatory standards.

Self-Assessment Questions

- Overview of risks posed by deployed AI systems, including emerging threats and updates to risk assessments.
- Regulatory developments and their impact on the organization's AI compliance.
- Insights into the performance and effectiveness of AI governance systems.
- Monitoring of ethical concerns, such as bias in data or algorithmic decision-making, and incident reports.

Good Practice

- ✓ Use of diverse information sources, including compliance, internal audits, and third-party assessments, to provide a holistic view of AI risks.
- ✓ Clear criteria for escalation of AI-related issues to senior management.

Bad Practice

- × Use of narrow, non-representative data for very specific use cases.
- × No criteria or supporting procedures for escalation to senior management.

Structure

AI & Partners
Amsterdam - London - Singapore

The organizational structure for AI governance should facilitate coordination and information sharing across the business. Firms should assign clear responsibilities for AI risk management and ensure teams are adequately resourced.

Self-Assessment Questions

- Who has ultimate responsibility for AI governance, including compliance, bias mitigation, and security?
- Does the structure promote cross-functional collaboration (e.g., between legal, technical, and compliance teams)?
- Are governance teams resourced proportionally to the complexity of AI systems and their associated risks?

Good Practice

- ✓ AI governance is coordinated across the business, with a strategy for addressing gaps and overlaps.
- ✓ Senior staff are engaged in AI governance and equipped with the necessary expertise.

Bad Practice

- × Governance efforts are siloed, and information sharing is ineffective.
- × Teams responsible for AI oversight lack resources or seniority.

Risk Assessments

AI & Partners
Amsterdam - London - Singapore

Understanding AI risks is critical to implementing proportionate and effective governance systems. Risk assessments should address factors like data quality, model performance, deployment contexts, and potential for misuse.

Self-Assessment Questions

- What are the primary risks associated with AI systems, including bias, transparency, and security?
- How are these risks identified, monitored, and addressed across the organization?
- Are risk assessments updated regularly to reflect emerging threats or changes in technology?

Good Practice

- ✓ AI risk assessments are comprehensive, considering diverse factors and data sources.
- ✓ Governance resources are allocated based on the level of risk identified.

Bad Practice

- × Risk assessments are superficial or treated as one-time exercises.
- × The focus is limited to internal risks, neglecting external societal impacts.

Policies and Procedures

AI & Partners
Amsterdam - London - Singapore

Organizations must establish clear, up-to-date AI governance policies that are accessible and understood by all relevant staff. These policies should address ethical, regulatory, and operational considerations.

Self-Assessment Questions

- How often are AI governance policies reviewed and updated?
- How does the firm ensure policies reflect emerging risks (e.g., bias or security vulnerabilities)?
- Are policies tailored to the organization's specific AI use cases?

Good Practice

- ✓ Documented AI policies cover key compliance and ethical requirements.
- ✓ Regular reviews ensure policies remain relevant to emerging risks.
- ✓ Independent audits verify policy effectiveness.

Bad Practice

- × Policies are generic and not adapted to the organization's specific AI risks.
- × Reviews are infrequent, and updates are reactive rather than proactive.
- × Staff lack awareness or training on policy requirements.

Recruitment, Vetting, Training, & Awareness

AI & Partners
Amsterdam - London - Singapore

Staff responsible for AI governance must have the necessary expertise, supported by robust training programs. Recruitment, vetting, and ongoing competence reviews should align with ethical and regulatory requirements.

Self-Assessment Questions

- Are staff adequately vetted to ensure they have the skills and experience required for AI governance?
- How does the organization ensure staff are trained on ethical AI practices and compliance requirements?
- Are performance incentives aligned to prevent risky or unethical AI-related behaviours?

Good Practice

- ✓ Training programs emphasize ethical AI, bias detection, and regulatory compliance.
- ✓ Staff competence is reviewed regularly, with corrective actions as needed.

Bad Practice

- × Training on AI governance is infrequent or ineffective.
- × Staff incentives prioritize speed or innovation over ethical considerations.

Thank you!

AI & Partners

Amsterdam - London - Singapore

E-mail

contact@ai-and-partners.com

Website

https://www.ai-and-partners.com/

Disclaimer

AI & Partners
Amsterdam - London - Singapore

For more information on this publication, visit https://www.ai-and-partners.com/.

About AI & Partners

'AI That You Can Trust' - Your trusted advisor for EU AI Act Compliance. Unlock the full potential of artificial intelligence while ensuring compliance with the EU AI Act by partnering with AI & Partners, a leading professional services firm. We specialise in providing comprehensive and tailored software solutions for companies subject to the EU AI Act, guiding them through the intricacies of regulatory requirements and enabling responsible and accountable AI practices. At AI & Partners, we understand the challenges and opportunities that the EU AI Act presents for organisations leveraging AI technologies. Our team of seasoned experts combines in-depth knowledge of AI systems, regulatory frameworks, and industry specific requirements to deliver strategic guidance and practical solutions that align with your business objectives.

To find out how we can help you, email contact@ai-and-partners.com or visit https://www.ai-and-partners.com.

Business Integrity

AI & Partners defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots professional services, regulatory interventions, and participating in industry groups such as AI Commons, we fight for fundamental rights in the artificial intelligence age.

AI & Partners' publications do not necessarily reflect the opinions of its clients, partners and/or stakeholders.