AI & Partners

Amsterdam - London - Singapore

EU AI Act

Self-Assessment List for Trustworthy AI

A Guide for Self-Assessment

March 2025

AI & Partners

Sean Musch, AI & Partners

Michael Borrelli, AI & Partners

Charles Kerrigan, CMS UK

Eva Dias Costa, PhD, JD | Lawyer & Bioethicist

Helen Yu, Tigon Advisory Corp

AI & Partners

Amsterdam - London - Singapore

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.

This report was prepared by Sean Donald John Musch and Michael Charles Borrelli. For more information visit https://www.ai-and-partners.com/.

Contact: Michael Charles Borrelli | Director | m.borrelli@ai-and-partners.com.

This report is an AI & Partners publication.

Contents

Introduction

In 2025, AI & Partners published the Self-Assessment List for Trustworthy AI (SALTAI) under the framework of the EU AI Act. This document serves as a self-assessment guide for organizations developing, deploying, procuring, or using AI systems, ensuring alignment with the regulatory and ethical principles outlined in the EU AI Act.

The assessment methodology is structured around the EU AI Act's risk-based classification system, which categorizes AI systems into four levels of risk:

- Unacceptable-Risk AI Systems;
- High-Risk AI Systems;
- Limited-Risk AI Systems;
- Minimal or No-Risk AI Systems.

This classification system offers a structured regulatory framework to ensure AI systems comply with fairness, transparency, and societal expectations. Organizations that integrate these principles into their compliance strategies reinforce regulatory adherence and public confidence.

This document presents the final Self-Assessment List for Trustworthy AI (SALTAI) tailored to the EU AI Act, building upon ethical principles and regulatory requirements. The development of this Assessment List spanned from 2024 to 2025 and incorporated industry input through stakeholder consultations, pilot implementations, and regulatory feedback.

Best regards,

Sean Musch

Founder/CEO

AI & Partners

The purpose of this SALTAI is to provide organizations with a structured framework for evaluating AI systems' compliance with EU AI Act requirements. It enables organizations to identify potential risks, implement mitigating measures, and ensure that AI applications operate lawfully, ethically, and transparently. The assessment process encourages active engagement with key compliance questions, fostering a culture of responsible AI governance.

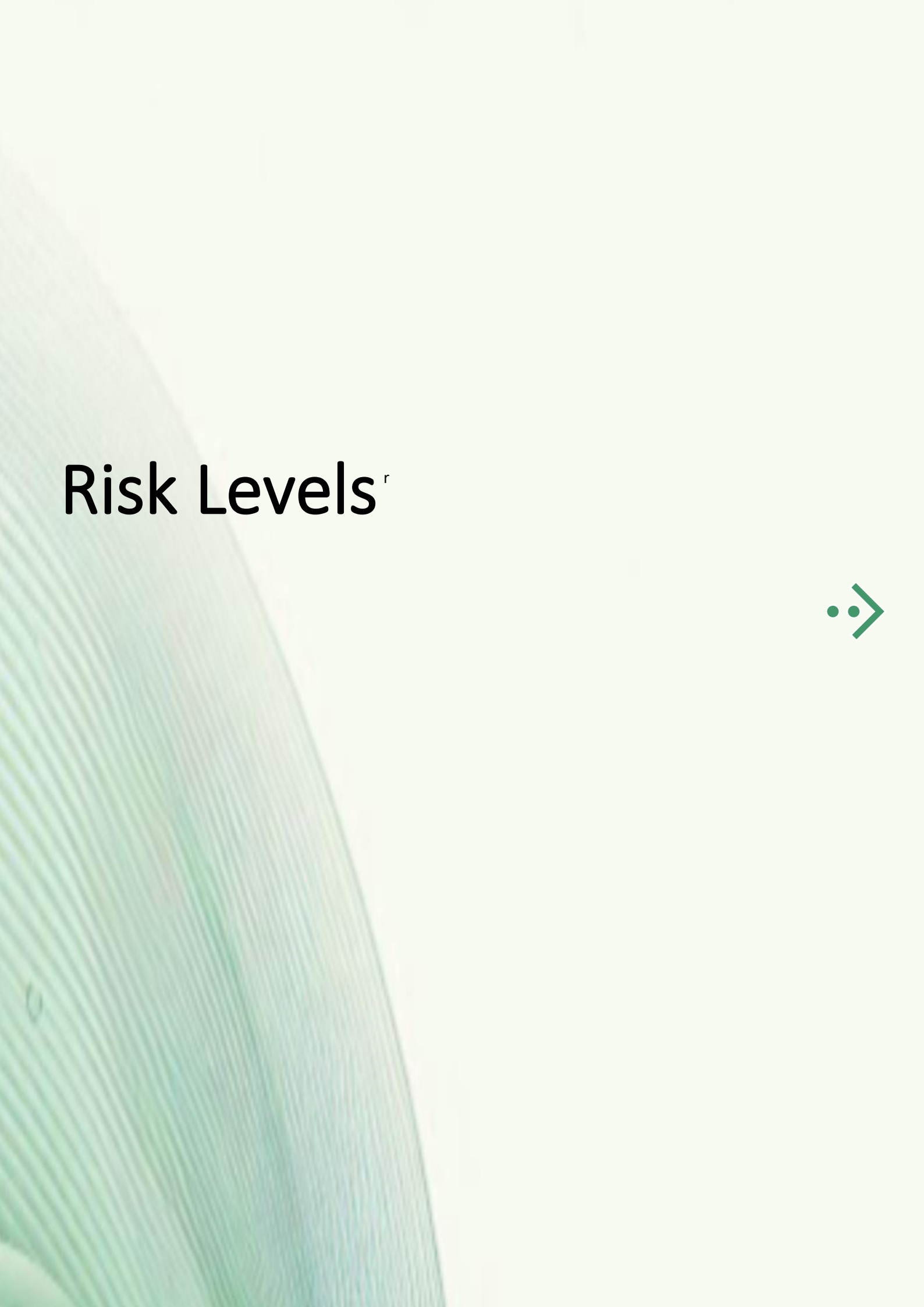
How to use this Self-Assessment List for Trustworthy AI (SALTAI)

The completion of this Assessment List should involve a multidisciplinary team with expertise in AI governance, regulatory compliance, technical development, and ethical considerations. Relevant stakeholders may include:

- AI developers and engineers;
- Data scientists and machine learning experts;
- Compliance and legal officers;
- Procurement and risk management professionals;
- Business leaders overseeing AI strategy;
- End-users and domain experts impacted by AI deployment.

If organizations face challenges in addressing certain assessment questions, external guidance from regulatory bodies, legal experts, or AI governance specialists may be required. This document also includes a glossary and supplementary resources to assist organizations in navigating compliance challenges under the EU AI Act.

Risk Levels[r]



REQUIREMENT #1 Unacceptable-Risk AI Systems

The European Union's AI Act introduces a risk-based classification for AI systems, ensuring that applications posing severe threats to fundamental rights, public safety, and democratic principles are effectively prohibited. Unacceptable risk AI systems represent a category of AI applications that contravene EU values by violating fundamental human rights, engaging in harmful manipulative practices, or enabling mass surveillance and discrimination. The prohibition of these AI applications is based on regulatory imperatives aimed at maintaining public trust in AI technologies. Compliance in this category is essential to ensuring the legitimacy and responsible deployment of AI systems.

These prohibitions are strictly enforced, meaning AI systems falling under this category cannot be developed, deployed, or used within the EU. The European Commission will issue additional guidance on enforcement since the official ban took effect on 2 February 2025.

Glossary

AI Manipulation; Biometric Categorisation; Emotion Recognition; Predictive Policing; Social Scoring; Real-time Biometric Identification.

1. Exploitation of Vulnerabilities & Manipulative AI

One of the most severe concerns surrounding AI is the ability to exploit human vulnerabilities, particularly in ways that manipulate individuals or groups without their awareness. AI systems designed to manipulate, deceive, or exert undue influence on users pose an unacceptable risk and are prohibited under the AI Act.

Key Questions for Evaluation

- Does the AI system target individuals based on age, mental or physical disability, economic vulnerability, or psychological state?
- Are subliminal techniques used to alter an individual's behaviour without their conscious awareness?
- Does the system engage in automated persuasion that could lead to economic, political, or personal harm?
- Are there safeguards to prevent AI-driven deceptive practices in marketing, recruitment, or service offerings?

Examples of Prohibited AI

- AI-powered gambling tools designed to exploit addictive behaviours.
- Algorithmic manipulation of political opinions through targeted misinformation.
- AI-driven financial decision-making tools that encourage risky financial behaviours among vulnerable populations.

2. Social Scoring & Mass Surveillance AI

AI systems designed for social scoring—evaluating individuals based on their behaviour, personal characteristics, or social interactions—are explicitly banned under the AI Act. Social scoring poses systemic risks by reinforcing discrimination, limiting freedoms, and creating unfair access to opportunities and services.

Additionally, mass surveillance AI systems that indiscriminately track and profile individuals—without targeted legal justification—are prohibited. These AI systems threaten the right to privacy, non-discrimination, and democratic freedoms.

AI systems designed to manipulate, deceive, or exert undue influence on users pose an unacceptable risk and are prohibited under the AI Act.

Key Questions for Evaluation

- Does the AI system generate a social score that influences access to services, employment, or opportunities?
- Does the system analyse personal behaviour for social control or law enforcement purposes?
- Are facial recognition or biometric surveillance tools deployed in public spaces without explicit consent or legal oversight?

Examples of Prohibited AI

- Government-run social credit systems restricting financial or social benefits based on behaviour.
- AI systems profiling job applicants based on personal lifestyle data or non-relevant characteristics.
- Automated public surveillance systems that track people's movements without targeted justification.

3. Predictive Policing & Facial Recognition AI

AI used for predictive policing—where individuals are assessed for potential criminal activity based solely on profiling—is banned. These systems risk perpetuating systemic biases and violating the presumption of innocence.

Similarly, the indiscriminate use of facial recognition AI for tracking or identifying individuals in publicly accessible spaces is prohibited, except in very narrow law enforcement contexts.

Key Questions for Evaluation

- Is the AI system used for crime prediction based on personal profiling rather than evidence-based investigation?
- Does the AI system continuously monitor public spaces without legal oversight?
- Are there measures in place to prevent racial, gender, or socio-economic bias in law enforcement AI?

Examples of Prohibited AI

- AI predicting the likelihood of future crimes based on personal background or social data.
- Indiscriminate CCTV-based facial recognition for real-time population tracking.
- Emotion recognition AI used in criminal investigations without consent or oversight.

4. Biometric Categorisation & Emotion Recognition AI

The use of biometric categorisation AI—which classifies individuals based on sensitive attributes like race, political beliefs, religious views, or sexual orientation—is prohibited. Such systems can lead to discrimination and unethical profiling practices.

Additionally, emotion recognition AI in workplaces and educational institutions is banned, except when used for essential medical or safety-related applications.

Key Questions for Evaluation

- Does the AI system infer or categorize individuals based on protected characteristics?
- Is emotion recognition used in a workplace or education setting for non-medical purposes?
- Are there documented justifications for biometric processing in sensitive applications?

Examples of Prohibited AI

- AI that predicts political leanings based on facial expressions or online behaviour.
- Workplace AI tracking employee emotions to assess productivity or mood.
- School-based AI tools monitoring students' emotional states without consent.

5. Enforcement & Compliance Measures

To ensure compliance with the AI Act's prohibitions, the following enforcement mechanisms are in place:

Regulatory Actions

- Ban on market deployment: AI systems classified under unacceptable risk cannot be sold, used, or distributed within the EU.
- Pre-emptive regulatory scrutiny: Developers must disclose AI functionalities to regulatory bodies for assessment.
- Fines and penalties: Organizations found violating these prohibitions face substantial financial penalties up to 7% of global annual revenue.

Guidance & Compliance Timeline

- The European Commission will release guidelines on enforcement before the ban enters into effect on 2 February 2025.
- Businesses developing AI systems must assess compliance and discontinue or modify prohibited AI applications immediately.
- Strict liability provisions ensure that AI developers, distributors, and users remain accountable for any unlawful AI deployment.

REQUIREMENT #2 High-Risk AI Systems

High-risk AI systems have a significant impact on individuals' safety, fundamental rights, and well-being. Under the EU AI Act, these systems are subject to strict regulatory oversight, requiring conformity assessments, transparency measures, and human oversight to mitigate risks. The Act lists specific high-risk AI applications, with periodic reviews to align with evolving technologies and use cases. High-risk AI systems must implement clear oversight mechanisms and explainability measures to ensure stability, reliability, and fairness in AI-driven decision-making.

AI systems classified as high-risk typically operate in critical sectors, including healthcare, employment, finance, education, law enforcement, and infrastructure. While high-risk AI is not prohibited, developers and deployers must adhere to rigorous compliance requirements to ensure ethical and lawful AI deployment.

Glossary

AI Risk Assessment; Conformity Assessment; Human Oversight; Safety-Critical AI; Fundamental Rights Impact; AI Governance.

1. Safety-Critical & Fundamental Rights Impact

High-risk AI systems are those that, if malfunctioning or misused, could pose serious harm to individuals or society. These systems are often integrated into healthcare, transport, and industrial automation, where safety, accuracy, and reliability are crucial.

Key Questions for Evaluation

- Does the AI system directly impact human safety, physical integrity, or health?
- Is the system integrated into medical devices, autonomous transport, or industrial machinery?
- Does the AI system make critical decisions about employment, education, or financial access?
- Have rigorous safety testing and risk assessment procedures been implemented?

Examples of High-Risk AI

- AI-powered medical diagnosis systems that influence treatment decisions.
- Autonomous vehicle control systems responsible for navigation and collision avoidance.
- AI models used in industrial robotics to ensure workplace safety.

2. Law Enforcement, Justice & Biometric AI

AI used in law enforcement, migration control, and judicial processes falls under high-risk classification due to its direct impact on individuals' freedoms and rights. These systems must undergo strict regulatory scrutiny to ensure fairness and prevent misuse.

Key Questions for Evaluation

- Does the AI system support law enforcement decision-making, such as risk assessments or profiling?
- Is the system used in border control or migration processes?
- Are biometric identification tools, such as fingerprint or facial recognition, used?
- Are there safeguards to prevent discriminatory biases in AI-powered legal applications?

Examples of High-Risk AI

- AI-driven risk assessment tools used by police to identify individuals for surveillance.
- Automated lie detection systems for immigration interviews.
- Facial recognition systems used for identity verification in law enforcement.

3. Employment & Education AI Systems

AI systems used in hiring, workplace monitoring, and education are classified as high-risk due to their potential to impact equal opportunities, fairness, and privacy. Employers and educators using AI for decision-making must ensure transparency and non-discriminatory outcomes.

Key Questions for Evaluation

- Does the AI system automate hiring decisions or assess employee performance?
- Is AI used to monitor employees' productivity or behavior?
- Does the system provide automated grading or student assessment?
- Are safeguards in place to prevent algorithmic bias and ensure fairness?

Examples of High-Risk AI

- AI-driven recruitment software that screens job applicants.
- Employee productivity monitoring tools powered by AI analytics.
- Automated grading systems that assess student performance.

4. Financial Services & Credit Scoring

AI systems used in credit risk assessment, loan approvals, and insurance underwriting fall under high-risk classification due to their potential for unfair discrimination and financial exclusion.

Key Questions for Evaluation

- Does the AI system evaluate loan applications or credit scores?
- Is AI used to automate financial decision-making?
- Are there mechanisms in place to ensure explainability and fairness in decision-making?
- Has bias in training data and model outputs been assessed and mitigated?

Examples of High-Risk AI

- AI-powered mortgage approval systems that assess creditworthiness.
- Automated insurance underwriting models that determine policy eligibility.
- Fraud detection AI that identifies suspicious transactions.

5. Critical Infrastructure & Public Services

AI systems operating in public services, energy, transport, and communication infrastructure are considered high-risk due to their potential impact on millions of people.

Key Questions for Evaluation

- Does the AI system control or influence energy grids, water supply, or transport networks?
- Is AI used in emergency response or disaster prediction?
- Are there fail-safe mechanisms to prevent AI failures in critical services?

Examples of High-Risk AI

- AI managing traffic control systems to reduce congestion and accidents.
- AI optimizing electricity distribution in smart grids.
- Automated systems monitoring cyber threats in public sector networks.

6. Transparency, Human Oversight & Conformity Assessment

To ensure high-risk AI systems comply with the EU AI Act, developers and deployers must implement strict transparency, oversight, and assessment measures.

Transparency & Explainability

- High-risk AI systems must be fully documented to ensure compliance and provide clear decision-making processes for stakeholders.
- Users should be able to understand AI-driven decisions affecting them.
- Clear audit logs and accountability mechanisms must be in place.

Human Oversight

- AI decisions must include human review mechanisms where necessary.
- There should be an option for users to challenge AI-generated outcomes.
- Human operators should receive specialized training on managing AI risks.

Conformity Assessment

- High-risk AI systems must undergo pre-market risk assessment before deployment.
- Continuous monitoring is required to detect risks during AI operation.
- Regulatory bodies may conduct external audits of high-risk AI applications.

7. Enforcement & Compliance Measures

High-risk AI systems are legally required to comply with the EU AI Act's strict regulations. Organizations must ensure that transparency, risk mitigation, and human oversight are properly implemented.

Regulatory Actions

- Mandatory risk assessments must be conducted before deploying high-risk AI.
- AI providers must ensure full documentation and regulatory reporting.
- Heavy fines (up to 6% of global turnover) may be imposed for non-compliance.

Guidance & Compliance Timeline

- The EU AI Office will publish detailed compliance guidelines before full enforcement.
- Organizations must align AI risk management processes with regulatory expectations.
- Regular updates and audits are required to ensure continued compliance.

REQUIREMENT #3 Limited-Risk AI Systems

Limited-risk AI systems present some risks but do not significantly impact fundamental rights or safety. Under the EU AI Act, these systems must adhere to specific transparency obligations to ensure that users are informed about their interactions with AI. While limited-risk AI does not face the same regulatory scrutiny as high-risk AI, developers and providers are encouraged to follow best practices for responsible AI deployment. While limited-risk AI systems face fewer regulatory requirements, transparency and user awareness remain key to compliance and responsible AI deployment. Organizations that follow best practices in this category strengthen AI governance and support public confidence.

Limited-risk AI applications are typically found in customer service, entertainment, personal assistants, and content generation. These systems may influence user decisions but should not manipulate, deceive, or create significant legal or financial consequences without user awareness.

Glossary

AI Transparency; User Awareness; Chatbots; Deepfakes; Automated Decision-Making; AI Disclosure; Algorithmic Nudging.

1. AI Transparency & User Awareness

Transparency is a key requirement for limited-risk AI. Users must clearly understand when they are interacting with AI and be able to differentiate AI-generated content from human-created content.

Key Questions for Evaluation

- Does the AI system engage directly with users (e.g., chatbots, virtual assistants, recommendation systems)?
- Are users clearly informed that they are interacting with AI rather than a human?
- If the AI system generates content (text, images, videos, etc.), is there a watermark, disclaimer, or label?
- Does the AI system use nudging or persuasive techniques that might influence user decisions?

Examples of Limited-Risk AI

- AI-powered chatbots for customer service that automate responses.
- Recommendation engines for music, movies, and e-commerce platforms.
- AI-generated news summaries or content creation tools.
- Virtual assistants (e.g., Siri, Alexa, Google Assistant) that process user commands.

2. AI-Generated Content & Deepfakes

With the rise of AI-generated media, ensuring clear disclosure and preventing misinformation is critical. Deepfake technologies and AI-created text, images, and videos must be labelled appropriately.

Key Questions for Evaluation

- Does the AI system create or modify text, audio, video, or images?
- Are deepfake or synthetic media techniques used?
- Are AI-generated outputs clearly marked so users can identify them?
- Is there a risk that users could mistake AI-generated content for real content?

Examples of Limited-Risk AI

- AI-generated art or music that enhances creativity.
- Deepfake entertainment content (e.g., movie special effects) with clear labeling.
- AI-driven writing tools that assist in drafting articles but do not generate deceptive news.

3. Automated Decision-Making & Personalization

AI systems that personalize user experiences or automate minor decision-making without serious legal, financial, or health consequences fall under limited-risk AI.

Key Questions for Evaluation

- Does the AI system influence user decisions through recommendations or nudging?
- Are users given control over personalization settings?
- Is there a mechanism for users to opt out of automated decision-making?
- Does the AI system explain why a specific recommendation or action was made?

Examples of Limited-Risk AI

- Personalized online ads based on browsing history.
- AI-powered learning platforms that adapt content based on user performance.
- Smart home assistants that adjust lighting and temperature preferences.

4. Ethical Considerations & Avoiding Manipulation

Although limited-risk AI does not pose serious harm, it is essential to ensure that AI does not manipulate or exploit users in ways that could lead to unintended consequences.

Key Questions for Evaluation

- Does the AI system use psychological tactics to persuade or nudge users without their awareness?
- Are AI-generated recommendations ethical and fair, avoiding deceptive tactics?
- Are safeguards in place to prevent over-reliance on AI-generated decisions?
- Does the AI system avoid promoting harmful, misleading, or discriminatory content?

Examples of Limited-Risk AI

- AI-driven advertising platforms that recommend products but allow users to control data usage.
- Fitness and wellness AI assistants that suggest health tips but do not provide medical advice.
- AI-based coaching or motivation tools that encourage productivity without coercion.

5. Compliance & Transparency Measures

To ensure compliance with the EU AI Act, limited-risk AI systems must implement clear disclosure policies and transparency measures.

Transparency Requirements

- AI-powered interactions must inform users they're engaging with AI.
- AI-generated content should be clearly labeled to prevent misinformation.
- AI-driven recommendations should provide explanations on how decisions are made.

User Control & Awareness

- Users should have the ability to turn off or modify AI-based personalization.
- AI systems should not force user engagement without an alternative option.
- Consent mechanisms should be in place when AI collects or processes user data.

Accountability & Oversight

- Developers should conduct regular audits to ensure ethical AI practices.
- Organizations must provide accessible documentation on how AI functions.
- User feedback mechanisms should allow for continuous improvement and bias detection.

6. Voluntary AI Best Practices

Although limited-risk AI systems do not have mandatory conformity assessments, developers are encouraged to follow best practices to ensure trustworthiness.

Best Practices for AI Developers

- Implement fairness and bias detection mechanisms to improve AI recommendations.
- Ensure AI explainability so users understand how AI-driven decisions are made.
- Provide opt-out options for users who prefer not to interact with AI.

Best Practices for Users & Organisations

- Educate employees and consumers on how AI interacts with personal data.
- Promote AI literacy to help users identify AI-generated content.
- Support transparency initiatives that align with ethical AI deployment.

7. Enforcement & Compliance Measures

While limited-risk AI does not require formal certification, organizations must ensure that transparency and disclosure guidelines are met.

Regulatory Actions

- Failure to disclose AI-generated content may lead to fines or restrictions.
- Misuse of AI for deceptive purposes (e.g., fake news generation) may result in legal consequences.
- Consumer protection agencies will monitor AI-driven business practices for compliance.

Guidance & Compliance Timeline

- The EU AI Office will release official guidelines on transparency requirements.
- AI developers must review existing AI applications and align them with ethical AI policies.

REQUIREMENT #4 Minimal or No-Risk AI Systems

Minimal or no-risk AI systems comprise the majority of AI applications that do not pose significant threats to fundamental rights, safety, or democracy. These systems are not subject to specific legal obligations under the EU AI Act, beyond compliance with existing laws such as GDPR, consumer protection, and cybersecurity regulations. However, providers of these AI systems are encouraged to adopt best practices for transparency, fairness, and ethical AI development.

Minimal or no-risk AI systems typically support productivity, automation, and convenience without directly affecting users' rights or well-being. Examples include spam filters, AI-powered search engines, grammar correction tools, and entertainment recommendation algorithms.

Glossary

AI Ethics; AI Usability; Consumer AI; Automated Assistance; Responsible AI; Fairness in AI.

1. Common Examples of Minimal or No-Risk AI

AI applications classified under minimal or no-risk typically enhance user convenience and efficiency while operating within existing legal frameworks.

Key Questions for Evaluation

- Does the AI system operate purely as an assistive tool without making critical decisions?
- Does the system comply with data privacy and security regulations?
- Are users given control over how the AI functions within applications?

Examples of Minimal- or No-Risk AI

- Spam filters that detect and block unwanted emails.
- AI-driven search engines optimizing information retrieval.
- Grammar and spelling correction tools improving written communication.
- Recommendation engines for movies, books, and music without major impact on user rights.

2. Voluntary AI Best Practices

While minimal-risk AI is not subject to mandatory compliance frameworks, developers should implement best practices to ensure transparency, fairness, and user trust.

Best Practices for AI Developers

- Ensure fair and unbiased algorithms to prevent reinforcing stereotypes or misinformation.
- Maintain transparent AI interactions, avoiding deceptive or manipulative practices.
- Implement user controls to allow customization and opt-out options.

Best Practices for AI Users & Organisations

- Educate users about AI functionalities and limitations to manage expectations.
- Encourage AI literacy to improve public understanding of AI-driven decisions.
- Promote responsible AI use through self-regulation and industry standards.

3. Transparency & Fairness Measures

Transparency and fairness ensure that minimal-risk AI systems remain ethical and reliable.

Transparency Requirements

- AI-generated recommendations should be explainable and easy to understand.
- Information about AI usage should be clearly disclosed to users.
- Developers should provide access to documentation detailing AI decision-making processes.

Fairness Considerations

- AI models should be tested for biases that may affect recommendations.
- Users should be able to modify AI-based personalization settings.
- AI outputs should be monitored to ensure they remain neutral and inclusive.

4. Compliance & Ethical AI Development

Even though minimal-risk AI does not have strict regulatory requirements, it must still comply with existing laws and ethical guidelines.

Compliance with Existing Regulations

- AI systems must adhere to GDPR when processing personal data.
- Consumer protection laws ensure AI-driven services remain safe and non-deceptive.
- Cybersecurity regulations mandate protection of AI-generated data against misuse.

Ethical Considerations

- Developers should conduct regular AI assessments to prevent unintended consequences.
- Transparency reports should outline how AI models function and evolve over time.
- Organizations should engage in stakeholder dialogue to promote responsible AI deployment.

5. User Control & AI Usability

Minimal-risk AI should be designed with user control and usability in mind, ensuring that individuals can interact with AI efficiently and without unwanted interference.

User-Centric AI Design

- AI systems should allow users to adjust preferences and settings.
- AI interfaces should be accessible to individuals with disabilities.
- Clear help guides and support should be available for users unfamiliar with AI functionalities.

Examples of User Control in AI

- Customizable search engine algorithms allowing users to refine queries.
- Adjustable recommendation settings for streaming services.
- AI-powered productivity tools offering manual override functions.

6. Encouraged Industry Standards & Certifications

While not required by law, organizations can improve AI trustworthiness by adopting voluntary industry standards and certifications.

Recommended AI Standards

- ISO AI Ethics Guidelines promoting responsible AI use.
- Fair AI Certification ensuring transparency and accountability.
- Human-Centred AI Design Frameworks improving accessibility and inclusivity..

Advantages of AI Certification

- Enhances user trust and credibility in AI applications.
- Encourages best practices in AI governance and fairness.
- Provides a competitive advantage by demonstrating ethical AI commitment.

7. The Role of Minimal-Risk AI in Society

Minimal-risk AI contributes to economic growth, technological progress, and enhanced user experiences. When responsibly deployed, these systems can improve daily life without introducing significant risks.

Positive Societal Impacts of Minimal-Risk AI

- Boosting productivity through automation and smart assistance.
- Enhancing creativity with AI-powered content generation tools.
- Providing inclusive solutions for users with diverse needs and abilities.
- Improving efficiency in industries such as retail, logistics, and education.

8. Enforcement & Compliance Measures

Minimal-risk AI does not require formal regulatory approval, but developers and providers should ensure responsible deployment.

Regulatory Actions

- Organizations failing to comply with general consumer protection laws may face penalties.
- Misuse of AI leading to privacy violations or unfair competition may result in legal consequences.
- EU regulatory bodies may review AI industry practices to ensure adherence to ethical AI principles.

Guidance & Compliance Timeline

- The EU AI Office will issue best practice guidelines for minimal-risk AI transparency.
- AI developers should periodically review AI systems to ensure they align with evolving ethical standards.
- Industry self-regulation groups will encourage responsible AI development and deployment.

Calls to action

1. Conduct a Self-Assessment Using SALTAI

Leverage the Self-Assessment List for Trustworthy AI in combination with appropriate AI governance technology to evaluate your AI system's risk level in accordance with the EU AI Act. Identify potential risks, gaps, and areas for improvement to align with regulatory expectations.

2. Implement Risk Management Strategies

Use the insights from your self-assessment to develop and implement robust risk mitigation strategies. Address transparency, fairness, and accountability concerns to ensure AI trustworthiness.

3. Engage Multidisciplinary Stakeholders

Involve legal, technical, and ethical experts in your AI governance processes. Collaborate with internal teams and external advisors to enhance compliance and best practices in AI deployment.

4. Align AI Systems with EU AI Act Requirements

Ensure that your AI applications meet the necessary legal obligations and industry standards. Stay ahead of regulatory enforcement deadlines by proactively integrating compliance measures into your AI governance framework.

5. Partner with AI Governance Practitioners

AI regulations and best practices are evolving rapidly. Stay updated on emerging guidelines, participate in industry discussions, and refine your AI governance approach to maintain compliance and trustworthiness over time.

Conclusion

The Self-Assessment List for Trustworthy AI (SALTAI) under the EU AI Act marks a pivotal milestone in the development of structured, ethical, and accountable AI governance. As organizations navigate the complexities of AI compliance, this self-assessment framework provides a practical tool for evaluating AI systems against regulatory and ethical standards. In establishing clear criteria for transparency, accountability, and risk mitigation, SALTAI supports organizations in aligning their AI applications with the EU AI Act's requirements while fostering responsible innovation.

However, effective implementation will determine the impact of SALTAI. Organizations face varying levels of readiness, with challenges such as integrating AI risk assessments into existing governance structures, ensuring meaningful human oversight, and balancing compliance with operational flexibility.

Small and medium enterprises (SMEs), in particular, may require additional guidance in adopting the self-assessment methodology while maintaining competitiveness in an evolving regulatory landscape.

Despite these challenges, early adopters are demonstrating the benefits of structured AI governance. Companies across industries—technology, finance, healthcare, and public services—are leveraging SALTAI to assess AI risks, strengthen compliance, and enhance stakeholder trust. Embedding ethical safeguards, continuous monitoring, and proactive risk mitigation into the AI development lifecycle means organizations illustrate how a structured self-assessment approach can drive both regulatory alignment and operational excellence.

For businesses and policymakers alike, SALTAI presents a unique opportunity to establish leadership in AI governance.

Using this framework, organizations can systematically identify gaps, implement corrective measures, and ensure their AI systems meet the highest standards of trustworthiness. As AI-driven decision-making becomes more prevalent, self-assessment tools like SALTAI provide a critical foundation for ensuring AI remains transparent, fair, and aligned with societal values.

Looking ahead, the long-term success of SALTAI will depend on continuous industry engagement, refinement of best practices, and alignment with emerging AI governance frameworks. As AI adoption expands, organizations will be evaluated on compliance, resilience, fairness, and transparency. A structured governance approach supports trust, stability, and alignment with societal expectations, reinforcing regulatory integrity and sustainable AI systems.

Organizations that integrate this self-assessment process into their AI strategy will position themselves at the forefront of responsible AI development, setting a benchmark for ethical, effective, and sustainable AI governance in compliance with the EU AI Act.

About AI & Partners

AI & Partners

Amsterdam - London - Singapore

AI & Partners – 'AI That You Can Trust'

At AI & Partners, we're here to help you navigate the complexities of the EU AI Act, so you can focus on what matters—using AI to grow your business. We specialize in guiding companies through compliance with tailored solutions that fit your needs. Why us? Because we combine deep AI expertise with practical, actionable strategies to ensure you stay compliant and responsible, without losing sight of your goals. With our support, you get AI you can trust—safe, accountable, and aligned with the law.

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

Contacts

Sean Donald John Musch, CEO/Founder, s.musch@ai-and-partners.com

Michael Charles Borrelli, Director, m.borrelli@ai-and-partners.com

Authors

Sean Donald John Musch, CEO/Founder

Michael Charles Borrelli, Director

References

European Parliament and The Council of the European Union, (2024), 2024/1689 Regulation (EU) 2024/1689 of the European Parliament and of The Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), accessible at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689 (last accessed 8th March 2025)

Important notice

This document has been prepared by AI & Partners B.V. for the sole purpose of enabling the parties to whom it is addressed to evaluate the capabilities of AI & Partners B.V. to supply the proposed services.

Other than as stated below, this document and its contents are confidential and prepared solely for your information, and may not be reproduced, redistributed or passed on to any other person in whole or in part. If this document contains details of an arrangement that could result in a tax or National Insurance saving, no such conditions of confidentiality apply to the details of that arrangement (for example, for the purpose of discussion with tax authorities). No other party is entitled to rely on this document for any purpose whatsoever and we accept no liability to any other party who is shown or obtains access to this document.

This document is not an offer and is not intended to be contractually binding. Should this proposal be acceptable to you, and following the conclusion of our internal acceptance procedures, we would be pleased to discuss terms and conditions with you prior to our appointment. Images used throughout the document have either been produced in-house or sourced from publicly available sources (see **References** for details).

AI & Partners B.V. is the Dutch headquarters of AI & Partners, a global professional services firm. Please see https://www.ai-and-partners.com/ to learn more about us.

Designed and produced by AI & Partners B.V