International Olympic Committee

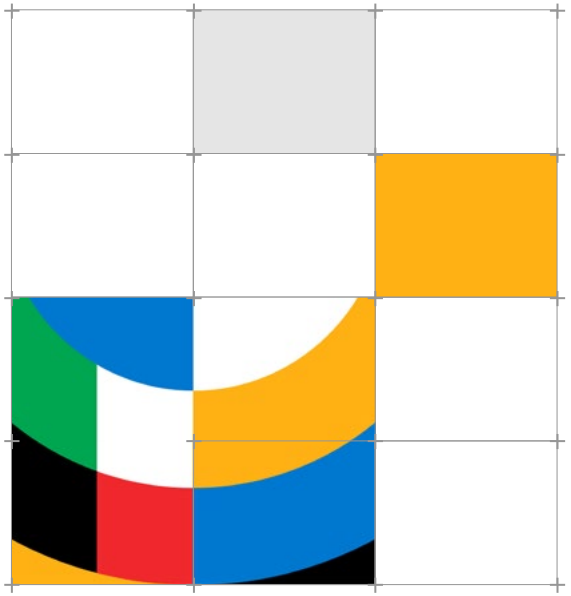
TRUSTWORTHY AI FRAMEWORK FOR THE OLYMPIC MOVEMENT

TRUSTWORTHY AI CHECKLIST TRAINING MATERIALS & FAQS

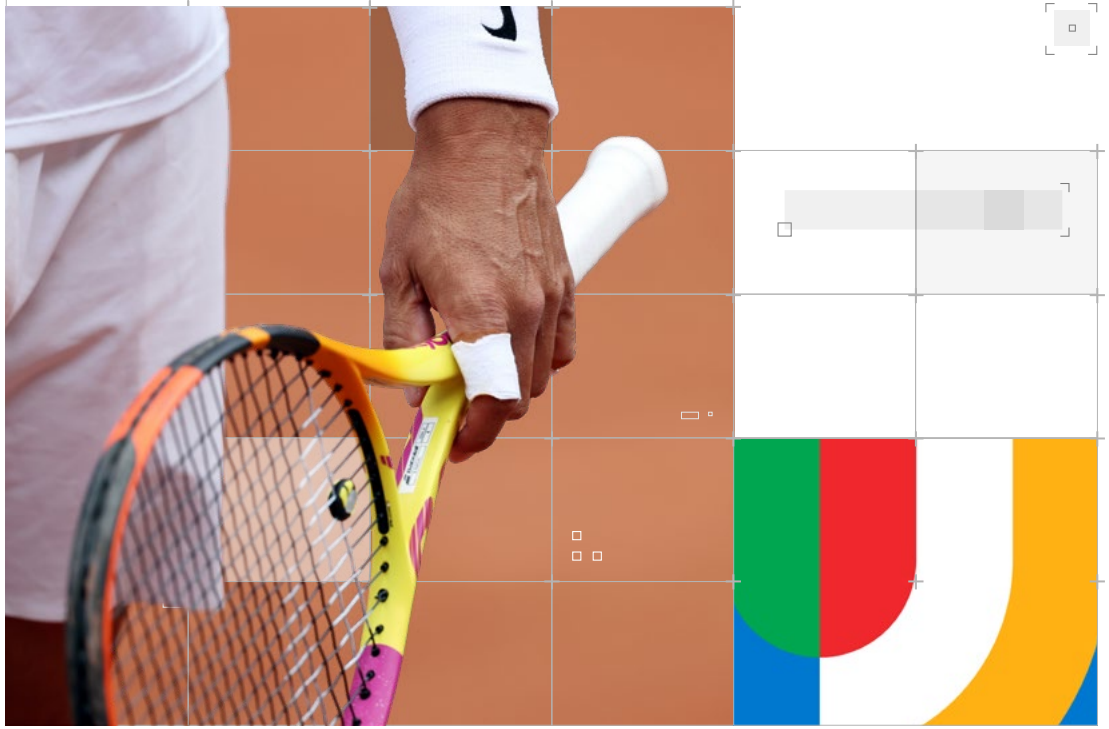
Olympic™ AI

CONTENTS

Trustworthy AI Checklist Instructions	03
Frequently Asked Questions (FAQs)	16



TRUSTWORTHY AI CHECKLIST INSTRUCTIONS



THE TRUSTWORTHY AI CHECKLIST

TRANSLATING PRINCIPLES INTO ACTIONS

The Trustworthy AI Checklist is a three-step process, carried out using an Excel document, that is designed to assess the inherent risk of your AI system or application, and to consider the trustworthiness of your current design and process.

STEP 1.
INHERENT RISK ASSESSMENT

Understanding your inherent risk

This initial assessment helps you gauge the fundamental risk level of your AI system or application before you apply any specific controls. It's about understanding the nature of the challenge.

How it works

You will answer 10 high-level questions:

- **AI Solution Profile**
  Covering the delivery method, objectives, usage patterns and deployment context of your AI system or application.
- **Potential Impact Factors**
  Assessing the potential for harm (physical or psychological), negative impacts on rights, the use or retention of sensitive data, and other critical operations.

Your outcome

You will receive an Inherent Risk Rating of Minimal, Moderate or High. This rating guides you on the levels of time, resources and scrutiny your initiative will likely require as you move forward.

STEP 2.
CORE AI CHECKLIST: TRUSTWORTHY AI STATUS

Managing risk with Trustworthy AI Principles

Once you understand the inherent risk of your AI system of application, the Core AI Checklist will help you actively manage it by applying the seven Trustworthy AI Principles for the Olympic Movement throughout your solution's lifecycle.

How it works

You will answer detailed questions across all seven Trustworthy AI Principles, covering such key subjects as privacy, safety, fairness and so on. These questions will assess the measures and controls that you currently have in place for your AI system or application, or that you are planning to implement.

Your outcome

The more effectively you have embedded the Trustworthy AI Principles, the higher your Trustworthy AI Status will be for each section. These ratings will show your progress in building a responsible AI system or application.

STEP 3.
RECOMMENDATIONS

Actionable recommendations for improvement

This final step provides concrete, tailored guidance to help you enhance the trustworthiness of your AI system or application based on your specific responses.

How it works

Based on your answers in Step 2, you will receive a detailed recommendation for each area. This includes:

- A concise action point for improvement.
- Specific aspects of your AI system or application on which to focus.
- Links to relevant guidelines, frameworks and best practices.
- Suggestions for internal or external experts who could provide further support.

Your outcome

You will receive a clear set of actionable steps to continuously improve your AI system or application and embed a trustworthy approach.

ACCESSING AND USING THE TRUSTWORTHY AI CHECKLIST

You can download the Trustworthy AI Checklist through the official IOC website. The Excel document has four worksheets, as follows:

Instructions

The Instructions worksheet offers clear, high-level guidance on how to navigate and effectively use the Trustworthy AI Checklist.

AI Checklist

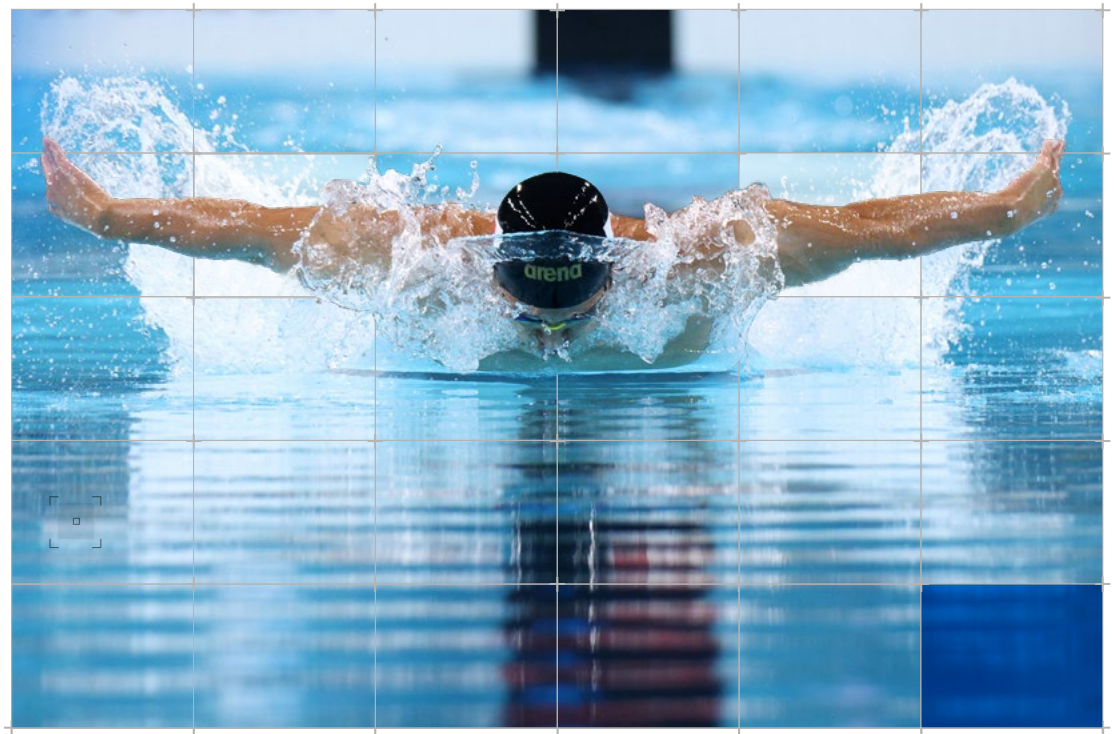
The AI Checklist worksheet enables users to evaluate the Inherent Risk Rating of an AI system or application, and ensure alignment with the Trustworthy AI Principles.

Glossary

The Glossary worksheet provides definitions of key terms and acronyms used throughout the Trustworthy AI Checklist to promote clarity and consistency.

Supporting Documents

The Supporting Documents worksheet provides additional resources and best practices to further strengthen the integrity and reliability of your AI systems and applications.



THE TRUSTWORTHY AI CHECKLIST

EXCEL INSTRUCTIONS

Download and open the Trustworthy AI Checklist for the Olympic Movement Excel document, then open the AI Checklist worksheet.

STEP 1.
INHERENT RISK ASSESSMENT

What to do

- **Read questions 1–10**

  Review the "AI Solution Profile" and "Potential Impact Factors" questions in column C (cells C5–C16) of the AI Checklist worksheet.

- **Select options**

  For each question, choose the most applicable option from the dropdown menus in column E (cells E5–E16).

- **Obtain your Inherent Risk Rating**

  Ensure you have answered all 10 questions within the "Inherent Risk Assessment" section to obtain an Inherent Risk Rating (cell E17).

STEP 2.
CORE AI CHECKLIST

What to do

- **Read questions ID 1 to ID 18.4**

  Review the questions covering all seven Trustworthy AI Principles in column C (cells C24–C131) of the AI Checklist worksheet.

- **Select controls**

  For each question, indicate whether any of the specific controls have been applied in column E (cells E24–E131).

- **Obtain Trustworthy AI Status**

  Answer all questions in each ID block to obtain the Trustworthy AI Status in column E (cells E23, E29, E35, etc).

STEP 3.
RECOMMENDATIONS

What to do

- **Consider recommendations**

  Examine the recommendations provided in columns G, H, I, and J of the AI Checklist worksheet. These recommendations are based on the Trustworthy AI Statuses obtained through the answers provided to each block of questions.

- **Study the summarised view**

  Refer to the Managed Risk Profile Dashboard (cells G2–I12) for a condensed view of your Trustworthy AI Status for all seven Trustworthy AI Principles based on your answers in the checklist. Review this against the Inherent Risk Rating (cell E17) to understand your progress to date and recommendations for next steps.

NEED HELP?

Tooltips (light bulbs)

Refer to the tooltips in column D of the AI Checklist worksheet for assistance in answering each question.

Examples

Consider the examples provided in the brackets to help answer each question. Note that these examples are for supporting purposes only and are not exhaustive.

Glossary

Refer to the Glossary worksheet for clear definitions of key terms and acronyms used throughout the Trustworthy AI Checklist.

Supporting documents

Refer to the Supporting Documents worksheet for additional guidance to answer the questions.

STEP 1. INHERENT RISK ASSESSMENT

UNDERSTANDING YOUR INHERENT RISK

This initial assessment helps you gauge the fundamental risk level of your AI system or application before you apply any specific controls. It's about understanding the nature of the challenge.

HOW IT WORKS

You will answer 10 high-level questions:

- **AI Solution Profile**
  Covering the delivery method, objectives, usage patterns and deployment context of your AI system or application.
- **Potential Impact Factors**
  Assessing the potential for harm (physical or psychological), negative impacts on rights, the use or retention of sensitive data, and other critical operations.

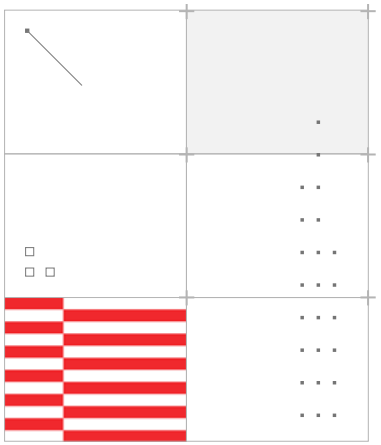
YOUR OUTCOME

You will receive an Inherent Risk Rating of Minimal, Moderate or High. This rating guides you on the levels of time, resources and scrutiny your initiative will likely require as you move forward.

INHERENT RISK ASSESSMENT

QUESTIONS 1-10

The Inherent Risk Assessment helps you understand the fundamental risk level of your AI system or application based on its core nature and potential impacts before any controls are in place.



AI SOLUTION PROFILE

1. **AI Solution Delivery:** Please select if the AI solution is built internally, bought externally, used as service, or if a hybrid approach is being used.
2. **AI Solution Objective(s):** Please select what your AI solution intends to achieve.
3. **AI Output Impact Scope:** Is the AI solution used to generate outputs primarily for internal or external use?
4. **AI Solution Infrastructure:** Is the AI solution's infrastructure hosted internally, externally or using a hybrid approach?
5. **Data Storage:** Is the data for the AI solution stored internally or externally?

POTENTIAL IMPACT FACTORS

6. **Physical & Psychological Harm:** Could a malfunction or error of the AI solution potentially lead to physical harm or injury, or significantly impact the psychological state or mental well-being of individuals (e.g. athletes, staff, spectators)?
7. **Data Processing:** Will the AI solution process personal identifiable information (PII)?
8. **Significant Impact:** Could the AI solution's decisions or actions affect an individual's rights, opportunities (e.g. eligibility for competition, opportunity to compete due to officiating errors), or access to essential services (e.g. access to employment, healthcare, education, housing, credit)?
9. **Vulnerable Groups:** Will the AI solution interact with or make decisions concerning vulnerable groups (e.g. children, individuals with disabilities, refugees, etc)?
10. **Critical Operations & Public Security:** Is the AI solution intended for use in critical infrastructure (e.g. venue security, athlete/spectator transport logistics, critical broadcast infrastructure, or energy supply for events), essential services (e.g. athlete/spectator medical care, event emergency response, or critical support services), law enforcement, border control, or national security applications?

INHERENT RISK RATING

Answer all questions in this section to receive an overall Inherent Risk Rating of Minimal Risk, Moderate Risk or High Risk.

Minimal Risk

Your AI solution has a low initial risk profile; proceed to the section below to confirm best practices and identify opportunities for continuous improvement.

Moderate Risk

Your AI solution presents some initial risks; continue to the section below for specific guidance on managing these areas responsibly.

High Risk

This rating is not a stop sign. Your AI solution has important considerations; the section below provides crucial guidance to address these areas responsibly and build a trustworthy solution.

INHERENT RISK ASSESSMENT

DETAILED INSTRUCTIONS

1.

Open the Trustworthy AI Checklist Excel workbook and navigate to the AI Checklist worksheet.

2.

For all 10 questions in the Inherent Risk Assessment section, press “Select...” and use the dropdown arrows on the right to choose the most applicable option.

3.

If you need additional support to determine the most applicable option, click on the “tooltip” buttons (blue lightbulbs).

4.

After selecting a response for each question in the Inherent Risk Assessment section, you will receive an Inherent Risk Rating, along with high-level guidance on how to proceed.

STEP 2. CORE AI CHECKLIST: TRUSTWORTHY AI STATUS

UNDERSTANDING YOUR TRUSTWORTHY AI STATUS

The essence of the Trustworthy AI Checklist lies in its step-by-step evaluation of control measures, which are designed to quantify and reflect the overall trustworthiness of an AI system or application.

HOW IT WORKS

You will answer each question of each step ID (in total, 18 IDs)

- **Step ID 1:** Answer all four questions to obtain your Trustworthy AI Status on clear ownership of the AI system or application.
- **Step ID 2–18:** Do the same for step IDs 2–18 – answer all the questions to receive a Trustworthy AI Status for each section.

YOUR OUTCOME

Trustworthy AI Status: You will receive a Trustworthy AI Status for each section: Strongly Trustworthy, Developing Trustworthiness or Trustworthiness Needs Action.

Managed Risk Profile Dashboard: The dashboard summarises your managed risk ratings per principle across the entire Core AI Checklist, providing a consolidated overview of your AI solution's risk posture after considering implemented controls.

CORE AI CHECKLIST

TRUSTWORTHY AI STATUS SUMMARY

For each question, select the option from the dropdown menu that best describes your AI system or application or current practices. As you complete each numbered ID section, you will receive a specific Trustworthy AI Status for that section.

STEP ID 1

Clear Ownership

STEP ID 1.1

Have you assigned a clear individual or committee accountable for the outputs produced by the AI solution?

STEP ID 1.2

Have you defined, documented, and communicated who is responsible for each stage of the AI solution lifecycle to all relevant internal and external stakeholders?

STEP ID 1.3

Have you clearly communicated to all internal and external stakeholders a point of contact for AI solution concerns?

STEP ID 1.4

Is ownership regularly reviewed and updated as the AI solution evolves?

- Click on the lightbulbs to the right of each section heading in the Core AI Checklist for a tooltip that articulates what the principle means in practice.
- Answer each step ID, even if your answer is “No” to a specific step. Once you answer all questions, you will receive a Trustworthy AI Status.
- If you are unsure or do not know the answer, please consult with colleagues or experts who might be able to help.

TRUSTWORTHY AI STATUS

Strongly Trustworthy

Your current approach provides a strong foundation. Continue these best practices and consider periodic reviews to sustain responsible innovation.

Developing Trustworthiness

This highlights opportunities to refine and strengthen your AI system or application. The recommendations offer clear guidance for enhancing your approach and fostering more trustworthy development.

Trustworthiness Needs Action

This indicates an area requiring focused strategic attention. Addressing these critical areas through careful thought and action will enable responsible and impactful AI innovation.

CORE AI CHECKLIST

DETAILED INSTRUCTIONS

1.

Review each of the step ID questions.

2.

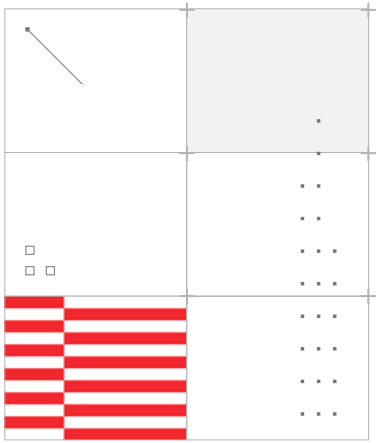
For each step ID, starting with step ID 1.1, press “Select...” and use the dropdown arrow on the right to choose YES, NO or N/A for each question.

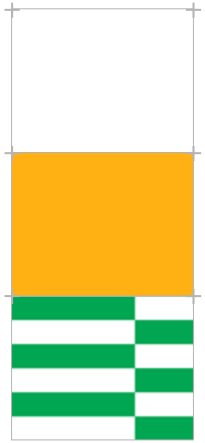
3.

If you need additional support to determine the most applicable option, click on the “tooltip” buttons (white lightbulbs).

4.

Answer all questions for step ID 1 (step ID 1.1–1.4) to obtain a Trustworthy AI Status on clear ownership for the AI system or application. Then answer all the following questions for step ID 2–18 to obtain a Trustworthy AI Status for each section.





STEP 3. RECOMMENDATIONS

UNDERSTANDING YOUR RECOMMENDATIONS

Each recommendation is split into a high-level recommendation, control areas to consider, resources to explore and key collaborators, and is tailored to the Trustworthy AI Status of each section (e.g. “Clear Ownership” under “Accountability Questions”).

HOW IT WORKS

The recommendations will automatically pop up when you have obtained the Trustworthy AI Status, as set out above in step 2.

YOUR OUTCOME

Based on the Trustworthy AI Status obtained, you will receive guidance on how to proceed with your AI system or application. This guidance typically falls into one of three areas:

- Sustaining strong trustworthiness
- Refining and strengthening critical attributes
- Thoughtfully preparing to take meaningful action

RECOMMENDATIONS

SUMMARY

For every section in the Core AI Checklist you complete (e.g. step ID 1), a tailored recommendation will appear based on your Trustworthy AI Status. These recommendations offer guidance and starting points for improving the trustworthiness of your AI system or application. For example:

	Control areas	Resources	Recommendation	Key collaborators
Strongly Trustworthy	1. Periodically review and update ownership assignments and responsibility matrices. 2. Continuously monitor the AI solution's evolution to anticipate changes in accountability needs.	1. Review best practices for AI governance frameworks and lifecycle management. 2. Consult guidelines on change management for evolving AI solutions.	Continue to maintain and proactively refine your robust ownership and accountability framework. Ongoing review ensures sustained clarity and effective governance.	1. Engage those responsible for overall AI strategy or governance for strategic oversight. 2. Consult internal or external risk management experts for periodic assurance on accountability.
Developing Trustworthiness	1. Develop clear, documented and communicated responsibilities for each AI solution lifecycle stage. 2. Establish formal processes for logging decisions, changes, incidents and communicating points of contact.	1. Review project management best practices for defining roles and responsibilities (e.g. RACI matrix). 2. Consult guidelines on incident management and stakeholder communication strategies.	Focus on strengthening key aspects of your accountability framework. Enhancing clarity, documentation and communication can significantly improve governance and stakeholder trust.	1. Collaborate with project management and AI development roles to define and document responsibilities. 2. Engage with legal function to establish clear points of contact and logging processes.
Trustworthiness Needs Action	1. Prioritise designating a single individual or committee as the ultimate owner accountable for the AI solution's outputs. 2. Formally document and communicate this ownership to all relevant internal and external stakeholders.	1. Review ethical AI frameworks that emphasise accountability and human responsibility. 2. Consult organisational governance guidelines for assigning ownership of critical AI solutions.	Strongly consider establishing clear ownership before proceeding. Assigning accountability for AI solution outputs is fundamental for effective governance, risk management and stakeholder trust.	1. Collaborate closely with senior leadership and legal experts to formally assign and document ownership. 2. Engage those responsible for AI governance or strategic oversight for approval of accountability structures.

RECOMMENDATIONS

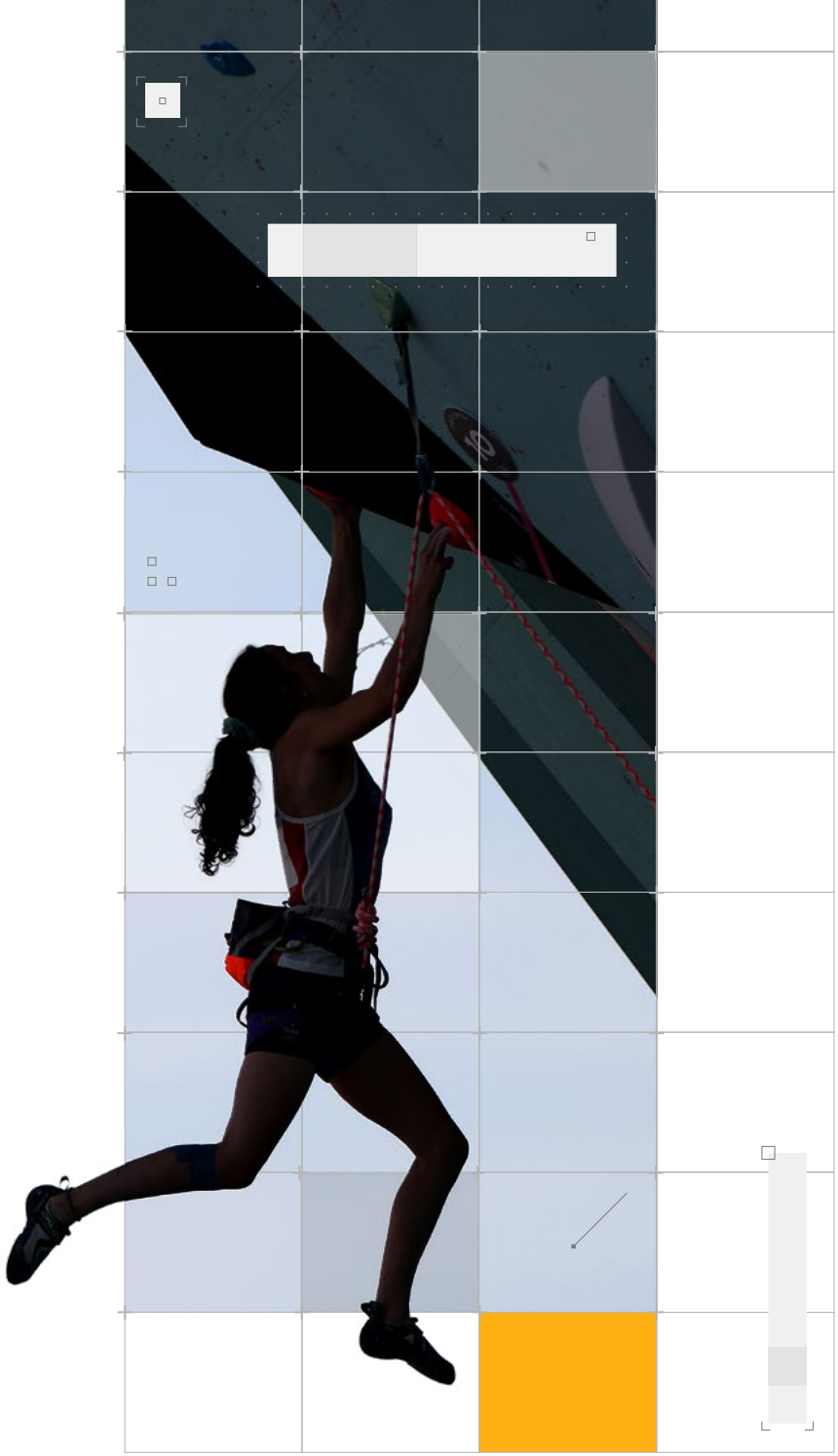
DETAILED INSTRUCTIONS

1.

The “Recommendations” section will be populated automatically after you have answered all the questions for step ID 1–18. Each recommendation will appear on the right of the Core AI Checklist.

2.

After completing all the questions for step IDs 1–18, you will see a summarised risk rating for each Trustworthy AI Principle at the top of the AI Checklist, next to the Inherent Risk Assessment.



FREQUENTLY ASKED QUESTIONS (FAQS)

FAQS

GENERAL

QUESTION	ANSWER
What is the purpose of this Trustworthy AI Checklist?	This Trustworthy AI Checklist helps users to assess the trustworthiness, ethical implications and potential risks of an AI system or application. It provides a structured framework for the responsible design, development, deployment and ongoing management of AI.
What does “Trustworthy AI” mean?	“Trustworthy AI” refers to AI systems or applications that are lawful, ethical and robust; that are designed to be reliable, safe, fair and transparent; and that respect human values. For a better understanding, please refer to the Olympic AI Agenda for the Olympic Movement.
Is the use of this Trustworthy AI Checklist a requirement to proceed with using an AI system or application?	Use of this Trustworthy AI Checklist is not mandatory. However, its use is strongly encouraged in order to effectively manage AI risks and implement the appropriate controls, ensuring that an AI system or application is and remains trustworthy.
Is this Trustworthy AI Checklist a legal compliance tool?	No. It is a guide for responsible AI development. It should be used alongside your legal and compliance efforts, not as a replacement for them.
Who should complete this Trustworthy AI Checklist?	It should be completed by the AI project lead, product owner or designated responsible individual and/or team in collaboration with technical, legal, risk and business stakeholders.
When should this Trustworthy AI Checklist be completed?	The Inherent Risk Assessment section should be done early in the AI lifecycle, ideally during ideation or planning. The full Core AI Checklist should be completed before deployment, and should be updated regularly.
Is there any supporting theory to complement the Trustworthy AI Checklist?	The Trustworthy AI Framework for the Olympic Movement contains the statement, rationale and key guardrails for all seven Trustworthy AI Principles. Additionally, refer to the Supporting Documents tab in the Trustworthy AI Checklist for further reading on each Trustworthy AI Principle.
What does “Select...” mean for the answers?	“Select” indicates a dropdown menu for answer selection. The answers are usually “Yes”, “No” or “N/A”, or other question-specific choices.
Can I select multiple options in the dropdown menus of the Trustworthy AI Checklist?	No, you cannot select multiple options from the dropdown menus. If more than one option is relevant, please choose the one that is most applicable to your AI system or application in order to obtain the most accurate Inherent Risk Rating.
What is the “Inherent Risk Rating” and how is it determined?	The Inherent Risk Rating provides a preliminary risk profile based on your responses to the initial risk questions before mitigation controls are considered.
What if I am unsure and don’t know the answer to a question?	If you are unsure, please consult with colleagues or experts who might have the answer. Only use “N/A” if a question truly is not applicable.
Are the provided examples for questions exhaustive?	The examples provided in the Trustworthy AI Checklist questions are non-exhaustive, as laws and regulations vary across different countries. Users should consider additional requirements specific to their local legal and regulatory context.
What happens after I complete the Trustworthy AI Checklist?	It generates recommendations, highlights control areas, and suggests next actions for risk management and governance.

FAQS

INHERENT RISK ASSESSMENT

QUESTION	ANSWER
What if my AI system or application is considered “High Risk” by the Inherent Risk Rating?	A “High Risk” rating is not a stop sign. It simply highlights important areas that need your attention. By completing the Core AI Checklist, you’ll find crucial guidance and actionable steps to address these risks responsibly and build a trustworthy AI solution.
Why should I complete the full Core AI Checklist if my risk is “Minimal”?	Even with minimal inherent risk, completing the full Trustworthy AI Checklist ensures a comprehensive review, helps build trust, and prevents overlooking risks or missing valuable guidance for your AI system or application.
What is “Personal Identifiable Information (PII)”?	PII is data that can be used to identify individuals directly, such as names, addresses or ID numbers, or indirectly, via combinations such as birthdates and genders.
What constitutes “Physical and Psychological Harm” in AI?	Any negative impact on physical safety or well-being. “Physical harm” is linked to some sort of physical system (e.g. drones). “Psychological harm” is when distress is caused by AI outcomes.
What is considered a “Significant Impact” by an AI system or application?	“Significant Impact” refers to AI-driven decisions or actions that materially affect rights, opportunities (such as employment or credit) or access to essential services.
Who are “Vulnerable Groups”?	“Vulnerable Groups” are populations more at risk from harm or discrimination, such as children, the elderly, refugees, people with disabilities or socioeconomically disadvantaged groups.
What are “Critical Operations and Public Security” AI applications?	This term refers to AI used for public safety and infrastructure, such as event security, energy, emergency response, broadcast, law enforcement and medical care.

FAQS

TRUSTWORTHY AI STATUS

QUESTION	ANSWER
Accountability Questions	
What does “Clear Ownership” (ID 1) entail?	“Clear Ownership” means assigning responsibility for the outputs of an AI system or application to a person or committee, defining roles across the lifecycle and keeping ownership up to date.
Why define accountability at each AI lifecycle stage (ID 1.2)?	Accountability ensures someone is always responsible for decisions/outcomes at every phase, supporting oversight and incident response.
Human Oversight Questions	
What is “Human Oversight” (ID 2)?	“Human Oversight” refers to the capacity for humans to review, intervene or override AI decisions through defined oversight rules and accountability.
When should human oversight or intervention apply (ID 2.2)?	Human oversight is generally recommended for all AI systems and applications. The level and type of oversight (e.g. monitoring, review, intervention) should be applied especially in high-stakes or significant scenarios, or when reliability, fairness or ethical/legal concerns could be compromised.
Third Parties Questions	
Why is it important to identify and document all third-party components (ID 3.2)?	It allows you to assess supply chain risk and ensure compliance, privacy, security and contractual safeguards.
What should I consider when evaluating third-party providers (ID 3.3)?	You should review compliance with laws, privacy practices, security, and ethical commitments.
Robustness and Reliability Questions	
What is the difference between “Robust Performance” (ID 4) and “Reliable Performance” (ID 5)?	“Robustness” refers to withstanding varied/unexpected conditions. “Reliability” means producing accurate outputs with relevant data.
What is “Data Drift” (ID 4.3)?	“Data Drift” refers to model performance loss due to shifting input data distribution. Monitoring reveals the need for adaptation or retraining.
What does “Equitable Performance” (ID 11.3) mean?	AI should yield fair, unbiased results across all demographic groups.
Testing and Validation Questions	
What is “TEVV” (ID 6)?	“TEVV” is short for “Testing, Evaluation, Validation, Verification” – a set of processes designed to ensure requirements and fairness are met before deployment.
Why test AI across environments, geographies, and groups (ID 6.2)?	Testing helps to ensure that AI performs fairly and consistently in all relevant contexts and populations.

FAQS

TRUSTWORTHY AI STATUS

QUESTION	ANSWER
Transparency and Explainability Questions	
What does “Disclosure” (ID 7) mean?	“Disclosure” means informing users about AI involvement, its purpose, its reasoning and its limitations/biases in understandable terms.
Why should I explain AI outputs to non-technical users (ID 7.3)?	Explanations build trust, enable understanding and support informed decision-making by users.
What kind of “Documentation” (ID 8) is expected?	All functional, technical and process aspects, including purpose, incidents, and decision trails – explained plainly for auditability.
Feedback and Contestability Questions	
What are “Feedback and Contestability” mechanisms (ID 9)?	“Feedback and Contestability” mechanisms are channels for users to provide feedback on or contest AI outcomes.
Why must stakeholder feedback be regularly actioned (ID 9.3)?	Responsiveness improves solutions, builds trust and resolves emerging issues.
Fairness and Impartiality Questions	
What is “Unwanted Bias” (ID 10.1) in AI?	“Unwanted Bias” is unfair discrimination due to data, algorithms or AI deployment methods.
Is all AI bias “Unwanted” (ID 10.1)?	Not necessarily. While unwanted bias leads to unfair discrimination, AI can also have intended differentiation – when the AI system or application is designed to differentiate based on relevant and justified factors (e.g. personalising recommendations, creating specific performance metrics, etc) to provide beneficial outcomes.
What does “Diverse and Representative” training data (ID 11.2) mean?	“Diverse and Representative” training data means that AI is trained on real-world, demographically diverse data sets.
Legal and Regulatory Questions	
What is the “EU AI Act” (ID 12.4) and what is its relevance?	The European Union (EU) AI Act is a landmark regulation classifying AI systems and applications by risk and setting rules for their development and use. It is highly relevant as a globally influential standard and provides a strong basis for understanding high-risk AI.
I am not from the EU, so why should I worry about the EU AI Act?	Even if you’re outside the EU, the EU AI Act can influence international standards, affect your supply chain, or apply to you if your AI system or application interacts with EU citizens.
What are “Data Subject Rights” (ID 12.3)?	“Data Subject Rights” include data access, correction, deletion, restriction, portability and objection to processing.

FAQS

TRUSTWORTHY AI STATUS

QUESTION	ANSWER
Data Retention and Privacy Questions	
What should a “Data Retention Policy” (ID 13.1) include?	Such a policy should include clearly set data retention durations, deletion/anonymisation procedures and data compliance rationale.
Why is data consent important (ID 13.2)?	Consent is fundamental for data privacy and lawful, transparent handling.
What is a “Lawful Basis” for data processing (ID 14.2)?	A “Lawful Basis” means that legitimate reasons for data use, such as consent or contract, must be defined and documented.
Safe and Secure Questions	
What “Security Risks” (ID 15.1) must AI systems or applications consider?	AI systems or applications must consider data breaches, model poisoning, adversarial attacks, illicit access, intellectual property (IP) theft, etc. Refer to the Supporting Documents sheet of the Trustworthy AI Checklist.
What are “Safety Risks” (ID 16.1) in AI?	“Safety Risks” refers to physical, psychological or societal harm caused by AI malfunction, error or bias.
Responsibility and Social Impact Questions	
What is the “Social Impact” (ID 17.1) of AI?	“Social Impact” refers to AI’s effects on people, communities and society – employment, rights, culture and perceptions.
What does “Respect Human Rights” (ID 17.4) mean for AI?	It means that AI must not violate privacy, must be non-discriminative and must not infringe any other fundamental rights.
Sustainability and Maintenance Questions	
What does “Sustainability” (ID 18.3) encompass?	“Sustainability” refers to minimising environmental impact, using resources efficiently, and remaining legally and ethically up to date.
Why design AI for “Easy Maintenance and Updates” (ID 18.2)?	Maintenance and updates ensure the AI system or application remains effective, accurate and adaptable to changing contexts over time.

THANK YOU