INTERPOL

unicri
United Nations
Interregional Crime and Justice
Research Institute

RESPONSIBLE
AI INNOVATION IN
LAW ENFORCEMENT
AI Toolkit

# Risk Assessment Questionnaire

Funded by
the European Union

INTERPOL

United Nations
Interregional Crime and Justice
Research Institute

Funded by
the European Union

# DISCLAIMER

The contents of this document are for information purposes only. INTERPOL and UNICRI assume no liability or responsibility for any inaccurate or incomplete information, nor for any actions taken in reliancethereon. The published material is distributed without warranty of anykind, either express or implied, and the responsibility for the interpretation and use of the material lies with the reader. In no event shall, INTERPOL or UNICRI be liable for damages arising from its use.

INTERPOL and UNICRI take no responsibility for the content of any external website referenced in this publication or for any defamatory, offensive or misleading information which might be contained on these third-party websites. Any links to external websites do not constitute anendorsement by INTERPOL or UNICRI, and are only provided as a convenience. It is the responsibility of the reader to evaluate the content and usefulness of information obtained from other sites.

The views, thoughts and opinions expressed in the content of thispublication belong solely to the authors and do not necessarily reflect the views or policies of INTERPOL or the United Nations, their member countries or member states, their governing bodies, or contributory organizations, nor does it imply any endorsement. Therefore, INTERPOL and UNICRI carry no responsibility for the opinions expressed in this publication.

INTERPOL and UNICRI do not endorse or recommend any product, process, or service. Therefore, mention of any products, processes, or services in this document cannot be construed as an endorsement or recommendation by INTERPOL or UNICRI.

The designation employed and presentation of the material in this document do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations, UNICRI or INTERPOL, concerning the legal status of any country, territory, city or area of its authorities, or concerning the delimitation of its frontiers or boundaries.

The contents of this document may be quoted or reproduced, provided that the source of information is acknowledged. INTERPOL and UNICRI would like to receive a copy of the document in which this publication is used or quoted.

# OVERVIEW

## What

The Risk Assessment is intended to support law enforcement agencies to evaluate the risks an AI system may pose, from a responsible AI innovation perspective. More specifically, it supports law enforcement agencies with identifying the potential adverse impacts on individuals, groups, and society as a whole, as well as the probability of such impacts occurring. An important part of the Risk Assessment is identifying and assessing the organizational, technical and security measures established as part of the design, development, procurement, deployment or use of the AI system. This will help agencies to assess the likelihood of unintended impacts, highlight risk levels, and provide an overview of the risks connected to the use of the AI system.

---

## When

It is recommended that this Risk Assessment should be used early in the design and development phases and when testing and evaluating an AI system. Beyond these defined periods, agencies may also benefit from running the Risk Assessment periodically over the course of an AI system's lifecycle, in order to make the best possible use of the insights it provides. For instance, the Risk Assessment can be helpful for decision-makers when de-terming whether to approve, change, or decommission an AI system, when handling residual risks, or as a tool to raise awareness among users of the adverse impacts of an AI system.

---

## Who

The Risk Assessment is designed to be completed by the team or staff member(s) within the law enforcement agency who are in charge of the overall AI project or a specific stage within the AI life cycle.

# TABLE of CONTENTS

# 1. Before You Start

Practicing responsible AI Innovation involves identifying and understanding the potential weaknesses and threats that may emerge during the AI innovation journey. It also involves taking informed action to prevent and mitigate such weaknesses and threats, all in accordance with the *Principles for Responsible AI Innovation*. These activities should be part of a law enforcement agency's broader risk management process, which should be defined and implemented at an organization-wide level.

- *LEARN MORE ABOUT RISK MANAGEMENT AND ITS IMPORTANCE IN THE* ORGANIZATIONAL ROADMAP.

An accurate assessment of the risks of the AI system that the law enforcement agency intends to use is a crucial step in this process.

This Risk Assessment will support you and your agency in this regard by aiding you to detect and evaluate the risks to individuals and communities that may emerge over the course of the lifecycle of an AI system that is used or intended for use in your agency.

Conducting this Risk Assessment can be considered a precondition for agencies if they are to appropriately and adequately develop strategies to prevent and mitigate the risks posed by an AI system; identify and implement the responses to such risks, including mitigation measures; and prioritize limited resources when responding to situations with different risk levels.

# 2. The Scope of this Risk Assessment

While there are different kinds of risk assessment that cover various types of risk – such as information and cybersecurity risks, reputational and financial risks, and data protection or human rights risks– this Risk Assessment focuses exclusively on the negative consequences for individuals and communities should the *Principles for Responsible AI Innovation* not be adhered to for any particular AI system used or intended for use by an agency. This Risk Assessment is not meant to replace any of these other kinds of risk assessment; neither has it been designed to incorporate these other kinds of assessment. Rather, it is intended to complement existing risk assessment practices that law enforcement agencies already carry out or are required to carry out under the applicable law.

# 3. Instructions

This Risk Assessment contains questions that concern:

- the likelihood of certain negative events or circumstances occurring.
- the impact of such events or circumstances on individuals and communities should they occur.

These questions draw on the *Principles for Responsible AI Innovation,* particularly the core principles of minimization of harm, human autonomy, and fairness, and the corresponding instrumental principles. The principle of good governance is addressed on two separate occasions. First, the extent to which law enforcement agencies follow the principle of good governance may influence the likelihood and/or the impact of a certain event. For example, ensuring the traceability of the decisions taken during the design and development of the AI

system increases the chances of identifying harmful human biases in the system, thus allowing for their early prevention. Second, the principle of good governance guides agencies and personnel in the identification and implementation of mitigation measures.

The Risk Assessment process includes a total of five steps, all of which are interconnected and will contribute to the overall effectiveness of the assessment. These steps include (1) Preparing, (2) Assessing, (3) Interpreting the results, (4) Communicating and (5) Maintaining.[1]

## STEP 1: Preparing for the Risk Assessment

Prior to conducting the Risk Assessment, it is important to first examine and fully understand the situation as a whole. To this end, you should endeavour to prepare answers to the following questions:

1. At what stage of the AI life cycle will the Risk Assessment be performed? What timeframe will it cover?

2. What are the potential limitations of the Risk Assessment? Which other types of risk assessments could provide additional information?

3. What sources of information will you be using to fill in the Risk Assessment? Are they sufficient or do you need access to certain other information? How can you gain access to this information?

4. What are the foreseen or observed weaknesses regarding the implementation of the Principles for Responsible AI Innovation? *Refer to the results of the "Principles in Action" exercise(s) in the* Responsible AI Innovation in Action Workbook.

5. What are the stakeholders of the AI system's implementation? *Refer to the results of the "Stakeholder Engagement" exercise(s) in the* Responsible AI Innovation in Action Work-book.

6. What is the context and mode of acquisition for the AI system? *Refer to the results of the "Gaps & Needs Analysis", "Value Mapping" and "Deciding how to get the AI System" exercises in the* Responsible AI Innovation in Action Workbook.

7. What is the AI system use case to be assessed? *Refer to the results of the "Use case analysis" exercise in the* Responsible AI Innovation in Action Workbook.

8. How could the AI system be misused or accessed by unauthorized users and what would be the consequences of that? *Refer to the results of the "Identifying possible misuses or unauthorized uses" exercise in the* Responsible AI Innovation in Action Workbook *and any information and cybersecurity risk assessment or similar risk assessments carried out in our agency.*

9. What possible negative impacts on human rights may result from the use of the AI system? *Refer to the results of the human rights impact assessment carried out in relation to the AI system*

## STEP 2: Filling out the Risk Assessment Questionnaire

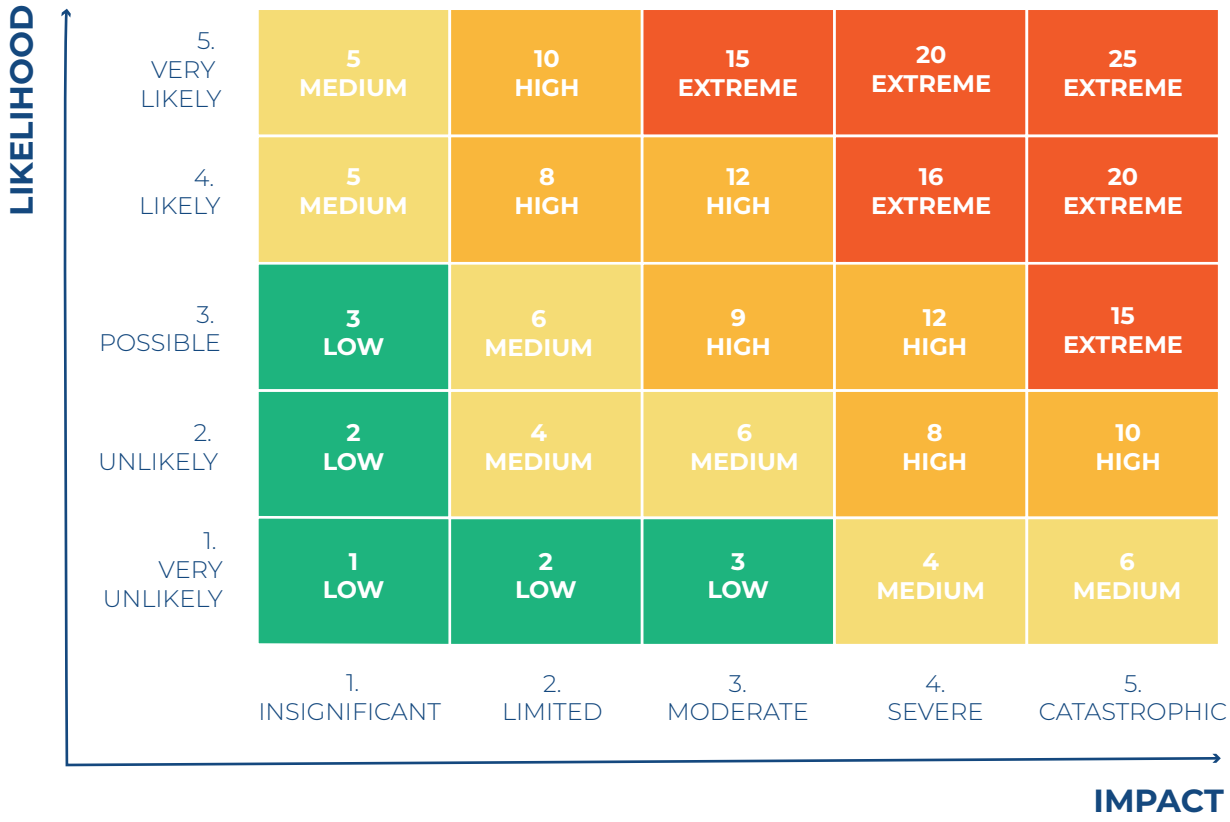
To conduct the Risk Assessment, you should complete the questionnaire below. This questionnaire is to be completed by the team or staff member(s) within the law enforcement agency who are in charge of the AI project or a specific stage within the AI life cycle. It may require consultation with other relevant internal or external parties who have the necessary knowledge and understanding of the potential risks of the AI system.

The Risk Assessment questionnaire is structured around two main categories: impact and likelihood. A score of 1 to 5 should be assigned to each of the questions provided under each of these two categories. Once all of the questions have been answered and scored, the respondent will be able to calculate the overall risk score by multiplying the impact score by the likelihood score for each risk (Risk Score = Impact x Likelihood). The risk score offers a quantitative measure of the risk level, thus enabling the law enforcement agency to understand specific risks which may undermine the Principles for Responsible AI Innovation.

ANNEX A contains a glossary of key terms used in the Risk Assessment Questionnaire.

## STEP 3: Interpreting the Results

Having determined the risk score, a risk level – classified as low, medium, high or extreme risk – can then be determined. The risk level demonstrates the extent or magnitude of a par-




ticular risk. Identifying the risk level can be helpful in communicating the results of the self-assessment. The risk matrix below may help with this exercise.

The table below indicates the scores that correspond to each risk level and provides a general interpretation of each.

| | SCORE RANGE | INTERPRETATION |
|---|---|---|
| **LOW RISK** | **1 to 3** | The likelihood of the event occurring is very low and/or, if it does occur, the impact on individuals and communities from a human rights and ethics perspective will be minimal. This may include AI systems that produce minor inaccuracies or when its use leads to temporary disruption of non-critical services. Despite being classified as low, these risks should still be managed and prevented or mitigated where possible. |

| | | |
|---|---|---|
| **MEDIUM RISK** | **4 to 6** | The likelihood of the event occurring is low, or, if there is a higher likelihood, the impact if it does occur will not be severe. This could involve cases such as unintentional bias in non-critical decision-making processes that do not lead to significant harm. These risks require more active management and planning to mitigate. |
| **HIGH RISK** | **8 to 12** | The event is likely to occur, or the impact if it does occur will be severe. This could include cases such as significant biases in critical decision-making processes or privacy violations that lead to serious harm. These risks require immediate attention and robust mitigation strategies. |
| **EXTREME RISK** | **15 to 25** | The risk is almost certain to occur, or the impact if it does occur will be extremely severe or catastrophic. This could involve cases such as widespread violations of human rights or other serious harm to individuals. These risks require urgent, comprehensive action, including redesigning or discontinuing the AI system. |

## STEP 4: Communicating the Results

Once the results have been obtained and interpreted, they should be conveyed to the relevant risk owner – the individual(s) or team(s) with the authority and accountability to administer and/or respond to the risks. This communication should include the risk score and a detailed explanation of the findings of the assessment, combined with the information gathered during the preparation phase. The risk owner should use all the relevant information to formulate an effective risk mitigation strategy, in collaboration with the individual or team responsible for the AI system at the stage in question.

The parties involved in this step can use the “Risk Response” exercise in the Responsible AI Innovation in Action Workbook to communicate the results of the Risk Assessment and outline the risk response.

## STEP 5: Repeating the Risk Assessment

The risk assessment process for an AI system is iterative. The Risk Assessment should be repeated over time, allowing for the continuous maintenance, monitoring and reevaluation of risks as circumstances evolve. There are two main circumstances under which the Risk Assessment should be repeated:

1. **Risk Reassessment Post Mitigation:** It is recommended that the Risk Assessment should be carried out again after mitigation measures have been implemented. This serves to assess whether these measures have effectively modified the risk level. If the risk level remains high, further measures may need to be taken. If the risk level is reduced, the measures may need to be maintained or adjusted accordingly.

2. **Periodic and Needs-based Assessment:** Given the highly dynamic nature of AI technology and its broad scope of application, the Risk Assessment process should be conducted periodically and as and when necessary. This is especially crucial when any risk-modifying factors have been identified. These factors can include the integration of new mitigation measures, changes in the technical components of the AI system, alterations in its operating environment, and the introduction of new stakeholders, among others.

These changes can significantly impact the risk profile of the AI system, necessitating a reevaluation of the associated risks.

The parties involved in this step can use the "Risk Response" and "Risk Monitoring" exercises in the Responsible AI Innovation in Action Workbook to help analyze and monitor the response to the AI system's risks.

# 4. Risk Assessment Questionnaire

| LIKELIHOOD (A)<br>1 – Very Unlikely; 2 – Unlikely; 3 – Possible; 4 – Likely; 5 – Very likely | | IMPACT (B)<br>1 – Insignificant; 2 – Limited; 3 – Moderate; 4 – Severe; 5 - Catastrophic | | RISK LEVEL (AxB) | RISK OWNER | OBSERVATIONS |
|---|---|---|---|---|---|---|
| 1. What is the likelihood that activities related to the AI system will lead to non-compliance with applicable laws and regulations?* | | How serious would the negative impact of such non-compliance be on individuals and communities? * | | | | |

** This question focuses on the threat to individuals and communities posed by a possible lack of compliance, and should not in any way be interpreted as overriding the core principle of lawfulness. Law enforcement agencies and personnel should, of course, not perform any activities that breach applicable laws and regulations.*

*Answering this question will require consultation with internal or external legal experts who are able to conduct a careful analysis of the legal and regulatory compliance risks. Before answering this question, it is important that agencies carry out a human rights impact as-sessment or an equivalent process in which the potential impact on human rights in relation to the AI system is identified, assessed and addressed.*

| | | | | | | |
|---|---|---|---|---|---|---|
| 2. How likely is it that vulnerabilities in the AI system's robustness will result in harm to individuals or communities? | | How serious would such harm be? | | | | |
| 3. How likely is it that vulnerabilities in the AI system's safety will result in harm to individu-als or communities? | | How serious would such harm be? | | | | |
| 4. How likely is it that inaccuracies in the AI system will result in harm to individuals or communities? | | How serious would such harm be? | | | | |
| 5. How likely is it that the use or misuse of the AI system will adversely affect the physical or psychological well-being of individuals or communities? | | How serious would such adverse effects be? | | | | |
| 6. How likely is it that the use or misuse of the AI system will adversely affect environmental welfare? | | How serious would such adverse effects be? | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7. How likely is it that excessive costs of implementing the AI system in terms of time, money, human effort and environmental impact will result in harm to individuals or communities? | | How serious would such harm be? | | | | |
| 8. How likely is it that limitations in the ability of humans to exercise control and oversight of the AI system will result in harm to individuals or communities? | | How serious would such harm be? | | | | |
| 9. How likely is it that the use or misuse of the AI system will limit users' ability to reach decisions independently? | | How serious would such limitations be? | | | | |
| 10. How likely is it that the type and amount of data used to train the AI system will have an impact on the privacy of individuals and their right to have control over their data? | | How serious would such an impact be? | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 11. How likely is it that the type and amount of data collected, stored and transmitted by the AI system will have an impact on the privacy of individuals and their right to have control over their data? | | How serious would such an impact be? | | | | |
| 12. How likely is it that the use or misuse of the AI system will interfere with individuals' private sphere and their capacity to self-govern? | | How serious would such interference be? | | | | |
| 13. How likely is it that a lack of knowledge of the AI system and its risks and limitations among its users will result in harm to individuals or communities? | | How serious would such harm be? | | | | |
| 14. How likely is it that an absence of public awareness that the AI system is being used will result in harm to individuals or communities? | | How serious would such harm be? | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 15. How likely is it that the inability of users and/or people affected by the use of the AI system to understand how and why the AI system has reached a particular outcome will result in harm to individuals or communities? | | How serious would such harm be? | | | | |
| 16. How likely is it that training the AI system using data of insufficient quantity or quality (for example, data with a lack of representation) will create or exacerbate inequalities or lead to discrimination? | | How serious would such an impact on equality and non-discrimination be? | | | | |
| 17. How likely is it that human biases reflected in the design and development of the AI system will have a disproportionate impact on certain individuals or groups? | | How serious would such an impact be? | | | | |
| 18. How likely is it that an insufficient consideration of and engagement with vulnerable groups throughout the AI life cycle will create or exacerbate the conditions that contribute to the vulnerability of such groups? | | How serious would such an impact be? | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 19. How likely is it that the use or misuse of the AI system will have a disproportionate impact on vulnerable groups? | | How serious would such an impact be? | | | | |
| 20. How likely is it that the use or misuse of the AI system will create or exacerbate inequalities or lead to discrimination? | | How serious would such an impact on equality and non-discrimination be? | | | | |
| 21. How likely is it that an insufficient consideration of different human characteristics and abilities during the AI system's design, development or deployment will create or exacerbate disadvantages for certain individuals or groups? | | How serious would such disadvantages be? | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 22. How likely is it that a lack of technological and/or organizational measures to allow AI system's users to challenge its outputs will have a negative impact on individuals or communities? | | How serious would such adverse effects be? | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 23. How likely is it that a lack of technological and/or organizational measures to allow the people affected by the use of the AI system to challenge its outputs will have a negative impact on individuals or communities? | | How serious would such adverse effects be? | | | | |
| 24. How likely is it that insufficient access to redress for those who suffer negative effects as a result of the use of the AI system will have a negative impact on individuals or communities? | | How serious would such adverse effects be? | | | | |

# ANNEX
# Glossary of Key Terms[2]

### Risk assessment

A risk assessment is the process within risk management that is designed to identify and evaluate the risks to individuals and communities that may emerge during the life cycle of a specific AI system.

### Risk

A risk consists of a threat to individuals and communities posed by potential circumstances and events related to the AI system that may arise at any stage of the life cycle. These are circumstances and events that have not yet occurred: they are hypothetical scenarios, to be used where there is un-certainty surrounding the effects of implementing a certain AI system for a particular use case.

In this Risk Assessment, the risk level is calculated using the following formula:

*Risk Level = Likelihood x Impact*

This formula gives us the risk level as a function of the probability of an occurrence (the likelihood) and the severity of the consequences of that occur-rence (the impact).

### Risk owner

The risk owner is the entity or individual within the law enforcement agency with the authority and accountability to administer and/or respond to a risk.

### Mitigation measures

Mitigation measures are any processes, policies, practices, or devices intended to decrease the risk level by: (1) decreasing the probability and/or se-verity of the impact of a particular event or situation; or (2) eliminating the source of the risk. It is important to acknowledge that these mitigation measures may not always succeed in reducing the risk level as intended, due to unforeseen events or insufficient understanding of the risks in ques-tion.

### Likelihood

Likelihood refers to the probability of a certain circumstance or event occurring. In this Risk Assessment, likelihood is defined on a scale of 1 to 5, cor-responding to the following:

1. Very Unlikely: There is a very low chance that the circumstance or event will occur. It would only happen under exceptional circumstances or in rare cases. This level generally corresponds to risks that, while possible, are considered negligible.

2. Unlikely: The circumstance or event is not expected to occur frequently or in the normal course of events. This level generally corre-sponds to occurrences that, while no longer considered negligible, are unusual or uncommon.

3. Possible: There is a fair chance the circumstance or event will occur. It may happen occa-sionally, and may be triggered by certain condi-tions, but it is not something that is ex-pected to happen consistently or frequently.

4. Likely: The circumstance or event is expected to occur frequently or in the normal course of events. It may not happen every time, but there is a substantial probability that it will occur.

5. Very likely: The circumstance or event is almost certain to occur. It is expected to happen most of the time, barring exceptional circum-stances that prevent it.

**Impact**

Impact refers to the severity of the potential harm or negative effect that the circumstance or event would have on individuals and communities if it oc-curred. For the purposes of this Risk Assessment, "individuals and communities" refers to any stakeholder that may be affected by the use of the AI system.

- *LEARN MORE ABOUT HOW TO IDENTIFY THE STAKEHOLDERS IN THE PRINCIPLES FOR RESPONSIBLE AI INNOVATION AND IN THE RESPONSIBLE AI INNOVATION IN ACTION WORKBOOK.*

1. Insignificant: If the circumstance or event were to occur, it would have minimal or no real impact on individuals or communities. It may cause slight inconvenience or minor dis-ruption, but it would not lead to substantial damage or harm.

2. Limited: If the circumstance or event were to occur, it would cause some disruption or damage, but the effects would be relatively con-tained and manageable. It might lead to a temporary setback or require some effort to correct, but it would not cause long-term or widespread harm.

3. Moderate: If the circumstance or event were to occur, it would cause a significant level of disruption or harm. This could involve substantial loss of resources or major incon-veniences. However, recovery would be relatively straightforward given the right correc-tive ac-tion.

4. Severe: If the circumstance or event were to occur, it would lead to serious harm or dis-ruption. This could involve major losses, significant harm to individuals, severe damage to society or the environment, or considerable legal or ethical implications. Recovery could be difficult, costly, or time-consuming.

# REFERENCES

1 National Institute of Standards and Technology. (2012). Guide for Conducting Risk Assessments (NIST Special Publication (SP) 800-30 Rev. 1). Ac-cessible at https://doi.org/10.6028/NIST.SP.800-30r1

2 International Organization for Standardization. (2009). ISO Guide 73, Risk management—Vocabulary. Accessible at https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

How to cite this publication: UNICRI and INTERPOL. (June 2023). Toolkit for Responsible AI Innovation in Law Enforcement: Risk Assessment Questionnaire

www.interpol.int
www.unicri.it

INTERPOL_HQ

@INTERPOL_HQ
@UNICRI

INTERPOL HQ
UNICRI

INTERPOL
UNICRI

@INTERPOL
@UNICRIHQ