INTERPOL

unicri
United Nations
Interregional Crime and Justice
Research Institute

RESPONSIBLE AI INNOVATION IN LAW ENFORCEMENT

AI Toolkit

Organizational Roadmap

Funded by the European Union

REVISED FEBRUARY 2024

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 reliance thereon. The published material is distributed without warranty of any kind, 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 an endorsement 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 this publication belong solely to the authors and do not necessarily reflect the views or policies of, nor do they imply any endorsement by, INTERPOL or the United Nations, their member countries or member states, their governing bodies, or contributory organizations. 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 Organizational Roadmap for responsible AI innovation provides an overview of and guidance on the organizational components that are required to apply the Principles for Responsible AI Innovation. The goal of this document is to support agencies to better understand the organizational components necessary for responsible AI, and to move toward organizational readiness.

WHEN

The Organizational Roadmap, as well as the associated Organizational Readiness Assessment Questionnaire, are designed to be consulted at the start of a law enforcement agency's journey towards responsible AI innovation. It may also help agencies that have already completed an Organizational Readiness Assessment Questionnaire to advance to the next stage of responsible AI maturity or readiness.

WHO

The Organizational Roadmap is designed to support the strategic side of a law enforcement agency. The intended users consequently include chiefs of police and executive leadership, as well as decision-makers in senior management positions outside the executive leadership, particularly those in technology and innovation units responsible for the use of AI systems. It may also be of more general interest to other stakeholders in a law enforcement agency's AI community.

Table of Contents

Building blocks for responsible AI innovation

Responsible AI innovation requires a particular organizational culture, people and expertise, and processes to be in place. These three components are the building blocks for responsible AI innovation in a law enforcement agency and, together, they position agencies to be able to implement the right measures, such as ensuring respect for human rights throughout their engagement with AI systems, being sensitive to changes in laws and regulations and ready to adapt to them, and using high quality de-biased data sets when developing AI systems.

In this document, we will explore these three components from the perspective of the information a chief of police and their executive leadership should have in order to take action to set their agency on a course towards responsible AI innovation and facilitate the implementation of the Principles for Responsible AI Innovation.

First, organizational culture. A major part of an organization's readiness to realize responsible AI innovation is its organizational culture and the way day-to-day incentives are set up to drive innovation in general. Organizational readiness therefore starts with organizational culture and we will look at how chiefs of police and executive leadership can shape the goals, processes, expertise, infrastructure, steps/milestones, and desired outcomes needed to foster a culture of responsible AI innovation in their agencies.

Second, people and expertise. Building on organizational culture, we will then examine the type of expertise required to make responsible AI innovation a reality and identify the key individuals within a law enforcement agency that should have such expertise and the kind of activities in which they should be involved.

Third, processes. With a view toward bringing all the elements together, we will finally identify and examine some of the main processes and initiatives that chiefs of police and executive leadership in a law enforcement agency should mandate into action to begin the process of getting organizationally ready to implement responsible AI innovation, as well the specific activities, people and expertise that should typically be involved in this process.

Organizational culture

WANT TO LEARN MORE?

See the "Developing a Responsible AI Strategy for your Agency" section in the annex.

The organizational culture of a law enforcement agency can be understood as the values, objectives, attitudes, and practices shared within the agency, which shape both the internal interactions between its personnel and external interactions with the public. The chief of police and executive leadership play a critical role in defining this organizational culture and guiding the behaviour of and within an agency. By forging their vision for the agency, making critical and time-sensitive decisions, managing change, and establishing a line of effective communication among personnel, the chief of police and executive leadership's actions are essential to ensuring due diligence and ethical conduct, as well as building trust with the community.

The chief of police and executive leadership's vision is often intentionally manifested in an explicit strategy, policy or vision statement aimed at expressing the aspirations and goals of an agency. In the context of responsible AI innovation, chiefs of police and executive leadership in some agencies have taken to adopting a *responsible AI strategy* that guides responsible AI innovation practices for the agency as a whole. While adopting a responsible AI strategy can help give shape to a vision for responsible AI innovation and the organizational culture around it, having the right organizational culture is just as instrumental to the implementation of the agency's responsible AI strategy. As in any aspect of modern policing culture, a strong organizational culture that promotes responsible AI innovation involves both internal and external interactions. In other words, implementing responsible AI innovation requires law enforcement agencies to build a collaborative and transparent culture both internally with their personnel and externally with the public. It also requires an active awareness of the societal context and the role this plays in policing. It is therefore important that law enforcement agencies are agile in their engagement of AI systems, as needs across diverse cultural or regional landscapes may differ.

In this section, we will explore how the chief of police and executive leadership of an agency can lay the groundwork for an organizational culture that fosters responsible AI innovation. However, before we do so, it is important to understand the significance of the role of organizational culture in successfully practicing responsible AI innovation.

WHY THE FOCUS ON ORGANIZATIONAL CULTURE?

Law enforcement agencies that wish to successfully implement the ***Principles for Responsible AI Innovation*** can best achieve this if the culture of the agency itself embodies, reflects and demonstrates these principles. More broadly however, focusing on organizational culture from the perspective of responsible AI innovation is also closely linked to fostering public trust, which is an absolute prerequisite for law enforcement in any country to fulfil their functions and duties.

The way AI systems are used can affect the way the public perceives and receives their use in law enforcement. Law enforcement agencies are therefore well advised to operate with an organizational culture that prioritizes openness, communication and positive interactions around this topic, and to show a clear commitment to the prevention and reduction of harm and the respect for individual liberties and human rights. At the same time, the prevailing law enforcement culture in a country or region will also positively or negatively influence the agency's use of innovative technologies such as AI systems. Consequently, putting in place a strong organizational culture around responsible AI innovation will also contribute to an agency's work on maintaining and building public trust. A law enforcement agency with a general trust deficit might have a hard time ensuring public trust in its use of AI systems. |

THE RIGHT MINDSET

Now that we understand the 'why' of having an organizational culture of responsible AI innovation, we can start to look at 'how' to get there. In this section, we will explore some general advice for the chief of police and executive leadership to consider when deciding to approach the issue of responsible AI innovation.

- **One step at a time:** As will be seen over the course of this Organizational Roadmap, and throughout the AI Toolkit, responsible AI innovation is no small feat. It will be a long and difficult process, and it is important to realize that by its very nature there is unlikely to be an end-state where it is 'finished'. At the same time, this journey toward responsible AI innovation takes place in largely uncharted waters. It is important to understand this and to come to terms with the fact that it will not be possible to know everything about this field, and instead to forge connections –often externally – to bring in the right expertise.

- **Start with the 'why':** Incorporating AI systems in policing should not be a simple and straightforward decision. The process of coming to a decision to use AI systems should start with a critical self-assessment of the need for a particular AI system. Incorporating

AI systems into policing is also something that requires support from and engagement with diverse stakeholders: those that directly use or interact with the system, such as end-users from the various specialized units and development teams; those indirectly associated with its use, such as regulators and interest groups; and those affected by its use, such as the public. In a responsible AI innovation context, clear communication with internal staff and secondary stakeholders about the need and added value of developing, procuring, and using a specific AI system is key. For the latter, open communication or even public consultation will help to build trust and cooperation by providing a sense of inclusion in law enforcement decisions and an implicit promise to deliver new or better services. For internal communication to relevant staff, the value and need of the specific AI system should be clearly communicated, most notably the way it will improve operational effectiveness and automate repetitive, mundane tasks that often take up a great deal of an officer's time. By starting with a critical reflection on the necessity of such systems, accountability and transparency measures can be designed to prevent excess and ensure respect for human rights is ingrained in the process.

- **Get familiar with the risks:** Introducing AI systems in a law enforcement context comes with its own set of risks. These risks are very much connected to the uncertainty surrounding the effects – both inside and outside the agency – of introducing AI systems. For instance, the introduction of AI systems may pose risks to the security and integrity of the agency's information systems, the agency's reputation and the trust of the public, its finances, the environment, social and political stability, the health and safety of both law enforcement personnel and individuals and the broader communities they serve, and so on. It is therefore important to be very familiar with the risks of AI systems in general, as well as the specific risks as they pertain to the applicable use case(s). In addition, it is important to ensure that the development and use of an AI system does not contravene existing legislation and that it is regularly checked to ensure it is up to date with legislative and regulatory changes. |► *Learn more about the risks of AI systems in the **Technical Reference Book** and about identifying the level or risk of an AI system to individuals and communities from the perspective of the Principles for Responsible AI Innovation in the **Risk Assessment Questionnaire**.*

- **Incentivize responsible innovation:** Incentives have long been considered an important way of realizing organizational change, including in policing, and their value in assisting an agency to transition smoothly toward a culture of responsible AI innovation should be carefully considered. Incentives can take many forms, such as recognition, leave or time off, the provision of equipment, and where appropriate they may even take the form of financial incentives. Highlighting the work of a unit or department on a specific

use case that manifests the agency's responsible AI innovation spirit, on social media for instance, may be another form of relatively "low cost-high impact" approaches to incentives. On the other hand, incentives can also take a more penal approach, with measures being taken against personnel, units or departments that do not comply with responsible AI innovation practices.

- **Be aware of the need for new institutional architecture:** Responsible AI innovation requires diverse people and expertise, as well as collaborative efforts at every level of the agency. Advancing responsible AI innovation will involve the onboarding of new expertise, (re-)assigning personnel to new tasks, as well as establishing partnerships with external stakeholders, particularly with industry, academia and civil society. It will also ideally entail the definition of new policies, such as a responsible AI strategy, standard operating procedures, and the establishment of new structures, such as a responsible AI innovation oversight committee. These elements will be discussed in further detail below, in the section on processes. While much of this may be substantively new, agencies should seek to leverage recent experiences to identify lessons learned and good practices from the establishment and institutionalization of data protection, information and cyber-security office/officers.

- **Be ready to commit resources:** Implementing new AI systems with a responsible approach in an organization will require certain resources. The development or procurement of the AI system will naturally entail upfront costs, but it is important to note that there may also be additional costs related to, for instance, the people and expertise required for its development and use, the training of end-users, the operation of an oversight committee, etc. This does however not always necessarily mean that additional funding needs to be identified or that new roles and positions need to be established. It could mean that the agency prioritizes certain responsible AI innovation tasks in pre-existing roles and positions, or re-allocates part of existing funds to responsible AI innovation initiatives. For example, a pre-existing ethics officer could be tasked with preforming some of the oversight activities or could even take the lead in putting together an independent responsible AI innovation oversight committee. Thus, while some extra resources will certainly be required, the shift to implementing responsible AI innovation in an agency does not always need to be prohibitively costly, if it makes good use of existing resources. This is especially true when an agency is taking its first steps on its journey toward responsible AI innovation.

- **Prepare for pushback:** Introducing the idea of responsible AI innovation and starting the process of implementing the necessary changes in an agency will be met with pushback. This could be because some staff perceive the introduction of AI systems as

requiring an additional layer of work – for instance, the need to upskill or obtain additional authorizations and submit additional documentation – and will therefore see it as a burden. The introduction of AI systems may also feed into individuals' fear of change or even of being monitored and watched by this new technology. Equally, introducing a new AI system for a particular unit will cause friction and will require time and patience, as the adoption of new technologies can often be a slow process. Deploying AI systems in law enforcement, particularly high-risk systems, is also likely to generate some degree of concern and require effective public engagement and stakeholder management. This engagement should ideally begin before the decision to proceed with the development or procurement of AI systems is made. While these pushbacks should not be seen as barriers, agencies should listen to the feedback, analyze it, and address it, as it can help refine an agency's strategy for the integration and eventual use of a new technology. |► *Learn more about how to identify and engage with stakeholders in the* ***Principles for Responsible AI Innovation*** *and in* ***Responsible AI Innovation in Action Workbook***.

- **Prepare to back down:** The decision to adopt a particular AI system within an agency should never be seen as a decision that cannot or should not ever be reversed. In fact, to effectively implement responsible AI innovation within a law enforcement agency, it is important to remember that a time may come when it is important to reflect on whether the AI system is of continued value or if the circumstances that allowed for its initial use have changed so as to make its use unlawful or undesirable. Should this occur, an agency should be ready (and have procedures in place) to halt, recalibrate, or even decommission the AI system. There are various circumstances that could bring about a decision such as this, including a change in legislation or pushback from the public regarding the use of a specific system. It is also important to have set metrics to determine the success of the system, and that continuous monitoring takes place to ensure that the use of the system continues to meet the overall law enforcement objective and that it is being used in accordance with the ***Principles for Responsible AI Innovation***. In the event that its performance does not meet the metrics set, the agency should be ready to halt, recalibrate, or even decommission the system. Metrics for the successful establishment of responsible AI innovation practices may include monitoring performance and reducing errors, control mechanisms, improving reporting and documentation, and the ability to carry out internal and external audits to improve accountability and, where applicable, raise concerns of explainability. |► *Learn more about this in* ***Responsible AI Innovation in Action Workbook***.

PRACTICAL EXAMPLE

Responding to Pushback from Officers on Body-Worn Cameras

The adoption and use of body-worn cameras (BWCs) demonstrates a classic challenge for law enforcement in the responsible use of AI systems, and the necessity for cultural change in operational practice by the organization and officers alike.

BWCs have been introduced in law enforcement agencies from North America to Europe, South Africa, Asia, and Oceania in response to reported cases of police brutality, malpractice, and police-involved deaths, and under mounting pressure from citizens, civil society groups, and policymakers to promote transparency and accountability. BWCs are often considered to be useful in restoring public trust in law enforcement agencies, especially ethnic minority communities and that their use by law enforcement officers can help reduce the number of complaints from citizens on the one hand, and misconduct and excessive use of force by the police on the other. While some studies have demonstrated this, others have found that BWCs can also contribute to increased tension between the police and the public.[1] In addition to the perceived benefits for increasing transparency and accountability, the use of BWCs can also help improve evidence collection. Notably, some BWCs have AI capabilities such as integrated facial recognition technology for the purposes of real-time facial recognition.[2]

Despite these perceived benefits of BWCs, their adoption has not been without pushback, with many officers arguing that the only purpose of having them was to "burn a cop" – in other words to expose officers to public scrutiny.[3] This often led to ineffective use of BWCs by officers, with many refusing to activate them while on duty. As a result, several different measures were implemented to promote the uptake of BWCs in policing, including:

- Internal policy and procedural changes to mandate their use.
- Legislative changes to mandate their use.
- Financial incentives to encourage officers to make routine use of BWCs.
- Disciplinary consequences for failure to make routine use of BWCs.

Available data as of 2016 estimated that about 47% of law enforcement agencies had acquired BWCs; for large law enforcement agencies, that number increased to 80%. Notably, 86% of law enforcement agencies that had acquired BWCs had also implemented a formal BWC policy.[4]

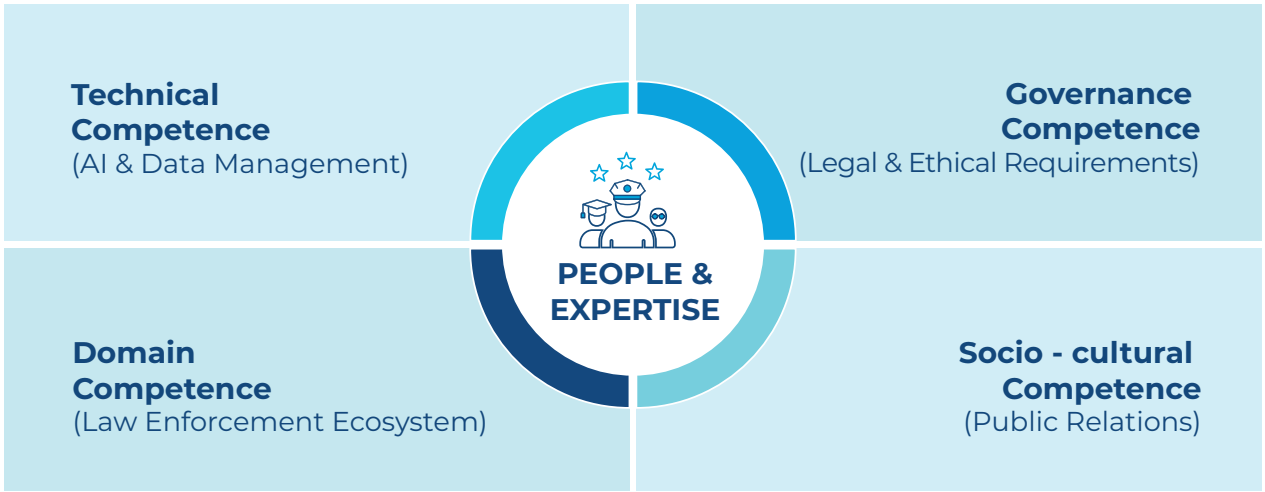
Analyzing the integration of BWCs into law enforcement shows that in cases where agencies did not sufficiently determine the 'why' and actively prepare for natural 'pushback' to the required cultural change, this change often generated conflict, both with internal and external stakeholders. However, in cases where agencies opted for a more informed, measured, and structured approach, officers and the public had a better understanding of the added value of BWCs, were less resistant to the cultural change, and more easily accommodated the transition.

One example of good practice that can also be seen with the adoption of BWCs was that when supported by a monitoring regime and active communication strategy to inform stakeholders, this also made it easier to understand the added value of the technology and facilitated cultural change.[5]

People and Expertise

In addition to having the right mindset, an agency needs the right people and expertise if it is to develop a responsible AI innovation culture and develop or procure and use AI systems responsibly. Indeed, just as AI systems cannot be developed without skilled AI scientists or engineers, the development and use of these systems in an ethical and human rights-compliant manner cannot be guaranteed without knowledgeable ethicists and human rights experts. Ensuring that an agency has access to the right people and expertise should be a priority for the chief of police and executive leadership, in conjunction with human resources teams. However, this is not a straightforward task, as many different types of people and expertise – both technical and non-technical– will be required at various stages, including some people and expertise with which law enforcement agencies may not be traditionally acquainted. While the nature of the competencies required will differ significantly, they can be broadly classified as follows:

- *Technical competencies*, consisting of the knowledge and skillset required to apply technical methods to solve a particular problem.
- *Domain competencies,* referring to competencies around policing, its role in society and the criminal justice system.
- *Governance competencies*, including competencies around human rights law and the ethical frameworks required to manage and implement AI systems responsibly.
- *Socio-cultural competencies,* referring to the competencies required to manage an agency's public engagement and build public trust with awareness of the social and cultural context.



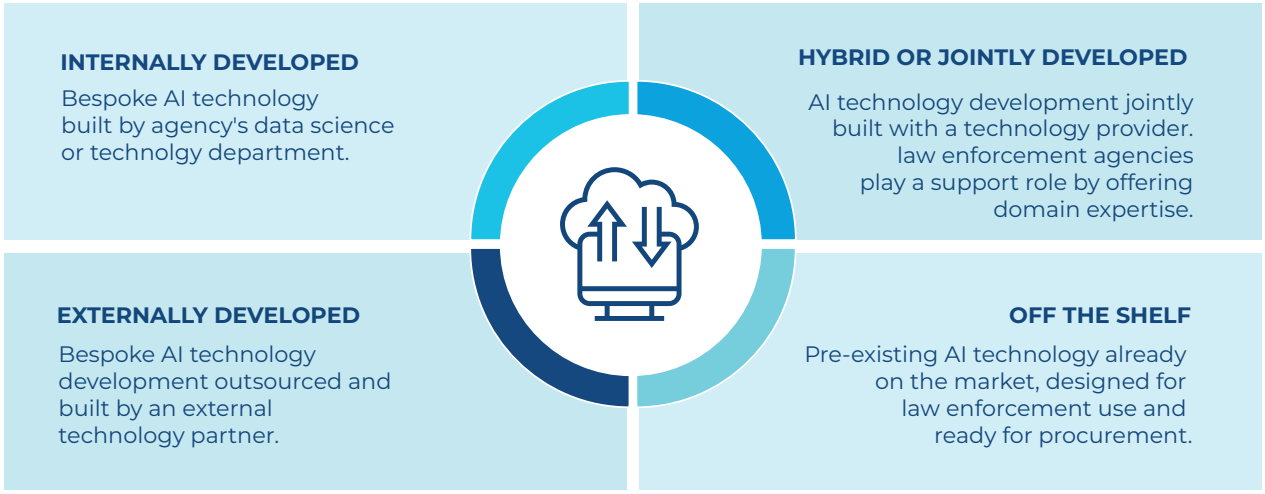
It is important to highlight that, aside from the AI system users who need to master the required technical and domain expertise, law enforcement agencies do not necessarily need to have in-house experts with all of these skill sets, as some may be outsourced. This is particularly the case for the technical development of the AI system. It may be sufficient for agencies to acquire the services or products of external experts through partnerships with academic institutions, private corporations, or even other government bodies. However, even when an AI system is procured externally, it is good practice for an agency to have some degree of internal technical knowledge and understanding. Another instance where these competencies may not necessarily be held in-house is when a responsible AI innovation oversight committee is established. This committee may be made up of external experts specializing in ethics, law, stakeholder management, public engagement, etc., ideally with a degree of independence compared with the regular structures of the agency. Given the nature of the role that such a committee plays, it may be advisable for the expertise to be located externally, although an agency may also opt to utilize and adapt an existing internal ethics oversight and accountability mechanism.

In addition to the four essential competency areas, it may be worth considering personal attributes such as gender, age, and ethnic and cultural background when building technology and innovation teams, specialized teams responsible for the end use of the AI system, and a responsible AI innovation oversight committee, etc. In this regard, it is generally good practice to try to build teams which are as diverse as possible, as diversity will also contribute to mitigating the risk of bias and unfairness in the AI system. |► *Learn more about the core principle of Fairness in the* ***Principles for Responsible AI Innovation***.

In the following subsections, we will look more closely at the four competency classes listed above, and will identify the specific types of expertise required and the people that should have this expertise.

TECHNICAL COMPETENCIES

Several different types of technical competencies are required for successful implementation of responsible AI innovation in law enforcement, and several different profiles will be required to champion it. Before exploring these competencies in more detail, it is important to first understand that there are four possible approaches law enforcement agencies can take when adopting AI systems: internal development, external development, hybrid or joint development, and procuring 'off-the-shelf' systems. The way an agency decides to approach development or procurement will generally be informed by factors such as the agency's capacities, time to production, and cost. This decision will, in turn, affect the type of expertise required and the extent to which this expertise should be held in-house – within the agency – or can be outsourced.



Generally speaking, in the event that an agency decides to develop an AI system internally it will of course need to have all of the technical competencies below in-house. However, opting to have a system developed externally or to procure it 'off-the-shelf' does not entirely negate the need for technical competencies: an agency should rely exclusively on an external provider. In fact, even in these cases, it is still advisable for the agency to have technical competencies, in particular for the purposes of the implementation and continued monitoring of the functionality of the AI system post-deployment. To perform this function, designated personnel will need some of the technical skills described below in order to detect and report errors and issues, and correct, halt, recalibrate, or decommission the system in case of failure.

Another area where a degree of in-house technical competencies is always essential – regardless of the origins of the AI system – is for end-users. Indeed, law enforcement personnel in specialized units who function as the end-users of AI systems should always have specialized training on the correct and responsible use of the technology, which will naturally entail a technical component. This is a crucial aspect of ensuring the responsible use of the technology. If and when an AI system is used in a criminal investigation, the relevant law enforcement personnel involved in the use of the system should have an appropriate understanding of the way it functions if they are to demonstrate the validity and integrity of any evidence obtained using the system to the courts.

Expertise	People	Observation
Programming	Technology and innovation team	Knowledge of relevant programming languages needed to build AI systems and knowledge of computer processing requirements to run AI systems. |▶ *Learn more about key elements in the **Technical Reference Book.***

Data management	Technology and innovation team	Knowledge of data pipelines, storage servers, audit trail, data security, and, when using on-premises data storage.
Cybersecurity	Legal and data protection officer, technology and innovation team, cybersecurity specialist	Monitor, detect, and investigate security threats, risks, and vulnerabilities. Knowledge of the security benefits and risks of cloud computing compared with on-premises storage.
AI application	Law enforcement system users in specialised units, training department, auditing, legal team, data protection officer, communications team	Understand the use case(s) and the capacities and limits of the technology and system used. Training (and certification where it applies) should be provided to ensure this understanding is aligned with the latest research and practices in the field. Users must also be able to detect errors and issues to report and monitor the performance of the AI system.
Tools to support responsible AI innovation	Responsible AI innovation oversight committee, technology and innovation team, legal team, data protection officer, communications team	A deep understanding of the technical tools or instruments, software, platforms, and guidance briefs that can support the responsible AI development and use. |► *Learn more about key elements in the **Technical Reference Book.***

Hardware handling capaci	Technology and innovation team	Familiarity with the hardware aspects of AI/ML systems, including distributed computing, GPU processors, and big data platforms, ensures efficient system operation and performance optimization.
Cloud computing capacity	Technology and innovation team	Proficiency in cloud computing is crucial as many AI systems leverage cloud-based resources for scalability and flexibility.

DOMAIN COMPETENCIES

Regardless of the way an AI system is obtained, it needs to be designed and developed to address the specific task and in a specific context. External technology providers may be unaware of the nuances and may lack expertise in the domain in which it is to be used. Even when AI systems are developed in-house by technology and innovation teams, the technical members of these teams who are tasked with development may also lack such understanding. The result could be a system that does not address specific needs, is biased, or provides information which is inaccurate for the intended context. As a result, it is important that developers, both internally and externally – and where it applies, technology integrators, who may be contracted to support the integration of a procured AI system into the agency – are in close contact with the end users or law enforcement personnel who have expertise in the relevant crime areas.

However, the importance of domain expertise is not restricted to developers and the design and development stage of systems. End-users of a system may also require specific domain expertise that goes beyond mere expertise in a specific crime area if they are to ensure the responsible use of an AI system. For instance, it is recommended that the end-users of facial recognition AI systems should be trained forensics facial examiners who have the requisite expertise to be able to perform image(s)-to-image(s) analysis using a rigorous morphological comparison and evaluation.

At the same time, particularly with respect to AI systems developed externally but also to a degree with systems developed in-house, it is essential that technology and innovation teams have access to expertise on the criminal justice system in the agency's jurisdiction. This will ensure

that if and when an AI system is used in the context of a criminal investigation, any evidence obtained through the use of this system will be admissible in the courts. Expertise in the field of criminal justice will help inform the way data is gathered, processed, retained or deleted and the way outputs are produced, in order to guarantee a fair trial and respect for privacy, to give one example.

Expertise	People	Observation
Crime, crime prevention, criminal investigations	Law enforcement personnel specialized in specific crime areas	Depending on the use case, the development and implementation of an AI system may require the involvement of experts in different areas of policing including financial crimes and fraud detection, narcotics, homicide, cybercrimes, human trafficking, biometrics, etc. A broader expertise in criminology may also be valuable, for instance in terms of helping to separate causal links from mere correlation.
Criminal justice and the principles of policing	Legal teams, internal affairs units, external criminal justice practitioners and academic experts	Closely tied to the expertise on criminal and procedural law in the governance competency below, developers of AI systems must have an understanding of the role of the police within the criminal justice system. This includes matters such as the kind of data that can be used, the underlying principles of policing and any associated codes of ethics, and the legality of using AI systems for evidence gathering. It is important for third-party teams building AI systems to understand any legal challenges the systems may present for prosecution and how to safeguard the admissibility of evidence obtained using such systems in their respective jurisdictions.

GOVERNANCE COMPETENCIES

The governance of AI, and consequently responsible AI innovation, requires broad expertise in laws, regulations, policies, procedures and ethics. Given the nature of law enforcement, agencies should by default have a good knowledge base in these domains. However, this will likely need to be expanded with specific specialized expertise in the ethical and human rights elements

of responsible AI innovation – arguably less traditional areas of expertise for law enforcement agencies. In this regard, agencies may seek to build partnerships with external stakeholders, in particular by inviting academic experts and legal professionals to engage with in-house staff and complement existing expertise. A prime example of when these partnerships may be beneficial is in the context of a responsible AI innovation oversight committee, which is a key aspect of building an organizational culture that fosters responsible AI innovation.

It is also important to clarify that one of the three areas of expertise described below specifically concerns the ***Principles for Responsible AI Innovation***. As it is an externally developed framework, agencies will not naturally possess this kind of expertise, but it is advisable that they aim to promote and develop this expertise within the agency and the people and teams in question to ensure that these principles are incorporated into the development and use of AI systems.

Expertise	People	Observation
Criminal procedural law	Legal teams; law enforcement system users in specialized units; technical development teams	Knowledge of national and any applicable international laws, specifically including any requirements or limitations regarding the use of new technology by law enforcement agencies.
National and regional laws, regulations and policies	Legal teams; responsible AI innovation oversight committee	Knowledge of national and any applicable international laws, in particular regarding human rights, AI, data protection and information security. Expertise in these areas is increasingly important given the growing number of AI regulations around the world that need to be considered. Some examples of globally significant regional frameworks include, but are not limited to, the African Union Convention on Cyber Security and Personal Data Protection;[6] and the European Union's General Data Protection Regulation,[7] the Law Enforcement Directive,[8] and the Directive on Security of Network and Information Systems.[9]

Principles for Responsible AI Innovation	Management; responsible AI innovation oversight committee; technical development teams; legal teams; law enforcement system users in specialized units	Knowledge of the Principles for Responsible AI Innovation as they pertain to specific use cases in law enforcement. These principles should guide law enforcement agencies in identifying, preventing and mitigating legal and ethical concerns and negative consequences of the use of AI systems for the benefit of society and to protect individual rights. |►*Learn more about this in the* ***Principles for Responsible AI Innovation.***

SOCIO-CULTURAL COMPETENCIES

The use of AI systems in law enforcement has generated some degree of concern among certain elements of the public and will continue to do so. As a result, public trust in the agency and its use of AI systems will have to be built and maintained through careful and measured public engagement. To do this effectively, agencies will need access to specific expertise in order to analyze and better understand the social context in which they operate and the implications of each AI system in that social context. This expertise may also help to provide additional input for an agency's internal organizational culture around responsible AI innovation. As with the aforementioned governance competencies, agencies may choose to complement any in-house expertise in this area with external partnerships. This will be particularly relevant for expertise in sociocultural analysis and social and psychological impact analysis, as these are areas in which internal expertise may be vulnerable to perceived or actual bias.

Expertise	People	Observation
Communication and public relations	Law enforcement public relations teams	Communication and transparency around law enforcement agencies use of AI systems is particularly important for creating public trust. Where appropriate, and in particular when the AI systems are intended to be public-facing, communication and transparency should be a priority and the development of a dedicated strategy to this end is advisable. Information to be made available to the public may include: • The purpose of the AI system to be deployed, the name and version of the software. • A clear definition of how it is used and the authorized use cases. • The processes and information used to develop the AI system. • The way data, in particular personal data, is collected, processed and stored. • The data-sharing policy in the event that data is shared with other organizations or third parties. • The list of teams, units or departments that have access to the AI system. • The results of audits or evaluations of the system's performance. • Any other relevant information that can be shared without compromising investigations. *|► Learn more about this in the **Principles for Responsible AI Innovation.***

Socio-cultural Context	External expert groups (practitioners, academics, civil society groups, and community leaders); responsible AI innovation oversight committee	An understanding of the national (and where relevant regional and local) sociocultural context that may affect the relationship between law enforcement and the public.
Social and psychological impact analysis	External expert groups (practitioners, academics, civil society groups, and community leaders); responsible AI innovation oversight committee	An understanding of how the use of AI systems by law enforcement could affect individuals and communities, as well as the behaviour of law enforcement personnel at various levels, and with this the agency's culture. For example, it would be important to know if the use of a specific AI system is seen as particularly controversial by certain parts of the community, which could discourage this community's engagement with law enforcement. Such knowledge could help to determine whether such a system is appropriate.

Processes

Having explored the ideal culture, people and types of expertise, we will now turn to the final component required for an agency to realize responsible AI innovation: the processes. Processes refer to specific initiatives that the chief of police and executive leadership should seek to promote, as well as the activities they should lead or mandate to enable the agency to develop responsible AI through the development, procurement and use of AI systems. Where relevant, specific individuals and expertise which should play a part in each initiative will be highlighted. These processes can, in some ways, be considered as precursors for enabling an agency to apply the ***Principles for Responsible AI Innovation*** and supporting them in doing so throughout the life cycle of an AI system. |► *Learn more about the AI life cycle in* the ***Introduction to Responsible AI Innovation*** *and learn how they apply throughout the AI life cycle in the* ***Responsible AI Innovation in Action Workbook***.

Before examining these processes, it is important to note that the nature and extent of the implementation of these processes should be proportionate to the risk of the AI system. While the guidance contained in this AI Toolkit is aimed at higher-risk AI systems, lower risk systems may not require such extensive efforts in terms of the recommended processes. Nevertheless, the processes described below can be considered general good practice for any agency. |► *Learn more about identifying the level of risk of a specific AI system in the* ***Risk Assessment Questionnaire.***

CARRYING OUT AN AGENCY-WIDE NEEDS AND CAPABILITY ASSESSMENT

Action: Designate a focal point to lead and conduct an assessment of the agency's needs and existing capabilities and the role or potential relevance of AI systems in this regard, in order to determine whether it is necessary and appropriate to develop, acquire, and integrate AI systems into the current agency structure, and what is required to do so. In order to carry out the assessment, the focal point will need to work with the technology and innovation team, legal team, responsible AI innovation oversight committee, psychosocial experts, and communications and public relations teams. The assessment will inform, in particular, the governance approach and (if not already established) the formation and mandate of the responsible AI innovation oversight committee.

KEY ACTIVITIES:

- Evaluate the indispensability/benefits of identified use cases, indicating if and how an AI system could be part of the solution. |► *Learn more in the* ***Responsible AI Innovation in Action Workbook***.
- Identify and analyze the potential benefits or risks for the agency of introducing an AI system – strategic, capability, financial, efficiency gains, errors, harm to public trust, etc.
- Assess the agency's readiness to implement an AI system. |► *Learn more in the* ***Organizational Readiness Assessment Questionnaire***.
- Assess the internal capacity and human capital required to operate an AI system. It is important to have dedicated capacity for assessing, evaluating, adapting and monitoring the system. |► *Learn more in the* ***Organizational Readiness Assessment Questionnaire***.
- Assess the cost of adopting the AI system, from procurement and use to engagement

and training of frontline officers and first responders.

- Estimate the potential return on investment in terms of hours saved, improvement of processes, etc.
- Analyze how to best integrate the new AI system into the existing technology infrastructure.

LAYING THE FOUNDATIONS FOR PUBLIC ENGAGEMENT

ACTION:

Task the public relations office to begin preliminary engagement with the public and other stakeholders such as non-governmental organizations, academia, human rights, and civil society groups, in order to better understand public concerns and help find mutual grounds for acceptability, accountability, transparency, and public buy-in. This may leverage or, in the event that they take place concurrently, even feed into the results of the agency-wide needs and capability assessment.

KEY ACTIVITIES:

- Define the extent of public engagement desired or required based on socio-cultural contexts or national culture, noting that some communities may wish to be more closely involved than others.
- Gather public responses through surveys on the use of AI systems in law enforcement.
- Engage in a public consultation process with the relevant stakeholders, addressing concerns expressed in the survey.
- Engage with communities to explain the need for an AI system and seek public participation in the implementation process.
- Inform the public on the specific use case to be operationalized and the value it brings to improving policing, as well as potential challenges or problems.
- Raise awareness of the agency's responsible AI innovation culture and highlight the strategies and approaches in place to assess risks and prioritize the ***Principles for Responsible AI Innovation***.

WANT TO LEARN MORE?

See the "Developing a Responsible AI Strategy for your Agency" section in the annex.

Defining the governance approach *Action:* Task the policy and legal teams, in consultation with the responsible AI innovation oversight committee, with defining and setting up a strategy for the governance of the use of AI systems. Ideally, this would involve the adoption of a responsible AI strategy, and should make use of the results of the agency-wide needs and capability assessment and findings from the preliminary public engagement.

KEY ACTIVITIES:

- Consider existing legal frameworks, legislation, and regulations that may support, inhibit or affect the use of AI systems in the agency more generally, and the need for a dedicated responsible AI strategy.
- Ensure that the responsible AI strategy aligns with the applicable national policies and laws and is within the scope of the agency's mandate to serve and protect.
- Ensure that this responsible AI strategy can be used as a benchmark to guide further evaluation and development of other systems and that it is not use-case specific.
- Understand the context in which each of the ***Principles for Responsible AI Innovation*** should be applied, taking into account the existing national legislation identified in the governance strategy stage.
- Understand how the principles might be integrated into the workflow of the agency's various units or departments depending on the use case.

SETTING UP AND ADHERING TO A RISK MANAGEMENT POLICY

ACTION:

Appoint a risk executive and task them with the preparation of a risk management strategy or policy that determines how your agency will assess, respond and monitor the risks involved in implementing AI systems.[10] Creating a risk management policy is the first step of a comprehensive risk management process. In the context of responsible AI innovation, risk management entails following a coordinated and rigorous process of understanding and addressing the risks that may emerge in relation to the implementation of any AI system and, indeed, AI systems in general. It should include the following activities:

KEY ACTIVITIES:

- Establish a risk management policy, specifying the approach to assess and address risks related to the implementation of AI systems, the teams or staff members in charge of specific tasks and those that are considered risk owners, and the timing and financial and organizational resources allocated to risk management.

- Assess the risks to individuals and communities related to the insufficient fulfilment of the ***Principles for Responsible AI Innovation*** during the planning stage of the AI life cycle or as early as possible. |► *Learn more about this in the* ***Risk Assessment Questionnaire***.

- Assess any other AI-related risks following the appropriate risk assessments and according to risk management policy.

- Take informed action towards responding to the identified risks, defining and following a comprehensive risk response. |► *Learn more about this in the* ***Responsible AI Innovation in Action Workbook***.

- Monitor the risk on an ongoing basis, revisiting the risk assessments' results and the risk response measures as needed, and at least at each stage of the AI life cycle and whenever there are changes in circumstances that might impact risk or risks response. |► *Learn more about this in the* ***Responsible AI Innovation in Action Workbook***.

- Repeat the risks assessments and any other activity within the risk management process as needed.

ESTABLISHING A RESPONSIBLE AI INNOVATION OVERSIGHT COMMITTEE

ACTION:

Mandate the establishment of a responsible AI innovation oversight committee within the agency that acts as a central pillar for its governance approach and custodian for its responsible AI strategy.

The oversight committee should include some of the following areas of expertise: ethics, law, stakeholder management, public engagement, etc. It should play the role of lead advisor on the ethical and human rights requirements for the responsible use of AI systems, bringing together the necessary stakeholders within an agency as and when necessary. The committee should seek to ensure responsible AI innovation throughout the system's entire life cycle, including planning, development, procurement, use and monitoring. Furthermore, the committee should aim to ensure that steps are taken to prevent and mitigate the negative consequences for individuals and society that may derive from law enforcement's use of AI systems. Ideally, the committee, in conjunction with a responsible AI strategy, will help to drive a culture of responsible AI innovation within the agency and build awareness and understanding of responsible AI innovation, as well as support the agency in staying up-to-date with the discourse around the topic.

The committee should be independent in nature in order to avoid concerns about a lack of impartiality, and to facilitate its work. Larger law enforcement agencies may consider establishing an independent office dedicated to responsible AI innovation or a working group/committee responsible for managing and implementing responsible AI innovation. On the other hand, smaller agencies may opt to consolidate the role and functions of such an oversight committee in one or more individuals. Nonetheless, centralizing all these tasks in one or even a few individuals risks creating a bottleneck that prevents the agency from innovating. The fact that no single individual can possess the full spectrum of expertise required to exercise this function should also be carefully considered.

KEY ACTIVITIES:

- Assess the human rights and ethical impacts by carry out impact assessments to identify adverse impacts on individuals, groups, or the wider community, including human rights impact assessments and data protection impact assessments. |► *Learn more about this in the* ***Principles for Responsible AI Innovation***.

- Assess the ethical and social cost/ramifications of implementing the identified use of an AI system in law enforcement. |► *Learn more about this in the* ***Principles for Responsible AI Innovation***.

- Assess any existing trust deficit or problematic relationships between vulnerable groups, the public, and state power structures that may affect the implementation of AI systems and public trust, and provide recommendations to address any issues.

Annex:
Want to learn more?

DEVELOPING A RESPONSIBLE AI STRATEGY FOR YOUR AGENCY

WHAT IS A RESPONSIBLE AI STRATEGY?

A responsible AI strategy is a guidance document, unique to each agency and aligned with the agency's overall policing goals and public safety objectives, that outlines and visualizes that agency's goal for AI innovation, the possible use cases, and a list of activities, priorities, dependencies and timelines, as well as an execution plan. It is an invaluable asset for any agency looking to implement AI systems, regardless of the level of progress within that agency in terms of AI.

WHY DEVELOP A RESPONSIBLE AI STRATEGY?

Whilst the AI Toolkit guides agencies towards responsible use of AI and can be an important point of reference, possessing a specifically designed and tailored to the agency strategic document is crucial to successfully leveraging AI in a responsible fashion. A strategy is additionally important for following the reasons:

- It serves a one-stop document clearly defining the agency's vision for AI innovation.
- It supports execution of the agency's vision, by outlining a clear plan and way forward.
- It supports internal teams to align with the vision and execution plan, but serving as a 'north star' document.
- It summarizes institutional priorities in a way that is easy to communicate to external stakeholders such as technology providers.
- It guides and informs discussions around resources and prioritization exercises for future projects.

Beyond this, having (and regularly updating) a responsible AI strategy makes it easier to keep to the ***Principles for Responsible AI Innovation*** when AI systems are purchased, designed and developed for specific purposes.

KEY ASPECTS OF A RESPONSIBLE AI STRATEGY

Each agency's Responsible AI Strategy will differ, however generally an AI strategy will include the following aspects:

- Agency vision
- Strategy for achieving this vision using AI systems
- Goal of the use of AI systems
- AI initiatives to be developed
  - Potential use cases
  - Objectives
  - Stakeholders
  - People and expertise
  - Timeline
  - Budget
  - Metrics for success
- Prioritization of use cases
- Technical and agency requirements
- Resources – time, money, people and environmental consideration

A STEP-BY-STEP GUIDE TO BUILDING AN AI STRATEGY

What follows is a series steps that law enforcement organizations can follow in order to better understand how to approach the development of a robust responsible AI strategy that drives digital transformation, enhances community safety, and shapes the future of their lawful and ethical policing operations. The steps should not be considered definitive, but rather indicative of a flexible framework adaptable to diverse organizational contexts.

1. **Assess your current AI maturity:** Evaluate your organization's current level of AI adoption, the availability of data, technical expertise, and existing AI projects. Completing the ***Organizational Readiness Assessment*** will help identify areas for improvement and determine the appropriate level of investment to reinforce your structural resilience in AI initiatives.

2. **Understand your business goals:** Clearly define the specific business outcomes you aim to achieve through the use of AI. This could include improving community service, optimizing operations, automating tasks, or developing new investigative tools and services.

3. **Identify AI opportunities:** Analyse your business processes, data assets, and public facing interactions to identify areas where AI can be applied to achieve your goals. Consider both short-term and long-term opportunities, and prioritize projects based on their potential impact and feasibility.

4. **Develop a clear AI vision:** Articulate a compelling vision for how responsible use of AI systems will transform your organization and its policing operations. This vision should align with your overall business strategy and inspire officers and employees to embrace AI adoption.

5. **Establish AI principles and governance:** Using the ***Principles for Responsible AI Innovation,*** reflect upon the principles and guidelines that will govern responsible AI innovation and use of AI development and deployment within your agency. This includes addressing issues of bias, privacy, and transparency.

6. **Create an AI roadmap:** Using the ***Responsible AI Innovation in Action Workbook,*** develop a detailed roadmap that outlines the specific AI projects, timelines, and resources required for implementation. This roadmap should be flexible enough to adapt to changing business needs and technological advancements.

7. **Invest in AI talent and skills:** Cultivate a pool of AI talent by hiring necessary experts, training officers and employees, and foster a culture of continuous learning. Provide opportunities for officers and employees to upskill and develop their AI knowledge and expertise – including through partnerships with local qualified academia. Refer to the guidance contained in this ***Organizational Roadmap.***

8. **Partnerships and collaborations:** Explore opportunities to collaborate with industry partners, research institutions, and technology providers to accelerate responsible AI adoption and gain access to specialized expertise.

9. **Continuous monitoring and improvement:** Regularly monitor the performance of your AI initiatives and gather feedback from stakeholders using the ***Risk Assessment Questionnaire.*** Implement continuous improvement cycles to refine AI models, enhance user experiences, and maximize the return on your AI investments.

10. **Legal and ethical considerations:** Emphasize the legal and ethical implications of AI development and deployment, as outlined in the ***Introduction to Responsible AI Innovation*** and the ***Principles for Responsible AI Innovation.*** Ensure that AI models are lawful, fair, unbiased, and transparent, and that AI solutions respect privacy and human dignity.

11. **Communication and alignment:** Communicate your AI strategy effectively to all stakeholders, including officers and all employees, the local community, and partners. Ensure that everyone understands the role AI plays in achieving law enforcement and organizational goals and the legal and ethical principles that guide its responsible use.

12. **Regular review and adapt:** Regularly review your AI strategy to ensure it remains aligned with your agency's goals and objectives, technological advancements, and evolving threat conditions. Make adjustments as needed to optimize your AI investments and maximize value creation for improved public safety.

ENDNOTES

1 Procon. (2021), "Police Body Cameras: Top 3 Pros and Cons". Accessible at: https://www.procon.org/headlines/police-body-cameras-top-3-pros-and-cons/

Tony Farrar. (2013) Self-Awareness to Being Watched and Socially-Desirable Behavior: A Field Experiment on the Effect of Body-Worn Cameras on Police Use-of-Force. National Policing Institute. Accessible at: https://www.policinginstitute.org/publication/self-awareness-to-being-watched-and-socially-desirable-behavior-a-field-experiment-on-the-effect-of-body-worn-cameras-on-police-use-of-force/

David Garrick. (Feb. 9, 2017). San Diego Union-Tribune. Accessible at: https://www.sandiegouniontribune.com/news/politics/sd-me-body-cameras-20170209-story.html

2 Security Journal UK. (Aug. 2021). 'Facial recognition technology introduced to body worn camera'. Accessible at: https://securityjournaluk.com/facial-recognition-body-worn-cameras/

3 Bryan, S. (2015), "Broward cities focus on pros, cons of cop body cams". Sun Sentinel. Available at: www.sun-sentinel.com/news/fl-body-cameras-hallandale-update-20150414-story.html (Accessed September 29, 2022).

4 Jessica Huff, Charles M. Katz, and Vincent J. Webb. (2018), "Understanding police officer resistance to body-worn cameras", Policing: An International Journal, Vol. 41 No. 4, pp. 482-495. https://doi.org/10.1108/PIJPSM-03-2018-0038.

5 Merseyside PEEL. (2019). Legitimacy: How legitimately does the force treat the public and its workforce?. His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) – Home. Accessible at https://www.justiceinspectorates.gov.uk/hmicfrs/peel-assessments/peel-2018/northumbria/legitimacy/detailed-findings/

Merseyside PEEL. (2020). Effectiveness: How effectively does the force reduce crime and keep people safe?. His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) – Home. Accessible at: https://www.justiceinspectorates.gov.uk/hmicfrs/peel-assessments/peel-2018/merseyside/effectiveness/

6 African Union Convention on Cyber Security and Personal Data Protection, adopted on 27 June 2014. Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Accessible at: https://eur-lex.europa.eu/eli/reg/2016/679/oj

8 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32016L0680

9 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning

measures for a high common level of security of network and information systems across the Union. Accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1683543287951<?> ISO Guide 73:2009 (en) Risk management — Vocabulary. Accessible at: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en; National Institute of Standards and Technology (NIST). (March 2011), "Managing Information Security Risk Organization, Mission, and Information System View": Accessible at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

10 ISO Guide 73:2009 (en) Risk management — Vocabulary. Accessible at: https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en; National Institute of Standards and Technology (NIST). (March 2011), "Managing Information Security Risk Organization, Mission, and Information System View": Accessible at: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

How to cite this publication: UNICRI and INTERPOL. (Revised February 2024).
Toolkit for Responsible AI Innovation in Law Enforcement: ***Organizational Roadmap.***

www.interpol.int
www.unicri.it

INTERPOL_HQ

@INTERPOL_HQ
@UNICRI

INTERPOL HQ
UNICRI

INTERPOL
UNICRI

@INTERPOL
@UNICRIHQ

www.ai-lawenforcement.org