

ARTIFICIAL INTELLIGENCE PLAYBOOK

For Justice, Public Safety and Security Professionals



Developed By:
IJIS Institute
AI Working Group

Contact:
Ashwini.jarral@ijis.org

21100 Ashbrook Place
Suite 150
Ashburn VA 20147

Tel 703.726.3697
Fax 703.726.3557
www.ijis.org

Abstract:

This playbook intends to provide guidance to the Justice, Public Safety, and Security Professionals in their implementation of their AI based capabilities and functionalities.

Published: April 2025



Playbook Principles

This *Playbook* is intended to help users in their journey to develop, implement, or utilize AI-based capabilities, which can be used at any point in the adoption lifecycle, even if you are starting from scratch!

- The plays included in the *Artificial Intelligence Playbook for Justice, Public Safety, and Security Professionals* were designed with the following principles in mind:
 - Artificial Intelligence capabilities or functionalities, are built on a set of principles that provide ways for organizations to make better decisions across systems, organizations, jurisdictions, and domains in considering its implementation.
 - Taking the if-you-build-it-they-will-come approach often does not work – it can be a costly failure, and it can result in irreversible damage to trust in AI-based capabilities and functionalities. The continuous engagement of the end user, lawmakers, efficacy groups, and community representatives throughout the entire process will increase the probability of success related to AI adoption.
 - Policies, Laws, Regulations, and Standards provide guardrails for the ethical and responsible implementation of AI and should be considered in every aspect of the development, training, and implementation of AI-based algorithms, model capabilities, and functionalities. If there is a reason for not following them, then those exceptions should be documented and discussed with the governance body members to reduce associated risks and liabilities.
 - Automation, guided training, and self-training are essential to developing AI models; it can significantly improve an organization's processes and their replication, but human oversight should always be part of the development, implementation, and ongoing monitoring to validate accuracy, reduce bias and the potential for ethical use issues.
 - Throughout the lifecycle, decisions are coordinated and made at the lowest possible level of organizational competency.
 - Almost every play is iterative in that initial trials often lead to repetition, but at a higher scale of implementation.
 - Any Company name, standards, and other best practices referenced in various plays are in no form an endorsement from the IJIS Institute and the working group members. They are used to provide information to the readers of the playbook.

There are also a few key principles that will help guide the use of this *Playbook*:

- The *Playbook* is meant to be functional at a starting-from-scratch level. However, we know that many different types of organizations at varying levels of experience will access these plays. For beginning users, consider the plays as a suggested roadmap and incorporate the tried-and-tested processes of your more

experienced team members. For more advanced users, take an opportunity to view these plays and see if there is anything you are missing in your current process.

- While the Playbook intends to make every Play valuable, we understand that players in various roles might have different interests or focuses when viewing the Playbook. The following table shows the targeted audience for each of the Plays based on roles: Executives, Operations, Technologists, Chief Information Security Officer/ Chief Privacy Officer (CISO/CPO), Legal Counsel, Governance, External Stakeholders, Human Resource, Finance, Chief Data Officer, and End Users.

PLAY # \ PLAY TAG	Executives	Operations	Technologists	CISO/CPO	Legal Counsel	Governance	External Stakeholders	Human Resource	Finance	Chief Data Officer	End Users
Play 1 - Establish Governance	x	x	x	x	x	x		x	x	x	
Play 2 - Use Case Identification	x	x	x	x	x			x	x		x
Play 3 - Ethical/Responsible Use		x	x	x	x		x	x			
Play 4 - Policy Development	x			x	x			x			x
Play 5 - Security and Privacy Consideration			x	x	x					x	
Play 6 - Stakeholder Engagement in Requirements and Implementations	x	x	x	x	x		x	x	x		x
Play 7 – Develop Risk Matrix	x		x	x	x	x	x				x
Play 8 - Technical Implementation		x	x	x	x					x	x
Play 9 – Funding	x	x			x			x	x		
Play 10 - Training and Education		x	x				x	x			x
Play 11 – Compliance and Standards	x		x	x	x	x					
Play 12 - Algorithm/Model Transparency			x	x	x					x	
Play 13 – Workforce Development	x	x	x	x				x			

Table 1 Play Tags



The *Playbook* was developed by the [IJIS Institute](http://www.ijis.org) Artificial Intelligence Working Group with support from various national practice associations.



Play 1: Establish Governance

Establishing and implementing a governance framework is crucial for overseeing AI implementation, utilization, management and promoting responsible deployment. Governance will assist in ensuring alignment with processes, policies and regulatory standards and AI capabilities that align with the organization's ethical and responsible use. Governance is the process in which decisions are made regarding use, operations, and constraints

- Establish and implement a governance framework to oversee AI utilization and management across the organization, promoting responsible deployment and ensuring alignment with policies and regulatory standards.
- Develop processes, policies, and frameworks that align with the tool or system's operational overview to ensure the effectiveness and impact of AI to be embedded, enabled, or developed within an organization.
- Adhere to accountability, Privacy, Transparency, Algorithmic Biases, Security, and Use Case ownership development.



KEY QUESTIONS

Questions to consider for accountability: decision ownership and capabilities, the skills and abilities to approve, deny, manage, and maintain a system or tool embedded, enabled, or developed within an organization.

- Are we going to dive as deep as Machine Learning Operations (MLOps) and portfolio-level ownership or frontline governance?
- Who has the authority to do what?
- Are you required to comply with certain overarching governance rules and obligations from your state, county, or tribal jurisdiction?
- What's my AI inventory? Who's managing the Intellectual Property (IP)?
- If developing the model: what is the source of the data, and who owns it? (ownership)
- Do I have the authority to use the data?
- Who is carrying the risk going forward?
- Who will mitigate the risk?
- How do you handle bias? What is the process in place to handle bias?
- Why should we use AI? What's the value/benefit? How are we going to manage it?
- How can you ensure it will not harm?

- Is it AI?
- How do you prevent the use of the application for criminal purposes?
- What if algorithms start training themselves? What are your guardrails?

CHECKLIST

- Accountability, Privacy, Transparency, Algorithmic Biases, Security, and Use Case ownership development
- Ensure all stakeholders are represented as part of the governance process
 - AI Ethics committee
 - Data Governance officer
 - Understand who the users are and who is affected by it
- Ensure decision-making processes
 - Have clear roles and responsibilities
- Protect against fraud and deception (marking documents)
- Implement AI to protect consumers
- Establish AI Inventory
- Clearly define risk management
- Inventory with a risk level matrix and impact analysis by Use Case and community
- Ensure public acceptance of the application

RESOURCES

- US Federal AI Community of Practice AI Governance Toolkit - <https://coe.gsa.gov/docs/AICoP-AIGovernanceToolkit.pdf>
- National Institute for Standards and Technology (NIST) AI Risk Management Framework (RMF) - <https://www.nist.gov/itl/ai-risk-management-framework>
- Bipartisan House Task Force on Artificial Intelligence Report (Governance Section) - <https://www.speaker.gov/wp-content/uploads/2024/12/AI-Task-Force-Report-FINAL.pdf>
- Europol Governance Model - <https://www.europol.europa.eu/cms/sites/default/files/documents/AI-and-policing.pdf>

- NVIDIA Trustworthy AI - <https://www.nvidia.com/en-us/ai-data-science/trustworthy-ai/?srsltid=AfmBOoof9Ba5oICQcHNnCCk0wZU4K1dijwaNjv2mEtj5MfTgioPCOglQ>



PLAY TAGS

- Executives
- Operations
- Technologists
- CISO/CPO
- Legal Counsel
- Governance
- Human Resources
- Finance
- Chief Data Officer



Play 2: Use Case Identification

Before buying or developing an AI-based capability, a Use Case needs to be developed to better understand how the capability or functionality will help address the organization's requirements, goals, and objectives. Identifying the Use Cases helps determine whether it is AI or not, including the associated risks and liabilities.



KEY QUESTIONS

- What capabilities/functionality are you looking for from AI?
- What is the goal that you're attempting to achieve with the adoption of technology, and what, if any, role do you foresee AI playing?
- What are the data requirements?
- What are the pain points in the organization?
- Can your agency map to an AI Use Case?
- Does the Use Case address the ethical/responsible use of AI?
- What are the associated risks/potential risks to consider?
- Who is championing the Use Case? Who are the primary users?
- What are the associated Cost factors to implement AI in the context of the developed Use Case and what is the Return on Investment (ROI)?
- Who will defend AI's solutions? How can you defend AI's recommendations?



CHECKLIST

- Risk Matrix
- Definitions on different types of AI capabilities
- Identify different types of stakeholders



RESOURCES

- US AI for Government - <https://coe.gsa.gov/coe/ai-guide-for-government/print-all/index.html>

- Use Case Decider -
https://billsantray.com/AI_or_not_AI_Use_Case_Decider_AI_or_Not_AI_Use_Case_Decider.html

PLAY TAGS

- Executives
- Operations
- Technologists
- CISO/CPO
- Legal Counsel
- Human Resources
- Finance



Play 3: Ethical/Responsible Use

Create a framework of principles and practices to ensure every AI tool aligns with organization values, emphasizing fairness, accountability, and transparency. This includes regular Bias Checks and Balances, Clear Accountability and Transparent Decision-Making.



KEY QUESTIONS

- What is the context of ethical use?
- Is the AI deployed and used ethically?
- What is AI used for?
- Do we have a framework of principles and practices?
- What/Who was used to train and develop AI based algorithms, capabilities, and functionalities?
- Is it an open/closed system?
- What is the likelihood of the impact? Who are you affecting?
- Do we have an ethical assessment?
- How do we look at the algorithms to minimize bias?
- What safeguards, such as guardrails, policies, and security controls, are in place to ensure the model is safe and reliable before deployment?
- How is AI going to affect the equity and equality of justice?



CHECKLIST

- No unauthorized secondary use of data
- Algorithms are tested for Fair and non-discriminatory purposes
- Developed Algorithms and models are transparent
- The development team owns the accountability for ensuring no bias or hallucination exists
- Utilize private, and secure design, development, deployment, and monitoring of an AI system or tool
- Ensure the human-centric impact and operate with a human in the loop

- Deployment and monitoring of the AI system
- Process for ethical assessment
- Process for algorithm evaluation
- Process to minimize bias
- Process to evaluate tool accuracy
- Develop a Terms and Conditions document to clarify terms of use and definitions.
- Make it easy to discern that it is an AI interaction with all the stakeholders



RESOURCES

- Carnegie Mellon University Ethical AI Checklist - https://insights.sei.cmu.edu/documents/2562/2019_010_001_636622.pdf
- AI Fairness in Practice - Guidance Brief - https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4731837
- NIST Governance section AI Playbook - <https://airc.nist.gov/airmf-resources/playbook/>
- Europol: <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing>
- ISO 42-001 Artificial intelligence — Management system - <https://www.iso.org/standard/81230.html>



PLAY TAGS

- Operations
- Technologists
- CISO/CPO
- External Stakeholders
- Legal Counsel
- Human Resources

4

Play 4: Policy Development

Organizations implementing AI-based capabilities and functionalities need to ensure that an AI use policy is in place that clearly describes how AI is being used and what controls are in place for its ethical and responsible use. The policy needs to be specific to the Use Case and should be used to train staff and communicate with the stakeholders including efficacy groups.



KEY QUESTIONS

- What policies and procedures do you have in place?
- What content is in those policies and procedures?
- How are you enforcing this policy?
- What are the Use Cases the policy addresses?
- Why? What are your needs, objectives, and intent?
- What stakeholders need to be involved in the development of the policy?
- Legal and ethical questions - what laws apply to you?
- How will you determine what AI to implement (Use Case development and review?)
- How will you govern the use of AI?
- How are you using these policies for training your staff?
- How does the policy address the Risks associated with the use of AI?
- How are policies being used for Community engagement and outreach?
- Is your policy too restrictive?
- How often should the policy be reviewed?
- What are the triggers for the policy review?
- How risky is the AI application? Not all applications are created equal



CHECKLIST

- Defining the scope of the policy
- Ethical considerations

- Accountability/Transparency
- Education
- Need to articulate how AI is a part of the solutions
- Human oversight
- Monitoring bias
- Policy expiration dates/timeframes
- Impact of algorithms on outputs
- Adoption of approved policies
- Keep tabs on policies “overlapping”



RESOURCES

- Toronto Police AI Principles - <https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology>
- National Center for State Courts (NCSC) AI Guidance - https://www.ncsc.org/_data/assets/pdf_file/0014/102830/ncsc-artificial-intelligence-guidelines-for-courts.pdf?utm_campaign=567273_%40the%20Center%20August%2028%202024&utm_medium=email&utm_source=newsletter&utm_content=v-0&dm_i=7L57,C5PL,5477GF,1TW8I,1



PLAY TAGS

- Executives
- CISO/CPO
- Legal Counsel
- Human Resources
- End Users

5

Play 5: Security and Privacy Consideration

Organizations implementing or utilizing AI-based capabilities and functionalities must ensure that they meet all the security and privacy requirements based on privacy laws and standards. Each organization is responsible for ensuring that they develop or acquire the algorithms or models that are properly vetted for security and privacy conformance.



KEY QUESTIONS

- Where is your data stored?
- What happens to your data once the AI uses it?
- Is the data model public? Or domain-specific?
- Is the data secure?
- Is the data trusted?
- What type of data is being used? Classification
- Is the data private?
- Is the data sensitive?
- Is the data Personally Identifiable Information (PII)?
- Where is the data going? Who is handling the data?
- Does the data need to be encrypted? What type of encryption?
- What type of standards need to be considered?
- How does the tool share data?
- What procurement/contract language is being used?



CHECKLIST

- Review against NIST Cybersecurity Framework (CSF), International Organization for Standardization (ISO) 42001, Criminal Justice Information Security (CJIS) Policy 5.9.5, etc.
- Check the security of the data's Application Programming Interface (API)
- Auditing/Logging

- Identify controls
- Understanding the different data sets
- See how Privacy Act affects AI
- Data sharing
- Data Restrictions
- Model/Architecture selection on Data Governance
- Privacy Impact Assessment
- Awareness of compliance
- Security breach handling



RESOURCES

- NIST AI Risk Management Framework - <https://www.nist.gov/itl/ai-risk-management-framework>
- MITRE's attack framework for AI - <https://atlas.mitre.org/matrices/ATLAS>



PLAY TAGS

- Technologists
- CISO/CPO
- Legal Counsel
- Chief Data Officer



Play 6: Stakeholder Engagement in Requirements and Implementation

Defining and convening all relevant stakeholders to ensure they are engaged in the AI lifecycle, from problem definition, Use Case development, algorithm/model development, and design of the associated capabilities before implementation.



KEY QUESTIONS

- What is the impact on the workforce?
 - How will you accommodate these workers?
- How will you involve the community/advocacy groups/lawmakers?
- How do you gain acceptance?
- How do you communicate with the stakeholders?
- Do you have a stakeholder management process in place?
- How do you measure success?
- How are biases affecting different groups?
- How do you plan to address stakeholders' resistance to implementing AI?



CHECKLIST

- When implementing, make sure AI is meeting all requirements
- Stakeholder management methodology
- Outreach and communications plan
- Sustained application testing program
- Continue to monitor results
- Reach out to empowered stakeholders
- Need to Identify User Groups



RESOURCES

- University of Cambridge, Stakeholder Involvement Framework - [Stakeholder Involvement for Responsible AI Development: A Process Framework](#)
- U.S. Leadership in AI - https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf
- Stakeholder Participation in AI - <https://arxiv.org/pdf/2111.01122>
- Stakeholders' Role in AI Projects - [Stakeholder roles in artificial intelligence projects - ScienceDirect](#)



PLAY TAGS

- Executives
- Operations
- Technologists
- CISO/CPO
- Legal Counsel
- External Stakeholders
- Human Resources
- Finance
- End Users



Play 7: Develop Risk Matrix

Any organization currently, or in the future, planning to use AI-based capabilities needs to develop a Risk Matrix to review all the risks associated with the AI implementation. The developed risk matrix will also help ensure the trustworthiness of the implemented capabilities and help manage the risks and liabilities.



KEY QUESTIONS

- Have you identified the full range of risks your application might cause?
- Have you developed a response plan?
- Is there a clear plan in place once they are identified?
- Who is responsible for risk management?
- Are roles clearly defined for who will accept, deny, or mitigate risk?
- What is the quality of your data? What are the rules associated with data?
- How do you train your users on hallucinations?
- Are they matching up the Use Case to the quality of the AI output?
- Why was this deployed?
- What are the risks of any unauthorized use of the application?
- Are you dealing with bad actors?
- Is the dataset introducing risk?



CHECKLIST

- Ensure you have risk management in place
- Risk Identification/Assessment
- Identify potential risks to design and technical development, reputation and impact of delivery
- List vulnerabilities and mitigation including security and privacy provisions
- Identify management and sustainability plan
- Review regulation, reliability, availability, and financial feasibility/viability

- Need clear categories of risk
 - Understand all variations of risk/unintended consequences
- Continuous monitoring
- Verification cycle - confirming accurate information, validation/trust



RESOURCES

- NIST AI RMF Process - <https://www.nist.gov/itl/ai-risk-management-framework>
- NIAT AI RMF AI 1.0 - <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf>



PLAY TAGS

- Executives
- Technologists
- CISO/CPO
- Legal Counsel
- Governance
- External Stakeholders
- End Users

8

Play 8: Technical Implementation

Defining and establishing implementation models to suit the specific organization. Use Case/requirements required by policy and process objectives. If developing or procuring AI capabilities, it is important to conduct all the due diligence in vendor/technology selection to ensure that systems are reliable, secure, and adaptable to future needs. Most importantly, all consideration is given to data ownership, security, privacy, and reuse to develop current and future models.



KEY QUESTIONS

- Do states need to be more precise in their policies?
- Is the data going into a generalized AI model?
- Can we replicate the model and give it to another agency?
- Will you be using my data to give the trained model to other agencies?
- Is the data allowed to leave a certain boundary/state?
- How do we announce AI is being used in certain situations?
- Where does the model reside and who owns the model or rights to use the model?
- What are the model's hosting possibilities?
- What's the volatility of the data in the system?
- Can your data be sold?
- Who owns the data once it is entered into the model?
- Is the data going to be fed as is, or will it be generalized/ scrubbed/ cleansed to train the model or used for the model?
- What type of procurement language needs to be there?
- How easy/difficult are the natural language capabilities within the AI?



CHECKLIST

- Explain the need for the AI model
- Understand different data rules/protocols from state to state
- Consider having at least 2 datasets (restricted vs. unrestricted datasets)

- Consider data sharing across smaller agencies
- Look into the model algorithm being used
- Know what your agency wants to do with the outcomes
- Two different paths of questions (building a model vs. procuring an existing model)
- Language in terms of whether predictions/predictive analytics can or cannot be used by an agency
- Draft clear technical requirements that vendors must meet
- Conduct a security assessment of AI tools before deployment



RESOURCES

- NIST AI RMF for Generative AI - <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf>



PLAY TAGS

- Operations
- Technologists
- CISO/CPO
- Legal Counsel
- Chief Data Officer
- End Users



Play 9: Funding

As an organization starts its journey to implement AI-based capabilities via either procuring a Commercial Off-The-Shelf (COTS) solution, or developing its own, it's important to identify all the cost factors to implement, sustain, and redevelop or retrain models in the future. These costs will help the organization identify the overall cost that should be utilized to develop business cases and identify short and long-term funding sources for AI-based efforts.



KEY QUESTIONS

- Where can you find funds?
- What are the conditions for utilizing these funds? (Law, Guidelines, Act, etc.)
- What is the business case for the applications?
 - What is the Use Case?
 - Cost-based analysis/ROI
 - How much does it cost? What value does it bring?
- How can we come up with shared Use Cases to share cost?
- What are some of the considerations we should have from funding?
 - Understanding the maintenance of the model/evolution of the model
 - Are you paying for just the services/projects you need? Or for governance and oversight?
- How long do we retain the data within the model?
- Are residual revenues available?
- Is it solving a problem in a meaningful way?
- Do you have an in-house staff? Or contractors?



CHECKLIST

- Shared services model
- Build your own model vs. off-the-shelf
- Be intentional about your solutions

- Understanding the operational/fiscal cycles/capital planning/people planning
- Awareness of budgets
- Awareness of lifecycle costs (total implementation)
 - How many are static vs. dynamic costs?
- Validate via Proof of Concept (POC) any risks to not waste funding
 - Manage stakeholder expectations to mitigate risks
- Create Low Touch / High Impact evaluation / Risk Matrix / Ranking
- Acquire AI talent



RESOURCES

- National Science Foundation - <https://seedfund.nsf.gov/topics/artificial-intelligence/>
- Google Funding - <https://aiopportunityfund.withgoogle.com/>
- Bureau of Justice Administration (BJA) - <https://bja.ojp.gov/funding>
- U.S. Grant - <https://www.usgrants.org/business/artificial-intelligence-researchers>



PLAY TAGS

- Executives
- Operations
- Legal Counsel
- Human Resources
- Finance

10

Play 10: Training and Education

Training and Education for staff, executives, and stakeholders are crucial for organizations in implementing AI-based capabilities and functionalities. The training and education need to be developed based on the Use Cases and organizational goals and objectives to ensure the ethical and responsible use of AI.



KEY QUESTIONS

- Who is getting trained?
- Is the provided training been effective?
- What kind of training is offered?
- Who are the key people that need training within the agency?
- What certifications are required/desired?
 - Foundational understanding vs. certification
- How will we measure the effectiveness of training to ensure it meets learning goals?
- Who will develop the content? Where is the content stored? How often does it need to be refreshed/updated?
- How will training be tailored to be relevant to the job title?
- How is AI already being used?
- How the end user benefit from the training?
- What is the impact on the workforce?



CHECKLIST

- List all the audience
- Explain what AI is and why it matters to the audience
- Online Training/In-person workshops, etc.
- Monthly Security Awareness
- Logging of who completed which training
- Train users on AI capabilities

- How to understand if AI is right
- Retraining/new training when new policies are released, or existing policies are updated
- Evaluating current training/existing courses
 - Check reviews
- Method of training (i.e. audio, video, FAQs, website, books, on-site training)
- Budget



RESOURCES

- United Nations AI Workforce Development - [understanding_the_impact_of_ai_on_skills_development.pdf](#)
- Snowflake AI Education Material - [Generative AI and LLMs for Dummies - Snowflake](#)
- U.S. Department of Education - [Artificial Intelligence and the Future of Teaching and Learning \(PDF\)](#)
- Police1 Article - <https://www.police1.com/vision/the-future-of-law-enforcement-training-harnessing-ai-for-advanced-officer-development#:~:text=By%20integrating%20AI%20into%20their%20training%20programs%2C%20law,and%20address%20the%20complex%20realities%20of%20modern%20policing.>
- U.S. Congress LE AI Directive - [Law Enforcement Use of Artificial Intelligence and Directives in the 2023 Executive Order](#)
- Thomson Reuters Institute - [AI training for state and local government agencies - Thomson Reuters Institute](#)



PLAY TAGS

- Operations
- Technologists
- External Stakeholders
- Human Resources
- End Users

11

Play 11: Compliance and Standards

The compliance and Standards landscape for AI is changing regularly and all the homework must be done upfront and on an ongoing basis to identify all the relevant compliances and standards that your AI implementation needs to comply with. In the absence of this compliance, organizations may be penalized in the future which can increase the risk and liabilities associated with AI implementation and use.



KEY QUESTIONS

- What standards need to be implemented?
- What are the compliance/conformance criteria?
- What standards are most beneficial for the specific Use Case?
- What expertise is required of the development team to ensure the standards are appropriately included in the solution designs?



CHECKLIST

- Basic Technology Standards
 - World Wide Web (www) conventions
- Justice and Public Safety Standards
 - National Information Exchange Model (NIEM) Open
 - Federal Bureau of Investigation (FBI) Criminal Justice Information Systems Security (CJIS) policy
- Security and Privacy Standards
 - NIST AI Risk Management Framework
 - ISO
 - 27001 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
 - 42001 - Information technology — Artificial intelligence — Management system
 - 12791 - Information technology — Artificial intelligence — Treatment of unwanted bias in classification and regression machine learning tasks
- Ethical Standards

- County/Municipal/State
- Data Governance policies
- Municipalities regulations to be approved by Use Case
- EU AI Act
- Data exchange
- Appropriateness identification
- Defining a specific list of standards that apply
- Ensure governance entity and stakeholders agree with the standards
- Whenever possible, seek training opportunities to become more familiar with existing standards and their application
- Risk Matrix
- Methods for validating conformance (application testing)
- Establishment of an AI Governance Committee as part of your policy



RESOURCES

- NIST AI Risk Management Framework - <https://www.nist.gov/itl/ai-risk-management-framework>
- ISO
 - 27001 - <https://www.iso.org/standard/27001>
 - 42001 - <https://www.iso.org/standard/81230.html>
 - 12791 - <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:12791:ed-1:v1:en>
- EU AI Act - <https://artificialintelligenceact.eu/>
- FBI CJIS Policy - https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/cjis_security_policy_v5-9-5_20240709.pdf
- NIEM Open - <https://niemopen.org/>
- Risk Matrix <https://ijis.org/wp-content/uploads/2025/03/IJIS-AI-Organizational-Level-Skills-and-Ability-Matrix.pdf>



PLAY TAGS

- Executives
- Technologists
- CISO/CPO
- Legal Counsel
- Governance

12

Play 12: Algorithm/Model Transparency

Organizations should document and be able to explain any decision that was reached utilizing AI-based capabilities and associated algorithms or models.

**KEY QUESTIONS**

- Do we have a transparency model developed?
- Which algorithms are being used and how are they designed, developed, and implemented?
- What “guardrails” are built in to check before it is deployed?
 - Built-in deployments, policy considerations, security controls
 - What third-party auditing efforts are put in place?
- How can the model’s transparency be ensured, including visibility from input to output?
- What privacy and data security measures are incorporated into the model?
- What testing, including beta testing and deployment checks, is being conducted to validate the model’s performance?
- How do we maintain the integrity of the model and prevent unauthorized manipulation?
- How is the model trained and developed (e.g., structured vs. unstructured data, supervised vs. unsupervised learning)?
- How do we account for and mitigate potential bias during model training and data handling?
- Are agencies ready to send data to a model?
- Do we have the procedures in place to send unbiased data into the model for an outcome?
- How do we ensure the integrity of the models?
- What processes are in place to detect and address hallucinations or inaccuracies in the model, and who is responsible for this oversight?
- What steps are being taken to ensure agencies are prepared to send unbiased and high-quality data to the model?
- What governance framework and auditing processes have been established for model development and operation?

- How is the model trained/developed? (Structured, unstructured, supervised, unsupervised)
- What auditing efforts are put in place?
- Who holds accountability and risk if the model produces errors or malfunctions?
- Are agencies prepared to implement quality control measures and validate the outcomes generated by the model?



CHECKLIST

- Roadmap for predictive algorithms
- Mitigate bias and hallucinations
- Different levels of use
- Accounting for second/third tier of AI within certain solutions
- Embedding AI needs to be transparent



RESOURCES

- Guide to AI Model Selection - <https://medium.com/predict/a-comprehensive-guide-to-optimal-ai-model-selection-93cbdf81c071>



PLAY TAGS

- Technologists
- CISO/CPO
- Legal Counsel
- Chief Data Officer

13

Play 13: Workforce Development

Developing and/or Implementing AI-based capabilities will require skill sets that organizations might not have, so determining the skills required is a very important step. It might require organizations to develop new job descriptions, training needs, and innovative methods for recruiting talent.



KEY QUESTIONS

- What operational/technical skills are available in-house, and what skills are missing?
- What are the options for getting missing skills (e.g., acquisitions, training)?
- What skill sets are needed to develop AI capabilities?
- What is required to maintain and sustain the model?
- What will the learning/training methods be for developing skills?
- What funding will be used for workforce development?
- How will you acquire workforce development and know that you are getting training/development that is relevant, accurate, and beneficial?



CHECKLIST

- Define technical and operational skills required
- Determine the staffing lifecycle and requirements
- Evaluate current staffing capabilities
- Define a workforce development plan
- Comparing TCO to the skills and abilities map after use case development and definition phase
- Include all relevant stakeholders
- Develop Retention Plan
- The ability to understand and evaluate data
- Digital fluency in the application/model
- Define the sustainability model



RESOURCES

- U.S. IT Modernization AI Guide for Government Chapter 4 - <https://coe.gsa.gov/coe/ai-guide-for-government/developing-ai-workforce/>
- Skill and Ability Mapping - <https://ijis.org/wp-content/uploads/2025/03/IJIS-AI-Risk-Matrix.pdf>



PLAY TAGS

- Executives
- Operations
- Technologists
- CISO/CPO
- Human Resources