disc
Data Integration Support Center
WestEd

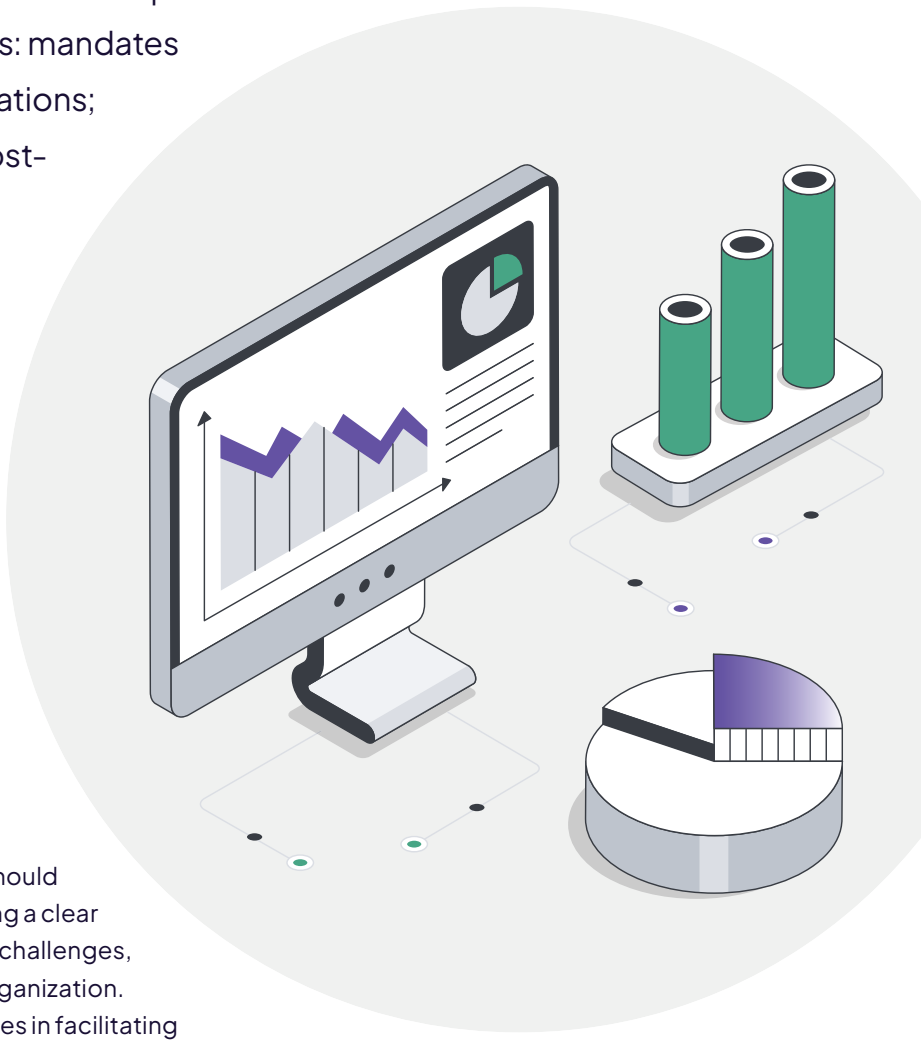
2025
September

SPOTLIGHT

Assessing Organizational Readiness for AI

AUTHORS:
Baron Rodriguez
Laia Tiderman
Sara Kock

As artificial intelligence (AI) gains momentum in the public sector, agencies are recognizing the need to assess their readiness before launching AI initiatives. Public agencies face unique challenges in adopting AI technologies: mandates to protect sensitive data; ethical obligations; and citizen expectations for quality, cost-effective services. Success requires careful planning and evaluation of capabilities, limitations, and risks.



This brief presents the AI readiness assessment framework developed by WestEd's Data Integration Support Center (DISC) to help agencies evaluate their capacity for AI implementation. The framework examines four key areas: organizational value, infrastructure and architecture readiness, privacy and security, and data readiness and governance. Through systematic examination of these areas, agencies can make informed decisions about proceeding with AI initiatives and identify areas needing further development.

Before adopting any AI initiatives, organizations should consider several factors. DISC recommends having a clear understanding of the risks, governance, benefits, challenges, staffing, training, and specific use cases for the organization. Additionally, DISC offers support to public agencies in facilitating discussions and forming strategies to create a strong foundation for AI implementation.

The Importance of Use Cases

Public agencies must develop use cases before conducting an AI readiness assessment. This foundational step ensures that the readiness assessment focuses on the agency's actual needs rather than abstract possibilities. For more guidance on developing effective AI use cases, refer to "Establishing Clear Use Cases for GenAI in Integrated Data Systems." Public agencies that need support with this prerequisite step can contact DISC, which facilitates use case development sessions. To learn how use cases translate into practice, review "Building a Secure Generative Artificial Intelligence Environment for Research Use," which details WestEd's implementation experience.

The Importance of an AI Readiness Assessment

An AI readiness assessment provides a comprehensive review of the agency's current capabilities, infrastructure, data landscape, and governance practices for a specific AI initiative. This approach ensures that each use case receives appropriate scrutiny based on its unique requirements, stakeholders, and challenges.

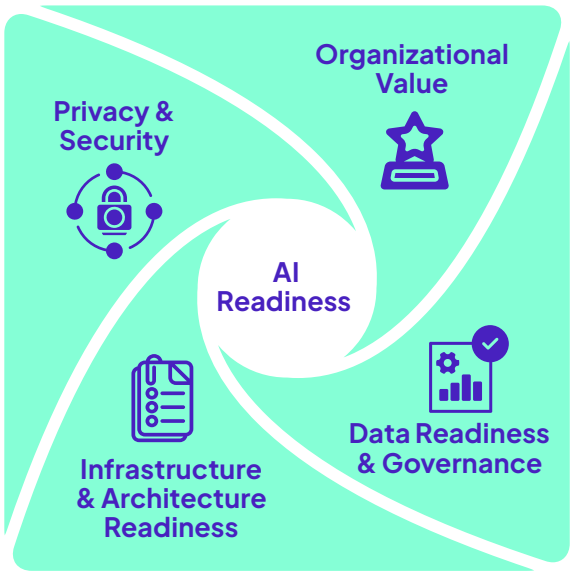
Conducting an AI readiness assessment delivers key benefits:

- **STRATEGIC ALIGNMENT:** Determines whether the AI initiative effectively addresses the identified need and supports organizational objectives.
- **GAP IDENTIFICATION:** Reveals weaknesses in capabilities, infrastructure, or data readiness, and provides a roadmap for improvement before proceeding with the AI initiative.
- **STAKEHOLDER ENGAGEMENT:** Builds shared understanding among business users, information technology (IT) staff, data owners, and legal experts, and increases support for the AI initiative.
- **RESOURCE OPTIMIZATION:** Guides effective allocation of staff time and public funds to the areas requiring the most attention and investment for the AI initiative.

The assessment is both point in time and use case specific. As agencies address gaps and capabilities evolve, new assessments will help determine if their position has improved. Each initiative requires separate evaluation because of unique technical requirements, stakeholder needs, and implementation challenges.

This strategic approach enables informed decision-making, risk mitigation, and responsible and sustainable AI adoption in the public sector.

AI Readiness Framework Areas



Key Area: Organizational Value

Assessing organizational value determines whether an AI initiative aligns with agency priorities and delivers meaningful benefits. This evaluation helps decision-makers understand the initiative's potential impact and feasibility within the agency's operational context.

Strong AI initiatives demonstrate the following:

- **CLEAR, MEASURABLE BENEFITS** in operational efficiency, cost savings, or service delivery, such as reduced processing time or improved accuracy.
- **FINANCIAL IMPACT** through both direct cost savings and indirect benefits such as enhanced decision-making or increased productivity. Return on investment calculations offer one method for evaluating these impacts.
- **STRATEGIC ALIGNMENT** with the agency's mission and priorities, ensuring that the AI initiative supports broader organizational goals.

Determining the value of an AI initiative requires evaluating several organizational and operational factors. Successful implementation often depends as much on stakeholder buy-in and change management as it does on technical execution. Agencies should assess their level of organizational readiness for change, including the following factors:

- **BUSINESS COMPLEXITY:** Complexity includes the involvement of new processes, the scope of changes to current processes, and the number of affected staff and departments. More complex initiatives likely will involve significant resources and pose greater risks, requiring careful evaluation of organizational capacity for change.
- **OPERATIONAL CRITICALITY:** Initiatives affecting critical operations such as public safety or financial transactions may require more stringent controls and oversight. The scale of deployment (e.g., pilot project, department-wide, or agency-wide) also influences resource and risk management and mitigation needs.
- **AI MODEL SOURCING:** This factor includes evaluating the agency's approach for acquiring or developing the AI model, whether it is creating the model in house, using machine learning platforms, or leveraging AI-as-a-Service (AIaaS) vendors. Each approach has implications for organizational capabilities, cost, timeline, and required expertise.

Organizational value assessment ensures that AI initiatives deliver meaningful benefits while remaining feasible within the agency's operational context. By evaluating both the initiative's potential value and organizational readiness for change, agencies can make informed decisions about proceeding with AI investments.

Return on Investment

When calculating return on investment for AI initiatives, agencies should consider both quantitative returns (such as staff hours saved or reduced error rates) and qualitative benefits (such as improved service quality or enhanced decision-making). The calculation weighs the total expected benefits against all costs, including implementation, training, maintenance, and staff time.

Key Area: Infrastructure and Architecture Readiness

Determining infrastructure and architecture readiness includes evaluating whether an agency's technical foundation can support AI development, deployment, and maintenance. Technically ready agencies demonstrate the following characteristics:

- **COMPUTATIONAL SCALABILITY:** The agency's server capacity and cloud readiness can handle AI workloads without compromising existing operations.
- **SYSTEM INTEGRATION CAPABILITY:** The established enterprise architecture can support AI solution integration while maintaining overall system stability.
- **DATA INFRASTRUCTURE MATURITY:** The data infrastructure is well understood and operationally capable of supporting AI storage, processing, and retrieval requirements.
- **DOCUMENTATION STANDARDS:** Clear architectural documentation includes diagrams, data flows, and system configurations for the proposed AI solution.

Additional infrastructure readiness factors include the following:

- **EXTERNAL DATA INTEGRATION:** The infrastructure has the capacity to incorporate high-volume data from external sources with varying formats and refresh frequencies.
- **SUSTAINABILITY PLANNING:** Documented plans address long-term viability, including startup costs, staffing requirements, ongoing maintenance, licensing, and training considerations.
- **TECHNICALLY READY STAFF:** The agency has adequate personnel with appropriate skills for model development, data quality management, and system maintenance. (See "Maintaining a Secure AI Environment: Resource Considerations" for detailed guidance.)

Agencies with mature technical architectures are better positioned to support AI initiatives while maintaining operational stability and system performance. Comprehensive assessment through cross-team collaboration ensures that agencies can identify and address technical gaps before AI implementation.

Creating Critical Documentation

Documentation serves as critical evidence of infrastructure and architecture capabilities during an AI readiness assessment. Without proper architectural documentation, agencies cannot effectively demonstrate their technical readiness. Therefore, agencies should prioritize creating this documentation before proceeding with the assessment.

Key Area: Privacy and Security

Data privacy and security require careful evaluation when implementing AI initiatives within public agencies. Although most agencies already have established security programs, AI technologies introduce new considerations that may require enhancements and updates to existing controls. Privacy- and security-ready agencies demonstrate the following characteristics:

- **COMPREHENSIVE DATA PROTECTION:** The agency has established processes for safely extracting, processing, and securing data throughout the AI lifecycle with Privacy by Design principles embedded in all initiatives.
- **OPERATIONAL MONITORING:** Comprehensive security management capabilities include patch management, security assessments of AI components, incident response for AI-related events, and accurate inventories of all AI implementations.
- **RISK-BASED DATA HANDLING:** The agency has a selection of encryption, data masking, or enhanced controls for unmasked sensitive data based on initiative requirements.
- **TAILORED SECURITY CONTROLS:** Security measures are tailored to the sensitivity level of the data being used, from standard protections for masked data to enhanced controls for unmasked sensitive information.
- **THIRD-PARTY SECURITY MANAGEMENT:** When using AIaaS or external vendors, the agency has established processes for evaluating vendor privacy and security capabilities, ensuring that they meet the same standards required for internal development, and providing ongoing monitoring of vendor compliance.

Beyond these core capabilities, agencies must also address several operational and policy considerations that support secure AI implementation. Additional privacy and security readiness factors include the following:

- **ACCESS AND AUTHENTICATION CONTROLS:** The agency has role-based access permissions and secure authentication infrastructure with comprehensive logging.
- **POLICY AND COMPLIANCE ALIGNMENT:** Updated privacy policies address AI-specific requirements and establish processes for evaluating regulatory compliance (Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act, etc.).
- **PRIVACY IMPACT ASSESSMENTS:** These assessments are conducted internally or obtained from vendors to identify and mitigate privacy risks.
- **STAFF TRAINING AND TRANSPARENCY:** The agency provides role-appropriate security training and clear communication about AI usage processes and approved tools.

By assessing privacy and security elements, public agencies can better understand their readiness to implement AI initiatives securely and responsibly. The AI readiness assessment helps identify gaps that should be addressed before proceeding with AI initiatives, ensuring that appropriate safeguards are in place to protect sensitive data and maintain public trust.

Key Area: Data Readiness and Governance

Data readiness involves two main themes:

- **DATA AVAILABILITY AND COMPLETENESS:** having comprehensive data inventories and access to all necessary data sources for the AI initiative
- **DATA QUALITY AND ACCURACY:** ensuring that data are accurate, complete, unbiased, and representative of the specific AI initiative

Public agencies should demonstrate that they have all the data the AI initiative needs and that these data meet quality standards for the AI readiness assessment. Agencies can meet this requirement by maintaining comprehensive data inventories and metadata systems that catalog, define, and document the data. Agencies may also implement data quality test plans—such as tests that determine whether data are in proper formats and relationship tests that evaluate logical consistency—to ensure that the data being consumed and processed by the AI initiative pass standards. In addition, agencies can establish ongoing processes for accuracy detection and review, with clear protocols that detail who conducts reviews, how frequently the reviews occur, and how issues are addressed. These processes must be well communicated across the organization so all staff understand their role in maintaining both data quality and data completeness.

Similarly, governance involves two themes:

- **DATA GOVERNANCE FRAMEWORK:** establishing organizational structures and processes for managing data throughout the project's lifecycle
- **POLICY AND COMPLIANCE MANAGEMENT:** developing policies for responsible/ethical use and ensuring compliance with legal requirements

The AI readiness assessment asks public agencies to demonstrate that they have the organizational structures and policies in place to manage data responsibly, including the following elements:

- formal data governance practices with clearly defined roles, responsibilities, and decision-making processes for data management
- centralized management of data quality issues, including processes for identifying, tracking, and resolving problems across all data domains
- responsible/ethical use policies that define principles and standards for AI development and deployment, addressing fairness, transparency, and human oversight
- compliance with state and federal laws regarding data, AI, privacy, and security, including thorough reviews of how legal frameworks affect organizational AI efforts
- AI governance structures, either as part of existing data governance functions or as standalone governing bodies, to ensure that AI risks are identified, mitigated, and managed effectively throughout the AI initiative lifecycle

Ensuring Data Completeness

Ensuring data completeness requires examining systematic gaps in data collection across time periods, geographic areas, and demographic groups. Agencies serving diverse populations must ensure adequate representation, including data from urban and rural communities and all demographic groups as well as data that account for seasonal variations for year-round services. Identifying and addressing these gaps is essential for fair and accurate AI implementations.

Conclusion and Recommendations

DISC's AI readiness assessment framework provides public agencies with a systematic approach to evaluate their preparedness across four key areas: organizational value, infrastructure and architecture readiness, privacy and security, and data readiness and governance. This use case-specific, point-in-time assessment enables agencies to identify gaps, develop improvement plans, and make informed decisions about AI investments.

Assessment outcomes vary significantly among agencies. Some may be ready to proceed immediately, others may need to address specific gaps, and some may require foundational capability development. Each result provides valuable strategic information for planning AI investments and resource allocation.

Public agencies should conduct comprehensive readiness assessments before launching AI initiatives. This proactive approach helps agencies avoid implementation challenges, optimize resource investments, and increase the likelihood of successful AI deployment that serves citizens effectively while maintaining trust and accountability.

Agencies interested in applying this framework can contact DISC for assistance with use case development and AI readiness assessment implementation.

How DISC Can Help

DISC at WestEd can facilitate productive conversations and assist in the development of an AI strategy for an organization's integrated data system (IDS). DISC offers technical assistance to public agencies free of cost, including the following services:

- training agency leadership and/or staff in generative AI best practices
- providing expertise on the scope and variety of AI tools to support data integration efforts
- developing use cases that leverage AI tools and aligning those use cases to the state's strategic priorities
- conducting neutral, external assessments of the maturity of the IDS and its capacity to support and scale AI technologies
- facilitating structured discussions to develop a foundation for the use of AI in the IDS

For more information on the AI services offered by DISC, visit disc.wested.org/focus-areas/ai/.

Suggested citation: Rodriguez, B., Tiderman, L., & Kock, S. (2025, September). *Assessing Organizational Readiness for AI*. WestEd.