

A Practical Guide to AI Readiness for Capital Programs

Lessons for evaluating AI adoption

Artificial intelligence is quickly becoming part of the conversation around public infrastructure and capital program management. But before your teams deploy AI tools, the proper governance, security, and oversight mechanisms must be in place.

Hugh Seaton, CEO of The Link and AI technologist, and a utility leader share insights into five key areas public agencies should evaluate before adopting AI.

1 Establish governance before deployment

One of the most important steps in AI adoption is creating clear policies before implementation begins. Without governance, employees may already be using AI tools independently, creating potential security, compliance, and data management risks. Establish policies that define acceptable use, oversight responsibilities, and review processes.

Who is responsible for AI oversight?

☐

Are policies documented and regularly reviewed?

☐

Have legal, HR, operations, and technology stakeholders been included in governance discussions?

☐

Key takeaway:

Establish AI governance before widespread organizational adoption. Clear policies should define acceptable use, assign oversight responsibilities, and help employees understand where AI can be trusted and where human judgment should be used.

2

Prioritize data security and compliance

You manage sensitive information related to infrastructure investments, funding, operations, and compliance. Any AI solution must demonstrate how it protects that data. When evaluating AI platforms, make it a goal to understand:

Where data is stored

☐

Who has access to it

☐

Whether data is used to train external AI models

☐

How the solution aligns with government security requirements

☐

What compliance certifications and controls are in place

☐

Security frameworks such as FedRAMP and other recognized standards can provide additional assurance when evaluating vendors.

Key takeaway:

Evaluation criteria should prioritize data protection first, not as an afterthought. Before adopting any AI solution, understand how your data is protected, who can access it, whether it is used to train other AI models, and how it supports your organization's security requirements.

3

Require transparency and auditability

AI-generated results should be explainable.

Transparency is essential for maintaining accountability and supporting audit requirements. You and your teams should be able to trace outputs back to the source data and understand how conclusions were reached.

Questions to ask include:

What information was used to generate the result?

☐

Can users verify source documents?

☐

Is there a clear record of how outputs were produced?

☐

Key takeaway:

Never rely on AI outputs your teams can't explain or validate. Make sure AI-generated results are transparent, traceable to their source data, and easy to verify.

4 Invest in employee training

Technology alone does not determine success. Employees need to understand how to use AI responsibly and effectively.

Training should address:

Appropriate use cases

☐

Data handling requirements

☐

Security considerations

☐

The limitations of AI-generated outputs

☐

When human judgment remains necessary

☐

Consider training to be a foundational part of any AI rollout strategy.

Key takeaway:

Train employees before giving access to AI tools. Training should include appropriate use cases, AI capabilities and limitations, security responsibilities, and when to use human judgment first.

5 Start small and validate through pilot programs

Rather than deploying AI across an entire organization, begin with targeted pilot programs.

Pilots provide an opportunity to:

Test security controls

☐

Evaluate compliance requirements

☐

Gather user feedback

☐

Measure business value

☐

Identify policy or process gaps

☐

Most importantly, pilots help determine whether a solution solves a real operational challenge and delivers meaningful value.

Key takeaway:

Successful AI adoption starts with controlled testing and measurable outcomes. Pilot programs can help identify policy or process gaps, gather user feedback, validate business value, and address potential challenges before AI is expanded across your organization.

AI has the potential to improve efficiency, increase capacity, and support better decision-making across large capital programs. However, successful adoption depends on more than technology.

Those best positioned to benefit from AI will be those that first establish strong governance, protect sensitive data, ensure transparency, train their workforce, and validate solutions through carefully managed pilot programs.

By focusing on these foundational elements, your organization can explore AI with confidence while maintaining the accountability and trust that public infrastructure programs require.

Get started