maximus

Federal Leaders Outline 4 Tips for Successful Data Governance

AS GOVERNMENT AGENCIES CONTINUE to implement transformative artificial intelligence (AI) solutions, agency leaders are engaged in a careful balancing act between adopting cutting-edge technologies at speed and scale while maintaining data integrity. The foundation for these two priorities is a comprehensive data governance strategy.

A recent roundtable discussion hosted by the Advanced Technology Academic Research Center (ATARC) and Maximus convened technology leaders from a variety of federal agencies to share the challenges and successes their organizations have encountered as they work to effectively **leverage data as a strategic asset**.

"Whether it be Artificial Intelligence (AI), machine learning or deep learning … technology has been evolving very quickly," one defense agency panelist said. "The question really becomes how do we take advantage of it?"

To answer that question, panelists highlighted the importance of fostering a data literate workforce, establishing a robust data governance strategy that clearly defines roles, ownership, and documentation requirements, and collaborating with external partners. Here are their top four tips to help federal agencies fully harness emerging technologies and streamline data governance:

1. Understand data: sources and structure for solutions.

Though AI can automate and simplify many traditionally manual tasks, it still requires human expertise. It's important that government technologists have a baseline understanding of the data driving innovative solutions, whether operational, tactical or enterprise data.

"As we automate many of our functions, if you don't have an understanding and context of the data, including its source, then it becomes more difficult to rely on the results for better outcomes," a military panelist said.

Establishing this knowledge base entails upskilling a workforce that can span up to five generations, many of whom, have experienced the transformation from a paper to a digital and now to a data-centric world. Training existing employees is essential to gaining efficiencies and expanding overall workforce effectiveness.

At the same time, many agencies are now investing in new employees who are already equipped with extensive data literacy. This supports the "Roadmap for Artificial Intelligence" **released** by the Cybersecurity and Infrastructure Security Agency (CISA), which includes expanding AI expertise in the workforce as one of its five lines of effort.

"As we go to automate many of our functions, if you don't have an understanding and context of the data, then it becomes harder to believe the results and have confidence in those results."

"CISA will continue to educate our workforce on AI software systems and techniques, and the agency will continue to actively recruit interns, fellows, and future employees with AI expertise," the roadmap states.

One panelist from a federal financial agency described the skills his agency looks for in new hires: "They are adept at systems architecture," he said, "and they understand the importance of the data integrity that's feeding the models within that architecture, in order to have the right monitoring [and] the right types of solutions that will give us signals as to when we're having difficulty with the integrity of the data that we're so reliant on."

2. Simplify data ownership.

On top of understanding the data fabric itself, navigating ownership can be a major challenge for many agencies. Traditionally siloed data management has led to complicated data use agreements, even between divisions in the same agency.

Such hurdles to efficient data sharing can make it "very difficult to be responsive and agile," a health agency panelist said, as the military panelist added, "to drive us to use these things across an enterprise … you have to be able to share data at a rate that we have not generally done."

As agencies work to truly maximize data as an asset, data governance strategies are now advancing beyond data use agreements to build in the comprehensive role establishment necessary for sharing data as easily and securely as possible.

In other words, "I want the enterprise to access all the data that they should be able to get to, while keeping private the necessary things that they shouldn't," the Maximus panelist said. "How do we make sure that the people accessing it have that authorization, and how do we make those things … seamless?"

3. Document everything.

The key lies in creating a robust data governance strategy, which can feel like a monumental task across such vast and diverse enterprises as government agencies. Governance starts as a set of shared standards and acceptability of use, which then needs to be applied and documented to each use case, one panelist described. For each data use case, the Maximus panelist recommended technologists begin by identifying the most important datasets to achieve the goal, building out context-aware policies, and considering user behavior in terms of security, device posture, and any network conditions that might impact the situation.

"As you're documenting and working with your technical people, then you'll be able to build out the path, and the model, and the plan," he said. To support governance efforts, agencies are creating groups of internal stakeholders supported by IT leadership to, as one panelist described work on "the governance and the overall framework for putting in a use case [and] defining the use case for advanced technology specifically related to artificial intelligence."

4. Partner with academia and industry.

Comprehensive data governance is not only necessary for collaboration within and between federal agencies, but also with external partners in academia and industry. These partnerships are crucial to realizing the full potential of modern, AI-driven tools and solutions.

For the defense panelist, such partnerships entail creating an acquisition research center to work with dozens of universities, "so we can leverage academia for thoughts, tools, techniques that we otherwise couldn't have."

Establishing governance strategies for sharing data with external collaborators brings a diversity of thought to government technology teams – perhaps academic researchers, students and industry leaders may find a new path or a new perspective for leveraging data.

These research groups and collaborative efforts are exciting and transformative, but their success depends on a firm foundation of data governance and management. Establishing governance rules may not be as thrilling as technology innovation, the Maximus panelist acknowledged, but it is critical work.

"It's important to identify roles and responsibilities, and write it down, so that you can map those roles to tools. Policy will affect those tools and roles as the program moves forward," he said. "Customers are using this approach to build a governance framework. … Context is everything, how it's being used, the what, the why, and ultimately, the outcome."

Learn more about how Maximus can help federal agencies establish a robust data governance foundation to support innovation.

"You have to identify roles and responsibilities, and you have to write it down, and you have to map how those move to tools."

maximus

moving people forward

https://maximus.com/federal