



Tips for Dealing With Data, Cloud or No Cloud

Relying on cloud technology has helped agencies improve service delivery and enhance efficiency — and in the last several years, more IT teams have taken advantage of cloud offerings. The results can be transformative. But the transition has created a hybrid world of cloud and non-cloud infrastructure, of old mainframes and AI solutions, and highlighted a need for consistency and clarity.

During a recent [GovLoop virtual training](#), experts discussed how to use and secure data, whether located in a physical data center or the cloud, and regardless of agency mission. The underlying message: Agencies need a unified, coordinated approach. Below are four focus areas the speakers explored.



Lean Heavily on Interoperability

Agencies are like islands, each one laser-focused on its own goals and operations, said Rebecca Cai, Chief Data Officer for the state of Hawaii. Such fragmentation locks data in various formats with limited or no cross-agency access. “That creates different challenges because we are not talking to each other,” she said. “We might not be using the same tool [or] the same cloud solution. So for a true citizen-centric service, this causes a [problem], not to mention security and compliance complexity.”

You need a centralized, automated platform that establishes **granular, policy-based controls** — for instance, allowing users to request access, define the purpose and duration, and enforce restrictions, such as no printing or downloading. “Everyone’s willing to share the data to support others,” said Cai, “but they need to ensure that the data use is always in compliance.”

Regardless of restrictions, the platform must allow people to analyze data using machine learning and other AI. “We need to make sure we secure [the data],” Cai explained, “and empower the user by using it.”



Classify and Tag Your Data

Silos are a problem in general, but they can be devastating during emergencies, when various agencies — health, disaster management, law enforcement, etc. — need a **clear, holistic view** of all relevant data.

“That’s when it’s really critical to make sure that we have a consolidated, consistent data governance structure where we can link the data together, have data lineage, ... understand what data we have and classify [it],” Cai said. “With [unreliable] classification tagging, there’s no visibility into all the data we have on hand to solve a certain business problem.”

Tagging data quality as red, yellow or green helps keep AI algorithms honest. But don’t try to create an all-encompassing classification system at once, Cai said. Focus on small opportunities, starting with high-value use cases such as disaster recovery — identifying, cataloging and securing all pertinent data before turning to other key scenarios. “We want to laser focus on the small projects and build on small successes step by step,” she said.



Work Together on Compliance & Security

Compliance is tricky when half an agency's data lives in the cloud. "We used to have a pretty good handle on things like what our regulatory compliance mandates were when everything was sitting under our roof," said Jeff Reichard, Vice President, Solution Strategy with Veeam. "But now it's sitting in other places."

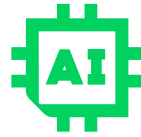
That creates security gaps, especially when security, compliance and infrastructure teams work separately — and falsely assume that cloud providers are responsible for protecting agency data. The more data sources that agencies draw from and analyze, the larger the footprint that's vulnerable to attack, he said.

"One of the things that's in our control is just getting the three [different teams] to **talk to each other early in the process**, so that we don't make mistakes or find out that we're exposed ... in ways that we didn't think about going into the problem," Reichard suggested. And adopt a "shift left" approach, that is, embed security and compliance into the development and deployment lifecycle.

"There's no silver bullet. People say, 'Oh, I have this tool, I have this AI.' It's [really] about how you use it, what recent problem you try to solve with it. That's how you can create impact."

Rebecca Cai
Chief Data Officer, State of Hawaii

→ [Click here](#) to watch the full session on demand and get more insights into using and protecting data in cloud and non-cloud environments.



Emphasize the Need for AI-Data Integrity

When drawing from unreliable, potentially insecure data, AI algorithms generate poor-quality results that can introduce bias and uncertainty into agency decision-making. With the rise of large language models and agentic AI, Reichard said, decisions increasingly are made by systems that operate like "black boxes," shining little light on the AI's rationale.

"It is certainly the case that governments and companies are going to find themselves needing to justify decisions they have made based on pointing large language models at AI data sets and be able to show that ... they really were acting without bias, with citizens' best interests at heart, with the best data that they could curate, to train their models and base decisions on," said Reichard.

Ensure data quality up front, then **guard that data so it's recoverable** using solutions such as Veeam technology, he said. "Despite the security of modern systems, you still need to plan around worse case scenarios, and you still need to make sure that the data is resilient," he added.

