

# Avert Disaster: How to Make Data and Systems More Resilient

When disaster strikes, whether because of a natural event or as a result someone's malintent, an agency must be prepared to bounce back — and quickly. It used to be that agencies could just pull from a backup file or system, but it's not quite that simple in today's modern IT environment.

At a recent GovLoop online event, [How Government Is Boosting Data Resilience, Disaster Recovery, Continuity of Operations and More](#), three experts from government and industry shared insights on prevailing approaches to being prepared.

## The participants

### Frank Indiviglio

*Chief Technology Officer at the National Oceanic and Atmospheric Administration (NOAA)*

### Peter Inzana

*Director, GoldenGate Product Management, Oracle*

### Jennifer Petry

*Oracle Database Administrator with the Akima family of companies*

## Challenges to Modernization

With modernization comes complexity, NOAA's Indiviglio said. For instance, agencies' shift to the cloud can complicate backups as it creates more places for data to be.

"Data moves through silos," he said. Agencies need "to track that to make sure we're backing up the right places and to know if it's okay to back it up at this initial state or if we have to back it up at the end."

Data security is the biggest pain point that Akima's Petry said she sees. It covers everything from a hacking or accidental deletion to inaccessibility of database backups, out-of-sync standby disaster recovery databases and lack of money to support backups.

"If somebody gets a hold of your backup, they could go and get the data from it," she said.

Cost is certainly a challenge, Oracle's Inzana added, noting that experiencing downtime can get expensive. "Across North America, a large company will experience about 87 hours per year in downtime, and if it's a mission-critical application, it can cost around \$350,000 per hour of downtime," he said.



## How to Create a Modern Disaster Recovery Strategy

The first step to determining where to focus time and money for disaster recovery is to prioritize systems and determine how much downtime your agency can tolerate for each, Inzana said. Generally, mission-critical systems rank high on the always-available list.

“It’s not just an infrastructure hardware approach. You’re also working at the data level and the people and process level because even once you move over to a backup system, everyone else’s connectivity needs to go over to that backup system,” he said. “Then when you want to restart and go back to the original, it needs to be dynamic, and it needs to work flawlessly for you to achieve that zero downtime and zero data loss.”

Trust is also crucial, Petry said: “Trust that the data is getting backed up as you expect it, whether you are putting it to disk and you are hoping that the disk doesn’t go bad or the machine doesn’t go bad, or whether you send it to tape and you pray that the backup team is backing up the right data, and that it’s recoverable.”

Verify that backup and recovery are happening correctly by conducting frequent test runs, such as tabletop and simulation exercises, Indiviglio recommended. “Make sure that ‘Hey, I can back this up, and I can recover it, and I can do the switchover,’” he said. Do this “not when it counts, but when you have time to fix the problems that you find.”

## Elements of Robust Recovery

In developing and evolving your backup plan, it can be easy to lose sight of what’s at the heart of it: data, Petry said. “Everybody wants it, including the bad guys, the hackers and ourselves,” she said. “We love when text messages come in, we want to know everything about the weather, our bank accounts [and] we want it all now. The takeaway would be to make sure [you] can access [your] data as soon as possible.”

Additionally, you need balance between what’s happening today and what to plan for tomorrow. “We can’t just assume that our growth curve will stay flat because we all know that won’t happen ... especially in the age of AI, where everything now is potentially going to be used for some other model,” Indiviglio said.

One thing to plan for is portability, he added. “There are now tools where you can make your workflows more portable so that they can quickly move from one provider to another if they need to,” Indiviglio said. “If we want to recover quickly ... the environment has to be to some extent portable.”

Ultimately, wherever you are with your backups, “you ideally want to have a zero recovery point objective, assuring that you haven’t dropped any data when you move over to the new system,” Inzana said, adding that the recovery time objective should also be zero. That means “you haven’t had any downtime, in theory, because the new backup fired up right away.”

 *To learn more, watch the full session on demand.*

