The health of your Disaster Recovery plan is important. Do you need a check-up?

How do you plan for the unexpected? Agency leaders know you can't just create a shelfware plan for a disaster – you have to actively remain on watch, ready to face the unknown. Having a well-tested Disaster Recovery (DR) plan is essential for an organization's ability to respond to and recover from any event that negatively affects operations. Investing in a comprehensive DR plan is no longer an option for today's agencies – it's too important, and could affect everything from customer satisfaction, data protection, and the ability to deliver the mission. And those are just the obvious ones.

The team at the Centers for Medicaid & Medicare Services (CMS) Healthcare Integrated General Ledger Accounting System (HIGLAS) and related systems learned this lesson well -- that DR is an ongoing process that demands constant attention. Chris Martin is the Director of CMS's Financial Management Systems Group responsible for HIGLAS's infrastructure, as well as its budget, reporting, and identity management systems. In this vital mission, Martin is supported by his partners at General Dynamics Information Technology (GDIT). As Martin says, proactively managing and leveraging a DR environment to its fullest capacity is "turning the unknown into the known." This case study illustrates that organizations shouldn't simply plan for the next major disaster—they should actively execute DR exercises by performing frequent real-life production scenarios.

It's time for a check-up

Requirements around disaster recovery

The CMS HIGLAS teams performed a remarkable weeklong production exercise highlighting the "art of the possible." As part of their overall modernization planning, the team performed a test that purposely failed over the entirety of their architecture into a DR environment. And it operated there for a full week, failing back to the production/primary site with zero data loss.

The HIGLAS Production DR exercise offered a new and positive DR perspective—by being innovative in the way they incorporated DR testing in operations while managing and maintaining their financial systems' architecture. DR should be much more than simply an insurance policy. As agencies and organizations start to finalize steps to comply with the new Executive Order on Cybersecurity, looking at cost-effective ways to use DR in innovative ways is an important consideration.

Step 1: Ask Questions

To plan for a robust disaster recovery program, the first step is simple. Ask questions. When CMS began to examine its systems, the team first defined the agency's overall mission. This included the HIGLAS payment system, hosted on Oracle application E-Business Suite. This system is crucial for millions of payments to flow at all times, regardless of a disaster or pandemic. After drilling down on every aspect of the payment process, the CMS team was then able to ask the right questions to enable building a robust DR plan.

But what are the right kinds of questions? James Donlon, Director of Solution Engineering at Oracle, offers a few steps. "First, what is your recovery time objective? How long can you be out before you need to be back up and running? The second question we always ask is, what is your recovery point objective? We can always re-process that or re-run that transaction. And so, driving what we do next really always starts with those two questions because that's going to determine how you plan how you prepare."

Initial questions:

1. What are your critical systems?
2. What is your recovery time objective?
3. What is your recovery point objective?
4. How much data, if any, can you afford to lose?
5. What about security?

Once the CMS team answered these questions while understanding their technology ecosystem, they began their recovery plan journey.

Step 2: Build the plan

Having the right technologies in place to ensure you have a DR plan without disrupting existing services is important. Martin notes, "It didn't happen overnight, and it didn't happen auto-magically either. There was a journey, and it started several years ago when we transitioned off of legacy hardware onto Oracle Exadata Database. As technology changes constantly, our environment changes constantly every three to six months. And as technology evolves, our environment evolves as well. We never stay status quo."

Keep in mind, the evolution of the cloud, cloud infrastructure, and pieces in an open, multi-cloud environment all offer investment options. Cloud options can be fast, and keep costs low.

Step 3: Test your Plan

Intel’s Chief Solutions Architect, Darren Pulsipher reminds users, “To test your business continuity plans, you've got to make sure that your team is educated on what it means to go through this process. And you know, if you don't have a business continuity plan that includes data breaches and ransomware - then you're already too late.” This means to take into account the cost and complexity of the plan, the skills of your workforce to address them, and the risks of failure possible.

For the HIGLAS team, planning for a test of their DR system was not an insignificant task. For an agency that completes over a billion dollars in transactions daily, they had to have confidence in their plan. The way you gain confidence in your plan is to test it. They tested 225 scenarios before deciding to change their standard test into something much bigger.

The team tested several scenarios and added complexity with each round. This resulted in the first-ever week-long Production DR exercise for CMS/HHS, demonstrating CMS has a proven DR/Continuity Plan for their financial system of record and budget. As Kamal Narang, Vice President & General Manager for the Federal Health Sector at GDIT, put it, “What this test demonstrated was a relentless passion for the mission on making sure that we are always on and payments can always flow through the HIGLAS system at all times.”

Step 4: Evaluate the success

CMS laid out the results for the HIGLAS DR efforts:

- **Seven** months of planning and execution, **30** production applications and tools, **41** external systems or end points connected, **six** hours to failover to DR, **six** hours to fall back to production
- **1,450** miles between primary and DR sites, **225** scenarios tested, **three** mock validations, **51** lessons learned
- **Six** days of production operations from DR, **1,254** distinct users
  - **21,246,396** claims processed, **$17,172,782,756.52** in payments
  - **29** stakeholder communications
  - **72** changes deployed at DR, **one** agile release, **11** incidents
- **Zero** data loss, service loss, performance/capacity issues, access/provisioning issues, transmission/connectivity issues

Step 5: Repeat

While you can test and retest theoretical situations, you have to remain nimble, agile, and open to the idea of the unknown. According to Darren Pulsipher, "no one really thinks of disaster as a ransomware attack or a data breach or a cyberattack, and we have to start broadening our definition of disasters, and how are we going to recover from them? The pandemic was another major disaster that caught a lot of organizations kind of flat footed. At first, then they had to react quickly so your DR plans your disaster recovery plans that you have are going to have to change a little bit from our traditional thoughts of what DR means."

To learn more about CMS HIGLAS's Disaster Recovery plan and lessons learned, watch the Oracle One Federal episode "Disasters Happen – Is your agency's IT continuity plan in place?" at **Oracle.com/OneFederal**

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.