

ENSURING BUSINESS AS USUAL:

Building a resilient government
with a secure cloud

In the midst of a global pandemic, state and local governments are grappling with how to best provide services in this new normal — and beyond. Cloud solutions could help spur agencies to continue like normal even when faced with a crisis.

With the backdrop of COVID-19, government agencies nationwide are adapting to fewer resources and a reduced workforce. Less tax revenues equal leaner budgets, and layoffs mean there is less manpower within each agency. Combined, these obstacles contribute to an economic challenge for city, county, and state localities attempting to provide communities with the services and information they need.

More than ever, government entities are embracing cloud solutions to ease the pain from COVID-19, says Bob St. Ledger, director of industry solutions at Infor, an enterprise cloud software company that helps governments transition to the cloud.

“Striving to remain resilient requires strategizing how governments can streamline their services offered to constituents,” he says. “How can we improve the way government runs to make the citizens and business partners really continue to thrive? Cloud offers the answer to these questions.”

The benefits of the cloud

Applying security and maintenance patches to government agencies’ aged, on-premises solutions — coupled with backups, disaster recovery, and the personnel it takes to maintain legacy applications — is labor intensive and comes with a significant price tag, St. Ledger points out. A move to the cloud, however, allows agencies to offset those costs.

A cloud service provider will handle hosting the application, applying all the patches, and securing the system through backups and disaster recovery. Amazon Web Services (AWS), Infor’s preferred cloud service provider, also offers elasticity for

when there’s high demand during the day or during a particular cycle when government service demands spike.

AWS GovCloud (US) Regions provides government customers the flexibility to architect secure cloud solutions that comply with key regulations and requirements such as FedRAMP High. It’s accessible only to U.S. entities and root account holders who pass a screening process. AWS GovCloud (US-East) and (US-West) Regions are operated by employees who are U.S. citizens on U.S. soil.

With AWS, governments can enhance reliability with cloud backups and cost savings by paying only for the cloud resources used. They can add scalable capacity any time. Users can access durable and cost-effective cloud storage managed by U.S. persons while meeting data security requirements. Additionally, IT systems can be backed up, stored, and recovered in seconds by supporting popular data recovery approaches that immediately fail over.

Cloud offers many capabilities that on-premises solutions don’t, including attractive user applications, mobility, and citizen or contractor portals, which are necessary in today’s world.

“Citizens and business partners demand modern technology and more business applications that mirror what people use in their private lives available for their work life,” St. Ledger says.

In other words, citizens want to be online, not in line.

“People don’t want to stand at a counter or fill out paper,” St. Ledger says.

Agencies now deliver tasks that typically involved a human, such as project reviews and inspections, virtually, thanks to



cloud technology. Departments that made the transition to the cloud prior to the pandemic successfully kept their licensing, permitting, and virtual inspections open, St. Ledger says, as opposed to entities that never made the move. Organizations that migrated their financial, human capital management, and payroll solutions to the cloud continued the government's business even when office access was limited, as well.

"That's where the cloud definitely will protect you against the current COVID-19 situation and, as we come out of this, whatever else might be thrown our way in the next few years," St. Ledger says.

Security in the cloud

A crisis isn't the only reason to adopt the cloud.

Being a resilient government means fending off digital assaults. As ransomware attacks continue to target government entities, hackers often exploit legacy applications and unpatched systems to gain entry. And the onslaughts are relentless and never-ending. In the last couple of years, nearly 200 state and local governments have succumbed to ransomware attacks — and those are just the publicly known incidents.

But there are ways to keep the bombardment at bay. Cloud solutions play a crucial role in efforts to block ransomware attacks. Even though these strikes could happen in the cloud, "with on-premises solutions, you are more exposed," St. Ledger says.

To make sure sensitive data is safe in the cloud, St. Ledger offers some tips for government leaders.

First, work with a vendor whose cloud platform and solutions meet a high level of compliance standards, such as those outlined in the Federal Risk and Authorization Management Program (FedRAMP) or the National Institute of Standards and Technology (NIST) guidance for access control and cybersecurity risk.

The state of Idaho selected Infor CloudSuite solutions for its statewide financials, supply chain, and human capital management based on Infor's unique FedRAMP-focused applications. The ability to scale and secure citizen data was one of their main drivers for choosing a FedRAMP-certified vendor.

"We wanted to modernize a system that not only gave us the ability to meet our current needs but gave us the platform ability to move forward as we continue to meet the future needs of the state over the next few years."

Josh Whitworth Chief Deputy Controller, Idaho

The cloud also helped California's Los Angeles County achieve 60 percent in cost savings and 17 percent in call reduction. The county used Amazon Connect to implement a virtual contact center to better handle calls from county employees facing IT issues. The all-in-one fully cloud-based solution slashed hold times by automating simple requests and made it easier to gather information and user feedback. Additionally, the solution added flexibility and mobility for agents, allowing them to spin up a remote contact center in an emergency and more.

Second, understand which business applications are needed to run and modernize your organization. Then, ensure the vendor provides those applications. Specifically, St. Ledger advises government IT leaders confirm vendors offer business applications that map to its needs, including financials, supply chain, human capital management, asset management, or licensing and permitting.

And third, IT teams should obtain a good grasp on the agency's reporting needs. It's important to ask if the vendor has a cloud reporting strategy that will let the agency use whatever data is in the cloud, on premises or in a hybrid environment, and make sure that data belongs to the agency, not the vendor.

"There are some vendors out there who want to own the data, but the data belongs to the government," St. Ledger says.

What to move to the cloud

Cloud is by no means a new technology; most agencies already have various applications both on-premises and in-progress with their cloud strategy. But many hesitate to migrate certain functions, such as financial, supply chain, and human capital management suites.

Take human resources, for example. Moving those workloads to the cloud allows access to more modern hiring and onboarding applications, such as behavioral modeling tools or other technologies to help automate the process and identify the best candidates for specific roles, St. Ledger says.



Reporting is another function that tends to stay on premises. But budget expenditures, grant success tracking, procurement analysis, among others, lend themselves well to a cloud environment—enabling agencies to better conduct analysis on the data.

“The better cloud reporting solutions can pull data from virtually any data source, whether it’s somewhere else in the cloud or on premises. They can read a spreadsheet or cards that need to be translated into meaningful data within a platform.”

Bob St. Ledger Director of Industry Solutions, Infor

More cloud, fewer problems

Many government leaders also worry about how long it would take or how costly it could be to migrate legacy platforms to the cloud.

“A lot of times, organizations may not have the appetite to do that,” St. Ledger adds.

With a company like Infor at their side, agencies can transition their applications in a much smoother way that leaves the tedious work to the cloud provider.

“That’s a huge burden that gets removed from an IT team’s shoulders and put into the cloud for your cloud service provider to manage,” says St. Ledger.
For example, Infor recently worked with Rainbow Municipal

Water District in California to move its business applications and financial supply chain to the cloud after wildfires in the area threatened to disrupt its operations.

“They actually moved to the cloud in response to these wildfires, worried their data center might be vulnerable to the fires,” St Ledger says.

Rainbow moved to a cloud data center, migrating all business applications and the entire financial and supply chain.

“That positioned them well prior to the pandemic because they were already operating in the cloud, allowing them to continue offering services to their citizens and constituents,” St. Ledger says.

Whether it’s another pandemic or wildfires, how can agencies steel themselves for the next unimaginable scenario? St. Ledger says it starts with reviewing their current cloud strategy and determining how to accelerate their move to the cloud.

“If you can really get your applications running in a secure cloud environment, then that should allow you to brace yourself for whatever next world disaster comes your way,” he says.

LEARN MORE

about how Infor can help your agency adopt secure cloud!

infor