Simplify Cloud Adoption With Managed Services

MARKET TRENDS REPORT

Executive Summary

Federal agencies have been steadily moving operations to the cloud for years now, in line with the Obama administration's Cloud First policy, now the Trump administration's Cloud Smart policy. Agencies are aware that getting to the cloud via an agreement with a cloud service provider (CSP) is only the first step in the journey. Once they have moved operations to the cloud, new challenges await.

Providers such as Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure (OCI), IBM Cloud and others deliver a solid framework for cloud operations and services, but what they provide only goes so far. Agencies have their own to-do lists, including the difficult task of migrating legacy applications and workloads to the cloud and efficiently managing operations once applications are set up. Agencies will need to ensure the security of sensitive information that can be exposed outside the confines of their secure enclaves or stolen by attackers exploiting an expanded cloud attack surface, according to the shared responsibility model.

Faced with shortages in both manpower and cloud knowledge, agencies could benefit significantly from cloud management expertise and guidance to fill the gaps in what service providers deliver. A managed service provider can help them take the best advantage of what cloud offers while avoiding pitfalls that lead to ineffective services, misspent money or risky cyber vulnerabilities.

To learn more about the challenges agencies face and how to best overcome these obstacles, GovLoop partnered with Credence Management Solutions LLC, a cloud managed service provider to the government. This report will describe how managed services for cloud hosting support can help solve the pressing issues of migration, operations and security.

By the Numbers

$7.8 billion

federal spending on vendor-furnished cloud computing goods and services forecast for fiscal year 2022.

Source: Deltek Federal Cloud Computing Market, 2020-2022

94%

of workloads and compute instances will be processed by cloud data centers by 2021.

Source: Cisco Global Cloud Index

57%

of federal respondents say they expect to use multiple public cloud providers.

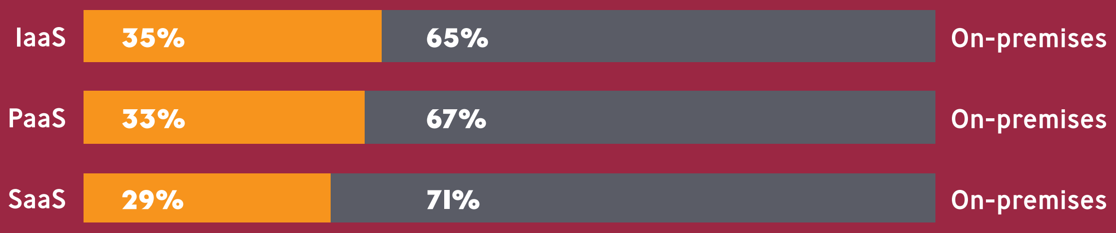
Source: Ponemon Institute, Cloud Adoption in the U.S. Federal Government

What makes migration to the cloud difficult?

- **65%** of respondents said the inability to achieve a strong security posture
- **61%** of respondents said the migration complexity across on-prem and cloud
- **60%** of respondents said the lack of visibility into resource utilization, metering and monitoring
- **59%** of respondents said workforce constraints
- **57%** of respondents said the inability to migrate workloads across cloud infrastructures
- **56%** of respondents said the inability to manage risks and enforce governance and policies

Source: Ponemon Institute, Cloud Adoption in the U.S. Federal Government

Percentage of agency mission-critical applications using Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) versus on-premises software applications:



Source: Ponemon Institute, Cloud Adoption in the U.S. Federal Government

Cloud Deployments Stretch the Bandwidth of IT Teams

THE CHALLENGE: CLOUD SERVICE PROVIDERS ONLY GO SO FAR

A cloud service provider provides a wide range of capabilities, including the cloud platform and infrastructure, application and storage services, and nearly unlimited scalability, along with protections for the hardware, software, networking and physical data center facilities running the cloud services.

Traditional CSPs "focus on the nuts and bolts and the building blocks of the cloud," said Atul Mathur, Chief Information Officer (CIO) at Credence and the technical program manager on several federal agency projects. "But when the rubber meets the road, and the applications are running in these CSPs' cloud environments, there are a lot of other things the government has to worry about."

Agencies have security responsibilities (such as their own platform, software and data) and must meet compliance requirements such as those in the Defense Department's (DoD) Security Technical Implementation Guides (STIGs). And they face other challenges, from dealing with legacy systems and applications, to managing operations well enough to incorporate advanced technologies such as artificial intelligence (AI), robotic process automation (RPA) and DevSecOps, a methodology that brings together an organization's development, security and operations teams.

Three areas of particular concern:

Security. First and foremost, the most important aspect of cloud computing for agencies is the security of their data. The Federal Risk and Authorization Management Program (FedRAMP) and the Defense Information Systems Agency's (DISA) Cloud Computing Security Requirements Guide (CC-SRG) establish the essential requirements for services delivered via the cloud, but agencies also have to ensure that they secure their platforms, applications, access control, operating systems (OS) and configurations.

Migrating workloads. Agencies need a comprehensive strategy that covers areas such as procurement, operating costs, employee training and migration timelines. Mission-critical applications may not translate easily to the cloud, and a lot of the aspects of management are not included in a provider's cloud service.

Operations. Managing a cloud environment — particularly a hybrid, multi-cloud environment — involves a lot of moving parts, including infrastructure to support mission-critical needs, applications and services. No one can be an expert in every area, so agencies may need expertise they may not have in-house in order to address all of their challenges.

THE SOLUTION: MANAGED SERVICES SUPPORT

A managed cloud services (MCS) provider, particularly one experienced in working with government agencies, can offer the expertise and knowledge necessary to help agencies adopt, migrate to and manage their complex cloud environments.

CSPs can provide infrastructure management, provision cloud environments and proactively manage service level agreements (SLAs). Service management components can provide 24/7 support, ensuring that applications are up and running, giving users access to the resources they need with short response times to review alerts, manage incidents and respond to critical issues.

A managed services provider can also help agencies make the most of their environments by supporting automation — which is essential at the speed of today's cloud operations — and DevSecOps adoption.

A provider can, for example, stand up or tear down a test environment; they can also configure files or applications in a quick, automated way, which eliminates the human error that can result from doing it manually, Mathur said. Compliance risk management, which helps ensure security while meeting the government's compliance requirements, is an essential service for agencies.

By providing end-to-end cloud management services, a provider also positions an agency to employ new technologies, such as machine learning, artificial intelligence and advanced analytics, to derive the most value from its data and to better share it both within and outside the agency. In addition to improving an agency's services, the streamlined approach will aid in meeting goals set forth for data-driven decisions outlined in the Evidence-Based Policymaking Act.

Best Practices in Cloud Deployments

A comprehensive cloud migration strategy should encompass areas such as enterprise architecture (EA) and portfolio management, infrastructure acquisition support and application rationalization — another critical step during a cloud migration, as every legacy system tends to have unapproved, unused or redundant "shadow IT" applications. But moving to the cloud is only step one. Here are some best practices that agencies should follow to get the full benefit of moving to the cloud:

Embrace cultural change

In many ways, the cloud represents an entirely new way of operating for agencies, and managing that change needs to involve the entire organization. "Getting the buy-in at the highest level, at the executive sponsor level, is the most important," Mathur said, "because everything flows down from there." Managers and employees down the chain can follow what Mathur called deep discovery — learning as much as they can about cloud migrations, and building relationships with program officers, contractors and others involved. A managed services provider can be critical in providing guidance.

Ensure information security

Data is the lifeblood of any agency and the security of that data — especially sensitive data such as personally identifiable information (PII), contracting data or program information — is paramount. Agencies looking for support should ensure that a provider is well-versed in the Federal Information Security Management Act (FISMA), FedRAMP, DISA's CC-SRG and other applicable requirements. This involves working with officials at the top of an agency as well as the IT professionals in the trenches. "Cybersecurity is not an afterthought," Mathur said. A provider needs to be prepared to work with cybersecurity teams from the start, and to engage agency leadership and oversight agencies such as DISA for DoD workloads.

Enable automation

One of the great advantages of a cloud environment is the speed with which services can be developed, deployed, monitored and updated due to automation. Whether it is testing in a DevSecOps environment or deploying full-stack solutions, agencies need to be sure that processes are reliably automated to eliminate errors, relieve agency personnel from spending their time on manual processes and ensuring that risks assessments and compliance requirements are performed in a timely fashion.

Practice good governance

A strong governance plan is essential to managing cloud resources. By emphasizing the people, processes and technologies being employed, governance helps keep track of how resources are being used, which reduces risk. It also helps eliminate shadow IT, while allowing employees to focus on the best use of their time.

Case Study: Speed of Migration

One government agency Credence has worked with underscores some of the challenges agencies commonly face, and the solutions MCS can provide. The agency provides a mission-critical, enterprise-wide service that cannot afford to slow down, let alone suffer downtime. Its leadership was looking to modernize a mission-essential hosting system with a move to the cloud.

The migration presented difficulties resulting from the monolithic environment in which some of the agency's applications resided, whether physically close to a data center or in a virtualized environment. Versions of databases and operating systems, designed to work in an on-premises environment, were unsuitable for the cloud. As part of the migration, the databases were updated and re-platformed to align with the applications, front-end servers and web servers operating in a cloud environment.

Credence, working with AWS as a member of its public sector Amazon Partner Network (APN), migrated five applications with more than 300 terabytes of data to AWS's GovCloud enclave within 138 days. "Off the bat, they saw a 30% improvement in performance," in processing and delivering reports – which are very much in demand in the agency's mission, Mathur said. Credence immediately was able to identify areas for improvement, such as where computing bottlenecks were and where the agency needed additional resources.

The migration, which involved a few mismatched but mission-critical legacy systems, had presented some complicated challenges. "But once you have a good team in place, and the right technology in place, no challenge is insurmountable," Mathur said.

HOW CREDENCE CAN HELP

Credence Cloud Managed Services (CCMS) can help agencies throughout the move to the cloud, starting with a process for choosing a cloud provider all to way to an authority to operate (ATO). Credence focuses 100% on support for government missions and has extensive experience in helping agencies deal with multiple cloud environments and with integrating a wide array of cloud applications. Its team can help agencies design, build and operate end-to-end cloud solutions, tailored to each agency, with the scalability, agility and automated speed of deployment are essential to cloud operations.

Credence has built a platform of MCS based on a multi-cloud infrastructure. The platform is a full service suite to include tier 2 and above help desk support, operations and maintenance (O&M) of hardened operating systems, middleware, databases, and available cloud native services, security operations, cybersecurity compliance, network monitoring, business intelligence analysis and reporting of cybersecurity metrics, automation, and cloud solution architecture blueprints. Credence employs trained and certified cloud professionals to provide the highest quality of services.

Credence has worked with U.S. federal, civilian and DoD organizations and can advise agencies on selecting a provider, how applications and services interoperate, as well as provide managed services covering infrastructure, applications, services, compliance and other key aspects of cloud operations. Filling the knowledge gaps in agency expertise, Credence can ultimately help deliver improved, secure and compliant mission-critical services at an affordable cost.

For more information, please visit www.credence-llc.com or email cloud@credence-llc.com.

Conclusion

The future of government agency operations, like that of almost every organization, lives in the cloud. Much of present business operations are growing through cloud's assimilation of government activities. CSPs offer agencies a platform for moving to the cloud with reliable service, great scalability and its own measure of security. But the rest — from migrating to the new environment to ensuring risk management and compliance — is up to the agencies themselves.

Agencies face a range of complexities involved in bringing their legacy applications into a new infrastructure and managing people, technologies and processes in a new environment, compounded by the internal shortage of cloud skills and expertise that affects nearly every organization these days. Cloud managed services, such as Credence Cloud Managed Services, can fill the knowledge gaps while guiding agencies through the potential pitfalls in procurement, migration and operations management, and set the stage for the next steps.

ABOUT CREDENCE

Credence Management Solutions, LLC (Credence) is a leader among industry in providing innovative management, engineering, and technology solutions to United States Federal Government clients. Credence has successfully supported military services, Department of Defense (DoD), and other Federal Government agencies since 2005, with more than 95% of our work being performed as a prime contractor with "Exceptional" Contractor Performance Assessment Report (CPAR) ratings. Credence has been listed on the Washington Technology Fast 50 list for four years in a row and the Inc. 500 | 5000 List of Fastest Growing Companies for eight years in a row. We have a Top Secret (TS) facility clearance, along with a Defense Contract Audit Agency (DCAA) approved accounting system. Additionally, Credence's processes have been externally appraised at Capability Maturity Model Integration (CMMI) Level 3 (SVC and DEV), System and Organization Control (SOC) 1 & 2 Type II accredited, and certified as International Organization for Standardization (ISO) 9001:2015, 20000:2011, 27001:2013, 27005:2011, 14001:2015, 17025:2017, and AS9100D-compliant. Our high-quality work and strong emphasis on our customers' missions have resulted in a rapidly expanding business, with over 1200 current employees.

For more information, please visit www.credence-llc.com or email cloud@credence-llc.com.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to info@govloop.com.

ABOUT AWS

AWS is designed to meet the needs of government agencies on their cloud journeys. Authorized as FedRAMP-High, the AWS Cloud can service a variety of government missions securely on an affordable and service-based plan.

More than 5,000 government agencies already depend on AWS, selecting either AWS GovCloud (U.S.) or more tailored offerings. Now, TIC 3.0 allows many more agencies to continue moving to the cloud securely and efficiently. After going to the AWS Cloud, agencies receive access to machine learning, mobility and citizen-facing services.

Learn more at aws.amazon.com/governmenteducation/government.

govloop

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop