The Journey From **Cloud First to Cloud Smart**

How to get started

Federal agencies are moving their workloads to the cloud to achieve greater efficiency, scalability and lower costs, and to provide the ability to incorporate modern processes and technologies. And yet, since the introduction of Cloud First over a decade ago — when federal agencies received authority to implement cloud-based solutions — many of those agencies have struggled with how best to get to the cloud. Moving to the cloud isn't as simple as lifting and shifting workloads.

It's imperative to evaluate all aspects of the enterprise as there are many factors to consider, and it's well worth the investment to perform an honest evaluation before moving forward. Specifically, agencies should evaluate when it makes sense to move to the cloud, what types of cloud models best suit agency workloads, and how to proactively address potential issues around security and cost optimization.

Want to accelerate cloud adoption beyond Cloud First? Think Cloud Smart and leverage the federal government's guidance for fully realizing "the promise and potential of cloud-based technologies while ensuring thoughtful execution that incorporates practical realities."[1]

[1] Federal Cloud Computing Strategy

S Strategy and Planning

M Managed Services

A Agility

R Return on Investment

T Transformation

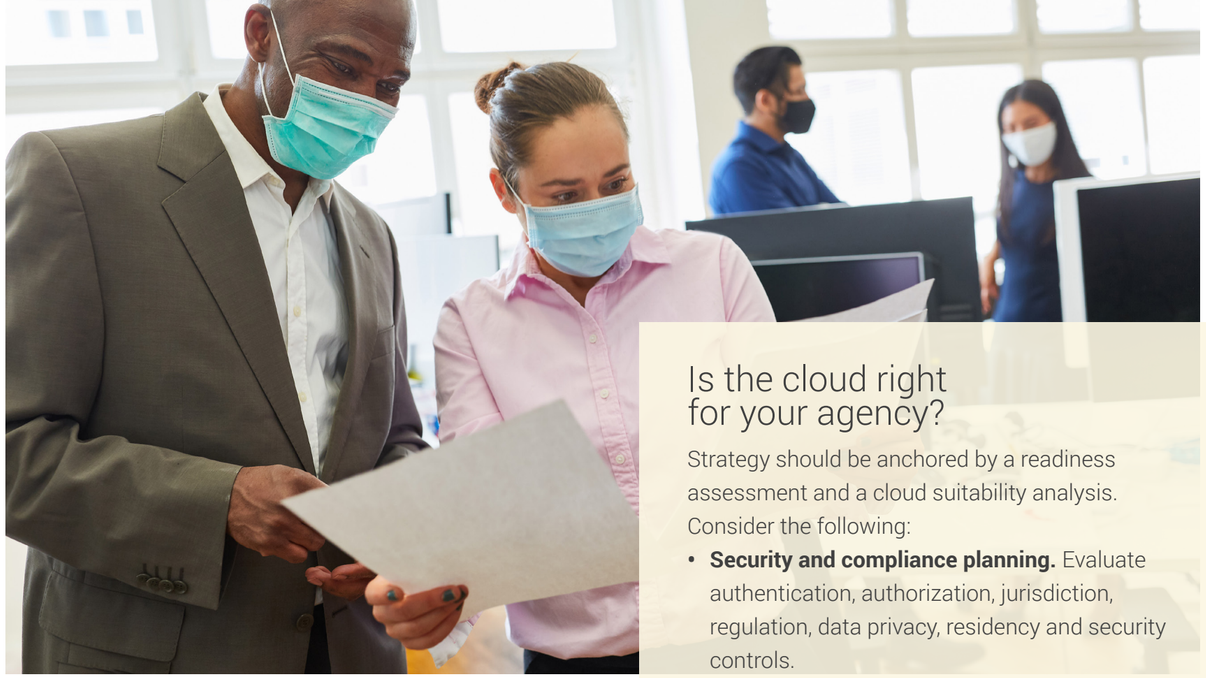
Strategy and Planning

The first step in making the right decisions is planning. By taking the time to thoroughly evaluate a potential move to the cloud, agencies can avoid making bad decisions. For example, good planning can help avoid duplicating efforts, making poor design decisions, causing performance and security challenges or cost overruns and creating new silos in the cloud.

"I've seen cases where an agency will stand up one cloud environment for a specific pilot project, a different cloud environment somewhere else for a similar program or project, without any up-front planning," says Shamlan Siddiqi, public sector chief technology officer for NTT DATA, a global business and IT services provider that services dozens of federal clients. "As those environments grow and more applications are added, it can get out of hand pretty quickly. Silos are formed and cloud usage bills are much higher than expected, because peaks and valleys weren't anticipated. Cloud is not about moving your workloads to a different infrastructure!"

Smart planning results in cloud smart

Proper strategy and planning go hand-in-hand. Evaluating a move to the cloud should start with basic assessment questions and then move on to strategy. To avoid becoming overwhelmed, it helps to break out these two areas and handle them separately. Begin by determining which workloads



are good candidates for the cloud. For each workload, ask:

1. How sensitive is the data or application? While the answer will depend on the agency's rules, and possibly a judgment call by senior decision-makers, certain data and systems containing sensitive data may not be good candidates for public cloud migration. If not, they may still be candidates for a hybrid cloud model.

2. How portable is the application? Some applications and systems are too architecturally complex to port effectively to the cloud. Or, they may have been built with tools and processes where the cost of migration outweighs the potential upside. In these cases,

Is the cloud right for your agency?

Strategy should be anchored by a readiness assessment and a cloud suitability analysis. Consider the following:

- **Security and compliance planning.** Evaluate authentication, authorization, jurisdiction, regulation, data privacy, residency and security controls.
- **Architecture.** Evaluate user interface and access points, as well as application complexity, size, internal/external dependencies, frequency of change and life expectancy.
- **Workload and performance.** Assess workload type, technology stack, current utilization, type of users, scalability, latency, elasticity, availability, throughput and variability of processing.
- **Environment topology.** Evaluate number of environments, production environment, usage, database, structured/unstructured data and middleware.
- **Financial and operational planning.** Evaluate operating costs, business value, risks to business criticality and business impact, business continuity, monitoring and tools/integration.
- **Automated discovery.** Assess OS type, OS version, number of processors, OS disk space, memory, network load balancing, database version and third-party components.

agencies may choose to keep the system on-premises. For applications that won't easily port to the cloud yet offer a strong cloud return on investment (ROI), consider an application modernization initiative that moves the system away from its legacy architecture to a container strategy in which the application is broken into microservices.

Choose wisely

For workloads slated to move to the cloud, agencies must decide cloud type, cloud provider and cloud tools. These complicated decisions depend on many factors. While the type of cloud will depend on the agency's workload needs, cloud tools will differ depending on the target cloud (private, public or hybrid). And if the agency uses some form of DevSecOps, it will require additional automation services. For example, Amazon Web Services (AWS) offers services to support DevOps processes like continuous integration and continuous delivery (CI/CD) with AWS CodePipeline for CI/CD orchestration, AWS CodeCommit for source and version control, AWS CodeBuild for continuous integration of compiled source code and AWS CodeDeploy for automated software deployment.

Confused?

You aren't alone, which is why agencies tend to choose their own model. While it can be tempting to choose a model or vendor with which IT staff are familiar, opt instead for the provider most appropriate for the agency's workloads and standardize. Standardization provides consistency, which decreases risk and improves operational efficiency and, in turn, grows agency productivity.

Achieve cloud security

It's important for agencies to adopt a proactive security approach with elements like zero trust architectures, DevSecOps processes for container scanning and a properly configured cloud access security broker (CASB) tool. Ensuring information systems adhere to relevant NIST 800-53 controls based on their risk rating should be paired with continuous monitoring of the environment. These practices will ensure foundational rigor when moving workloads to the cloud while maintaining compliance to proper controls in public and/or private clouds.

Cloud providers understand agencies are limited to suppliers that fully comply with the Federal Risk and Authorization Management Program (FedRAMP) and offer government-specific cloud offerings.[2] For example, AWS GovCloud gives agencies the flexibility to architect secure cloud solutions that comply with FedRAMP. However, agencies can dilute that security through misconfiguration or complexity. It's up to each agency to evaluate and mitigate the potential security risks of moving specific applications to the cloud.

[2] U.S. General Services Administration Federal Risk and Authorization Management Program.

Selecting the right infrastructure

Any agency charged with consolidating data centers into a single cloud has a lot to think about. While some might move forward decisively and quickly, others take the time to evaluate all options. That's the route one major regulatory agency chose, and it turned out to be a very good idea. The agency avoided integration complexities and security issues while ensuring the best ROI possible.

The agency started by fully understanding the needs and requirements for the architecture, its dependencies and security. As a result of that analysis, decision-makers chose an approach for migrating all data to a private cloud and standardizing on a platform that would allow developers to begin building cloud-native applications. The new infrastructure helped the agency reduce capital expenditures, create efficiencies in operational expenditures and avoid potentially damaging security breaches.

S Strategy and Planning

M Managed Services

A Agility

R Return on Investment

T Transformation

Managed Services: Get and stay cloud smart

The managed services provider (MSP) model offers access to highly skilled extended teams that specialize in the needs of agencies. This is extremely beneficial because the industry-wide lack of cloud computing skills has kept some agencies from pursuing cloud adoption at a greater scale. The benefits of cloud computing are moot without the cloud talent to architect, build, manage and maintain cloud systems. MSPs can even help agencies with workload evaluation, application rationalization and other important cloud adoption decisions. Their expertise can also help provide depth to the evaluation of which agency resources will benefit most from the managed services model.

Often, agencies opt to take on some of the responsibilities themselves and outsource others. For example, it's not uncommon for agencies to undertake smaller projects or maintain control of assets with data privacy and sensitivity issues. Conversely, MSPs are often called upon to manage initial assessments, large cloud migrations, new cloud-native application development, financial management and ongoing workload monitoring and management.

S Strategy and Planning

M Managed Services

A Agility

R Return on Investment

T Transformation

Agility: The Argument for DevOps

For greater agility and responsiveness, agencies should strongly consider a DevOps approach. DevOps increases the speed with which cloud-native applications are developed and deployed because it often makes use of automated pipelines that increase productivity and reduce errors manual processes may introduce. It also creates a more collaborative environment between development and operations teams as developers take greater ownership of code throughout the software development lifecycle and operations can create self-service environments that streamline the development process.

Making a smart cloud even smarter is DevSecOps. It adds security to development and operations processes, baking security into automated pipelines to ensure code is inspected as it flows through, while also baking security controls into self-service development products. DevSecOps favors the use of cloud-native technologies like containers, microservices and serverless development because they build on DevOps processes to further improve functionality, the user experience and overall quality, as well as reduce deployment failures, foster collaboration and speed development.

Like many of their commercial counterparts, agencies use DevOps processes to facilitate the streamlined build of new, cloud-ready applications that can take advantage of modern technologies and efficiencies. DevOps-inspired automation can result in processes, such as migration factories, for the repeatable migration of applications to the cloud.

Agencies have plenty of resources when it comes to adopting DevOps best practices. In addition to seasoned integrators and partners, the government has developed valuable resources. For example, the recently created DevOps Community of Practice on digital.gov helps agencies share best practices and lessons learned.[3] NIST is also developing guidance on DevOps and DevSecOps for agencies.

[3] DeveOps Community of Practice

Modernizing at mission speed

Over the past several decades, a major military organization has relied heavily on a mainframe-based supply chain platform to ensure its divisions have the supplies they need. Over time, the platform, which processes more than 60 million transactions annually, became slow, complex and expensive to manage.
To ensure the organization could continue supplying inventory to its units, leaders decided to modernize the system and move as much of the platform as possible to AWS GovCloud.

Working closely with the organization, NTT DATA used DevOps workflows like CI/CD to modernize the system. Today, the high-performance system supports mission needs in near-real time and stands ready to adopt new technologies as required. The new system saved the organization $25 million in annual hosting costs.

ROI: Ensure the best return on cloud

An important part of the Cloud Smart adoption process is evaluating ROI, which should include analyzing operating costs and the risks to mission criticality. By evaluating these factors, agencies can better understand which workloads will provide the best ROI in the cloud and which may be better off remaining on-premises. Strongly controlling these measures is critical to agencies achieving the expected cloud ROI.

How do agencies measure whether a cloud project is really paying off? There are multiple ways to evaluate cloud ROI, but many of those methods don't take into account everything they should. Often, ROI evaluations only consider upfront and ongoing costs. Yet, metrics like improved agility and flexibility, uptime, scalability and application performance can have a significant bearing on the results.

It's smart to focus on ROI

The time to start measuring the ROI of a cloud investment is well before the cloud project begins. In the months preceding the project, agencies should evaluate potential operating, integration and ongoing support costs; mission value and impact; and the cost of issues like business continuity, monitoring and expected demand. Be sure to build in visibility and insight across budgets, procurement and lifecycle so that they can ultimately map to cloud spend.

An agency's chargeback model is critical to the ROI process. Used by most agencies to allocate costs, the CIO's office will typically keep tabs on cloud usage by mission area and charge the cloud costs back to the mission office. Financial transparency and chargeback models should be flexible enough to change as an agency use cases and associated workloads scale and change. More proactive tracking of resources, processes, detailed cost models and financial reporting associated with technologies can help provide more financial transparency. With this data, agencies can optimize costs, better justify IT investments and make better decisions that help improve their ROI.

Right-sized instances

If a cloud project passes all these hurdles, the agency's next step is choosing the right cloud cost model. AWS, for example, offers three cost models. The first is called On-Demand Instances. This model charges for every second the cloud instance is used, with no long-term contract or commitment. It's the most expensive model but can be appropriate for some mission-critical workloads, especially those with unpredictable demand. Too many organizations make the mistake of using this model routinely, which can drive up costs unnecessarily.

The second type of cloud model AWS offers is called Reserved Instances. It requires a commitment of one to three years in return for a significant discount. This model is best for known workloads with predictable demand. The last model, called Spot Instances, is the lowest cost tier. With idle capacity, low cost and no commitment, Spot is best for flexible workloads and one-time actions or transactions. Understanding these cloud models is key to achieving positive ROI. By using the wrong cost model, agencies can drive up costs quickly — and unnecessarily.

Important considerations for positive ROI

- Include lead time for all stages, from commit to deploy
- Factor in time spent on unplanned and rework
- Calculate failure recovery time and unplanned incidents
- Evaluate deployment frequency (for DevOps workloads)
- Measure employee satisfaction, especially among high-performing teams
- Document improvements in user satisfaction
- Investigate failure rates and change failure rates

ROI evaluations don't stop once the workload moves to the cloud. Agencies can use a tool like AWS Cost Explorer to monitor cloud spend and identify underutilized resources for optimizing their cloud environment and producing desired ROI.

Transformation

With the right planning and focus, agencies can achieve their goals — improved operational efficiency, lower costs, better integration with other applications and solid security. In addition, they'll set the foundation to take advantage of emerging cloud-native technologies like microservices and serverless computing, which will allow them to further transform and optimize agency operations for security, speed and quality.

Cloud-native technologies

Microservices, a popular way of breaking development into small reusable components, speeds development because teams work on single aspects of an application's function, independent of others, allowing them to release updates when they're completed. In addition, microservices can be leveraged for reuse. By creating a library of microservices, developers can simply pull functionality together for deployment as needed.

A Cloud Smart strategy also allows agencies to take advantage of serverless application development; serverless removes the operational aspects of development completely by offloading them to a cloud provider. This approach allows developers to focus on developing application functions without worrying about the infrastructure required to do so. For example, the AWS Lambda event-driven, serverless computing platform

automates the rest of the process of application deployment, creating infrastructure stacks as required, leaving developers to code rather than manage infrastructure. Applications that require extremely fast time to market, heavy data processing, and mobile- or user interface-intensive applications are ideal serverless use cases. While not as well-used as microservices today, serverless development is growing. According to Forrester Research, about half of organizations either currently use or plan to use serverless architecture within the next 12 months[4].

Smart transformation

Putting in place the right building blocks today is the best way to prepare for tomorrow. With a smart cloud foundation rooted in solid strategy and planning, agencies will be able to capitalize on transformative technologies that improve business functions now and well into the future. In addition to microservices and serverless computing, agencies can use their Cloud Smart investments to adopt leading-edge technologies like artificial intelligence, machine learning and the internet of things to continuously deliver smart results that further the agency's mission.

Get started today.

Set up your agency for success, be Cloud Smart.

About NTT DATA Services

NTT DATA Services partners with clients to navigate and simplify the modern complexities of business and technology, delivering the insights, solutions and outcomes that matter most. As the largest division of NTT DATA, a top 10 global business and IT services provider, we combine deep industry expertise with a comprehensive portfolio of consulting, application, infrastructure and business process services.

S Strategy and Planning

M Managed Services

A Agility

R Return on Investment

T Transformation

[4] Jeffrey Hammond and John Rymer with Christopher Mines, Abigail Livingston and Kara Hartig. "Serverless Development Best Practices." Forrester Research. October 2, 2019.