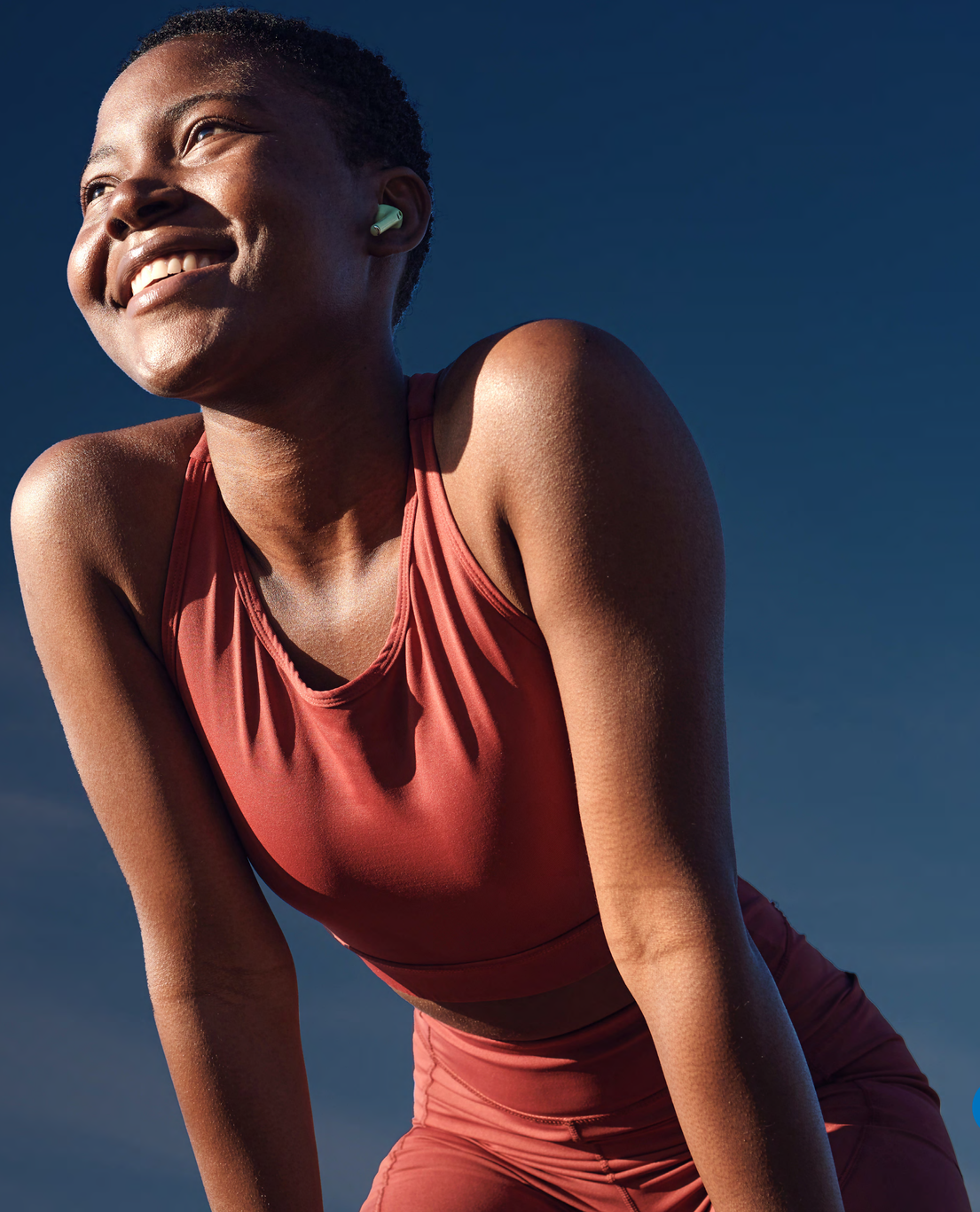
Start smart

A guide to smart cloud transformation



The benefits of cloud computing are well known — greater efficiency, scalability, lower costs and the ability to incorporate modern processes and technologies. Cloud First, introduced by the U.S. government over a decade ago, first gave federal agencies authority to implement cloud-based solutions.[1] Yet, many agencies have been slow to embrace the cloud. Rather than see cloud initiatives as the marathon they are, organizations may see adoption as a sprint. Something for which they're ill-prepared.

Cloud has transitioned from a technology disruptor to a capability enabler. Organizations are no longer simply lifting and shifting workloads. They're leveraging the cloud to drive real business innovation. However, cloud adoption still requires good preparation, planning and management, including a careful evaluation of all aspects of your enterprise. It's well worth the investment to perform an honest assessment before the start. Specifically, agencies should evaluate:

1. When it makes sense to move to the cloud
2. What types of cloud models best suit agency workloads
3. How to optimize costs and proactively address potential security issues

With each administration cybersecurity becomes a more pressing priority. The Executive Order on Improving the Nation's Cybersecurity encourages the federal government to "bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises or hybrid."[2]

To get started with cloud, we recommend a S.M.A.R.T. start approach — Strategy and planning, Managed services, Agility, Return on investment (ROI) and Transformation.

Strategy and planning

Starting smart on your cloud marathon route means preparation. Take the time to thoroughly evaluate a potential move to the cloud. That way, your agency can avoid making bad decisions. For example, good planning can help you avoid duplicating efforts, making poor design decisions, causing performance and security challenges or cost overruns, and creating new silos in the cloud.

“Moving to the cloud isn’t something where you just jump right in. If you were running a marathon, it would require months of training,” says Noel Hara, Public Sector Chief Technology Officer at NTT DATA, a global IT services provider with dozens of federal clients. “If you’re moving your agency to the cloud, you have to be in it for the long run — evaluating environments, applications, workloads, usage and infrastructure. While we can’t always see the finish line, you need to look at where you want to be in the future.”

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. Don’t be overwhelmed. Break out these two areas and handle them separately. Determine 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 your agency’s rules, and a potential 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, your agency may choose to keep the system on-premises. For applications that won’t easily port to the cloud yet offer a strong cloud ROI, consider an application modernization initiative. It’ll move the system away from its legacy architecture to a container strategy that breaks the application into microservices.

Choose wisely

For workloads slated to move to the cloud, organizations must decide cloud type, cloud provider and cloud tools. These complicated decisions depend on many factors. While the type of cloud will depend on your 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’ll require additional automation services.

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 usage, 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.

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
- AWS CodeDeploy for automated software deployment

Confused?

You're not 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 your workloads and then standardize on it. Doing so provides consistency, which decreases risk and improves operational efficiency and, in turn, boosts agency productivity.

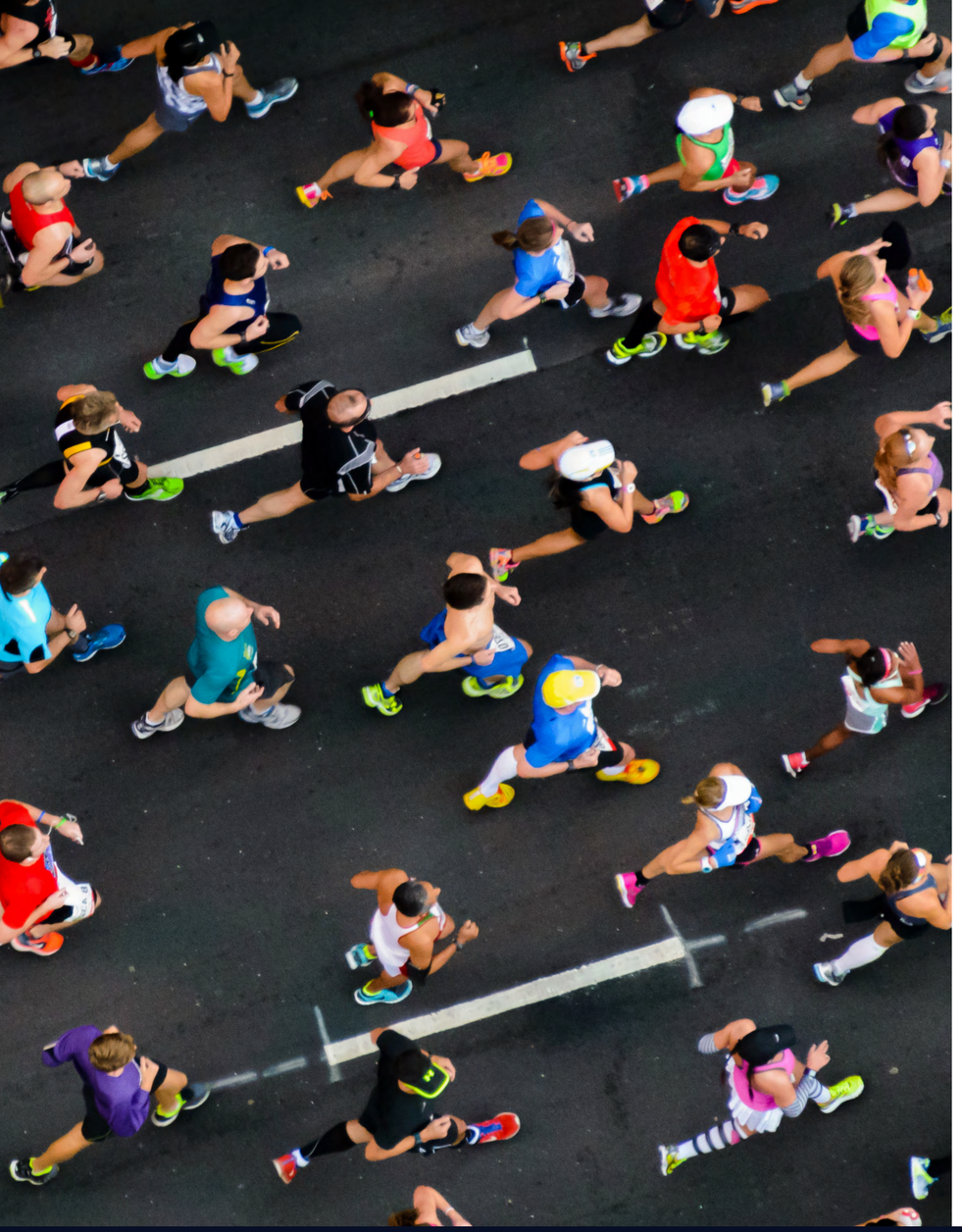
Achieve cloud security

It's important for agencies to adopt proactive security measures. Think of it as stretching and warming up your muscles for the miles ahead. Your approach should include elements like zero trust architectures, DevSecOps processes for container scanning and a properly configured cloud access security broker (CASB) tool. Making sure information systems adhere to relevant National Institute of Standards and Technology (NIST) 800-53 controls based on their risk rating should be paired with continuous monitoring of the environment. These practices will provide foundational rigor when you move workloads to the cloud while maintaining compliance with 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). That's why they offer government-specific cloud offerings.[3] For example, while AWS's commercial offering in the U.S. is FedRAMP Moderate, AWS GovCloud gives agencies the flexibility to architect secure, FedRAMP High compliant cloud solutions. However, agencies can dilute that security through misconfiguration or complexity. It's up to each organization to follow security best practices as part of the cloud shared responsibility model.

Selecting the right infrastructure

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

The agency started by fully understanding the needs and requirements for the architecture, its dependencies and security. Following that analysis, decision-makers chose a data migration approach for a private cloud. After standardizing on a platform, developers began building cloud-native applications. The new infrastructure helps the agency reduce capital expenditures, create efficiencies in operational expenditures and avoid potentially damaging security breaches.



Managed services: Start and stay cloud smart

The managed services provider (MSP) model offers access to highly skilled extended teams that specialize in the needs of your organization. Much like a runner might consult with a nutritionist or a trainer. This expertise is extremely beneficial because the industry-wide lack of cloud computing skills has kept some government 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 you with workload evaluation, application rationalization and other important cloud adoption decisions. Their expertise can also help provide depth when evaluating which enterprise resources will benefit most from the managed services model.

Often, agencies opt to take on some of the responsibilities in-house 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 may outsource some or all aspects when they're tasked with managing initial assessments, large cloud migrations, new cloud-native application development, financial management, and ongoing workload monitoring and management.

Agility: The argument for DevOps

For greater agility and responsiveness, organizations should strongly consider a DevOps approach. DevOps increases the speed with which you can develop and deploy cloud-native applications. It often uses automated pipelines that increase productivity and reduce errors manual processes may introduce. DevOps also creates a more collaborative environment between development and operations teams. Developers take greater ownership of code throughout the software development lifecycle. The operations group can create self-service environments that streamline the development process.

What makes a smart cloud even smarter? DevSecOps, by adding security to development and operations processes. It bakes security into automated pipelines to be sure code is inspected as it flows through. It also bakes security controls into self-service development products. DevSecOps favors using cloud-native technologies like containers, microservices and serverless development. They build on DevOps processes to further improve functionality, the user experience and overall quality. These technologies also reduce deployment failures, foster collaboration and speed development. Think of it as equipping yourself with the best running gear.

Government agencies leverage DevOps processes to build cloud-ready applications that use 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 adopting DevOps best practices and centers of excellence (CoEs). In addition to seasoned integrators and partners, the government has developed valuable resources such as the DevOps Community of Practice.[4] It helps agencies share best practices and lessons learned. NIST is also developing guidance on DevOps and DevSecOps for agencies.

Service reliability engineering (SRE)

Think of SRE as the difference between simply running a marathon and achieving your personal best finish. In a dynamic and agile environment, applying software development principles — and applying them to IT infrastructure and operations from the onset — will help propel the right outcome for any cloud strategy. The focus of the SRE practice is on automation, system design and improvements to system reliability. A great example of this is the now common use of infrastructure as code tools like Terraform, Ansible and AWS CloudFormation and ARM templates to deploy infrastructure in a consistent, repeatable and programmatic fashion.[5]

How do you achieve a personal best in any marathon? Hard work and a continuously evolving training plan. Think of SRE as your cloud's personal training plan to achieve success.

Modernizing at mission speed

Over the past several decades, the U.S. Air Force has relied heavily on a mainframe-based supply chain platform to make sure 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. 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 Air Force $25 million in annual hosting costs.

ROI: Bet on a winner

An important part of cloud adoption 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 on-premises. Strongly controlling these measures is critical to achieving your expected cloud ROI.

There are multiple ways to evaluate cloud ROI, but many of those methods don't consider everything. ROI evaluations may only consider upfront and ongoing costs. Yet, metrics like improved agility and flexibility, uptime, scalability and application performance can have a significant bearing on ROI.

It's smart to focus on ROI

You should start measuring the ROI of a cloud investment well before the cloud project begins. In the months preceding the project, organizations should evaluate potential operating, integration and ongoing support costs, as well as mission value and impact. Then there are the costs of issues like business continuity, monitoring and expected demand. Be sure to build in visibility and insight across budgets, procurement and lifecycle so you can ultimately map them to cloud spend.

For example, an organization's chargeback model is critical to the ROI process and most agencies use such a model to allocate costs. The CIO's office typically keeps tabs on cloud usage by mission area and charges the cloud costs back to the mission office. Financial transparency and chargeback models should be flexible enough to change as your use cases and associated workloads scale and change. You'll have more financial transparency if your organization proactively tracks technology-related resources, processes, detailed cost models and financial reporting. 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 mile markers, the next step is choosing the right cloud cost model. AWS, for example, offers three cost models across its main compute EC2 service. 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 mission-critical workloads with unpredictable demand. Too many organizations make the mistake of using this model routinely, which can increase costs unnecessarily.

The second type of cloud model AWS offers is called Savings Plans. It requires a commitment of one to three years in return for a significant discount. This model is best for 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 fault tolerant applications and one-time actions or transactions. Understanding these cloud models is key to achieving a positive ROI. Agencies that use the wrong cost model risk increasing costs quickly — and unnecessarily.

ROI evaluations don't stop once the workload moves to the cloud, because nothing stays the same in cloud. When looking at the ongoing ROI of any cloud initiative, you should embrace the discipline of cloud financial management known as financial operations (FinOps). FinOps will help inform, optimize and operate the ever-changing and therefore continuous ROI.

Important considerations for positive ROI

- Include lead time for all stages, from commit to deploy
- Factor in time spent on unplanned work 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

Transformation

With the right planning and focus, government agencies can achieve their goals — improved operational efficiency, lower costs, better integration with other applications and solid security. It also sets the foundation for using emerging cloud-native technologies like microservices and serverless computing. These tools allow you to further transform and optimize agency operations for security, speed and quality. Think of it as crossing the finish line and looking forward to the next event on your list.

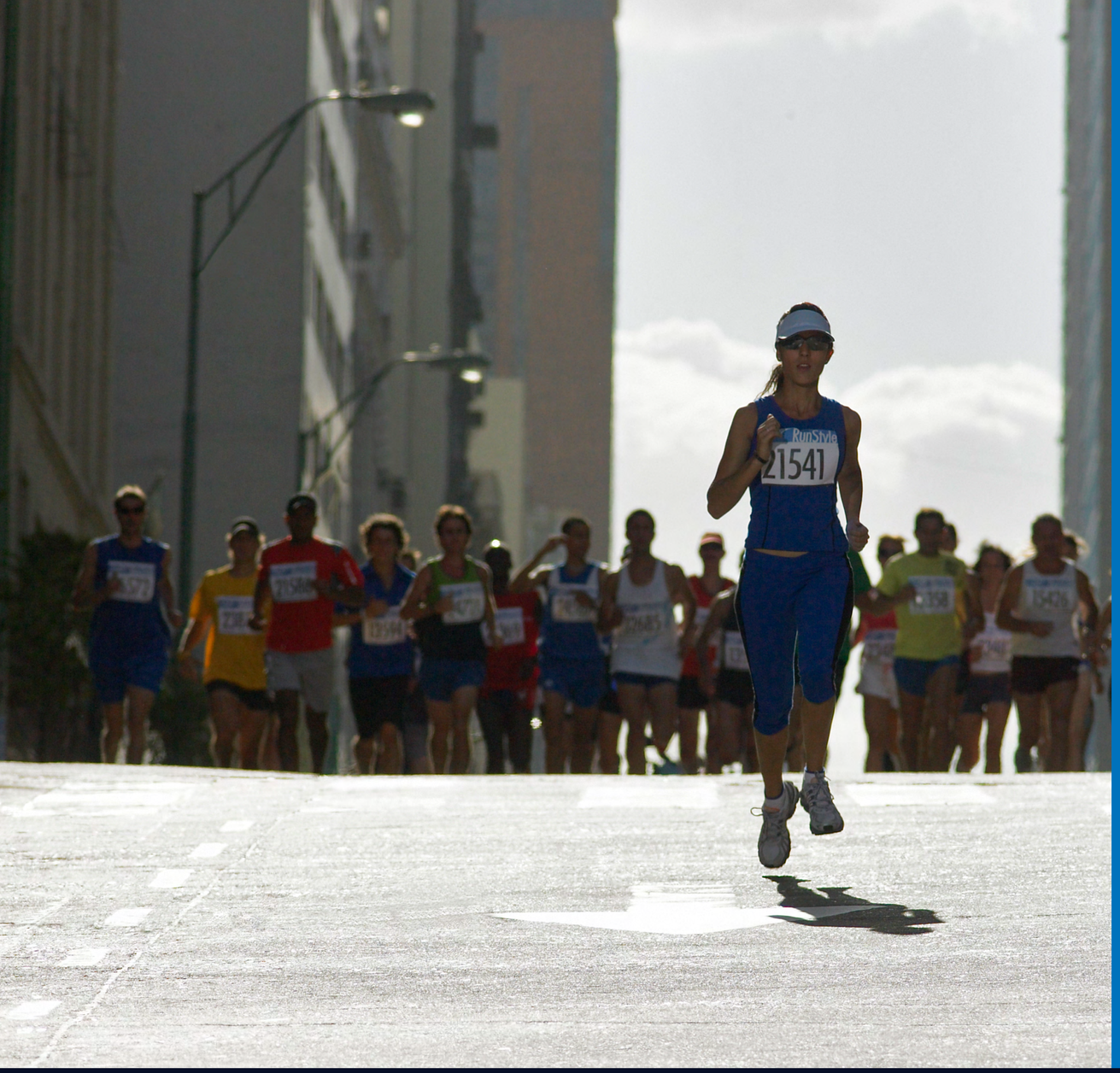
Cloud-native technologies

Microservices is a popular way of breaking development into small reusable components. It speeds development because teams work on single aspects of an application's function, independent of others. This approach allows teams to release updates when they're completed. You can also leverage microservices for reuse. By creating a library of microservices, developers can simply pull functionality together for deployment as needed.

Following a S.M.A.R.T cloud strategy allows agencies to take advantage of serverless application development. Serverless completely removes the operational aspects of development by offloading them to a cloud provider. This now staple 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. It creates infrastructure stacks as required, leaving developers to code rather than manage infrastructure. Ideal serverless use cases include applications that require extremely fast time to market, heavy data processing and intensive mobile or user interfaces. Many organizations are leveraging multiple serverless solutions to develop and manage their applications.

Smart transformation

Putting in place the right building blocks today is the best way to prepare for tomorrow. With a S.M.A.R.T. cloud foundation rooted in solid strategy and planning, agencies can capitalize on transformative technologies that improve business functions now and well into the future. With microservices, serverless computing and cloud investments, organizations can adopt leading-edge technologies. Tools including artificial intelligence, machine learning and the internet of things will help you continuously deliver results that further your agency's mission.



About NTT DATA

NTT DATA Services partners with clients to navigate and simplify the modern complexities of business and technology. We deliver 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.

Set up your agency for success. Start S.M.A.R.T.

Get started today

Sources:

1. Suzette Kent. “Federal Cloud Computing Strategy.” Executive Office of the President of the United States. June 24, 2019. https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf
2. The White House. “Executive Order on Improving the Nation's Cybersecurity.” Briefing room | Presidential Actions. May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
3. U.S. General Services Administration. Federal Risk and Authorization Management Program. https://www.gsa.gov/technology/government-it-initiatives/fedramp
4. DevOps Community of Practice. https://digital.gov/communities
5. Tamekia Reed. “How Many Tools Does It Take to Build a Cluster: Terraform, Vault, and Consul in Government IT.” HashiCorp. July 21, 2019. https://www.hashicorp.com/resources/how-many-tools-build-cluster-terraform-vault-consul-govt-it

Visit us.nttdata.com to learn more.

NTT DATA is a $30 billion trusted global innovator of IT and business services. We help clients transform through business and technology consulting, industry and digital solutions, applications development and management, managed edge-to-cloud infrastructure services, BPO, systems integration and global data centers. We are committed to our clients’ long-term success and combine global reach with local client service in over 80 countries.