Quadrint
Experience Powering Intelligence

Steps for Successful Federal Government Cloud Adoption

Federal Government stakeholders face ongoing challenges to expand corporate and mission capabilities while increasing service delivery speed.

Modern Service Delivery

Decision makers need a dynamic view of data to effectively predict and improve outcomes. Legacy IT silos are unable to efficiently adapt capabilities; share data; integrate access controls; or provide a responsive, easy-to-navigate, and intuitive user experience.

As a result, there has been a shift to cloud-based service delivery driven by several market forces:

- Data-centric architectures and the rapidly expanding volume and sources of data are changing the scale and approach to IT modernization.
- Cloud environments are able to continously update and enforce cybersecurity controls and protect data.
- Commercial innovation is focusing on cloud native capabilities.

Industry is investing heavily in cloud technologies that can bring significant benefits to Government organizations. But where to start? Quadrint can help.

Discover and Assess Phase

Every cloud migration should begin with a thorough assessment of the current state of the system to determine and recommend appropriate courses of action for transitioning the workload. Discovery, assessment, and evaluation activities are performed to determine how best to optimize business value as workloads are moved to the cloud.

An important consideration is understanding how moving to the cloud will impact various business areas. The Amazon Web Services (AWS) Cloud Adoption Framework states that the following should be considered:

- **Business** – Well-timed application migrations minimize disruption to core mission capabilities
- **People** – Communication and guidance is key to ensure changes are well understood
- **Governance** – Compliance with Government-specific governance, risk management, and compliance controls are required for success
- **Platform** – Solution must meet stated as well as unstated requirements while including required functionality such as maintaining business continuity during migration
- **Security** – Compliance with federal laws such as FISMA and FISCAM is a must
- **Operations** – Monitoring and maintaining the solution is key to achieving mission goals

Interpreting these elements and incorporating them into an integrated approach that best fits your organization will provide the basis for a low-risk cloud adoption.

Select a Migration Approach

Based on information obtained from the Discovery and Assess phase, the next step is to make recommendations on the best course for transitioning a specific application to the cloud. During this process, the Government must be kept informed of the benefits and possible pitfalls of the various recommended migration approaches. Following are five common migration strategies based on best practices from Garnter, AWS, and Microsoft.

Re-hosting or “Lift and Shift”: This strategy is used to quickly meet migration timelines. It may still result in a somewhat lower total cost of ownership (TCO) by re-hosting to a cloud platform and provisioning only the resources you need for the period of time they are needed. Quadrint has used this approach to rapidly enable cloud adoption. In our experience, re-hosting workloads is the most commonly used strategy because many customers have aggressive cloud adoption schedules and choose to move to the cloud as rapidly as possible as a first step, and then re-evaluate applications for further cloud optimizations in a follow-on effort.

Re-platform: This strategy also focuses on optimizing for speed of migration, but also makes a few key changes to better integrate with key technologies present in the cloud environment. One option would be moving to a database-as-a-service such as the Amazon Relational Database Service (RDS), which offloads patching and administration to the cloud service provider. In our experience, this provides a value-added service that allows agencies to maximize their own resources to focus on agency priorities by shifting the administrative burden to the cloud service provider at a reasonable cost premium. Another option is on-premise SAN cloud provider storage solutions, which are unavailable in the cloud. Re-platforming is the second most used migration strategy after re-hosting, but requires careful consideration of cost vs. benefit of each update included with the initial migration effort.

Re-factor/Re-architect: This strategy re-imagines how the application is architected using cloud native features. Our experience is that this approach takes more time to execute than re-hosting or re-platforming but may be required to cost-effectively adapt capabilities, share data, integrate access controls, and provide a positive user experience. One example of re-factoring is migrating a specific workload capability to a serverless architecture. Re-architecting should be considered when it is necessary to reduce licensing costs and software acquisition times while increasing scalability. When re-architecting an application, it is important to use industry best practices, such as the AWS Well-Architected Framework, to provide structure and guidance.

Re-purchase: This strategy is a viable approach when specific portions of the overall workload can leverage pre-built and supported services or applications within the new cloud environment. Our experience is that this requires some integration work, but decreases the organization’s acquisition, deployment, development, and administrative overhead by integrating with externally supported applications and services. Quadrint provides re-purchase support through adoption of a software storage appliance to provide robust, highly available storage services in the cloud. This can reduce acquisition time by leveraging the on-demand, pay-as-you-go pricing model. It offloads support to the vendor from whom the software appliance was purchased and alleviates the need to develop a custom storage solution.

Retire: During the evaluation period, you may discover applications that are no longer needed and can be decommissioned as part of the migration effort. Our experience is that this typically requires reevaluating current requirements and surveying active users to inform decisionmakers of the best option for next steps.

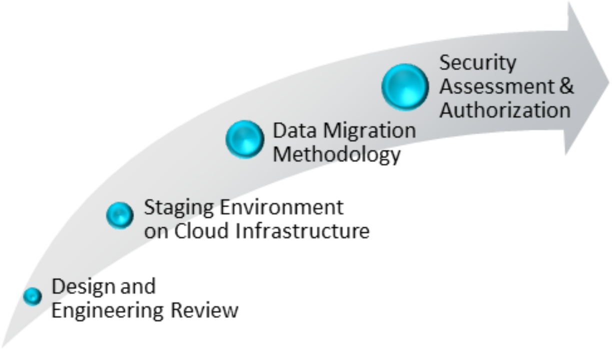
> **Cloud technology adoption requires agencies to prioritize migration planning, sustainment, and organizational maturity to realize the full benefit of these services. Adoptions fail when organizations buy solutions without proper identification of requirements and intended outcomes–which can lead to a project not launching, a service failing at peak need, or simply redundant purchasing across the enterprise.**

Retain: Some applications may require extensive re-factoring before they can be transitioned. During one of our federal customer engagements, Quadrint migrated 20+ applications to the cloud over the course of two years. Workloads migrated during the latter part of the second year needed reevaluation because they were very complex and required more time to ensure good design and proper adherence to the migration methodology.

Execute the Migration

Every cloud migration project must have a methodology to track work products and milestones. Quadrint successfully uses the Scaled Agile Framework (SAFe), which has enabled Quadrint to increase technical team capacity by 88%. This approach is combined with secure development lifecycle software development processes and integrated DevOps tools to provide a holistic solution delivery methodology.

There are four key steps in the migration process: conducting a thorough design and engineering review, building a staging environment, developing a data migration methodology, and conducting a successful security assessment. Following these steps, the migration and transition process becomes a series of deployment, validation, cutover, and decommissioning activities that can be rolled back at any point in the process.


Security Assessment & Authorization
Data Migration Methodology
Staging Environment on Cloud Infrastructure
Design and Engineering Review

Cloud Migration Steps

Step 1: Conduct a Design and Engineering Review
The migration process starts by reviewing the information obtained up to this point to ensure there are no changes in the architecture and no gaps in the assessment. Following are key requirements we review:

- Architecture, network, and data-flow diagrams
- Security model
- Estimated infrastructure costs
- Storage, backup, and high-availability solutions
- Data migration methodology
- Application versions
- Service level agreements
- Business Continuity and Disaster Recovery)
- Identity and Access Management (IdAM)
- Technical activity plan

Step 2: Build a Staging Environment on the Cloud Infrastructure
Our experience has shown that staging systems greatly simplifies the move to cloud. For our Government customers, Quadrint successfully deployed staging versions of the to-be production architecture for each of 20 successful cloud migrations. This approach significantly reduces migration risk because any issues or required modifications are identified before actual migration occurs. We also recommend a staging environment approach for more significant technical changes, such as applications that are re-hosted or re-platformed in the cloud. Actual data gathered from the Discovery and Assessment phase and the design and engineering review is used to build the staging production system in the cloud environment.

The staged system serves as the new production environment and is the system used as the basis of evaluation during the security assessment. Because the staged system is used to conduct test migrations of system services from the legacy data center to the cloud, it can expose any gaps in the technical activity plan that can be addressed prior to the actual migration.

The staged environment is used to test and validate all aspects of the to-be architecture – web, application, storage, compute, database migration, networking, performance, connectivity, load balancing, and common file sharing. It also helps determine what infrastructure and/or architectural modifications are necessary to ensure successful operations by validating successful testing of production processes, jobs, scripts, custom code, backup, and recovery. A staged environment also is used for documented systems and user acceptance testing, and in instances where we conduct operational readiness reviews when seeking approval from a Government customer to proceed with a migration.

Step 3: Develop a Data Migration Methodology
Minimizing service downtime during a migration is accomplished through careful planning and understanding of both the applications and the data being migrated. Choose an appropriate time for an authorized outage (if necessary), considering things such as key stakeholder and agency component accessibility, business requirements, agency deliverables, human resource functions, security functions, and personnel dependencies. When properly throught out and executed, a proven data migration strategy is a key component of ensuring a successful migration effort.

Quadrint has experienced a number of migrations where the production transition was rather insignificant and resulted in zero impact to the customer. The ability to conduct a migration with little to no end-user impact truly defines a successful effort. To reduce downtime during a migration, an initial data synchronization is completed, after which a synchronization routine is established. This ensures consistency between the legacy system and cloud system data throughout the period that the staged environment is being built and evaluated. Our practice is to maintain this approach until a time just shortly before production cutover because it greatly simplifies the amount of time required to conduct a successful migration. Web, application, and database services can be stopped for shorter periods while the final synchronization completes, reducing long synchronization times and lengthy outages on transition day.

Each migration is different, but our experience has shown that pre-building assets and infrastructure, pre-staging data, and having automated data validation procedures in place are vital to minimizing time spent in a degraded or unavailable state during a migration activity.

Step 4: Conduct a Security Assessment and Authorization
The final step in executing a cloud migration is the security assessment. Cloud-based applications may present unique accreditation challenges that some organizations have limited experience with and, therefore, may not be fully prepared to adjuticate. Our team of security experts is accomplished in this area, as demonstrated by our ability to routinely achieve authority to operate (ATO) for our Government customers.

Our expert personnel are available at all phases of the security assessmentand ready to respond to questions or provide system demonstrations – all with the goal of obtaining ATO for the system in the cloud while strictly adhering to NIST, ICD 503, DoD RMF, and other Government regulations and industry risk management guidelines.

Operations Support and Optimization

As a systems integrator, Quadrint support doesn't end with the successful cloud migration. We continue to provide service delivery support as needed to maintain service operational health. We accomplish this using monitoring tools configured and integrated during the planning and build stages and metrics gathered to tune and optimize the allocated resources as application functionality and load change over time.

Automation is Key
Prior to automation, the primary activities of system sustainment involved applying operating system updates and responding to hardware events, with an occasional deployment of new application functionality. Agencies today need a responsive partner who understands that systems must evolve at high velocity to securely deliver services needed to execute agency missions. This can best be accomplished by using extensive automation to deploy applications, monitor application health, scale in response to load, and validate that all relevant security controls are operating as expected. Over time, the system automation increases as new technologies or methods of coding are added to the solution during the regular release cycles inherent in cloud deployments.

Dashboards are High-Value Additions
The ability to view synchronized key performance indicators allows operations teams to easily spot and predict common failure scenarios, identify trends when performing capacity planning, and pfacilitate cost-optimization planning. Dashboards are useful for providing solution stakeholders with dynamic data to keep them apprised of the overall picture while also staying informed about the indicators they find most important.

Optimization Leads to Sustainabiliy
Optimization balances the capacity of resources used to deliver the solution with running the solution cost-effectively to deliver a positive user experience. By monitoring peak user workloads and downtime, appropriate automation can be added to dynamically adjusted resources for cost efficiency. Because system loading changes over time, we recommend validating loading predictions shortly after migration, again after the first month, and then quarterly thereafter. If long-term utilization of even portions of a system is predictable, we recommend purchasing reserved capacity, when available, to take advantage of discounts (~40%) as an advanced cost-optimization path.

How Quadrint Can Help You

Quadrint has proven success in Government cloud modernization projects. For one Federal Government customer, Quadrint is responsible for supporting the entire portfolio of corporate systems – documenting, assessing, and prioritizing requirements for systems that support more than 2,000 business functions.

Like many federal agencies, this customer was contending with legacy systems that were inefficient and costly to adapt to changing policy requirements, emerging technologies, and new service delivery models. Prior to cloud migration, legacy systems were highly customized and had complex interdependencies that made it difficult to upgrade, thus requiring specialized support teams.

After assessing the IT environment and applying our data migration strategy, Quadrint migrated a portfolio of applications from an on-premise data center to an AWS cloud environment – all engineered to Quadrint's high-availability standards to ensure no disruption to daily operations. Since implementation, new capabilities have been incorporated in various product suites, new cloud native development stacks have been introduced, and modular Agile development with appropriate configuration controls have proven successful.

With the professional support of our application experts, Quadrint has helped this federal customer achieve an increased uptime of 99.98% and a reduction of 25% in infrastructure costs. This has resulted in measurable improvements in data lifecycle management planning, master data management, data governance, data warehouse design and implementation, data ingest standards, and configuration management. Within one year of cloud adoption, the customer had access to all planned service capabilities.

Whether you are just discovering what cloud means to your organization or you have already started the journey, Quadrint is the partner who can help you unlock the value of cloud that will help optimize your organization.

Sources

» AWS Cloud Adoption Framework
https://d0.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf

» AWS Migration Whitepaper
https://d1.awsstatic.com/whitepapers/Migration/aws-migration-whitepaper.pdf

» AWS Well-Architected Framework
https://d1.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf

» Federal Cloud Computing Strategy, "From Cloud First to Cloud Smart" https://cloud.cio.gov/strategy/

» National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) Overview
https://csrc.nist.gov/projects/risk-management/risk-management-framework-(rmf)-overview

Contact Us

Quadrint Headquarters
3190 Fairview Park Drive, Suite 360, Falls Church, VA 22042

Ben Goss
Chief Growth Officer
ben.goss@quadrint.com

Andy Spohn
Chief Technology Officer
andy.spohn@quadrint.com