DELIVERING THE VALUE OF THE CLOUD
DSA Cloud Solutions

DSA

Employee-Owned, Mission-Driven

CURRENT STATE OF THE CLOUD

Cloud computing's key benefits – scalable information technology (IT) assets, increased service segregation and isolation, and greatly reduced operating costs – are continually enhanced through market competition and rapid advancements in technology. The Federal Government's commitment to cloud computing is embodied in the "Cloud Smart" strategy, which calls for increased cloud adoption. Combined with the Federal Risk and Authorization Management Program (FedRAMP) cloud security certification, these elements embody the interdisciplinary approach to IT modernization that the Department of Defense (DoD) enterprise needs in order to provide improved return on investments, enhanced security, and higher quality services to the Warfighter.

In June 2019, the Federal Chief Information Officer (CIO) Council shifted way from Cloud First to Cloud Smart - This was the first cloud policy update in seven years, offering a path forward for agencies to migrate to a safe and secure cloud infrastructure. The cloud enables "on-demand access to shared and scalable pools of computing resources with the goal of minimizing management effort or service provider interaction." - NIST

DSA CLOUD SERVICES

Data Systems Analysts, Inc. (DSA) cloud computing services and solutions address infrastructure and skilled personnel hurtles that previously limited cloud adoption, but are now executable and affordable. DSA offers proven DoD cloud computing services in four key areas outlined in Figure 1. These services enable customers to plan, execute, adapt and protect their critical mission capabilities. By utilizing modern infrastructure and managed services available through the cloud, DSA provides DoD customers a path to greater scalability, reliability and agility in the performance of their mission. Each service area is discussed in greater detail below.

Figure 1 - DSA Cloud Computing Services

LEVERAGING THE CLOUD

The first stage in our service is to guide our DoD customers in defining and prioritizing their needs using an iterative approach to achieve optimal cloud performance. Specifically, DSA performs the following tasks:

As recognized in the 2018 National Defense Strategy (NDS), "Cyberspace is now a war fighting domain. In order to compete and win in this domain, the total Army must leverage modern information technology (IT) and methodologies to transfer itself into an agile, lean, Software enabled as a Service that can respond to adversaries on the digital battlefield at the speed of war." – Lieutenant General Bruce Crawford, CIO/G-6 and Paul Puckett, Director of Enterprise Cloud Management Office (ECMO).

Needs Analysis: We start by defining and prioritizing your objectives and needs. We review your mission requirements, strategic IT plan, IT portfolio management, IT security posture, and budgetary constraints.

Interviews: We interview system owners and end users to verify that all of your needs and priorities are defined and accounted for in your requirements.

Assessment: We know how to assess your application's capabilities and select the best path forward to the cloud. Applications typically fall into one of three cloud categories:

- Cloud Hosted –Your application can readily be hosted in the cloud. If so, you can do that first and receive the associated cost reductions while you determine the application's long-term status.
- Cloud Optimized – Your application cannot be hosted in the cloud as is. Efforts will need to be made to update application components to achieve readiness to move to the cloud.
- Cloud Native – This strategy focuses all resources on the mission challenge and uses the cloud service provider for all infrastructure operations within the cloud. The key to this approach is understanding the operational characteristics of your mission need (e.g., operating hours, workload surge characteristics, development requirements, and the number and size of requests). The operational characteristics affect operational costs. Does the requirement call for bursty workloads or sustained workloads? Do you need a "no-code" option or highly orchestrated functions to manage containers? The analysis of alternatives that DSA provides ensures our customers are able to make informed and cost effective decisions.

Identify Cloud Solution Options: We then identify the DoD Cloud Computing Security Guide (SRG)-compliant cloud solution options that can effectively address your needs, priorities, and requirements. These are based on the "6 Rs" of application migration including:

- Re-Hosting: whether it is on premise to cloud or re-hosting due to changes in cloud security requirements, DSA has the experience to guide you through re-hosting.
- Re-platforming: DSA advises clients on how to reduce overall cost of ownership. Our re-platforming service reduces overhead for management of systems by opting to utilize managed services offered by cloud service providers (CSPs).

- Re-factoring/Re-architecting: CSPs onboard new FedRAMP certified services every day. These services enable your application to swap out custom coded services for cloud native services that will optimize application performance in the cloud. DSA Cloud Architects are on top of these advances, integrating new functionality into our client's cloud application to drive improved performance, scalability, and security.

For the U.S. Army MilTech solution, DSA is re-platforming 11,588 SharePoint 2019 sites from DISA data centers into the MS Azure Impact Level 5 cloud. Completing test migrations, workflow validation and RMF for the environment, DSA has migrated the 1st customer into this environment to provide improved services, scalability, elasticity, and resiliency.

- Re-Purchasing: In today's budget conscious environment, capital expenditure dollars are scarce. DSA has the experience and expertise to navigate you through the challenges of defining which "as a Service" offerings are best for your mission needs. We assess and advise on application architecture readiness for transition to subscription pricing services or to leverage a commercial system in a FedRAMP environment.
- Retiring: Rationalizing your portfolio of applications for migration to the cloud may require tough decisions to retire applications which no longer have a meaningful mission value. DSA's discovery processes will align your inventory with mission objectives for a complete 360 degree assessment.
- Retaining: Not all applications are in a position to be moved to the cloud or even refactored in the cloud. DSA Cloud Architects will assess your application environment and recommend the best and most cost effective solution to get you to the cloud.

Analysis of Alternatives (AoA): Our readiness assessments include an AoA to determine your mission drivers and return on investment strategy for optimal cloud adoption.

Requirements Definition: We develop the definitive set of requirements – including all cybersecurity requirements – to ensure the solution addresses all of your mission needs.

Detailed Design: Finally, we develop the detailed design templates to support rapid and repeatable provisioning to ensure the solution is sound, clearly defined, secure, and ready for implementation.

The outcomes of these steps enable both Cloud Migrations and Application Development/Modernizations. When your DoD-compliant cloud solution is approved, DSA can support the full life cycle activities of planning, implementation, testing, deployment, and training, thereby achieving Authority to Operate (ATO) and production sustainment.

CLOUD MIGRATION

The second service provides our DoD customers with the detailed approach to achieving their cloud migration objectives. Specifically, DSA performs the following tasks:

Cloud Migration Planning: DSA cloud readiness assessment provides customers the best "6 R" migration strategy for each workload. Our complexity analysis tools identify application dependencies that present hurtles to successful migration. DSA migration planning identifies which characteristics inside the application will impact migration. This covers code that may have to be changed, network connectivity, interfaces to other applications, access to required data stores, and enabling user access. The outcome of this analysis is an architecture roadmap and project plan to remediate these risks in achieve your cloud migration objective.

Two Phase Design and Implementation Process: DSA implements cloud migration (i.e., re-hosting applications in the cloud) through a phased design and implementation process. We define service and technical requirements, develop the plan for the application to achieve ATO, and develop and document the configuration, operation, and support requirements for management in the cloud. Figure 2. Outlines the steps within each phase.

Phase 1 – Design

1. Perform Inventory Validation
2. Define System Cloud Architecture
3. Conduct Security Control Impact Assessment
4. Define Data Synchronization Strategy
5. Conduct the Cloud Shaping Workshop
6. Obtain Approval to Implement

Phase 2 – Implementation

7. Setup resource templates and Configure the Cloud Environment
8. Backup the Data, Restore in the Cloud, and Conduct a System Regression Test
9. Update System Documentation
10. Obtain Customer Acceptance and Handoff to Production
11. Support Legacy System Disposition (If applicable)

Figure 2 - DSA Two Phase Process

The reference to re-hosting as a "Lift and Shift" implies that relocating applications to the cloud is simple. However, the process is more complex. Engineering teams supporting applications must re-establish security controls, monitoring and management, and application's connectivity in the cloud.

DSA's Design and Implementation Process embodies our successful experience in cloud migration by ensuring we identify and address the operational realities and all technical migration issues to create a complete solution.

The Air Force Air Education and Training Command (AETC) faced difficulty transitioning between development and sustainment. DSA took over the effort and guided re-hosting in the Microsoft Azure Cloud, giving the government full oversight and direct control of operational costs.

Communications and Outreach: DSA's communications and outreach efforts start during the assessment phase with intimate understanding of operations and technical architecture. DSA initiates migration-unique communications and outreach plans. The communications and outreach identify workloads moved and those that were not moved to the cloud due to a joint decision process to maintain a hybrid environment, retire the application, or replace it. Communications document the level of impacts to applications and identify new technical interdependencies that exist in the migrated application. In capturing the configurations of cloud resources and costs of their use, DSA hands over documentation on the fully configured workloads that spin up or down to ensure optimal cost management. Finally, as part of outreach to the operations and maintenance vendor, DSA walks through any new governance and operations activities for management of the new environment, including updates to compliance with Army and DoD guidance.

APPLICATION DEVELOPMENT AND MODERNIZATION IN THE CLOUD

The third service executes on the application development and modernization activities required to migration DoD customers to the cloud. Specifically, DSA performs the following tasks:

Design: The best cloud application architectures meet current requirements and provide flexibility to securely address changes. The use of DevSecOps platforms to automate code management, testing, and security yields closer alignment with customer priorities and a process of continual refinement (called "Fail Fast") that ensures the resulting products are secure and tailored to DoD needs and user preferences.

For the U.S. Department of Agriculture Farm Production and Conservation organization DSA developed a solution using Amazon Web Service (AWS) Fargate and Elastic Container Service to host containerized microservices that provided improved performance and scalability. We used AWS Elastic Load Balancer and AWS Batch to manage ingest queues and provide consistent performance when the system dynamically scales to run thousands of bulk ingestion jobs.

- ***Designing Application Architectures for the Cloud:*** DSA uses the current implementation and mission demands to assemble architecture practices tailored to customer needs, scale, and cybersecurity requirements. The associated best practices include designing the application as a collection of reusable services and APIs and decoupling the data from the application. The use of microservices and containers is a natural fit for implementing cloud-native applications.
- ***Designing for Performance in the Cloud:*** Effective performance in the cloud takes planning and careful design. DSA designs performance from the start by tuning existing designs and refactoring services to improve application performance and lower costs. For example, you can optimize communications performance by combining communications between components into a data stream or a group of messages. We define auto-scaling of processing to address components (such as server instances) that need to be scaled up or down in response to changes to workload demand. These steps enable applications to maximize the benefits of automatically scalable cloud resources.
- ***Designing for Security in the Cloud:*** Developers must balance the competing demands of rapid delivery against security while obtaining and maintaining the application's ATO. At the strategic level, this is accomplished by applying the Risk Management Framework (RMF) from the National Institute of Standards and Technology (NIST), which we discuss below. At the tactical level, the leading approach for secure application development is DevSecOps. As with the Agile and DevOps approaches, cross-team collaboration is a cornerstone of this approach. It also employs frequent, iterative development cycles, and benefits from standardization of environments and automation tools for development and testing of code. However, DevSecOps integrates the security team, its processes, and its tools into the entire DevOps workflow. Limited trust and zero trust security models are architectural patterns to secure access to processing and data. DSA implements these models to enhance security beyond strong authentication by placing limits on authorization, including: (1) increasing granularity of access controls, (2) limiting the duration of access without revalidation, (3) limiting the amount of data that can be accessed by roles, (4) performing all system actions with the user's authorization and not based on "trusted components", and (5) implementing tools and processes to ensure data is protected at both at rest and in motion, so that only the

For the U.S. Army's Intelligence Community Information Technology Enterprise (IC ITE), DSA implemented an Agile Scrum approach to developing the IC ITE cloud technical architecture. We increased efficiency by using the Ansible, Puppet, and OpenSCAP tools to automate the management, configuration, and security of the development environment in the AWS cloud. We ensured software quality by using the Jira, Confluence, SonarQube, and GitLab tools to manage and automate development and testing.

authorized party can access the data. DSA integrates security into the entire software lifecycle by tailoring modern methods and tools to fit the DoD culture. Our disciplined tailoring of these methods and tools reduces schedule and cost risks, and ensures the effectiveness of security controls in our DoD customer's cloud applications.

Development: DSA's cloud development strategies reduce the time and cost required to develop or modernize, test, and deliver cloud-based applications. We leverage key features of modern cloud environments such as: deployment templates for infrastructure, rapid allocation and disposition of IT assets, and modern automated development and test tools. This enables faster development with secure and consistent processes and tooling while reducing upfront investment.

For the Air Force, DSA leveraged Azure DevOps Build Pipeline to link the check-in and build processes, and integrated the Azure Key Vault to manage both 3rd Party licenses and DoD certificates for software signing during the build process. The DSA implementation of these tools provide the government a consistent, repeatable, CI/CD based delivery process, traceability from enhancement request to versioned product, and confidence in a securely signed software deliverable.

SECURING THE CLOUD

The fourth service applies a comprehensive, lifecycle approach to cloud security. Opportunities exist, through tested infrastructure and managed application services like Web Application Firewalls, Load Balancers, and Content Delivery Networks to reduce the attack surface. DSA ensures security of DoD applications in the cloud by designing and implementing secure, DoD-compliant cloud solutions, navigating the ATO process, and getting you visibility into the application's security status. Specifically, DSA performs the following tasks:

Apply the RMF to Ensure Application Security in the Cloud: The RMF (Figure 3. shown below), consists of a continual, six-step risk management process. The RMF integrates security into all aspects of the application lifecycle and coordinates security activities across IT organizations and stakeholders. In essence, the FedRAMP and DoD SRG certifications standardize the application of the RMF to the cloud and overlay cloud-specific security requirements and tasks on each step of the RMF. DSA applies the RMF to support DoD cloud projects.

Apply Best Practices in Cloud Security to include:

- ***The Shared Security Responsibility Model***. The CSP and the client share security responsibilities. The CSP ensures the underlying cloud infrastructure is secured to mitigate threats and attacks. The client implements security for the application (e.g., for content they store and the web services they deploy) located in the cloud. DSA will identify the controls your application can inherit from the CSP, saving you both time and money.
- ***Secure the Supply Chain***. In addition to the security controls in FedRAMP and those prescribed in the SRG, the DoD is integrating the CMMC into its security posture to not only certify cloud solutions, but also validate related supply chains are maintaining minimal security controls in their networks. DSA provides supply chain risk management assessments to identify vulnerabilities and approaches to mitigate risk.
- ***Identity and Access Management.*** Identity Access Management and Multifactor Authentication ensure that the user is who they say they are and that they have access to only the data they need. Role based access models and access tokens are techniques to limit access and trust for applications within a cloud security architecture.
- ***End-to-End Data Encryption***. Encryption mitigates the risk of data being exploited if the application or its hosting system is compromised. In DoD-approved clouds (such as milCloud

2.0), we encrypt data using AWS S3 managed keys for data-at-rest and configure Elastic File System (EFS) to use TLS tunneling for data-in-transit.

- ***Penetration (Pen) Testing***. Executing approved "cyberattacks" identifies and exploits weaknesses and determines how they enable access to your systems and data. DSA conducts Pen Test services for Federal cloud-based applications, networks, and control systems worldwide. We use a range of standard tools and a proven process that complies with NIST SP-800-53, Center for Internet Security Controls and Benchmarks, and SANS Institute best practices.

Achieving ATO: DSA ensures your compliance with the formal assessment and certification processes that enable cloud security to achieve the stringent capabilities required for DoD computing. These include:

- The implementation of the NIST RMF under DoDI 8510.01
- Cybersecurity Maturity Model Certification (CMMC)
- The standardization of cloud security through FedRAMP
- The FedRAMP extensions defined in the DoD SRG
- DoDI 8530.01, Cybersecurity Activities Support to DoD Information Network Operations

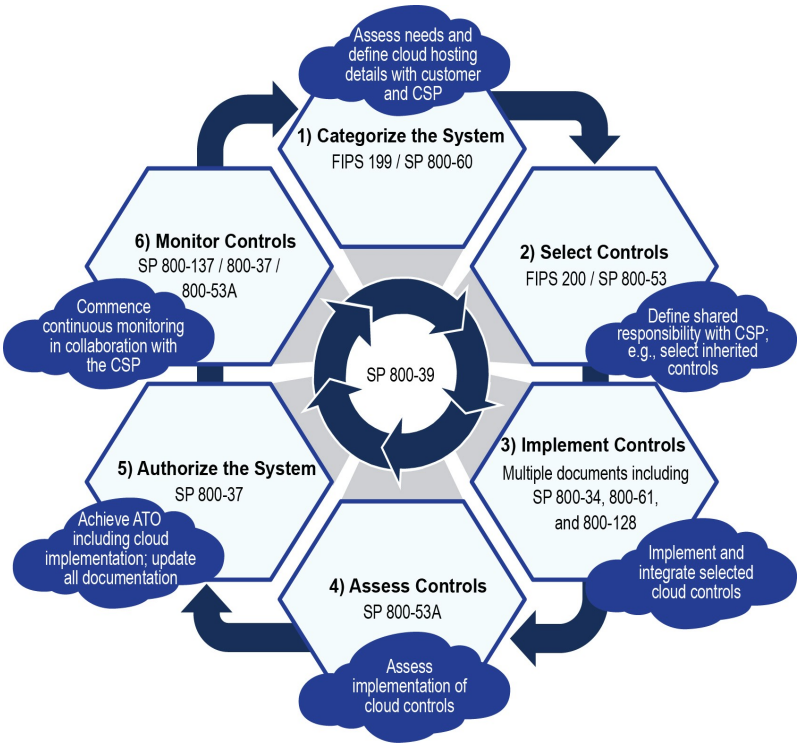

Figure 3 - RMF Six Step process