GUIDING PRINCIPLES FOR SUCCESSFUL CLOUD ADOPTION IN GOVERNMENT

vmware®

Table of Contents

TRADITIONAL PILLARS OF IT DESIGN

PEOPLE
Diverse needs of IT and end users within organizations must be incorporated into cloud design and plan.

PROCESS
Designing cloud services that span from infrastructure to platform.

TECHNOLOGY
Choosing the right technology for implementation. Key elements for selection: intelligent placement of services, capacity management, infrastructure neutrality, and automation and orchestration efficiencies.

Introduction

Cloud computing is gaining traction among government agencies seeking to modernize infrastructure, enhance security, and improve R&D computing power. Budget pressures, along with growth in the sophistication, stability, security and types of cloud applications, have also increased demand.[1] With proposed infrastructure modernization legislation (the MGT Act) nearing passage and new guidance from OMB's revised A-130 giving priority to cloud for certain investments, now is the time for every agency to prepare in earnest for hybrid cloud. This primer is designed to put your agency on the path to successful cloud adoption.

Government agencies face increasing difficulties integrating cloud services with existing infrastructure and operations. Organizations within the DoD and Intelligence Community, as well as civilian agencies, are pursuing strategies focused on the multidimensional value of cloud services, such as agility, scalability, innovation, and business growth,[2] yet many teams struggle with the complexity of migration and successful cloud transformation. A well-planned approach can help government agencies address the fundamental principles of cloud services and enable them to successfully begin or continue on their journeys to the cloud.

Approach

Planning and provisioning of cloud services is different from traditional IT services. To achieve successful cloud transformation, agencies need to plan for a holistic approach designed around the traditional pillars of IT design—People, Process, and Technology (PPT). An effective cloud adoption plan will address PPT in six key areas: Vision, Cloud Strategy, Team Enablement, Cloud Security, Application Migration, and Operations. The comprehensive plan should provide guidance about cloud services and deployment models that map to the agency's organizational goals, inclusive of tactical activities. With the right plan, agencies can execute on a cloud strategy that meets mission, security, and efficiency goals.

Guiding Principles

Vision

The cornerstone to garnering support for cloud transformation is the ability for a team to clearly and descriptively communicate the vision. The vision statement articulates an agency's need and how the new cloud model will solve specific challenges such as meeting a directive, replacing a system, or improving operational efficiency. A vision statement also documents the agency's high-level goals, as seen in the sample statement below. With a proper communication plan, stakeholders will understand and accept the shared vision and will collaborate in developing the desired state.

Sample Vision Statement

The Office of IT will leverage a secure 'Cloud Service Broker' model that will automate and standardize the IT infrastructure while reducing operating costs and time to deliver applications. The Office of IT will provide flexible, elastic, and cost effective multi-cloud services with High Availability (HA) and Disaster Recovery (DR) enhancements that enable agencies with best-in-class services and an epic customer experience.

vmware®

Cloud Strategy

After developing and communicating the vision, the next step is to develop a cloud strategy. The strategy focuses on defining principles, goals, and priorities. All stakeholders should have clear expectations and roles in the transformation. The cloud strategy also translates business requirements into people, process, and technology specifications. Example principles in use today are compliance with FedRAMP, adhering to a Cloud-First approach, and leveraging existing cloud environments. For example milCloud 2.0 [plans] to reduce hosting costs by up to 70%[4] making agency clouds more accessible and cost-effective solutions. After the organizational stakeholders agree on the strategy, a cloud roadmap is developed. The cloud roadmap describes specific goals, milestones, and strategies in achieving the vision. The cloud roadmap serves as a vital tool in visualizing agency goals, objectives, priorities, and schedules, and also defines the success criteria.

Phase 1.0	Phase 2.0	Phase 3.0	Future State
Technical Foundation	Cloud Foundation	Service-Driven Cloud	IT as a Service (ITaaS)
• Enable cloud broker platform	• Prototype HA/DR automation	• Disaster Recovery as a Service (DRaaS)	• Deliver ITaaS to Departments/Agencies
• Automate server provisioning	• Onboard public cloud-hosted services	• Cloud service costing and reporting	• Multi-cloud elasticity
• Implement core ITSM processes, including CMDB, asset management, and application mapping	• Define and improve upon ITSM processes	• Policy-driven, end-to-end automation	• Cost control and cloud service show back
• Develop network, DR, HA, and security strategies	• Enhance security with network micro-segmentation	• DevOps strategy, tools, and planning	• DevOps across people, process, and technology
	• Standardize physical infrastructure		• Continuous delivery and integration

Figure 1. Cloud Journey

Team Enablement

An integral component of the cloud strategy will be a discussion of staff development and transitioning the cloud environment to operations. While reusable aspects of traditional IT exist, cloud systems introduce new elements in how to support the mission. A function of leadership is to address skills gaps and ensure support staff can manage the new cloud services. According to industry research, the need for resources is the new concern for cloud adoption.[5]

Identifying and communicating the correct definition of cloud computing will prevent confusion and misunderstanding. The industry accepted definition of the cloud as defined by the National Institute of Standards and Technology (NIST) states: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." Therefore, it's also important to align system integrators, vendors, and internal stakeholders—both technical and senior management—with the agency's current and future needs, beginning early on when defining system requirements.

Because the agency's cloud will be a culmination of traditional disparate IT services, customers may find it difficult to identify a clear "owner." It is recommended to segment the cloud into a shared services model and assign owners accordingly. For example, Disaster Recovery-as-a-Service may be supported by a multi-functional team. However, there should be a single owner to drive SLAs, lifecycle management, and operations. Defining roles also assists in identifying gaps that exist within the agency. Breaking down traditional IT silos and supporting services horizontally across the IT stack will require a more specialized and flexible skillset. A dedicated plan to enable and train staff is likely to result in increased value and efficiencies in adopting innovative solutions within the cloud.

Cloud Security

Often government agencies refrain from building cloud solutions because of security concerns as IT is responsible for securing every interaction between users, applications, and data. It's not always clear how the cloud solution is protecting these interactions while at the same time meeting compliance requirements (e.g., FedRAMP).

Cloud services and security should co-exist in the new cloud paradigm. For organizations adopting cloud, having visibility and control into the cloud environment are essential to mitigating security risks. Cloud environments enable simultanous protection and compliance across application infrastructure, identity, and endpoints. Implementing security solutions across these three areas ensures security is applied across people, process, and technology. For example, VMware recommends applying a ubiquitous software layer across application infrastructure and endpoints so agencies can maximize the visibility of the interaction between users and applications, and align security controls and policies to protected applications.

Application Migration

An application migration strategy is an essential facet to successfully achieving cloud adoption. Cloud solutions are not necessarily a silver bullet to solving technology challenges or saving money; however, having a well-developed and agency-specific application migration strategy yields a drastic reduction of risk in achieving cloud adoption objectives.

A phased approach is essential to a migration strategy as is the identification and prioritization of applications. While the need may seem obvious, many agencies struggle to migrate legacy applications or are met with cultural opposition. The following high-level steps increase the success of application migration:

1. Identify agency goals

2. Create application migration criteria

3. Assess application dependencies and service redundancy

4. Prioritize systems and applications

5. Develop reusable migration processes

A phased approach will efficiently identify which applications can be moved to the cloud, and will also identify which applications are not cloud candidiates and require legacy support. Similarly, agencies can assuage fear of risk by testing the application's infrastructure requirements and dependencies in a development environment, virtualizing legacy appliacations, or focusing on non-mission-critical applications.

Operationalizing Cloud Services

Once an application is migrated to the cloud, there are additional requirements (often times overlooked or simplified) to operating and maintaining cloud services. New or modified policies, processes, and procedures (3Ps) are required for operational activities such as in-house system integration, backup and recovery, and configuration management. As typical cloud environments begin as greenfield deployments, agencies have the opportunity to redefine the 3Ps through the use of reference documentation that contains the design, installation, and operational needs of the cloud environment. Defining and documenting the cloud environment contributes to developing services automation (e.g., administration, self-service, etc.) and internal communications (e.g., service capabilities, outages, etc.) resulting in standardized and efficient operations.

Achieving Cloud Adoption

Common challenges associated with adopting cloud in highly regulated environments involve vision, strategy, enablement, security, migration, and operationalization. Elements inclusive of cloud strategy—end-user experience, visibility, cost-transparency, performance monitoring, endpoint management, legacy system support, and resource utilization—also require a new or modified approach in comparison to traditional IT processes. VMware addresses these challenges by employing a top-down advisory approach with a holistic technology view, executive support strategy, and focus on operationalization. Combining these elements with industry-leading experience results in cloud environments that deliver long-term success without compromising security or incurring additional risk.

VMware solutions enable government IT to transform complex environments and operations while meeting current security challenges. VMware is uniquely positioned with its products, solutions, and professional services to enable the design, development, migration, and adoption of customers' cloud environments to meet the needs of agency missions and objectives.

For more information on VMware Cloud Services, please visit https://cloud.vmware.com/

Works Cited

1. Deltek. (2016, October). Federal Priorities: Cloud, Big Data, Mobility, and Data Centers, 2016-2021

2. Gartner. (2017, February 22). Gartner Says Worldwide Public Cloud Services Market to Grow 18 Percent in 2017. Retrieved from Newsroom /Press Release: http://www.gartner.com/newsroom/id/3616417

3. Colombus, L. (2017, April 23). Forbes / Tech in the Cloud. Retrieved from Forbes: https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/#26a2f2441848

4. Lazar, M. (2016, November 3). Current Cloud Computing Statistics. Retrieved from INSIGHT: https://www.insight.com/en_US/learn/content/2016/11032016-current-cloud-computing-statistics.html

5. Norton, N. (2017, October). Current Cloud Computing Statistics. Retrieved from The Drumbeat: https://www.disa.mil/NewsandEvents/Drumbeat

vmware®