The 11th Commandment: Thou Shalt Migrate to the Cloud

Emily Hagerty, Orly Olbum, and Brian Flynn

ABSTRACT

And God gave unto Moses on Mt. Sanai and to General Dunford in the Pentagon the 11th Commandant: *Thou Shalt Migrate to the Cloud*.

This paper presents research that supports cloud brokers, mission owners, program offices, and agency cost components in their quest for the Holy Grail – *cost effective* and *cyber-security compliant* migration of legacy systems and data to the cloud. It offers innovative artifacts to support up-front requirements and trade-space analyses and back-end cloud design, build, testing and deployment, including:

- A Cloud Acquisition Process Breakdown Structure (CA PBS) that details the steps required to execute a cloud acquisition and that supports cloud architecture and design choices
- A Cloud Work Breakdown Structure (CWBS) for Investment and Sustainment
- A framework for a Business Case Analysis (BCA) for cloud acquisition
- Insights on cloud service and deployment options
- A comparison of vendor space.

The research, importantly, supports SECDEF direction to "….strengthen and streamline commercial operations within the Department … and to meet the challenging task of building cloud strategies for requirements related to military operations and intelligence support."

INTRODUCTION

The adoption of cloud computing by the public and private sectors continues to accelerate, enticed by the cloud's *potential* to deliver cost savings, faster time to market, flexibility to respond quickly to shifts in customer/warfighter demands, and, last but not least, better capability to leverage advances in artificial intelligence and cybersecurity. Consequently, over 80% of fortune 500 companies and many federal departments and agencies, right or wrong, have adopted a cloud-first policy.

Simply put, cloud computing uses the Internet (or the "cloud") as the delivery platform for providing users with virtual CPUs, servers, storage, networking, databases, applications software, data analytics, and intelligence, in addition to other capabilities. Users pay only for the cloud services they use, akin to charges for the use of utilities such as water or electricity.

At first blush, the use of cloud computing might appear rather simple to evaluate and estimate. Commercial cloud calculators unfortunately compound this misconception; too often they're in the nature of marketing mechanisms.

In reality, acquisition programs or mission/functional areas such as financials, logistics, supply and personnel lack requisite knowledge of the complete breadth and depth of their legacy applications, systems interfaces, quality and quantity of data, and choices available in the cloud. Further, Cloud Service Providers (CSPs) have continued to develop and enhance their Cloud Service Offerings (CSOs) in the "cloud stack," or the pyramid of Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Some of the major CSPs now offer almost a dozen choices in databases alone – making the landscape more complicated than ever to understand and evaluate.

Programs that rush blindly to the cloud without executing a comprehensive business case analysis (BCA) run the risk of forgoing many of cloud's potential benefits while also unnecessarily incurring additional costs. Potential cost overruns and ineffective implementations might occur due to poor understanding of factors such as the size of legacy applications, the number and complexity of system interfaces, the quantity and quality of data to be migrated, the need for business process reengineering, and the general complexity of the defense environment. These problems can be mitigated by proper up-front analysis as detailed in this paper.

Our investigation and hands-on experience with several historical and on-going acquisitions identifies the following gaps in cloud migration efforts:

- **Cloud Tradespace Myopia**
  - Preferred system and cloud vendor identified too early
  - Limited view of tradespace when, in reality, there's a large number of architectures and offerings

- **Complexity of Effort**
  - Failure to fully assess the state of legacy systems including information flows, system interfaces, and quantity and quality of data
  - Failure to adequately understand the cloud acquisition process

- **Cloud Cost Estimating Early On**
  - Lack of a cloud Cost Element Structure and a CES data dictionary

- **Cloud Linkages**
  - Lack of a crosswalk between Cloud WBS and MILSTD-881D, and linkage to DoDI 5000.75[1]

- **Cloud Cost Data**
  - Data must drive the analysis, but there is very little DoD cloud cost history and the data that exists is hard to collect and unstructured

- **Cloud Cost Risk Analysis**
  - New challenge for the cost community; e.g., initial storage requirements

- **Cloud Cost/Capability Tradespace**
  - Challenge finding the "knee in the curve"
  - E.g., cloud security versus cost or "cold" versus "hot" cloud data storage.

This paper addresses these gaps by providing the insights and innovative artifacts to help organizations achieve better cloud performance, to mitigate total ownership costs, and to meet system affordability thresholds.

[1] DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," USD AT&L, 2 February 2017

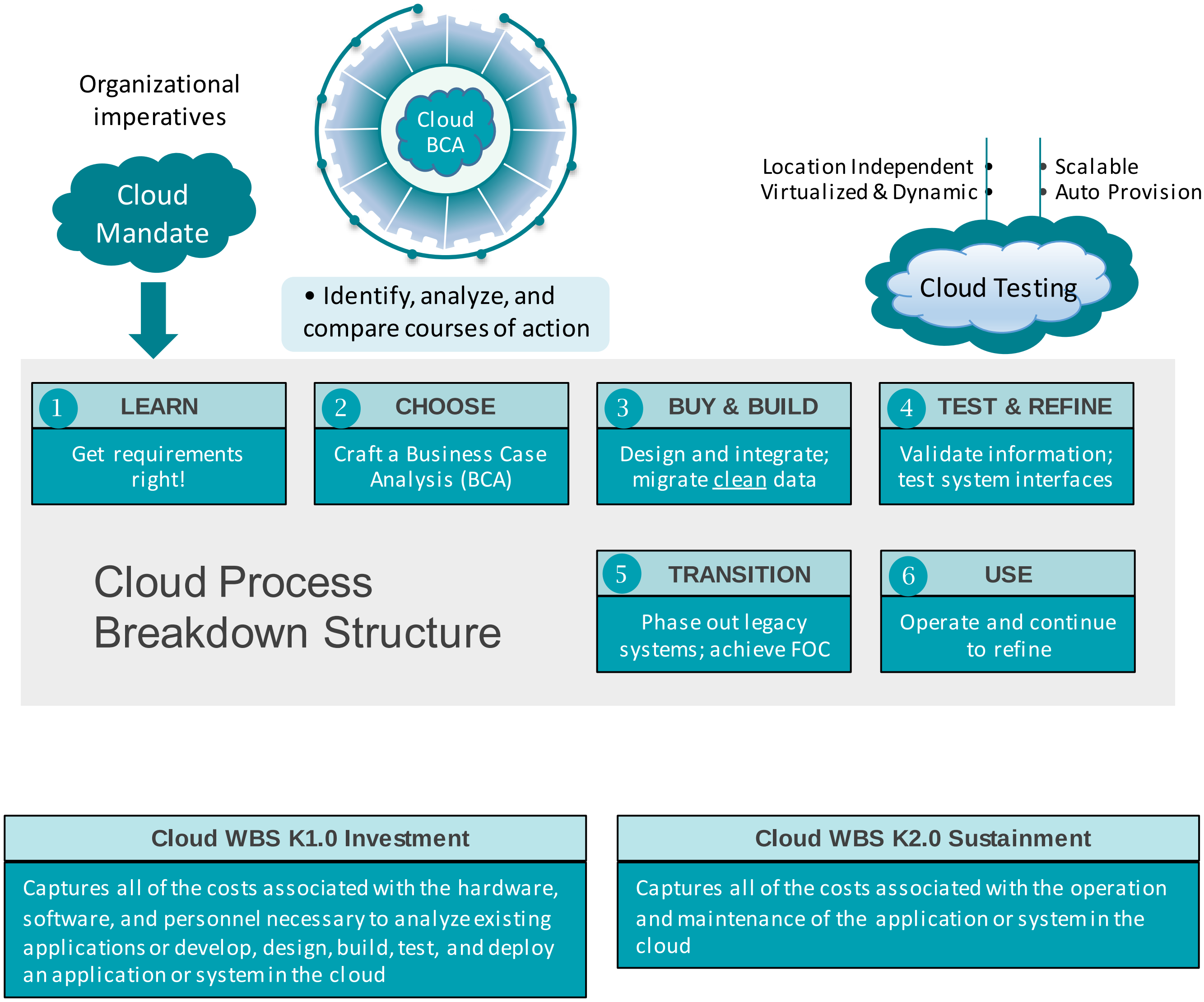
Our intent is straightforward -- prevent kneejerk cloud migration decisions and incomplete cloud cost estimates prejudiced by cloud service providers' narrow view of the cloud challenge in the national security operating environment. To that end, and as illustrated in Figure 1, this paper presents the first-ever, comprehensive:

❑ **Cloud Acquisition Process Breakdown Structure** that details the steps required to migrate to the cloud, from upfront requirements and design to backend system refinement, testing, and deployment

❑ **Cloud Framework for BCAs** that details all the steps needed to formulate alternative cloud architectures, to collect and analyze data, and analyze and life-cycle costs and benefits of alternatives, and to make key tradeoffs between cost, capability, and risk

❑ **Cloud Work Breakdown Structure** that considers all costs – from existing application discovery through the sustainment of a cloud solution – that are neither captured nor referenced in cloud service providers' online cost calculators.

We are extremely excited to share this important advance in cloud cost analysis capability with the community and hope it stimulates further thought, collaboration and advances!


Organizational imperatives
Cloud Mandate
Cloud BCA
• Identify, analyze, and compare courses of action
Location Independent •
Virtualized & Dynamic •
• Scalable
• Auto Provisioned
Cloud Testing
1 LEARN
Get requirements right!
2 CHOOSE
Craft a Business Case Analysis (BCA)
3 BUY & BUILD
Design and integrate; migrate clean data
4 TEST & REFINE
Validate information; test system interfaces
Cloud Process Breakdown Structure
5 TRANSITION
Phase out legacy systems; achieve FOC
6 USE
Operate and continue to refine
Cloud WBS K1.0 Investment
Cloud WBS K2.0 Sustainment

Cloud WBS K1.0 Investment

Captures all of the costs associated with the hardware, software, and personnel necessary to analyze existing applications or develop, design, build, test, and deploy an application or system in the cloud

Cloud WBS K2.0 Sustainment

Captures all of the costs associated with the operation and maintenance of the application or system in the cloud

Figure 1: Cloud Process Breakdown Structure (CA PBS), Cloud BCA, and Cloud WBS

CLOUD MIGRATION MANDATE

Across DoD there has been a mandate to migrate to the cloud, with the underpinning goal of achieving cost effective and cyber-security compliant migrations of both systems and data.

Any capability gap within DoD can be evaluated as a combination of *problems, opportunities*, and *directives*. A *problem* is an adverse situation that prevents an organization from fully achieving its mission, vision, and goals. An *opportunity* provides the chance to improve systems and processes. Finally, a *directive* is a new regulatory or statutory requirement.

DoD has recognized that legacy-systems are *problems* and that the cloud presents *opportunities*. Furthermore, the mandate for defense components to migrate to and consume cloud resources is formalized in Department *directives*.

For example, the Deputy Secretary of Defense recently prioritized the adoption of cloud technology to "….strengthen and streamline commercial operations within the Department" and to build "cloud strategies for requirements related to military operations and intelligence support."[2] The Joint Requirements Oversight Council (JROC) further stated that "… efforts for accelerating to the cloud are critical in creating a global, resilient, and secure information environment that enables warfighting and mission command, resulting in improved agility, greater lethality, and improved decision-making at all levels."[3] Even bolder still, the Department of the Navy issued a Cloud first strategy that requires components to "… design, transfer, host, operate, and sustain IT capabilities with Commercial Cloud Service Provider (CCSP) hosting environment to the maximum extent possible."[4]

In summary, cloud technology presents an opportunity that DoD has mandated be exploited. Migrating to the cloud is no longer a *suggested* best practice. It has, through these mandates, become *the* best practice whether or not proven. However, blindly deciding to adhere to the "go to the cloud" mandate in the absence of thoughtful analysis from the cost community will likely result in selecting the wrong cloud solution or cloud migration method.

[2] "Accelerating Enterprise Cloud Adoption Update," Deputy Secretary of Defense, 8 January 2018

[3] "Joint Characteristics and Considerations for Accelerating to Cloud Architectures and Services," Joint Requirements Oversight Council, 22 December 2017

[4] "Navy Commercial Cloud Brokerage Policy," DON Deputy Chief Information Officer (Navy), VADM Jan Tighe, 17 Dec 2017

CLOUD INTRODUCTION

Cloud computing is a broad term that describes a wide range of services. For programs to understand how the cloud can be valuable to their organization and for cost analysts to develop accurate and defensible estimates, it is important to understand what the cloud really is and its different components. Due to the cloud being a broad collection of services, organizations can choose where, when, and how they will use cloud computing, increasing the complexity for cost analysts to estimate the resources that the cloud offers, often collectively described as "compute, network, and storage." This section of the paper provides an introduction to cloud basics, terminology, offerings, and cost implications.

Cloud computing is a model for on-demand network access to a shared pool of configurable computing resources such as servers, storage, and databases, with rapid, automatic, and elastic provisioning on a pay-for-use basis.

The generally accepted definition of *cloud computing* comes from the National Institute of Standards and Technology (NIST). The NIST definition begins as follows:

"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."

This essentially means that cloud end users can use portions of bulk resources that can be acquired quickly and easily.

According to NIST, key tenets of the cloud computing model are:[5]

- On-Demand Self Service. Computing resources such as server time and network storage are automatically and rapidly provisioned without the need for human interaction

- Broad Network Access. Capabilities are available over the network and accessible by heterogeneous clients

- Resource Pooling. Resources such as storage, processing, memory and virtual machines serve multiple consumers simultaneously

- Rapid Elasticity. Capabilities such as virtual machines and containers are rapidly and elastically provisioned to quickly scale in and out based on fluctuating demand. To the consumer, the resources available can be purchased in any quantity at any time

[5] NIST SP 800-145: http://csrc.nist.gov/publications/PubsSPs.html

- Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability such as storage, processing, and bandwidth

To maximize the benefits of cloud computing, a solution must demonstrate these particular characteristics.

CLOUD PLAYERS

Figure 2 presents a generic and high-level cloud-computing architecture based the Navy's cloud governance structure, the DoD 5000.75 acquisition framework, and a model from the National Institute of Standards and Technology (NIST). The architecture identifies the major actors in the cloud ecosystem along with their activities and functions.

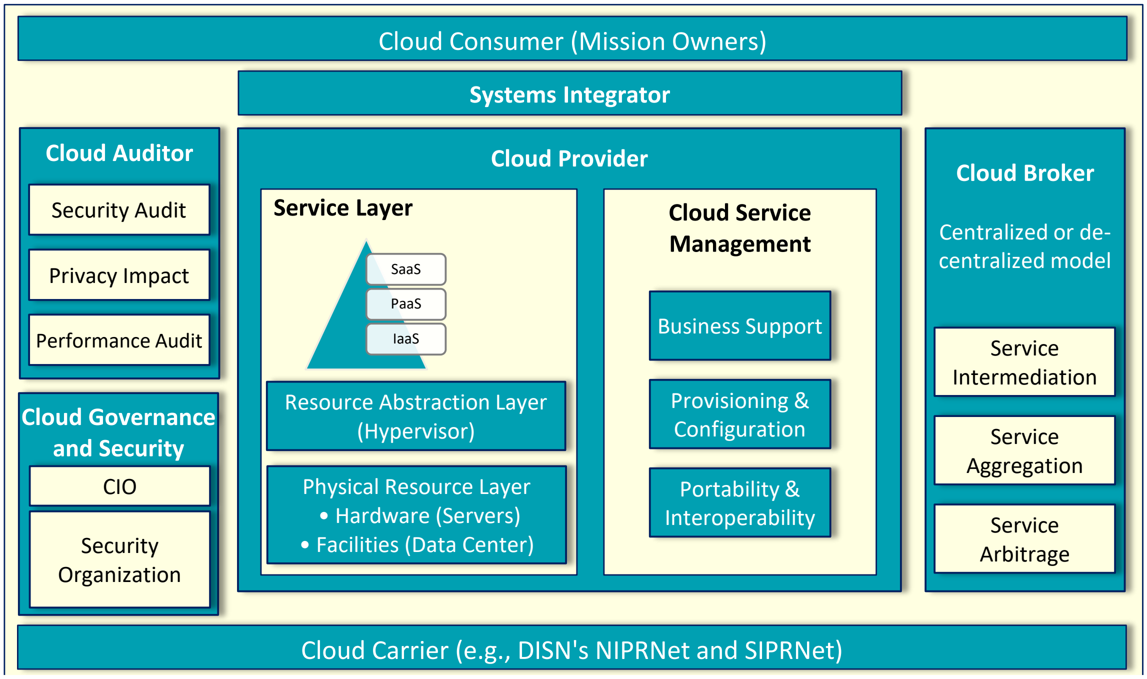


Figure 2: Cloud Computing Reference Architecture

- Cloud Consumer. The cloud consumer is the mission or application owner. This can also be considered as the set of stakeholders in a functional community such as personnel, maintenance, logistics, supply chain management, or program management. The cloud consumers use various elements of the cloud stack to run their operations, for whatever deployment model they choose such as private, public, or hybrid.

- Cloud Provider. A cloud provider is a company that provides a cloud-based platform, infrastructure, application, or storage services to other business or individuals. Cloud providers are also referred to as cloud service providers, or CSPs. Importantly, a Cloud

Service Offering (CSO) is the IaaS/PaaS/SaaS solution available from a CSP, and a CSP might provide more than one CSO.

- Cloud Broker. A cloud broker is an independent entity that acts as an intermediary between the purchaser of a cloud computing service and the seller of that service. The cloud broker manages the use, performance and delivery of cloud services and negotiates relationships between cloud consumers and cloud providers. Through knowledge of CSP capabilities and prices, Service Level Agreements, and mission requirements, the cloud brokers help make the best match between supply and demand of cloud services. A cloud broker can help a cloud consumer view all options on an equal scale. Cloud brokers provide services in three categories, as defined by NIST, which are aggregation, arbitration, and intermediation.

    - Aggregation. A cloud broker combines and integrates multiple services into one or more new services. The broker provides data integration and ensures the secure data movement between the cloud consumer and multiple cloud providers.

    - Arbitration. Service arbitrage is similar to service aggregation except that the services being aggregated are not fixed. Service arbitrage means a broker has the flexibility to choose services from multiple agencies.

    - Intermediation. For the Navy cloud, this function includes helping mission owners of legacy systems determine their cloud acquisition strategy; managing customer access to the NECC; and monitoring cloud performance.

- Cloud Auditor. A cloud auditor is an independent third-party who can assess services, system operations, performance and security of the cloud.

- Cloud Carrier. The cloud carrier provides the connectivity and transport of cloud computing services from CSPs to cloud consumers.

- Systems Integrator. Business system program offices typically have a systems integrator (SI). These companies help define best practices and cloud implementation roadmaps. They may also assist in analyzing and consolidating legacy applications, systems, and data prior to migrating to the cloud.

CLOUD COMPUTING STACK

Cloud computing, often described as a stack, has a broad range of services built on top of one another under the name *cloud*. This cloud computing stack is often described as a pyramid of three services, where Infrastructure as a Service (IaaS) is the foundation of the pyramid, Platform as a Service (PaaS) is the middle, and Software as a Service (SaaS) is the top and are referred to as the Cloud Delivery Models.

However, as cloud offerings evolve, CSOs within each category of service have continued to expand, making the distinctions and boundaries between the three less clear.

The following explanations and observations are intended to help inform and shape the design of cloud architecture, ensuring that all elements of a cloud life-cycle cost estimate are captured.

Infrastructure as a Service. IaaS delivers cloud computing infrastructure to organizations, including servers, network, operating systems, and storage, over the Internet through virtualization technology. IaaS provides the same technologies and capabilities as a traditional data center without having to pay for maintenance or management. IaaS cloud service providers typically charge users based on the number of *instances*, or CPU power, memory, and storage consumed in one hour. Another billing option is *reserved pricing* where customers pay upfront for locking in their requirements in exchange for significant discounts on price. Different from SaaS or PaaS, IaaS consumers are responsible for managing various aspects, such as applications, runtime, OSes, middleware, and data. However, cloud providers of IaaS manage the servers, hard drives, networking, virtualization, and storage. Some providers also offer services outside of the virtualization layer, such as databases or message queuing.

Platform as a Service. PaaS is a complete development and deployment environment in the cloud, provided on a subscription basis. PaaS brings the benefits to the software development world that SaaS brought for applications. PaaS can be defined as a computing platform that enables the quick and easy creation of web applications without the necessity of buying and maintaining the underlying software and infrastructure. PaaS is similar to SaaS except that, rather than being software delivered over the web, it is a platform for the creation of software that is delivered over the web. PaaS includes a wide range of resources such as preinstalled and configured databases and middleware to enable the delivery of solutions ranging from simple web applications to sophisticated enterprise resource planning products. PaaS can be either public or private, or a combination of the two. Public PaaS runs on an infrastructure that is shared by many organizations. Private PaaS runs on an infrastructure that is used exclusively by a single organization.

PaaS is especially useful in an environment such as DoD with many geographically and organizationally dispersed stakeholders, especially when they need to interact with each other and with software engineers in development and testing process. PaaS is especially useful when multiple developers are working on a development project or when other external parties need to interact with the development process. Importantly, PaaS supports agile software development and the guidelines of DoDI 5000.75 since it eases the difficulties around rapid development and iteration of software. PaaS, on the other hand, may not be particularly appropriate in cases where application performance requires signification customization of underlying hardware and COTS software.

PaaS, however, might not always be the best delivery option. For example, if an application needs to be highly portable in terms of where it is hosted, if proprietary languages or approaches would impact the development process, or if a proprietary language would hinder later moves to another provider and create vendor lock-in.

As the Cloud matures, anticipated PaaS subscriptions fees will be for tools and capabilities such as relational databases, data migration, analytics and artificial intelligence, cloud service integration, and security.

Software as a Service. Software as a service (SaaS) is defined as software that is deployed over the Internet. A provider can license a SaaS application as an on-demand service to customers through a variety of ways: either through a subscription, through a pay-as-you-go model, or at no charge, when there is opportunity to generate revenue from streams other than the user, such as from advertisement.

SaaS, however, may not always be the best delivery option. These situations might include applications that require extremely fast processing of real-time data but where limited network bandwidth impedes execution, applications for which legislation or other regulations does not permit data being hosted externally, or applications for which an existing on-premises solution fulfills the organization's needs

In each case the CSP will license their application to customers as an on-demand service, either through a subscription or through a pay-as-you-go model. A cloud broker will likely continue the current best-practice of negotiating enterprise-level pricing agreements with the vendors to obtain economies-of-scale discounts. Overall, each cloud model offers its own specific features and functionalities, and it is crucial for any organization to understand the differences and potential cost and performance implications. Whether a program requires cloud-based software for storage options, a platform to create customized applications, or complete control over an entire infrastructure without having to physically maintain it, there is likely a cloud solution available. No matter the option, properly migrating to the cloud is the future of business and technology, and it is necessary to be properly informed.

CLOUD DEPLOYMENT MODELS[6]

One of the key elements of cloud computing is the deployment model, or the paradigm of making software available and ready for use. A cloud deployment model represents a specific type of cloud environment, primarily distinguished by ownership, size, and access. In practical applications, there is no best model and different models are available to meet different requirements. Common deployment models, defined below, are public, private, community, and hybrid.

Public Cloud

The public cloud is a cloud environment that is publicly accessible and is owned by a third-party CSP. The resources on public clouds are usually provisioned via the cloud delivery models and are generally offered to cloud consumers at a cost or through other avenues (such as through advertisements). The cloud provider is responsible for the creation and maintenance of the public cloud and its resources. Therefore, the public cloud may be owned, managed, and operated by a CSP, academia, or a government organization, or some combination of them. It exists on the premises of the cloud provider. The public cloud generally employs a utility model with a pay-as-you-go feature for users. Organizations are only responsible for what they use, and are sharing physical server space with other tenants as well as network, storage and hardware. The public cloud support connectivity over the Internet and is best suited for information that is not sensitive.

Private Cloud

A private cloud is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units within a corporation or defense organizations within a command). Private clouds enable an organization to use cloud computing technology as a means of centralizing access to IT resources by different parts, locations, or departments of the organization. The use of a private cloud can change how organizational and trust boundaries are defined and applied. The actual administration of a private cloud environment may be carried out by internal or outsourced staff. The private cloud is particularly suited for cases where a high level of security is required. That is, resources in the private cloud are not shared with other tenants as in the public cloud model.

Community Cloud

A community cloud is similar to a public cloud, however its access is limited to a specific community of cloud consumers. The community cloud can either be jointly owned by the community members or by a third-party CSP that provisions a public cloud with limited access. The community cloud may also be on- or off-premise. The infrastructure in this model is

[6] "Cloud Deployment Models," Arcitura Education Inc., arcitura.com, Accessed 13 Feb 2019.

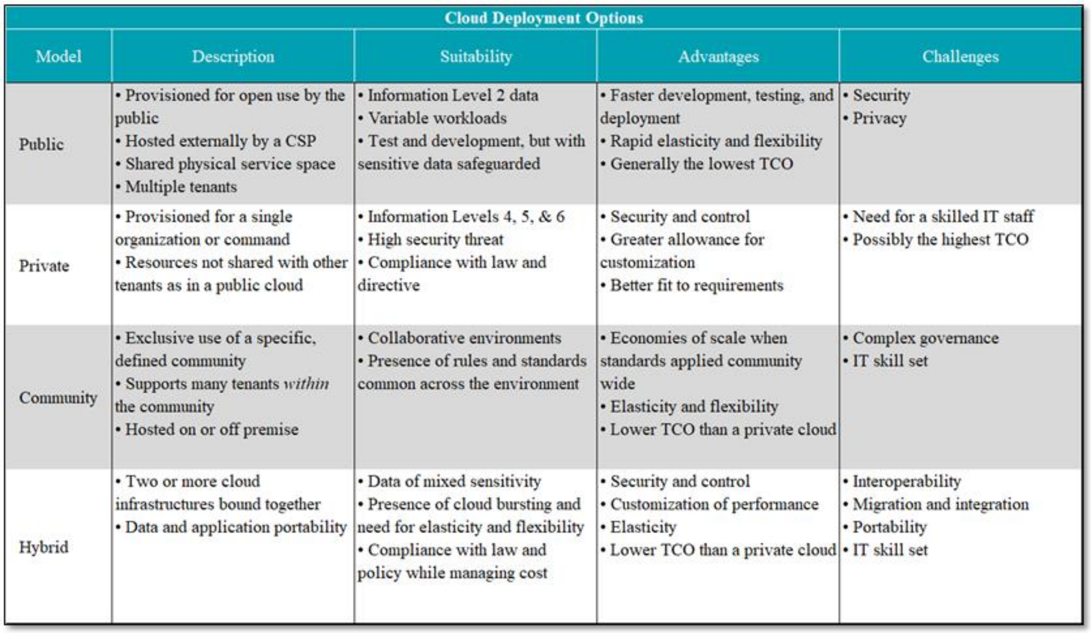
provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns such as mission, security, policy, and compliance with statute and regulation. In defense, examples of community clouds are GovCloud from the CSPs and milCloud. At least one major CSP has plans to build a defense cloud for the exclusive use of DoD clients and their applications.

Hybrid Cloud

A hybrid cloud is a cloud environment comprised of two or more different cloud deployment models. For example, a cloud consumer may choose to deploy cloud services processing sensitive data to a private cloud and other, less sensitive cloud services to a public cloud. While a hybrid cloud combines two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, these infrastructures are bound by standardized or proprietary technology that enables data and application portability. One of the benefits of portability would be load balancing between clouds. For example, an organization may stay on premise or in a private cloud space during regular or off-peak times but use parts of a public cloud to handle peak usage. However, hybrid deployment architectures can be complex and challenging to create and maintain due to potential differences in cloud environments. Further, management responsibilities are more difficult since they are typically split between the private add public CSPs.

The choice of the deployment model – public, private, hybrid, or community – depends largely upon factors such as workload patterns (e.g., steady, predictable bursting, or unpredictable bursting), security demands, program and DoD instructions and policy, the classification of hosted data (e.g., IL 2, 4, 5, or 6).

Furthermore, key issues arise related to interfaces, security, reliability, business continuity, latency, and life-cycle costs. A Business Case Analysis (BCA) should address all of these. Figure 3 provides rules of thumb to support the decision calculus.



Cloud Deployment Options

Model	Description	Suitability	Advantages	Challenges
Public	• Provisioned for open use by the public • Hosted externally by a CSP • Shared physical service space • Multiple tenants	• Information Level 2 data • Variable workloads • Test and development, but with sensitive data safeguarded	• Faster development, testing, and deployment • Rapid elasticity and flexibility • Generally the lowest TCO	• Security • Privacy
Private	• Provisioned for a single organization or command • Resources not shared with other tenants as in a public cloud	• Information Levels 4, 5, & 6 • High security threat • Compliance with law and directive	• Security and control • Greater allowance for customization • Better fit to requirements	• Need for a skilled IT staff • Possibly the highest TCO
Community	• Exclusive use of a specific, defined community • Supports many tenants *within* the community • Hosted on or off premise	• Collaborative environments • Presence of rules and standards common across the environment	• Economies of scale when standards applied community wide • Elasticity and flexibility • Lower TCO than a private cloud	• Complex governance • IT skill set
Hybrid	• Two or more cloud infrastructures bound together • Data and application portability	• Data of mixed sensitivity • Presence of cloud bursting and need for elasticity and flexibility • Compliance with law and policy while managing cost	• Security and control • Customization of performance • Elasticity • Lower TCO than a private cloud	• Interoperability • Migration and integration • Portability • IT skill set

Figure 3: Cloud Deployment Options

CLOUD VENDOR MARKET SPACE

Cloud vendor space describes the main players in the world of cloud computing for the government. While many Cloud Service Providers (CSPs) exist and are prepared to support any or all of the cloud stack, the main players are evident. Our research into these major vendors (i.e., Amazon, Google, IBM, Microsoft, Oracle, Redhat, and Salesforce), including thorough discussions with the larger CSPs, leads to a logical framework for cloud brokers and mission owners to employ.

IaaS

- The major CSPs generally have the same offerings regarding the bottom of the cloud stack. Compute and storage capabilities are similar across the board, but as IaaS grows, different CSPs refine different offerings, such as containers and Kubernetes. Other vendors adapt and mature to compete.
- CSPs often offer government services via a "government cloud" on isolated servers, but some CSPs are even going as far as establishing government only clouds for DoD's use alone. The need of government for cloud isolated from regular internet and access pushes the major CSPs to support instances approved at Information Impact Level (IIL) 5 or 6.

- Most of the major CSPs provide calculators to compute costs of hosting on the cloud using their services, but are similar in functionality and content even though accesses and presentations differ across the board.

Vendor Differentiation

- Many of the major vendors such as Oracle, Microsoft, Google, and IBM emphasize providing services that cover the entire cloud stack; IaaS, PaaS, and SaaS.
- The dominant player in IaaS, Amazon, has little to no offerings in the SaaS part of the cloud stack. By contrast, Salesforce excels in SaaS services but offers no IaaS capabilities.
- The vendors in enterprise-level software for SaaS offerings of interest to DoD are Microsoft, SAP, and Oracle.
- As cloud matures, PaaS is receiving more focus, and thus more support by the major vendors.

Vendor Competition

- The CSPs generally differentiated themselves based on speed and price until recently. However, three different sources independently shared that today's price differences for IaaS between two of the major CSPs is only two percent. This delta is statistically significant.
- The battle between CSPs will grow to include concerns about security, compliance with DISA's SRG, service level agreements, hybrid cloud management, and hybrid cloud management as the IaaS market matures.
- CSPs develop improved capabilities for data sharing between multiple clouds, as well as for clouds to connect to on-premise servers and non-cloud data centers.

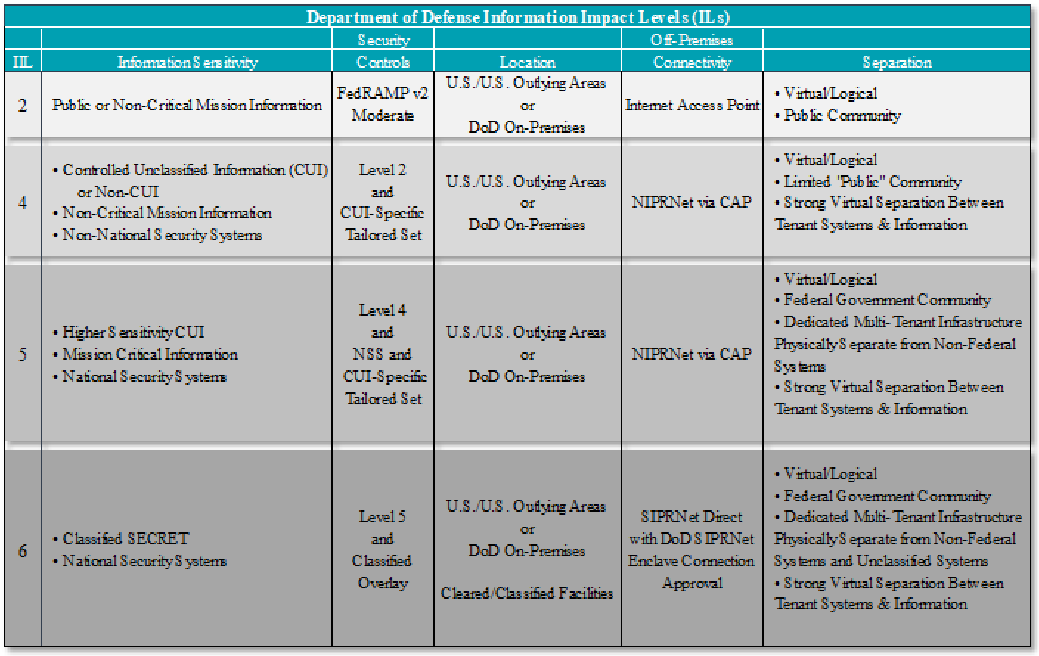
Artificial Intelligence

- AI has become increasingly attractive to the major CSPs, who are strongly inserting machine learning and other types of artificial intelligence into their offerings. AI algorithms adapt automatically if inputs change
- For example, last year Oracle created a self-maintaining database for the cloud and Amazon developed SageMaker, which enables developers and data scientists to quickly and easily build, train, and deploy machine learning models at any scale.

CLOUD SECURITY

OVERVIEW

To ensure cloud acquisitions meet the security requirements that exist for DoD, DISA uses the information impact levels (ILs) of Figure 4 to assess a CSO.[7] These impact levels range from level 2, publically releasable and non-mission critical unclassified information, to levels 4, 5, and 6 that require higher levels of protection.



Department of Defense Information Impact Levels (ILs)					
		Security		Off-Premises	
IIL	Information Sensitivity	Controls	Location	Connectivity	Separation
2	Public or Non-Critical Mission Information	FedRAMP v2 Moderate	U.S./U.S. Outlying Areas or DoD On-Premises	Internet Access Point	• Virtual/Logical • Public Community
4	• Controlled Unclassified Information (CUI) or Non-CUI • Non-Critical Mission Information • Non-National Security Systems	Level 2 and CUI-Specific Tailored Set	U.S./U.S. Outlying Areas or DoD On-Premises	NIPRNet via CAP	• Virtual/Logical • Limited "Public" Community • Strong Virtual Separation Between Tenant Systems & Information
5	• Higher Sensitivity CUI • Mission Critical Information • National Security Systems	Level 4 and NSS and CUI-Specific Tailored Set	U.S./U.S. Outlying Areas or DoD On-Premises	NIPRNet via CAP	• Virtual/Logical • Federal Government Community • Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems • Strong Virtual Separation Between Tenant Systems & Information
6	• Classified SECRET • National Security Systems	Level 5 and Classified Overlay	U.S./U.S. Outlying Areas or DoD On-Premises Cleared/Classified Facilities	SIPRNet Direct with DoD SIPRNet Enclave Connection Approval	• Virtual/Logical • Federal Government Community • Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems and Unclassified Systems • Strong Virtual Separation Between Tenant Systems & Information

Figure 4: Department of Defense Information Impact Levels (ILs)

CSPs achieve a DoD Provisional Authorization (PA) at impact level 2 for their cloud service offerings once they are able to demonstrate compliance with the controls of the Federal Risk and Authorization Management Program (FedRAMP). PAs at the higher impact levels require additional demonstration that a vendor can meet more stringent security requirements.

The four ILs align the criticality and sensitivity of data to access and separation requirements in a cloud environment. Cloud consumers must choose both a CSP and their respective CSO that suit functional needs as well as possess the PA appropriate for the data's IL. The PA and supporting documentation is then leveraged in granting an Authorization to Operate (ATO) in the cloud.

[7] DoD Cloud Computing Security Requirements Guide (SRG) v1r; 6 March 2017, DISA; http://iase.disa.mil/cloud_security/Pages/index.aspx

COST IMPLICATIONS

Importantly, additional costs will be incurred for enhanced security at the higher IL4 and IL5 levels. DISA's Secure Cloud Computing Architecture (SCCA) is a set of services that provides the same level of security the agency's mission partners receive when hosted on-premises or on one of DISA's physical data centers.

All Impact Level 4 and 5 data must be secured according to the requirements described in DISA's SRG, and namely, any data hosted in commercial cloud environments must use the Cloud Access Point component of the SCCA to connect to the Defense Information System Network (DISN).

The SCCA has four components: Cloud Access Points (CAP), a Virtual Data Center Security Stack (VDSS), Virtual Data Center Managed Services (VDMS), and a Trusted Cloud Credential Manager (TCCM).[8] These components are visualized depicted in Figure 5.

- *Cloud Access Point*. The CAP provides access to the Cloud as well as boundary protection of DISN from the Cloud, and firewall and intrusion detection and prevention cybersecurity capabilities. The CAP is specifically tailored to operate at DoD Impact levels 4 and 5.

- *Virtual Data Center Security Stack*. The VDSS provides DoD Core Data Center (CDC)-like network security capabilities such as firewall, intrusion detection, and intrusion prevention systems. It also provides application security capabilities such as web application firewall (WAF) and proxy systems. VDSS capabilities can be provided as-a-Service by a third party vendor (for IaaS) or a CSP (for IaaS and SaaS).

- *Virtual Data Center Managed Services.* This pillar includes features such as management, security, and privileged user access. Five services fall within VDMS, including the Host-Based Security System and Assured Compliance Assessment Solution. They enable mission partners to configure and deliver security policies, push upgrades, and manage roles and security policies. VDMS functionality applies directly to IaaS environments but may not be specifically applicable to PaaS and SaaS CSOs as such functionality may be inherent to the associated CSP and validated through the DoD PA.

- *Trusted Cloud Credential Manager.* The TCCM is an individual or entity appointed by the DoD mission owner's Authorizing Official (AO) to establish plans and policies for the

[8] Adapted from "Department of Defense Security Cloud Computing Architecture Functional Requirements, V2.9. 31 January 2017

control of privileged user access to establish, configure, and control a mission owner's Virtual Private Cloud (VPC) configuration once connected to the DISN.

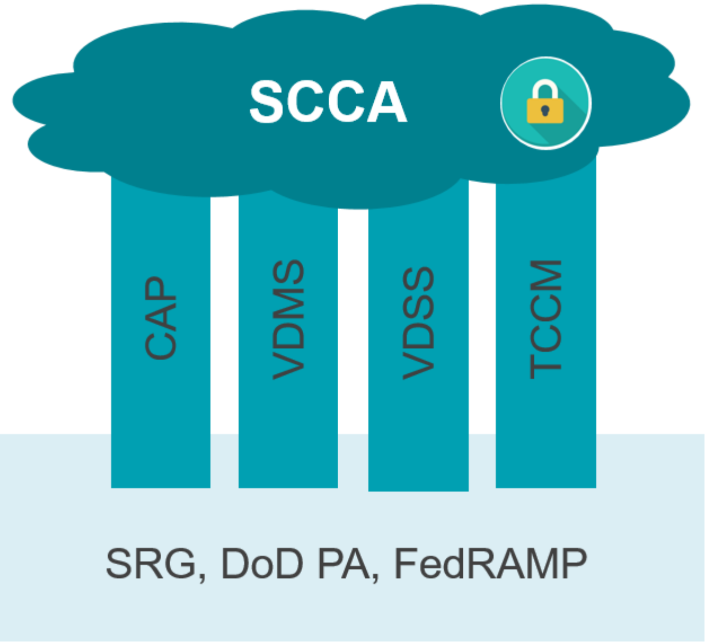


Figure 5: Secure Cloud Computing Architecture (SCCA) Components

THE CLOUD ACQUISITION PROCESS

FRAMEWORK

Figure 6 displays the process for acquisition and sustainment of cloud computing. The process includes all considerations throughout the lifecycle of a cloud acquisition, from defining mission requirements, choosing a solution using a BCA, and then implementing the cloud solution.

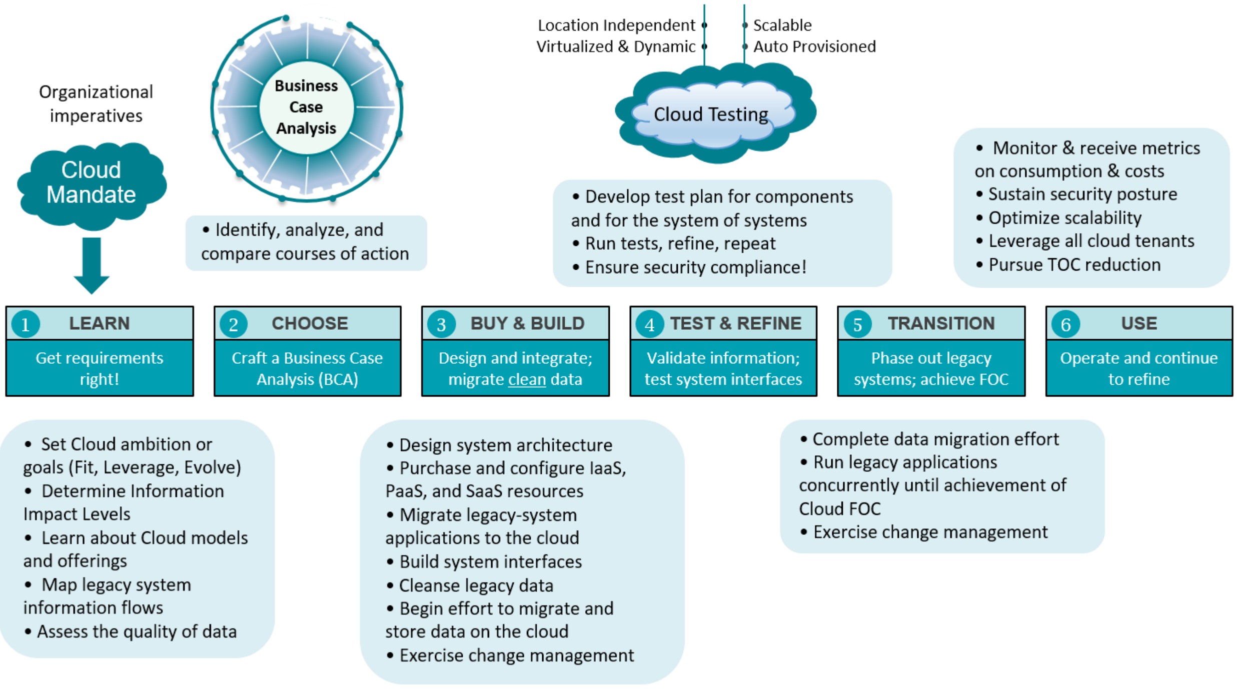

Organizational imperatives
Cloud Mandate
Business Case Analysis
• Identify, analyze, and compare courses of action
Location Independent
Virtualized & Dynamic
Scalable
Auto Provisioned
Cloud Testing
• Develop test plan for components and for the system of systems
• Run tests, refine, repeat
• Ensure security compliance!
• Monitor & receive metrics on consumption & costs
• Sustain security posture
• Optimize scalability
• Leverage all cloud tenants
• Pursue TOC reduction
1 LEARN
Get requirements right!
2 CHOOSE
Craft a Business Case Analysis (BCA)
3 BUY & BUILD
Design and integrate; migrate clean data
4 TEST & REFINE
Validate information; test system interfaces
5 TRANSITION
Phase out legacy systems; achieve FOC
6 USE
Operate and continue to refine
• Set Cloud ambition or goals (Fit, Leverage, Evolve)
• Determine Information Impact Levels
• Learn about Cloud models and offerings
• Map legacy system information flows
• Assess the quality of data
• Design system architecture
• Purchase and configure IaaS, PaaS, and SaaS resources
• Migrate legacy-system applications to the cloud
• Build system interfaces
• Cleanse legacy data
• Begin effort to migrate and store data on the cloud
• Exercise change management
• Complete data migration effort
• Run legacy applications concurrently until achievement of Cloud FOC
• Exercise change management

Figure 6: The Cloud Acquisition Process

CLOUD PROCESS MAJOR STEPS

The major steps of the cloud acquisition process are explained below. Combined, these steps make up a Process Breakdown Structure, a detailed roadmap to be utilized along with the Cloud Acquisition Work Breakdown Structure (following section). These steps were informed following an extensive literature review as well as thorough conversations with a handful of the major CSPs. The steps below sync with the main steps in the WBS, though CSPs frequently combine the steps.

1. Learn

The first stage of the process is essential to the following steps. Perhaps most importantly, mission owners should identify problems and opportunities. This includes assessing the existing on-premise environment, determining the scope of the migration, and preparing a plan for project implementation. Setting upfront requirements includes becoming familiar with the mandate for the mission owner's specific department. Additionally, this step includes the assessment of system interfaces and instructs business owners to establish objectives for system enhancements.

2. Choose

   This step provides a framework for crafting a Business Case Analysis (BCA) and analyzing business processes. The BCA will assess the cost, capabilities, and risks for each of the alternatives. In order to do so, this step includes the identification, definition, and prioritization of system requirements for the target cloud environment. Items such as inputs, outputs, processes, level of scalability and elasticity, and security may be specified in order to fulfill objectives laid out in step 1. This step may also bring in use cases to inform these requirements. To assist in decided which type of cloud is best for system requirements, this step establishes a catalogue of strategies for cloud build out.

3. Buy & Build

   Utilizing input from the previous two steps, this step builds out the structure of the target cloud environment. In this step, virtual machines, configuration of cloud stack applications, and data migration take place. Frequently a third party such as a system integrator or a Managed Services Provider (MSP) will be utilized.

4. Test & Refine

   The next task for the mission owner is to test the target cloud environment using smaller portions of the on-premise at first. These pilot runs along with use cases will inform the refinement part of this step and will advise any software changes that need to be made as the programs, applications, and data are migrated to the target environment.

5. Transition

   While programs, applications, and data are slowly being tested and migrated, step 4 continues while the target environment is being used. Cloud performance and cost is optimized while the mission owner choose appropriate usage while scaling up and down according to need and storage requirements. The on-premise environment often runs concurrently with the target environment while business practices laid out in earlier steps are being implemented.

6. Use

   This step addresses Operations & Sustainment efforts to maintain business practices and effectively run all programs and applications in the target cloud environment. Hardware and software needs may change as the environment matures and is being fully utilized. Storage needs may change, which potentially significantly impacts cloud maintenance costs going forward, as well as security requirements depending on the data being hosted.

CLOUD WORK BREAKDOWN STRUCTURE

OVERVIEW

A work breakdown structure (WBS) is a hierarchical framework appropriate for organizing a program into logical building blocks that have associated costs. A WBS assists cost analysts in understanding a program/system and also ensures that all relevant costs are included in an estimate. Further, the implementation of a standardized WBS template, as accomplished through the implementation DoD's MIL-STD-881D[9] and the OSD's Operating and Support Guide [10] , facilitates apples-to-apples comparisons between analogous programs and systems.

However, neither the MIL-STD-881-D (Appendix J, "Information Systems/Defense Business Systems") nor OSD's Operating and Support Guide include WBS elements that address migrating and sustaining a cloud environment. This paper addresses this void by offering a WBS for cloud acquisition and sustainment that can be implemented across DoD. It is based on extensive research and, to ensure comprehensiveness, was also mapped to MIL-STD-881-D (Appendix J, "Information Systems/Defense Business Systems") and OSD's Operating and Support Guide. As with any WBS, there should be an appropriate amount of tailoring to capture all of the distinct characteristics or unique attributes of the application, system or program that is considering migrating to the cloud. Finally, limitations and difficulties in data collection will inevitably influence the level of WBS detail possible for a given cloud cost estimate.

The WBS templates are divided into Investment (k.1.0) and Sustainment (k.2.0) to capture the complete costs associated with considering a migration to the cloud. It is important to note and emphasize that commercial online cloud calculators do not contain what some could argue is the most imperative work for a successful cloud migration – the upfront analysis required to: a) assess the readiness of legacy systems for cloud migration; b) analyze alternative solutions; and c) prepare those systems for migration. The WBS developed through this research addresses these critical costs and more. It is a seminal comprehensive evaluation of all costs required to successfully evaluate, develop and deploy a cloud solution.

[9] MIL-STD-881D, "DEPARTMENT OF DEFENSE STANDARD: WORK BREAKDOWN STRUCTURES (WBS) FOR DEFENSE MATERIEL ITEMS," 9 April 2018.

[10] "OPERATING AND SUPPORT COST-ESTIMATING GUIDE," 2014.

Top-level WBS definitions for Investment (k.1.0) and Sustainment (k.2.0) in a cloud-acquisition environment follow:

WBS k.1.0: Analysis and Cloud Migration Investment

- Captures all of the costs associated with the hardware, software, and personnel necessary to analyze existing applications or develop, design, build, test, and deploy an application or system in the cloud. Includes all efforts required to:
    - k1.1: Assess the readiness of legacy systems for cloud migration, including existing problems or opportunities
    - k1.2: Capture utilization rates and storage, network, compute, and cybersecurity requirements
    - k1.3: Translate operational needs into system performance and configuration specifications
    - k1.4: Analyze cloud service and deployment models and offerings from vendors based on requirements
    - k1.5: Conduct business case analyses to present alternative cloud solutions, which include tradeoffs between cost, capability, and risk
    - k1.6: Design, configure, test, and deploy the cloud solution

WBS k.2.0 Cloud Solution Sustainment

- Captures all of the costs associated with the operation and maintenance of the application or system in the cloud. Includes all efforts required to:
    - k2.1: Provision hardware and software (IaaS, PaaS, and SaaS)
    - k2.2: Store and retrieve data from the selected cloud solution
    - k2.3: Protect the security of data and information flow within the cloud and at boundary points
    - k2.4: Maintain configuration control and change management
    - k2.5: Maintain software, while considering bundled agreements, a cloud solution with many applications, and the use of SLAs
    - k2.6: Maintain cybersecurity requirements
    - k2.7: Provide for managed services, either through a third party or cloud broker, including help-desk support

During investment (WBS k.1.0), cloud hosting, development, and test assets are likely required in the IaaS, PaaS, and SaaS stack to accomplish such tasks as establishing and configuring virtual machines, porting legacy-system software to the cloud, and testing and optimizing the prototype solution. Cloud subscription fees are required and incurred for each of these activities.

Some of these same identical license fees become recurring costs in the sustainment phase, such as the use of virtual machines. Other license fees associated with PaaS and SaaS applications come into full play in the post-IOC environment.

APPLICABILITY

The WBS, both Investment k.1.0 and Sustainment k.2.0, is all-inclusive for legacy-system cloud migrations in DoD and is intended to capture the totality of investment costs that might arise. Importantly, the WBS *informs* but does *not fully cover* all of the cost elements required for a major, new-start software development effort as the WBS was more developed to assist in getting legacy, on-premises systems migrated to the cloud successfully.

The WBS is tailorable, by design and intention. The actual WBS employed in generating a POE, ICE, ICA, or CCP will almost certainly differ from the construct here depending upon the size and scope of the acquisition program, its stage in the software development lifecycle (defined by DoDI 5000.75), and the quality and quantity of cost and programmatic data available to the cost estimator.[11]

APPLICATION MIGRATION METHODS

As discussed in the previous section, much of the important work in evaluating a legacy application or system is not captured in the readily available commercial online cost calculators. A cost analyst, and therefore the program s/he supports, cannot fully grasp the totality of options and costs of migrating to the cloud without considering all cloud migration methods. It is this process, commonly referred to at the 6 Rs shown in Figure 7, that is imperative to successfully preventing kneejerk decisions to migrate to the cloud and, in turn, supporting a successful migration.

[11] POE = Program Office Estimate; ICE = Independent Cost Estimate; ICA = Independent Cost Assessment; and CCP = Component Cost Position

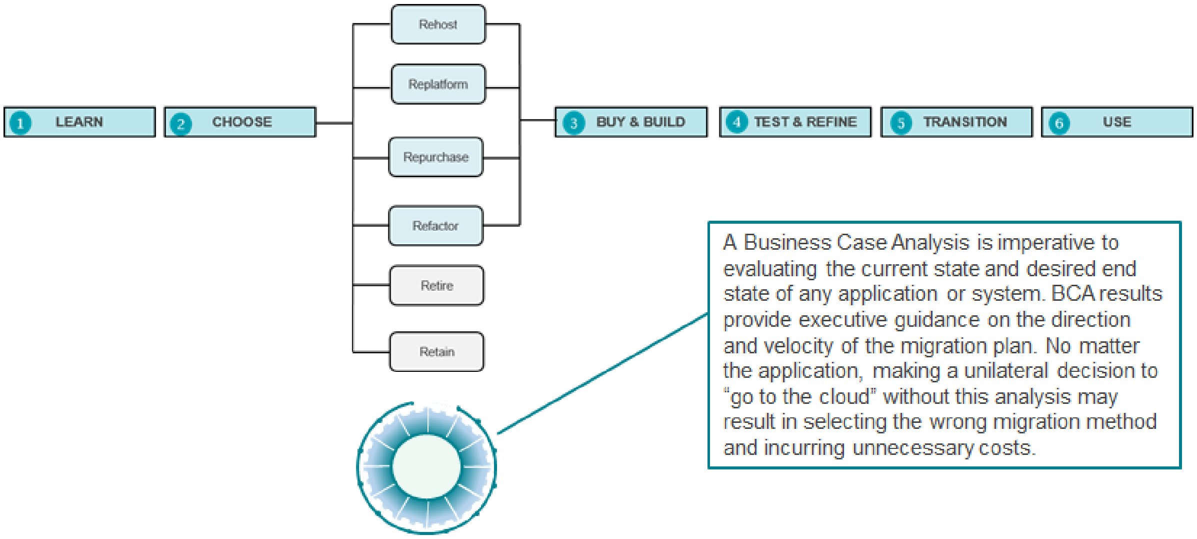

1 LEARN
2 CHOOSE
Rehost
Replatform
Repurchase
Refactor
Retire
Retain
3 BUY & BUILD
4 TEST & REFINE
5 TRANSITION
6 USE
A Business Case Analysis is imperative to evaluating the current state and desired end state of any application or system. BCA results provide executive guidance on the direction and velocity of the migration plan. No matter the application, making a unilateral decision to "go to the cloud" without this analysis may result in selecting the wrong migration method and incurring unnecessary costs.

Figure 7: Application Migration Methods within the PBS

As Dr. Kelly Fletcher, Deputy Director, Department of Homeland Security (DHS) Program Analysis and Evaluation (PA&E), stated, "Migrating to the cloud should be "a forcing function to say, 'What applications do I really need?' 'Do we need to move it? Do we need to keep it around at all? Do we need to build a new one?'" The 6 R's described below detail how a program office can systematically conduct such an evaluation.

An organization has six options, commonly referred to as the 6Rs, to evaluate when considering a cloud migration. It is imperative that these be included in any cloud migration BCA to fully evaluate all available courses of actions (COAs). These options are:

- Retain: The option to retain the existing application(s) or system(s) as-is
- Retire: The option to remove the application(s) or system(s)
- Refactor: The option to move the application(s) or system(s) to the cloud with an invasive rearchitecting and recoding
- Repurchase: The option to purchase a different product, common with SaaS
- Replatform: The option to move the application(s) or system(s) to the cloud with a small amount of up-versioning to benefit from cloud infrastructure
- Rehost: The option, also known commonly as "life-and-shift," to move the application without making any changes to its architecture

Two of the 6Rs include decisions to not migrate an application or system to the cloud. Some example reasons to *Retain* an application would be if there had been a significant sunk cost for on-premises architecture, thus necessitating the organization to continue with existing assets and practices. This example illustrates the importance of knowing the life-cycle cost of applications and their supporting datacenter infrastructure. Another example of when to retain an application is whether the legacy operating systems or applications are not supported in the cloud or if the business justification is found to be insufficient, both of which would be unearthed during the BCA process.

Example reasons to *Retire* an application are a bit more straight forward, and highlight the importance of the first step of the PBS, "Learn" and further underscore Dr. Kelly Fletcher's sentiment. During the Learning Phase applications may be found to be no longer required, could be duplicates of other applications, or there may already be work underway to consolidate or decommission older applications.

The remaining four 6Rs, *Repurchase*, *Refactor*, *Replatform*, or *Rehost*, can then be selected according to a wide variety of factors within a program or throughout DoD writ large. These options would be uncovered and analyzed during the BCA process and emphasize the best practice of working with subject matter experts to fully understand application architecture and requirements.

Figure 8 below shows a sample decision tree with example considerations for how organizations can utilize the 6Rs in fully informing the cost benefit analysis process for a potential cloud migration.

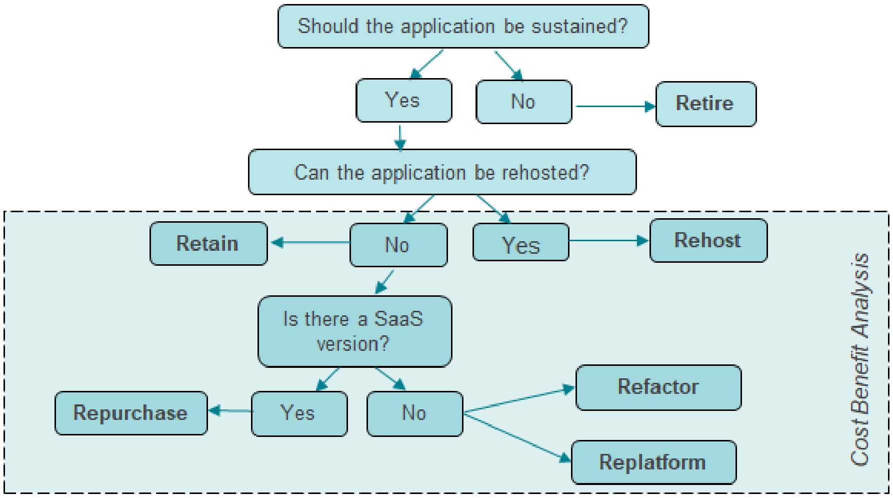


Figure 8: The 6Rs - Application Migration Methods

Sample considerations for which method to select can include:[12]

- Is there a compelling event or pain point for the organization?
  - If there is a push to evacuate the current hosting environment, a fast Rehosting method may sometimes be the only option.

[12] Adapted from Chambers, S. "A Practical Guide to Understanding the 6Rs for Migration to AWS," Cloudsoft, 27 March 2018.

- Is the application available in the current marketplace?
  - Repurchasing an application that is available may prove to be fastest way to both cut costs and operate on the cloud. This option would come with the associated costs of disposing of the previous application.
- Does the program or enterprise have the skills required to both manage and prepare the application for a cloud migration?
  - If the application requires work to either Refactor or Replatform, but those skills do not exist within an organization or funding is not available to outsource the work, the only option may be to Repurchase or Rehost.
- What is the desired future-state of the application or system?
  - If an application is intended to evolve over the next several years and skills either exist or can be outsourced, Refactoring may be the best approach.

The graph below illustrates the speed and cost at which applications can typically migrate relative to which type of migration method.

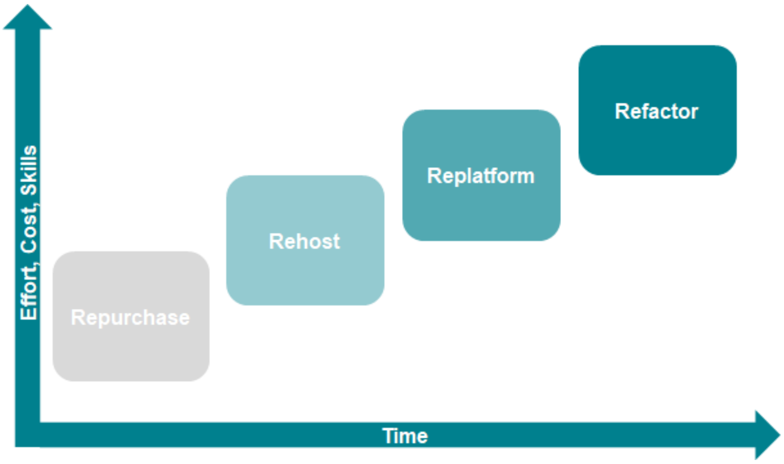


Figure 9: Cost, Effort, Skills, and Time Application Migration Tradeoffs

Although Refactoring is both initially the slowest method and carries with it the greatest cost and requirement for skills, it potentially delivers the greatest agility and ability to exploit cloud offerings and innovation. Ultimately, effort, cost, skills, and time are all potential drivers of which migration method is appropriate.

In summary, although there are six migration methods from which to choose, a program must conduct a business case analysis to fully analyze the current state of the application(s) or system(s) in question as well as their desired end state. And, it is imperative to emphasize that these costs are not included in the readily available commercial cost calculators. Blindly deciding to adhere to the mandate to "go to the cloud" without this detailed investigation and analysis may result in selecting the wrong migration method and incurring unnecessary costs.

CLOUD BUSINESS CASE ANALYSIS

The cloud remains full of confusing choices. Public, private, or hybrid? Which components of IaaS, PaaS, and SaaS to buy? At what price? And what about security?

To address these questions, the authors have created the comprehensive framework of Figure 10 for capturing the life-cycle costs, benefits, and risks of migrating to the cloud. The framework supports the development of a robust Business Case Analysis (BCA) that recognizes that there are alternative ways to meet organizational objectives for cloud services. It emphasizes the exercise of due diligence in the all-important upfront work of defining requirements and examining solution space to include alternative cloud architectures. Get this part wrong and the cloud acquisition will fail. The framework also emphasizes cloud design and build, data cleanings and migration, and the capture of life cycle costs and risks for all of the alternatives.

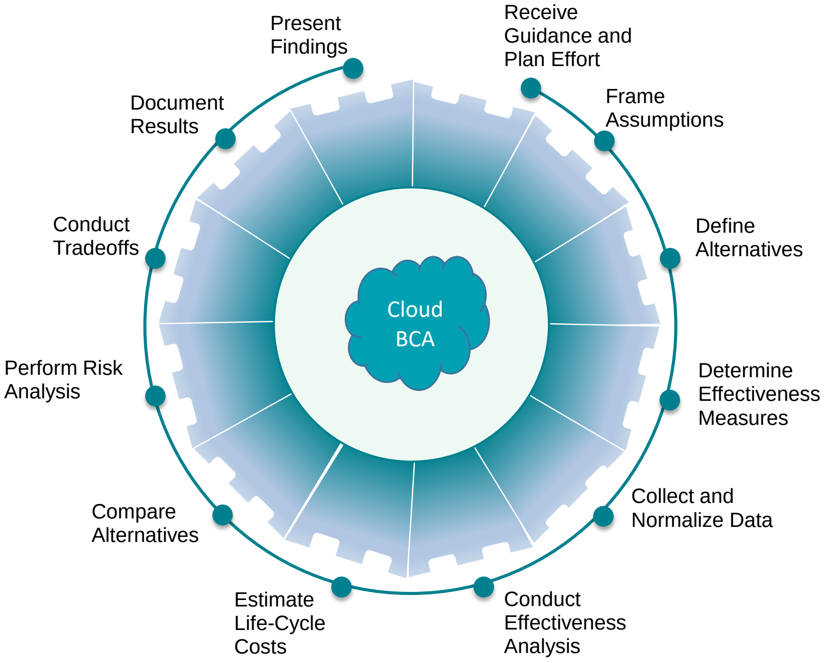
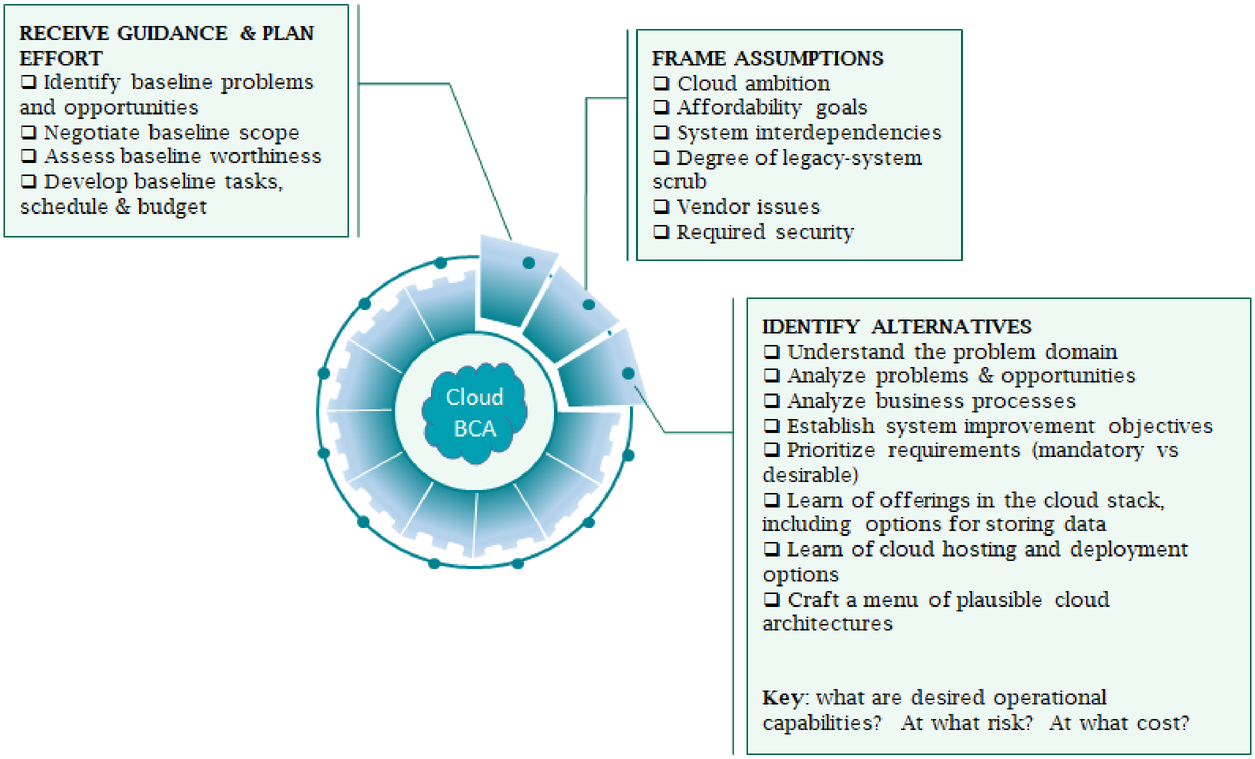

Present Findings
Receive Guidance and Plan Effort
Frame Assumptions
Define Alternatives
Determine Effectiveness Measures
Collect and Normalize Data
Conduct Effectiveness Analysis
Estimate Life-Cycle Costs
Compare Alternatives
Perform Risk Analysis
Conduct Tradeoffs
Document Results
Cloud BCA

Figure 10: Cloud Acquisition BCA Framework



RECEIVE GUIDANCE & PLAN EFFORT
❑ Identify baseline problems and opportunities
❑ Negotiate baseline scope
❑ Assess baseline worthiness
❑ Develop baseline tasks, schedule & budget

FRAME ASSUMPTIONS
❑ Cloud ambition
❑ Affordability goals
❑ System interdependencies
❑ Degree of legacy-system scrub
❑ Vendor issues
❑ Required security

IDENTIFY ALTERNATIVES
❑ Understand the problem domain
❑ Analyze problems & opportunities
❑ Analyze business processes
❑ Establish system improvement objectives
❑ Prioritize requirements (mandatory vs desirable)
❑ Learn of offerings in the cloud stack, including options for storing data
❑ Learn of cloud hosting and deployment options
❑ Craft a menu of plausible cloud architectures

Key: what are desired operational capabilities? At what risk? At what cost?

Figure 11: Frame Assumptions and Identify Alternatives

CLOSING THOUGHTS

As discussed throughout this paper, migrating to the cloud is not without its challenges. Although organizations are moving to cloud environments to increase flexibility and recognize cost efficiencies, balancing the use of different cloud environments to optimize rewards and estimating the cost of those initiatives present certain challenges.

First and foremost, due to the various mandates to migrate to the cloud, there is often a push to select a CSP prior to completing the appropriate analysis of alternatives. The commercial offerings are seen as comparable or synonymous, often leading programs to misjudge the trade space reality and select CSPs too early. This rush to migrate to the cloud coincides with a lack of due diligence in analyzing existing system requirements to understand information flow and interfaces and the associated cloud acquisition process. Without this understanding, selecting the appropriate solution and migration method is difficult and can incur unnecessary costs and rework.

Second, cloud cost estimating capability is in its infancy and represents an obstacle to informed decision making. The abundance of commercial cloud cost calculators, which do not address the cost of important upfront work, have muddled the landscape and misrepresented the entirety of effort required to migrate to the cloud. Up until the pivotal research described in this paper, there was no WBS and associated data dictionary and, to this day, there is no cloud data that has been collected in a consistent and comparable manner. As a result, there are neither widely accepted metrics for measuring cloud adoption rates nor established benchmarks for organizations that are transitioning to the cloud. Thus, implementing a standardized WBS (i.e., something similar to what's presented in this paper) and data collection methods is vital to the cost community's ability to estimate cloud migration and sustainment.

This paper serves as a thorough introduction and resource for cost estimators throughout DoD to assist in understanding cloud requirements, cloud service provider offerings, and cloud cost. However, there is much more work the cost analysis community needs to accomplish to understand the cost of cloud and ensure that DoD cloud decision makers do the same. We hope that the important advance in cloud cost analysis capability reflected in this paper is the impetus for other members of our community of practice performing complementary research.

REFERENCES

WEBSITES

Defense Information Systems Agency

- Department of Defense *Cloud Computing Security Requirements Guide*, Version 1 Release 3; 6 March 2017
    - https://iasecontent.disa.mil/cloud/SRG/index.html

- DISA cloud computing services
    - https://www.disa.mil/en/Computing/Cloud-Services

- DISA Cloud Symposium, 12 Dec 2017
    - https://www.disa.mil/NewsandEvents/Events/Cloud-Symposium
    - Site hosts these presentations
        - DISA Cloud Playbook
        - Cloud Computing: Crawl, Walk, Run, Fly
        - milCloud 2.0
        - On-Site Managed Services
        - Secure Cloud Computing Architecture

- DISA Cloud Symposium, 15-16 May 2018
    - https://www.disa.mil/en/NewsandEvents/Events/DISA-Cloud-Symposium-2018
    - Site hosts these presentations
        - DISA Cloud Playbook
        - Cloud 101
        - Migrating Applications to the Cloud
        - Secure Cloud Computing Architecture (SCCA)
        - milCloud 2.0 Overview
        - DOD Cloud Computing - Evolving Capabilities for the Next Generation of Computing
        - Acquiring Cloud Services - A Contracting Officer's Perspective
        - Cloud Computing Security Requirements Guide

- Department of Defense (DoD) Cloud Connection Process Guide
    - https://disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/CCPG.pdf

National Institute of Standards and Technology

- Definition of cloud computing
    - http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

- Cloud computing synopsis and recommendations
  - https://csrc.nist.gov/publications/detail/sp/800-146/final

- Cloud computing reference architecture
  - https://www.nist.gov/publications/nist-cloud-computing-reference-architecture?pub_id=909505

- Cloud computing roadmap
  - https://www.nist.gov/publications/us-government-cloud-computing-technology-roadmap-volume-i-high-priority-requirements?pub_id=915112

- List of NIST cloud computing documents
  - https://www.nist.gov/itl/nist-cloud-computing-related-publications

Cloud Cost Calculators

A sample of calculators:

- Amazon
  - https://calculator.s3.amazonaws.com/index.html
- Google
  - https://cloud.google.com/products/calculator/
- IBM
  - https://console.bluemix.net/pricing
- Microsoft
  - https://azure.microsoft.com/en-us/pricing/calculator
- Oracle
  - https://cloud.oracle.com/cost-estimator

A sample of pricing information:

- Salesforce
  - https://www.salesforce.com/products/sales-cloud/pricing
- SAP
  - https://cloudplatform.sap.com/pricing.html

Policy Memos

“Accelerating Enterprise Cloud Adoption Update,” Patrick Shanahan, Deputy Secretary of Defense, 4 January 2018

“Joint Characteristics and Considerations for Accelerating to Cloud Architectures and Services,” Joint Requirements Oversight Council, 22 December 2017

"Navy Commercial Cloud Brokerage Policy," DON Deputy Chief Information Officer (Navy), VADM Jan Tighe, 19 December 2017

"Accelerating Enterprise Cloud Adoption," Deputy Secretary of Defense, 13 September 2017

"Navy Cloud First Policy," Janice Haith, Director, DON Deputy CIO, 1 February 2017

"Commercial Cloud Business Case Analysis Policy," Janice Haith, Director, DON Deputy CIO, 27 January 2017

"Additional Guidance Regarding Acquisition and Use of Commercial Cloud Computing Services in the Department of the Navy," Robert Foster, DON CIO, 17 May 2016

POLICY GUIDELINES

Navy Cloud Brokerage Playbook Volume I: Governance Model Roles and Responsibilities, PEO EIS

Navy Cloud Brokerage Playbook Volumes II through VII: TBD

MIL-STD-881D, "Department of Defense Standard: Work Breakdown Structures (WBS) for Defense Materiel Items," 9 April 2018

"Cloud 101 PEO EIS Commercial Services," Travis Methvin, PEO EIS, 13 December 2017

SPAWAR Systems Center Atlantic, "FY18 Service Catalog for Data Center and Commercial Hosting Services," version 1.0, 30 August 2017

DoD Instruction 5000.75, "Business Systems Requirements and Acquisition," OUSD (AT&L), 2 February 2017

OSD CAPE "Operating and Support Cost-Estimating Guide," 2014