



The 11th Commandment: Thou Shalt Migrate to Cloud

ICEAA Conference May 2019

Speaking Today



Emily Hagerty

Emily Hagerty provides cost estimating support for Technomics' DoD clients. Emily is a Navy veteran with 14 years of service within DoD. Emily is a Certified Cost Estimator/Analyst (CCEA) and a Project Management Professional (PMP). She holds a B.S. in Communications from Boston University and a M.B.A. in Enterprise Resource Planning from University of Scranton.



Orly Olbum

Orly Olbum is an analyst at Technomics, Inc. with experience in data acquisition, database management, statistical analysis, and cloud computing. She supports the Air Force Cost Analysis Agency (AFCAA) through data procurement and training efforts on the Contracts Database project. She graduated from Penn State with a B.S. in Applied Statistics.



Brian Flynn

Brian Flynn supports national security efforts at Technomics' Arlington, VA, headquarters. Brian is a plank owner of the Naval Center for Cost Analysis where he spearheaded an ASN(FM&C) effort in capability portfolio analysis and represented the DOD in NATO initiatives in cost analysis. Brian is a recipient of DON's Distinguished Civilian Service Award and ICEAA's Lifetime Achievement Award. He holds Ph.D., M.A. and B.A. degrees in Economics from Georgetown University and Virginia Tech.

Agenda

- Cloud Cost Estimating Environment and Challenges
- Cloud Basics
- Research Products and Lessons Learned
- Future Work for the Cost Community

Cloud Mandate

- **DEPSECDEF¹**
 - Prioritizes 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”
- **Joint Staff²**
 - “... 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”
- **Air Force³**
 - “Develop strategy, policy, and guidance for AF use of **private and public cloud computing** services in support of the Air Force Information Networks”
- **Navy⁴**
 - **Cloud first** strategy requires components to “... design, transfer, host, operate, and sustain IT capabilities with Commercial Cloud Service Provider (CCSP) hosting environment to the **maximum extent** possible”
 - Deputy DON CIO (Navy) modified the requirement to reflect a “**Navy Cloud**” First strategy
- **Marine Corps⁵**
 - “**Cloud services** are needed to move applications and associated data to the point of need. Old “reach-back” models are too slow and are most susceptible to service outages during times of network segregation, especially at the tactical edge. **Cloud services** also are a crucial component to our mobility strategy both in warfighting and business (e.g., recruiting) operations.”

¹“Accelerating Enterprise Cloud Adoption Update,” Deputy Secretary of Defense, 8 January 2018

²“Joint Characteristics and Considerations for Accelerating to Cloud Architectures and Services,” Joint Requirements Oversight Council, 22 December 2017

³Air Force Chief, Information Dominance and Chief Information Officer; SAF/CIO A6; 2014

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

⁵“Marine Corps Strategy for Assured Command and Control,” March 2017

Cloud Capability Gaps

1 CLOUD TRADESPACE MYOPIA

- ❑ Preferred system and cloud vendor identified too early (Navy experience)
- ❑ Limited view of tradespace reality: a large number of architectures and offerings

2 COMPLEXITY OF EFFORT

- ❑ Assessing the state of legacy systems
- ❑ Understanding information flow and interfaces
- ❑ Understanding the cloud acquisition process

3 CLOUD COST ESTIMATING EARLY ON

- ❑ Lack of a cloud WBS (until now)
- ❑ Lack of a cloud data dictionary (until now)

4 CLOUD LINKAGES

- ❑ Crosswalk between Cloud WBS and MILSTD-881D
- ❑ Linkage to DoDI 5000.75

5 LACK OF CLOUD DATA

- ❑ Data drives the analysis
- ❑ But data is often hard to collect, unstructured
- ❑ Very little cloud history in DoD

6 CLOUD COST RISK ANALYSIS

- ❑ New dimension for the cost community
- ❑ E.g., initial storage requirements

7 CLOUD COST/CAPABILITY TRADESPACE

- ❑ Challenge in find the knee in the curve
- ❑ E.g., cloud security versus cost
- ❑ E.g., “cold” versus “hot” cloud data storage

Challenges

- Scarcity of data on cloud migration efforts
- Inconsistent definitions across government and industry
- Lack of a Cloud Process Breakdown Structure and Cloud Work Breakdown Structure
- Rationalization of cloud migrations
 - Analysis of legacy systems
 - Cost, capabilities, interfaces
 - 6 R's of Application Migration (Retain, Retire, Rehost, Replatform, Refactor, Rearchitect)
- Absence of cloud migration cost metrics and CERs

Implement guidance from DHS and DoD on cost estimating to support cloud migrations.

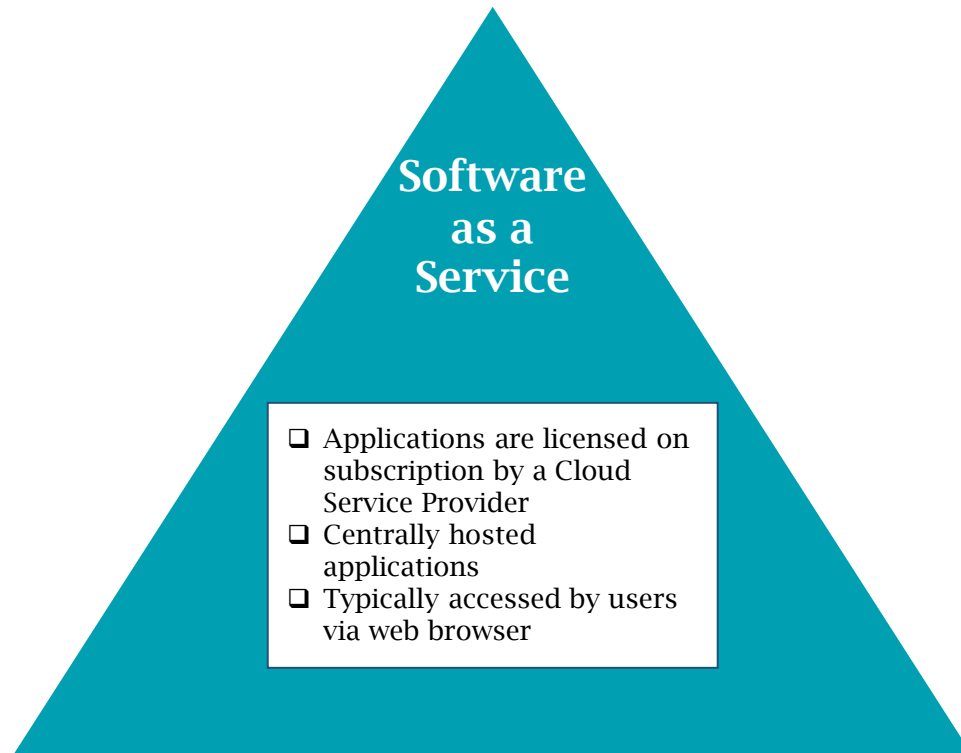
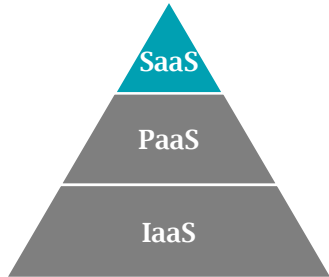
Cloud Basics

- 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
- Key tenets
 - On-Demand Self Service
 - Broad Network Access
 - Resource Pooling
 - Rapid Elasticity
 - Measured Service

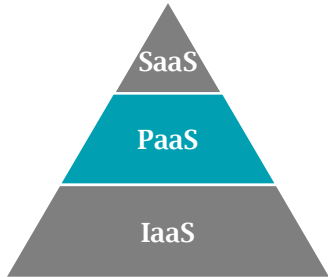
Cloud Basics – Deployment Models

Cloud Deployment Options				
Model	Description	Suitability	Advantages	Challenges
Public	<ul style="list-style-type: none"> Provisioned for open use by the public Hosted externally by a CSP Shared physical service space Multiple tenants 	<ul style="list-style-type: none"> Information Level 2 data Variable workloads Test and development, but with sensitive data safeguarded 	<ul style="list-style-type: none"> Faster development, testing, and deployment Rapid elasticity and flexibility Generally the lowest TCO 	<ul style="list-style-type: none"> Security Privacy
Private	<ul style="list-style-type: none"> Provisioned for a single organization or command Resources not shared with other tenants as in a public cloud 	<ul style="list-style-type: none"> Information Levels 4, 5, & 6 High security threat Compliance with law and directive 	<ul style="list-style-type: none"> Security and control Greater allowance for customization Better fit to requirements 	<ul style="list-style-type: none"> Need for a skilled IT staff Possibly the highest TCO
Community	<ul style="list-style-type: none"> Exclusive use of a specific, defined community Supports many tenants <i>within</i> the community Hosted on or off premise 	<ul style="list-style-type: none"> Collaborative environments Presence of rules and standards common across the environment 	<ul style="list-style-type: none"> Economies of scale when standards applied community wide Elasticity and flexibility Lower TCO than a private cloud 	<ul style="list-style-type: none"> Complex governance IT skill set
Hybrid	<ul style="list-style-type: none"> Two or more cloud infrastructures bound together Data and application portability 	<ul style="list-style-type: none"> Data of mixed sensitivity Presence of cloud bursting and need for elasticity and flexibility Compliance with law and policy while managing cost 	<ul style="list-style-type: none"> Security and control Customization of performance Elasticity Lower TCO than a private cloud 	<ul style="list-style-type: none"> Interoperability Migration and integration Portability IT skill set

Cloud Stack - Components



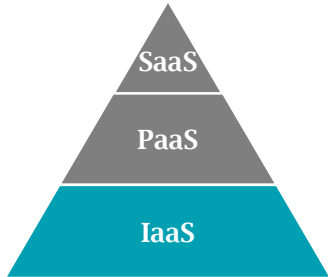
Cloud Stack - Components



Platform as a Service

- ❑ Complete development and deployment environment provided on subscription basis
- ❑ Resources include preinstalled and configured databases and middleware
- ❑ Solutions range from simple web apps to sophisticated enterprise resource planning products
- ❑ Runs on infrastructure shared by many organizations or by a single organization

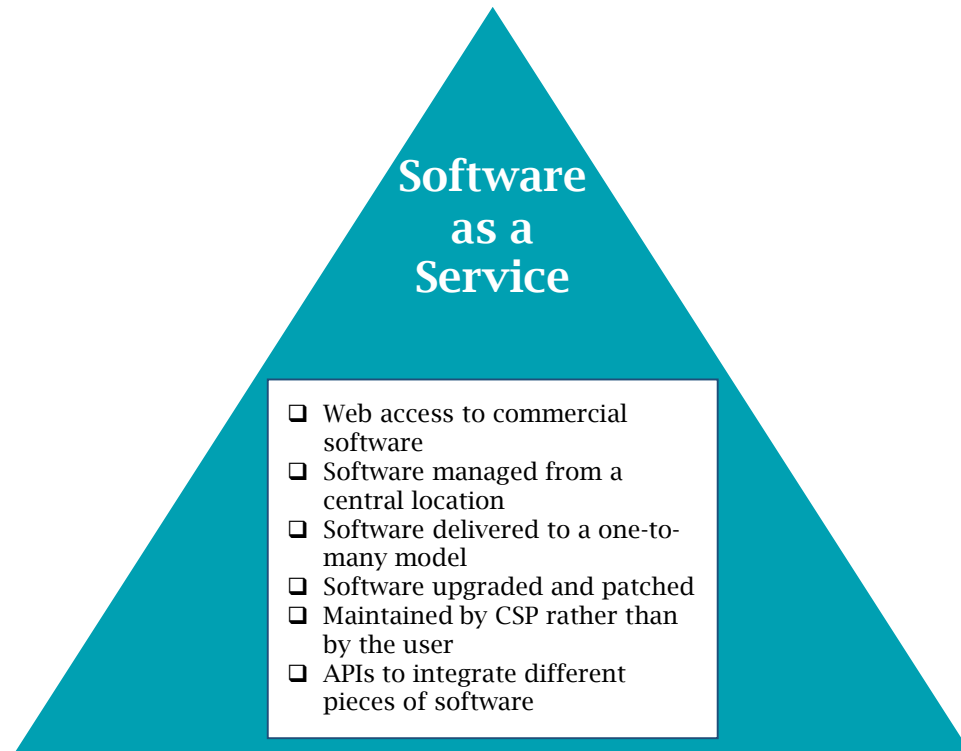
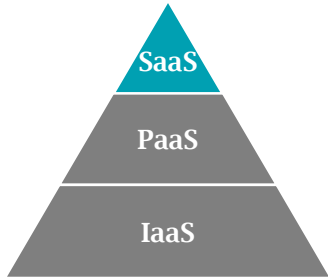
Cloud Stack - Components



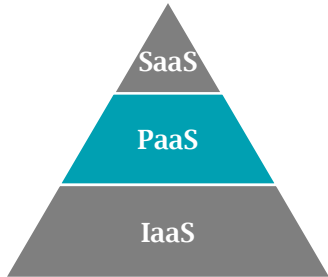
Infrastructure as a Service

- ❑ **Compute.** A rapidly provisioned, elastic computational capability that enables applications to run and scale automatically. The major vendors provide instance isolation for sensitive environments
- ❑ **Storage.** Secure and scalable capability for storing data in the cloud with many options available such as use of non-volatile memory, flash memory, with backup and archival storage available
- ❑ **Networking.** Connection by CSP that enables isolation of your cloud environment and linkage of physical network to private network

Cloud Stack - Characteristics



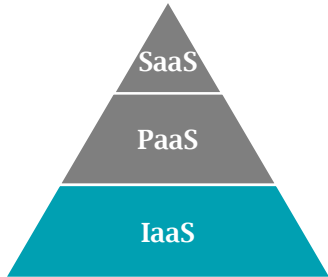
Cloud Stack - Characteristics



Platform as a Service

- Instant access to app development and deployment (DevOps)
- Rapid scale up and down as needed
- Web-based interface tools used to interact with software
- Ability to develop/deploy nearly every type of app
- Multitenant architecture to support team collaboration
- Built-in scalability

Cloud Stack - Characteristics



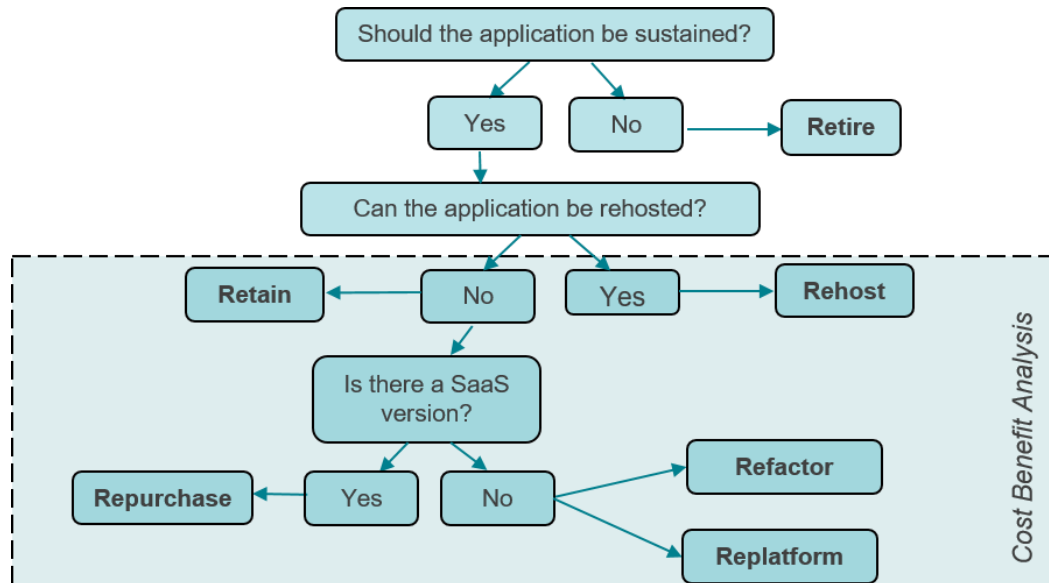
Infrastructure as a Service

- ❑ Create an unlimited number of virtual machines with storage and compute power
- ❑ Use of utility pricing model - costs are incurred based on resources consumed
- ❑ Flexibility to dynamically scale the environment to meet requirements
- ❑ Elastic computing where users initiate a request to change usage of infrastructure resources

Application Migration Methods

Method	Description
Rehost	Also known as "lift and shift," involves moving the application without making changes to its architecture
Replatform	Move application(s) to the cloud with a small amount of up-versioning to benefit from cloud infrastructure
Repurchase	Purchase a different product, common with SaaS
Refactor	Move application(s) to the cloud with a more invasive rearchitecting and recoding
Retire	Remove the application(s)
Retain	Retain the existing application/system as-is

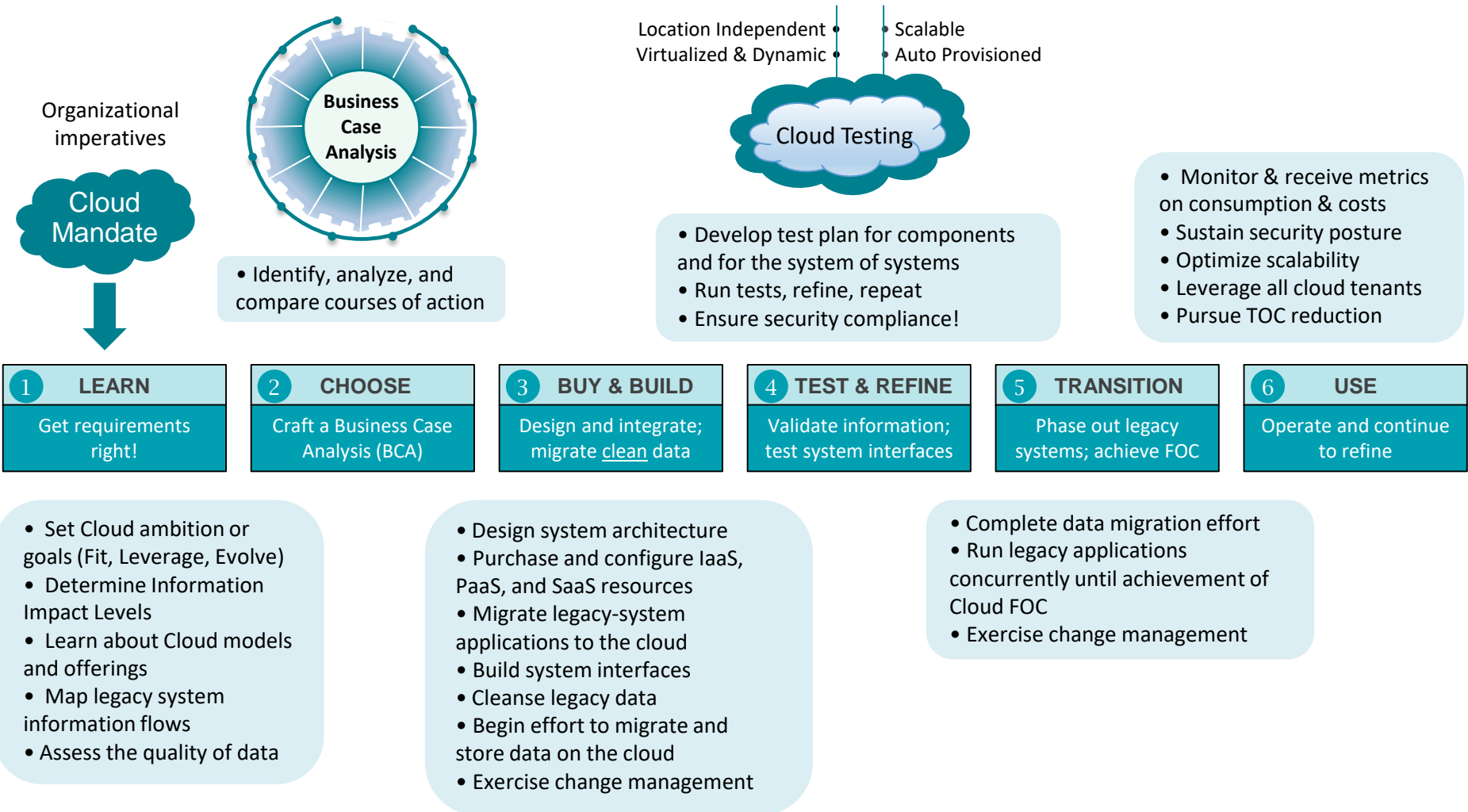
Migrating to the cloud should be a “a forcing function to say, ‘What applications do I really need?’ ‘Do we need to move it? Do we need to keep it around at all? Do we need to build a new one?’” – *Dr. Kelly Fletcher, Deputy Director DHS PA&E*



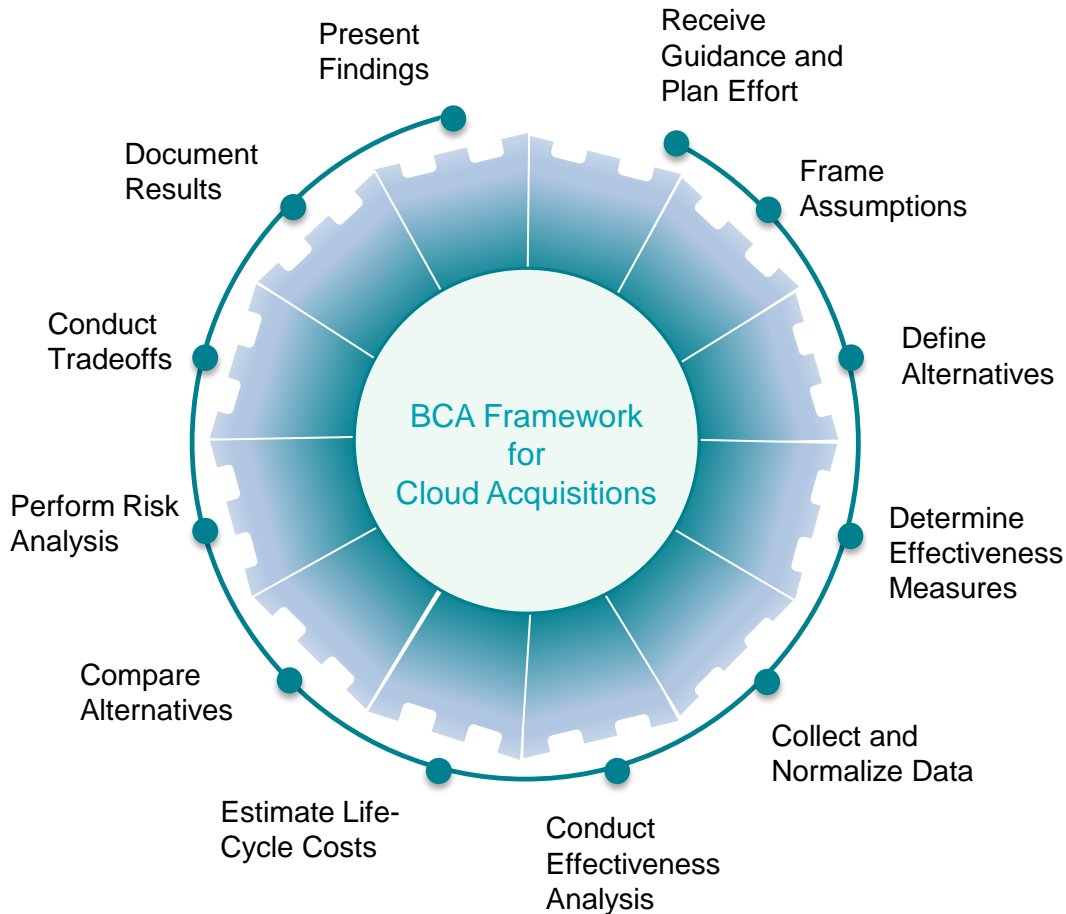
Technomics Cloud Achievements

- Conducted **ground breaking research** to compile the multitude of cloud guidance and offerings across DoD and industry
- Wrote **the first** Cloud Cost Estimating Guide that compiles Guidance and Best Practices across DoD and industry
- Developed **the first** Cloud Work Breakdown Structure
- Developed **the first** Cloud Process Breakdown Structure
- Developed **the first** Cloud Cost Estimating Methodology Matrix

Process Breakdown Structure



Cloud BCA Framework

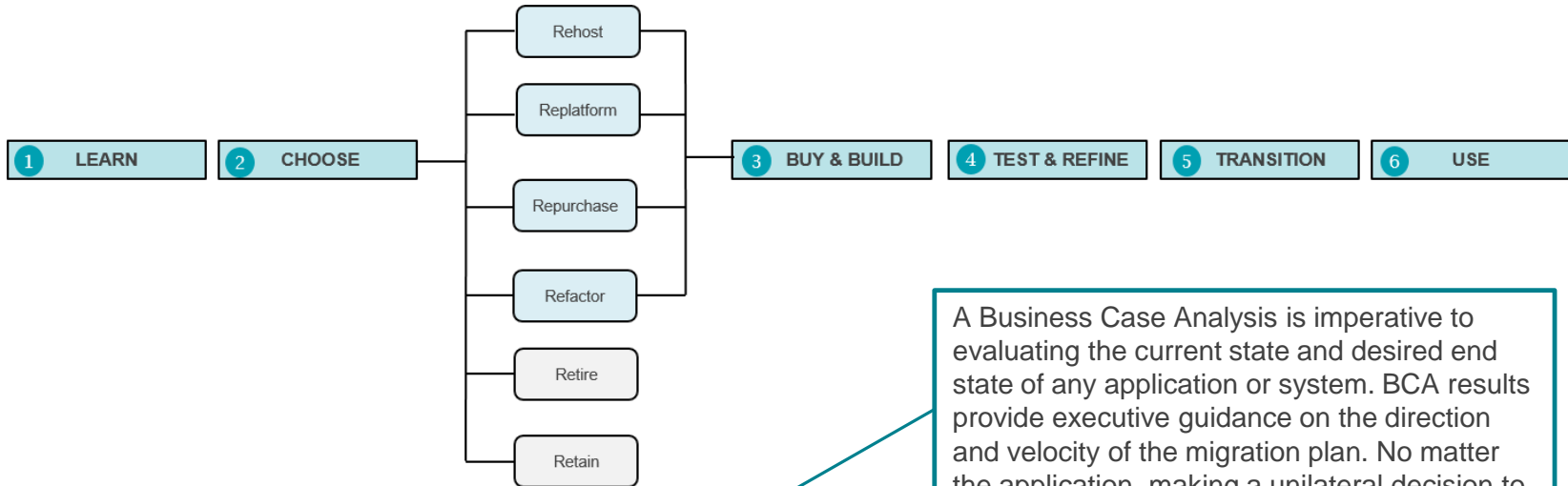


Sample of issues to address

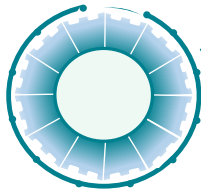
- What is solution space, including alternative system architectures?
- What services are needed in the cloud stack (IaaS, PaaS, SaaS)?
- What is the most cost/effective cloud deployment model (Public, Private, Community, Hybrid)?
- What the ideal compute hosting environment (On Premise, Off Premise, Combination)?
- Which of the legacy applications are cloud ready, which need modification, and which are not cloud compatible?
- What is the quality of legacy-system data? Does it need cleansing prior to movement to the cloud?
- What is the COOP/DR requirement and which applications require it?
- Which CSPs meet cloud requirements? Are they approved at required ILLs?
- What are the life-cycle costs for each alternative?
- Are migration costs included?
- Who will manage the cloud environment?
- What are business rules and billing units?
- What kind of system reliability is required, at what cost, and at what risk?

Copyright © 2019 Technomics, Inc.

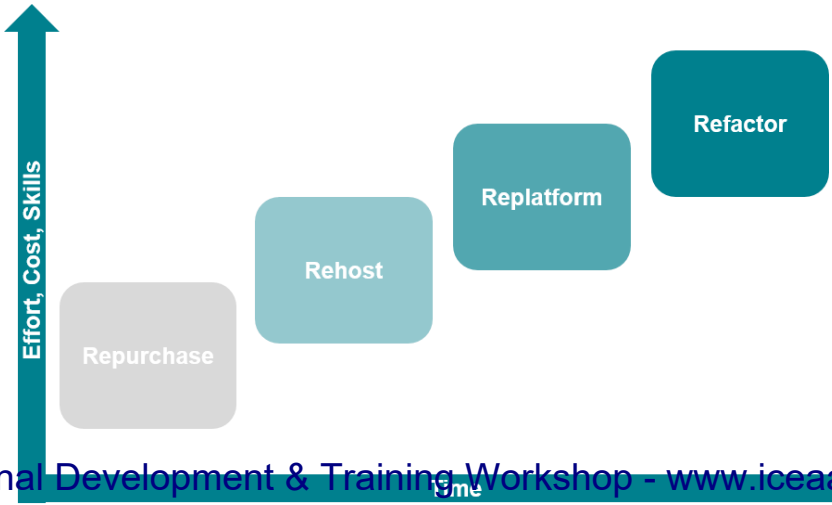
Migration Methods within the Process



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.



Ultimately, effort, cost, skills, and time are all potential drivers of which migration method is appropriate.



Cloud WBS

Impetus: There was no existing WBS template within MIL-STD-881D for a business system that will be migrated to or sustained in a cloud environment

- **Investment k1.0**

- **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

- **Sustainment k2.0**

- **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

The Cloud Work Breakdown Structure templates are tailorable, as each application or system has different requirements that must be analyzed and addressed

PBS, WBS and Data Collection Linkages

PBS & CES for Discovery & Analysis



Functional & System Engineering Teams

- ❑ Major Cost Elements in Discovery & Analysis Phases:
 - System Engineering, including Cloud Managed Service Provider
 - Program Management, including Governance IPTs
 - Functional (Business Process) IPTs
 - Change Management
 - IaaS for rapid/agile prototyping (in some circumstances)
 - Data evaluation and migration

Legacy Costs to Collect

- ❑ Direct Costs
 - Hardware and Software
 - Physical Servers
 - Software Licenses
 - Maintenance Contracts
 - Warranties
 - Supplies, material, spare parts
 - IT Operational Costs
 - Cost of labor for maintenance of servers, databases and other IT
 - Cost to maintain facilities that house IT hardware (real estate, staffing, HVAC)
 - Cost of connectivity to the Internet
 - Business Operational Costs
 - Cost of labor associated with using the legacy systems (i.e., disbursing checks)
- ❑ Indirect Costs
 - Overhead accounts
 - Accounting, finance, recruiting
 - Cost of IT downtime (loss of productivity)

The relationship between the cloud acquisition process, the major elements of cost, and the requirements for data collection to support life-cycle cost estimates

Future Work for the Cost Community

- Demonstrate proof of concept
 - Apply to a BCA
 - Apply to a POE, ICE, or ICA
 - Review with PM's and CSP's
- Define rationale for *inputs* to cloud calculators
 - Drivers
 - Environment
 - Requirements
- Gather cloud data
 - Programmatic and cost
 - From historical cloud acquisitions
 - DoD, DHS, others
- Refine the cloud CES and PBS
 - Socialize the product
- Develop CERs for cloud acquisitions
- Compare cloud cost calculators
 - Deep dive
 - Develop instructions
 - Highlight challenges and define tips (i.e., data storage is sometimes free but *retrieval* is not)



Questions?

Online References

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>

Online References

Vendor Calculators

AWS Instances

<https://aws.amazon.com/ec2/instance-types/>

AWS Dedicated Instances

<https://aws.amazon.com/ec2/purchasing-options/dedicated-instances/>

AWS Dedicated Hosts

<https://aws.amazon.com/ec2/dedicated-hosts/>

AWS Calculator

<https://calculator.s3.amazonaws.com/index.html>

Google Calculator

<https://cloud.google.com/products/calculator/>

IBM Calculator

<https://console.bluemix.net/pricing>

Microsoft Azure Calculator

<https://azure.microsoft.com/en-us/pricing/calculator>

Oracle Calculator

<https://cloud.oracle.com/cost-estimator>

Salesforce Pricing Information

<https://www.salesforce.com/products/sales-cloud/pricing>

SAP Pricing Information

<https://cloudplatform.sap.com/pricing.html>



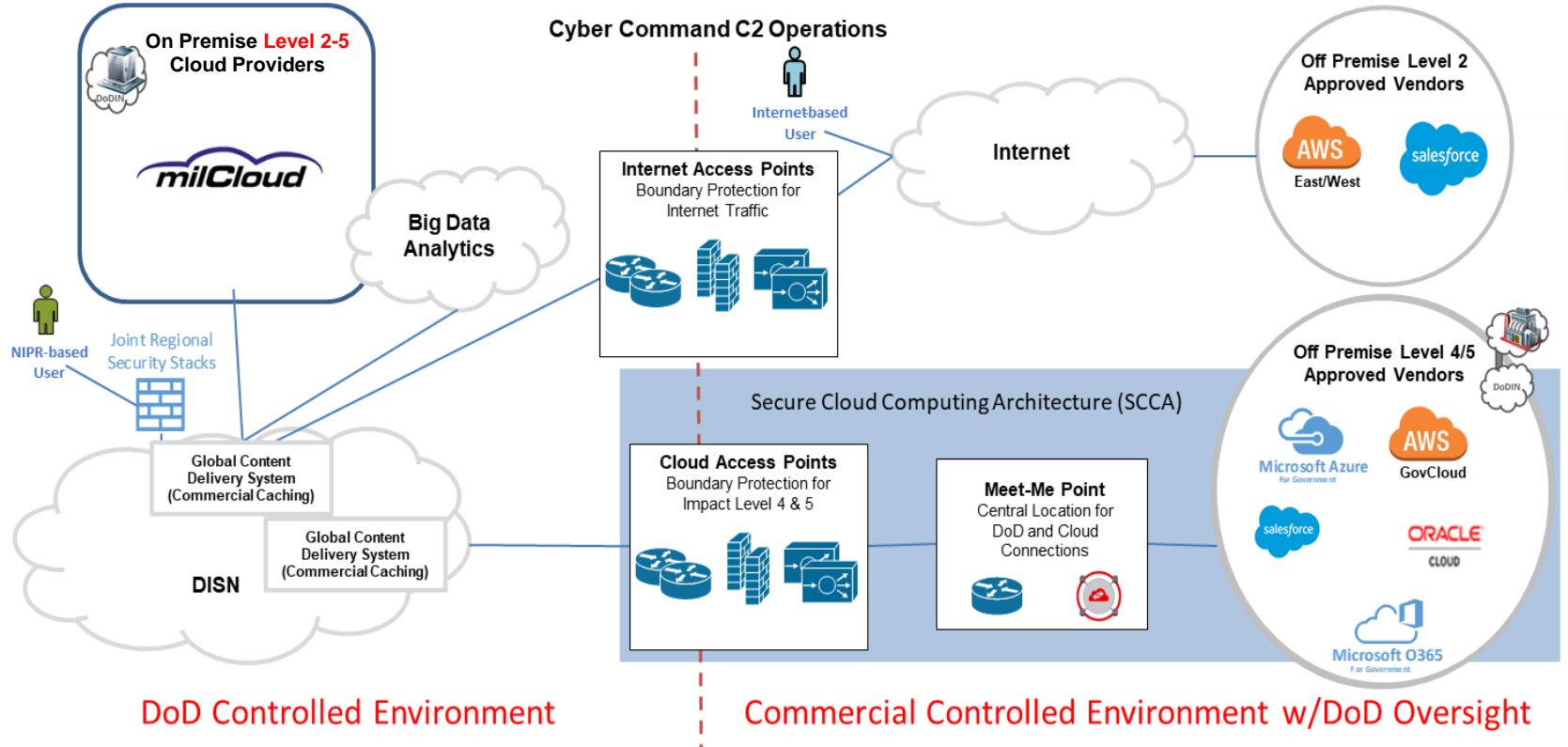
Backup

Cloud Security

- The Defense Information Systems Agency (DISA) uses information impact levels (IILs or ILs) to ensure security requirements are met for cloud acquisitions in the DoD

Department of Defense Information Impact Levels (IILs)					
IIL	Information Sensitivity	Security Controls	Location	Off-Premises 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	<ul style="list-style-type: none"> Virtual/Logical Public Community
4	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Virtual/Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information
5	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Virtual/Logical Federal Government Community Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information
6	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

Cloud Security



DISA Cloud Environment

DISA milCloud 2.0

- milCloud 2.0 is the DoD version of IaaS cloud environment connecting commercial offerings to government-protected servers
- Customers have the offerings of a commercial vendor with the added security measure
- Security
 - DISA deploys DoD Secure Cloud Computing Architecture (SCCA)
 - Includes “enterprise-level cloud security and management services”¹
 - SCCA provides cloud access points (CAPs) for customers to access commercial cloud environments while utilizing DISA security measures

¹DISA DoD SCCA Fact Sheet

Security Cost Implications

- As security requirements become tighter, costs will rise for programs hosted in the cloud
- A cloud access point (CAP) is required for boundary protection for ILs 4 and 5, consisting of 4 pillars (each but the first a chargeable cost)

