DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Migrating Applications to the Cloud

Mr. John Hale
Chief, DISA Cloud Services
May, 2018

Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.

Cloud Migration Steps

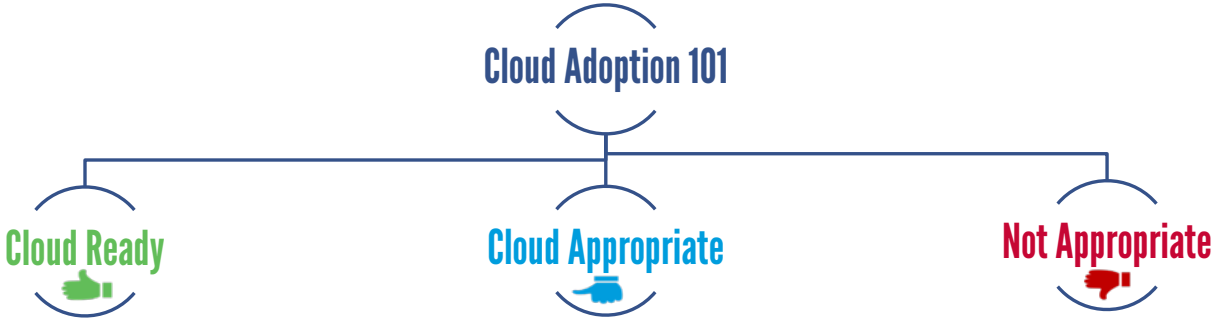
- **Survey Existing Applications**
- **Application Rationalization**
- **Decisions/Funding**
- **Migration Activities**
- **Lesson's Learned**

Rinse, Repeat!

Impact Levels

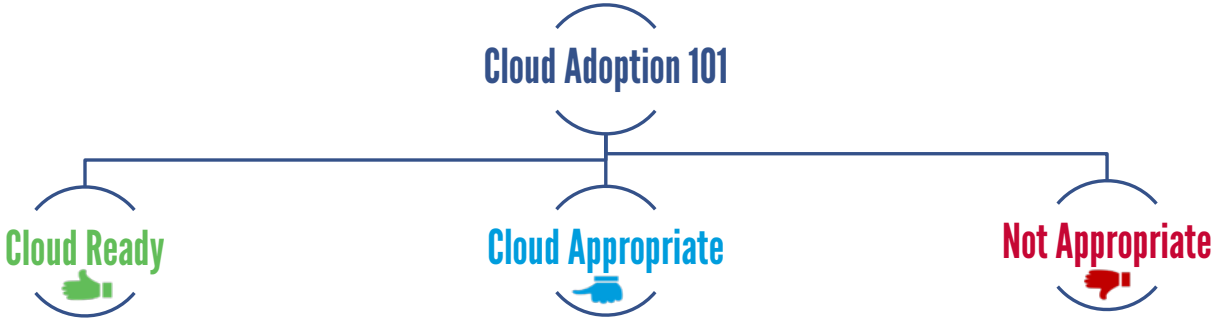
- **Impact Level 2 (IL2) – Unclassified Data (public data) – requires shared or dedicated infrastructure**
- **Impact Level 4 (IL4) – Unclassified Sensitive Data (FOU, CUI, etc) – required shared or dedicated infrastructure with strong evidence of virtual separation controls and monitoring**
- **Impact Level 5 (IL5) – Unclassified Sensitive Data (NSS, PIAA, HIPA) – required dedicated infrastructure**
- **Impact Level 6 (IL6) – Classified Data (Secret, etc) – required dedicated infrastructure approved for classified information**

Application Categorization



	Cloud Ready	Cloud Appropriate	Not Appropriate
Financial	• Application architecture supports cloud adoption without requiring costly changes. • Mission area will break even in costs. • Cloud pricing models can address current application delivery and availability.	• A small investment is needed to update applications. • The application scales and can take advantage of the cloud maintenance model.	• Application would have to be completely re-engineered to make it cloud ready. • The costs to modernize the application are too significant to be beneficial.
Security	• The application's security/impact level is supported by cloud technology. • The application has baked in security or a strong plan to acquire required cloud security.	• Application meets most cloud security standards. • Application can leverage provided cloud security.	• Application does not meet DoD security policy or security standards for on or off premise cloud environments. • Application does not securely operate in the cloud.

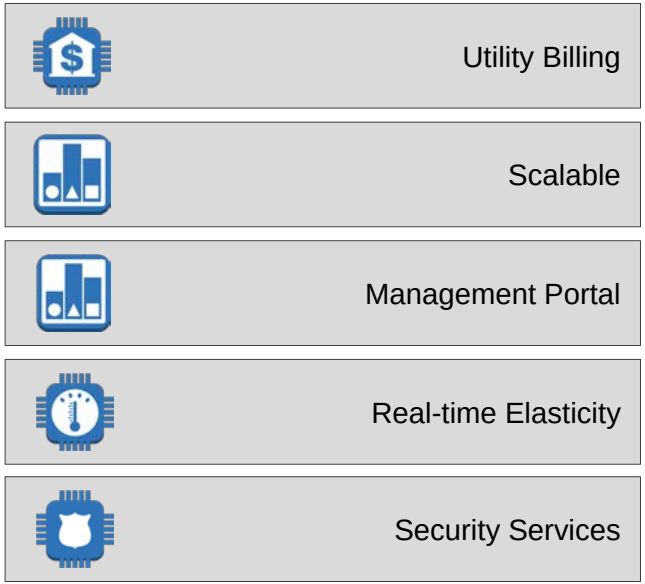
Application Categorization (Cont.)



	Cloud Ready	Cloud Appropriate	Not Appropriate
Operations	• Modernized backup and recovery standards and processes. • Software-based resiliency model. • Application management is not host-based. • Application functions can be sustained in the cloud successfully.	• Evolving application architecture that will address rapid infrastructure changes and failovers.	• Application has too many dependencies on other systems and/or interfaces. • Complicated hardware. • Application is hardware dependent for failovers and redundancy.
Contracting	• There are vendors with cloud capabilities that meet mission requirements. • There is a contracting vehicle that support capability acquisition.	• Application Requirements are clearly identified.	• No contract available to move the application to the cloud. • Undefined application requirements.

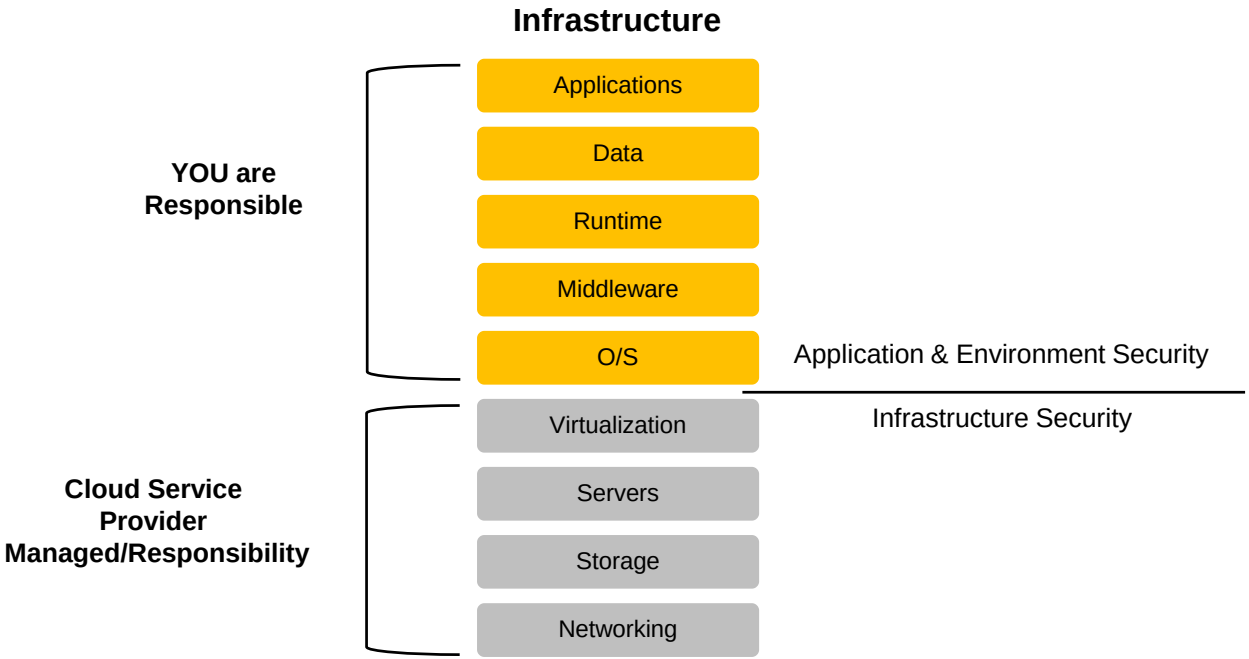
What is cloud?

- **In reality, cloud is:**



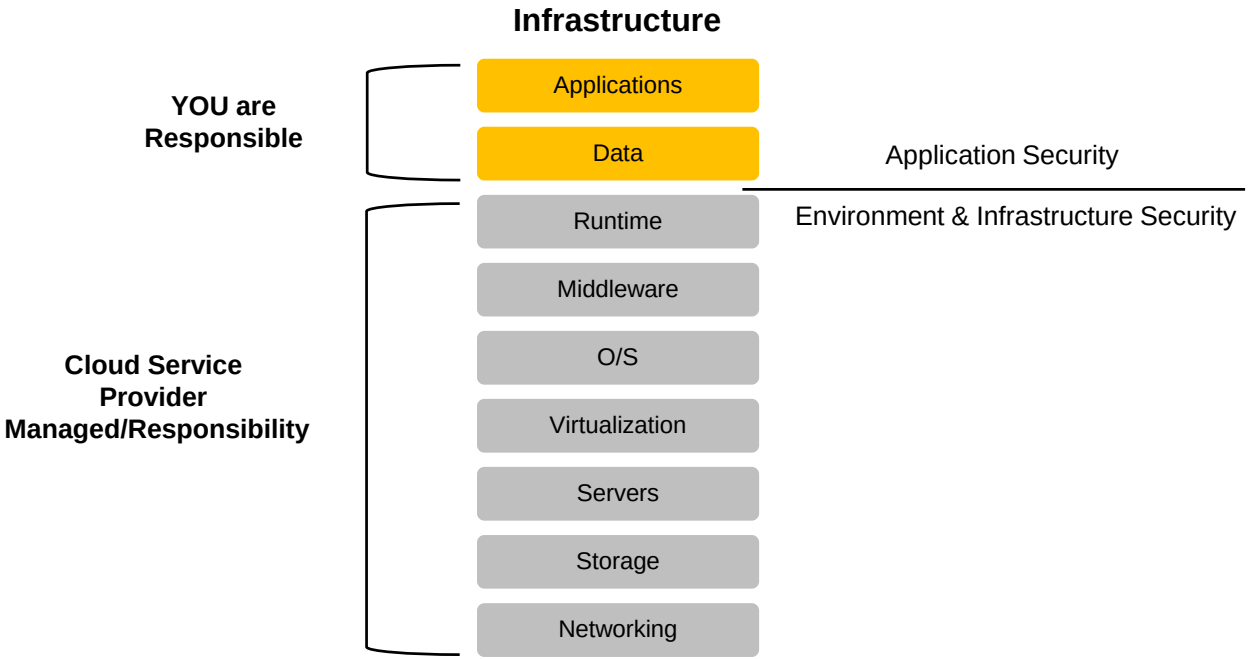
Cloud Models

Infrastructure as a Service (IaaS)



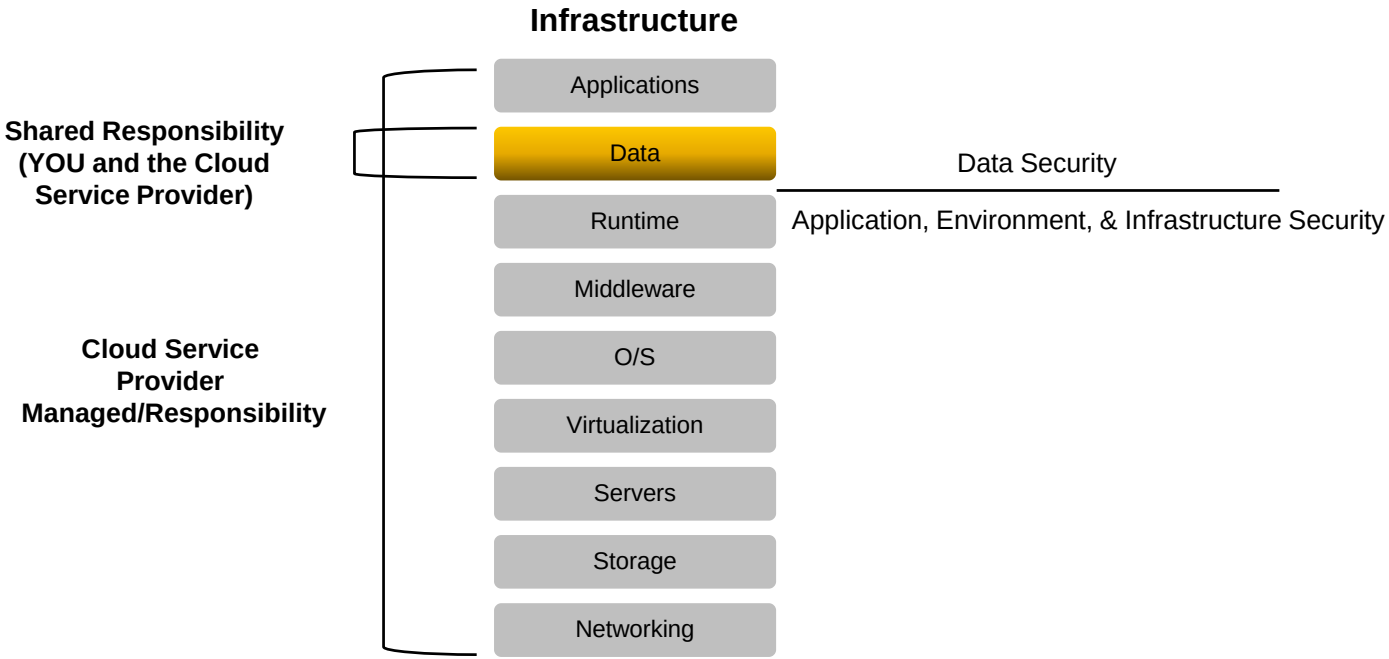
Cloud Models (Cont.)

Platform as a Service (PaaS)



Cloud Models (Cont.)

Software as a Service (SaaS)



Lessons Learned

Technical Challenges

- **Applications not cloud ready - some may never be ready due to cost to modernize**
  - **Not all app owners have access to skills and resources to modernize apps for the cloud – milCloud 2.0**
- **Commercial cloud business model not always aligned to DoD heavy transactional data I/O requirements... easier for isolated applications or minimal I/O to legacy systems. (High I/O drives cost)**
  - **DoD working to provide direct network connection to small number of commercial cloud providers to offset this cost and eliminate data "meters"**
- **Applications Existing DoD Security Solutions are not cloud aware**
  - **Secure Cloud Computing Architecture (SCCA) deployed January 2018 to provide basic security services in a shared cloud environment**

Lessons Learned (Cont.)

Business Management Roadblocks

- **Business decisions challenging**
  - **Lack of a single place for application owners across DoD to find all available Cloud solutions and understand which one to choose (features, price, etc.)**
  - **App owners don't understand new paradigm and responsibilities with commercial IaaS missing key cost in analysis (i.e. system administration, application of security, etc.)**
  - **Current hosting costs don't show subsidized component costs (electric, HVAC, building space, etc.) making apples to apples comparison difficult**

- **Funding not available for application owners to modify apps to be cloud-ready**
  - **Application rationalization data should help to decide which apps get funding for modernization**

- **Policies for specific types of data (NC3, OCO) protect where data can be processed and/or stored for mission assurance**
  - **App owners don’t always understand how to translate requirements to commercial facilities (search and seizure of commercial property, data sovereignty, etc.)**

rate us

take the 3-question survey
available on the AFCEA 365 app

visit us

DISA Booth # 443

follow us

Facebook/USDISA

Twitter/USDISA

www.disa.mil

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

www.disa.mil **/USDISA** **@USDISA**