Considerations for Test & Eval in the Cloud

Chris Goldberg
Chief Architect, IBM GBS Managed Services and Cloud Solutions

© 2016 IBM Corporation

Cloud Service Provider Offering Overview

- **What Clouds Are Out There?**
  - FedRAMP is the most up-to-date source for CSP offerings and their accreditation levels
    - https://marketplace.fedramp.gov/#/products?status=Compliant&sort=productName
    - IaaS/PaaS/SaaS offerings from Adobe, Amazon, AT&T, BMC, Box, CGI, Cisco, ESRI, Google, HPE, IBM, Microsoft, Oracle, ServiceNow, Verizon, and many more.

- **How Do I Choose The Right Cloud for My Organization**
  - One Size Fits All Does Not Apply to Cloud
  - Different CSPs, different CSOs, different perspectives – all pointing toward the need for a hybrid strategy to cloud adoption.

- **How Do I Start The Process: Cloud Consumer Perspective**
  - Have a design principle for your system and how you need it to support your business
  - Realize you won't have control over the CSP offering/infrastructure/etc…but you do control your data
  - Focus on building "loosely coupled" systems – i.e. think modularity, portability to support your hybrid model
  - Think about your ideal "transition in" and "transition out" scenarios from a cloud environment, these will shape your evaluations of CSOs
  - Understand the development, testing, production, & retirement ecosystem for your workload so you can best align CSOs to your needs

Considerations for Moving to the Cloud

- **Test and Monitoring Tools Available**
  - In general CSOs will offer some tools and most will allow you to bring in any 3rd party tool you need to support the following needs
    - Infrastructure Tools (up to the OS)
    - Application Migration strategies and tools (middleware and above)
    - Data transformation strategies and tools (i.e. SQL to No-SQL)

- **Metrics that can be tracked**
  - System Monitoring Metrics: CPU, Disk, Network, RAM utilization – the basics up to the OS
  - Application Monitoring: Synthetic transactions, workload footprinting, load simulation
  - Security Metrics: Logs, SIEM, Vulnerability Scanners
  - Integration of all of the above to ITSM tool and processes

- **How is test different in the cloud** (standalone systems plugged into a DoD network vs cloud)
  - Network considerations: “Direct” circuits, DISA CAPs, MTIPS/TIC, VPN
    - One of 5 NIST characteristics of cloud computing is “broad network access” - how do we connect multiple disparate networks across a cloud / on-prem ecosystem
  - How do I migrate data between cloud and on-prem
    - What are the technical options and limitations?
    - What is the cost?

Certification and Accreditation Considerations

- First - Understand your governance framework (NIST, CC SRG, STIG, FIPS, FISMA, etc..)

- Next – Understand what level of accreditation your CSO is authorized for
  - –NIST 800-53 is the baseline
  - –FISMA H/M/L, FedRAMP H/M/L, TIC Overlay, HIPAA Overlay build on top of NIST 800-53

- Next - How do I draw my security boundary? What is in scope and what isn't?

- Control inheritance: Understanding what controls are in place, who provides that control, and what responsibilities you as a tenant have to ensure the controls are working as designed

- Continuous Monitoring: How to ensure that your deployed cloud workload stays compliant