Total Ownership Cost of Cloud Cybersecurity

Washington Area ICEAA Lunch
31 July 2018

Zachary Jasnoff
VP, Business Services
Price Systems, LLC

David Cass
VP/CISO
IBM Global Cloud Security Services

Richard Mabe
Sr. Solutions Consultant
Price Systems, LLC

Foreword

- Continuation of IBM and PRICE Systems combined research on evaluating the Total Ownership Costs related to Cloud migration and hosted services for Business Systems
- Focus of this paper: thoughts on the costs and benefits associated with Cybersecurity for Business Systems that migrate whole or in part to the Cloud

Overview

- Cloud solutions for IT and Cybersecurity
- Cloud Migration Approach
- Total Cost of Ownership (TCO)
- An Integrated Framework for Cybersecurity Related TCO
- Cybersecurity cost trade-offs for business systems migration
- Conclusions

 | ***Decades of Cost Management Excellence***

Why Use a Cloud Solution for IT?

Cloud is a means to an end…

Faster to market	Higher Quality	↓ Cost ↑ Flexibility	Repeatable & Scalable	Secure & Compliant
Enable experimentation Fall or succeed fast Accelerated releases Rapidly add capacity	Frequent user feedback Fewer errors Analytics based decisions Resiliency thru automation	Transparent/variable structure Affordable infrastructure Service provider choice Address technical debt	Standardization (No Snowflakes) Reference implementations Skill acquisition/upgrade Expansion consistency	Fewer audit exceptions Regulatory requirements Process control structures Client confidence

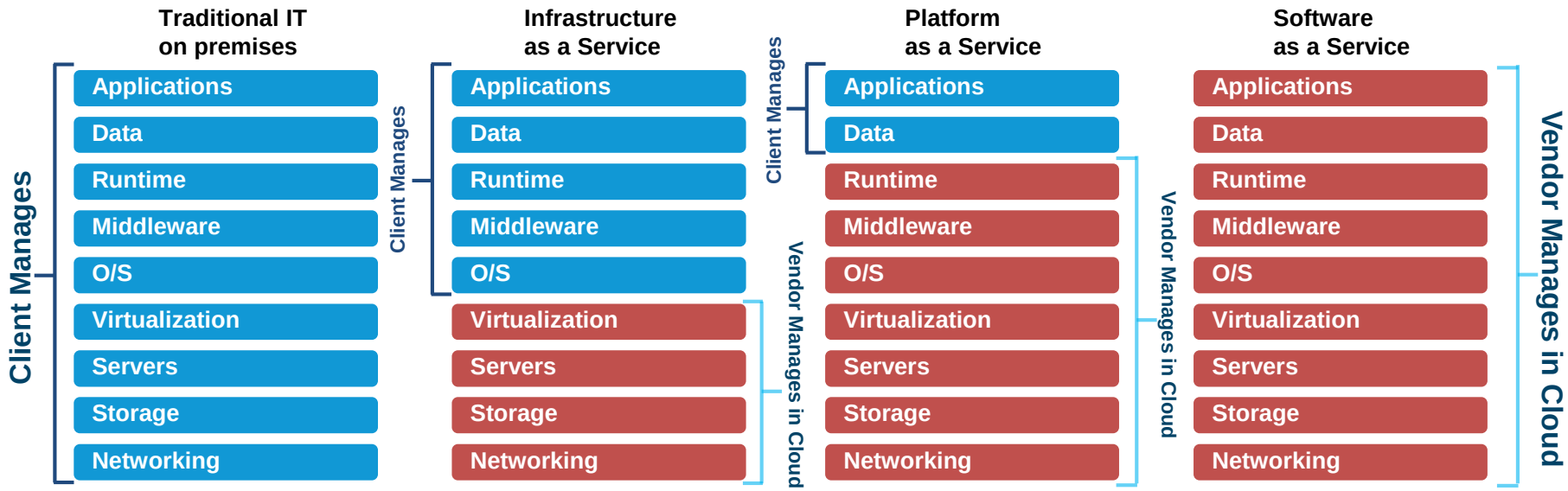
…that requires organizations to transform, and consider -

- *How to deliver capabilities while improving quality*
- *How to interact and react with clients*
- *How to think about technical debt*
- *How to ensure cyber security requirements are met and cyber threats are mitigated*

 | ***Decades of Cost Management Excellence***

Multiple Service Delivery Models

Management requires a hybrid approach for Services Integration involving the Client and the Cloud Vendor



Integration of Roles, Processes, Information, and Technology covers the new cloud models needing additional service management

Additional Service Management Needed

Provided by Cloud Provider

Cloud Security Concerns

Top Cloud Questions from Leadership

- Are we protected from the latest threats?
- Have we protected our most critical data?
- Do we have access to the right skill sets?
- Are we adapting to changing platforms?
- Are we operating at an appropriate maturity level for our industry?
- Are we communicating our risks clearly to our leaders and our board?
- Are we maximizing the value of our security investments?

 | *Decades of Cost Management Excellence*

Cloud Security Concerns

Industry compliance standards* and data protection are the main inhibitors to *adopting* a cloud solution ….. for example:

Privacy and Compliance – adapting to a threat-aware, risk-based approach vs. a compliance based, box checking approach for managing compliance

Data Protection - protect the personal data of hundreds of thousands of customers whose personal information was compromised in a data breach that occurred between November 2013 and April 2014.
Source: http://topclassactions.com/lawsuit-settlements/lawsuit-news/53582-att-to-pay-25m-in-data-breach-settlement-with-fcc/

Human error/Insider threat – More than half of data breaches are caused by *insiders*, including employees, third-party contractors and partners.
Source: http://www-03.ibm.com/security/data-breach/2015-cyber-security-index.html?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

Security skills gap - experts predict a shortage of 1.5 million open and unfilled security positions by 2020.
Source: Frost & Sullivan Report, 2015

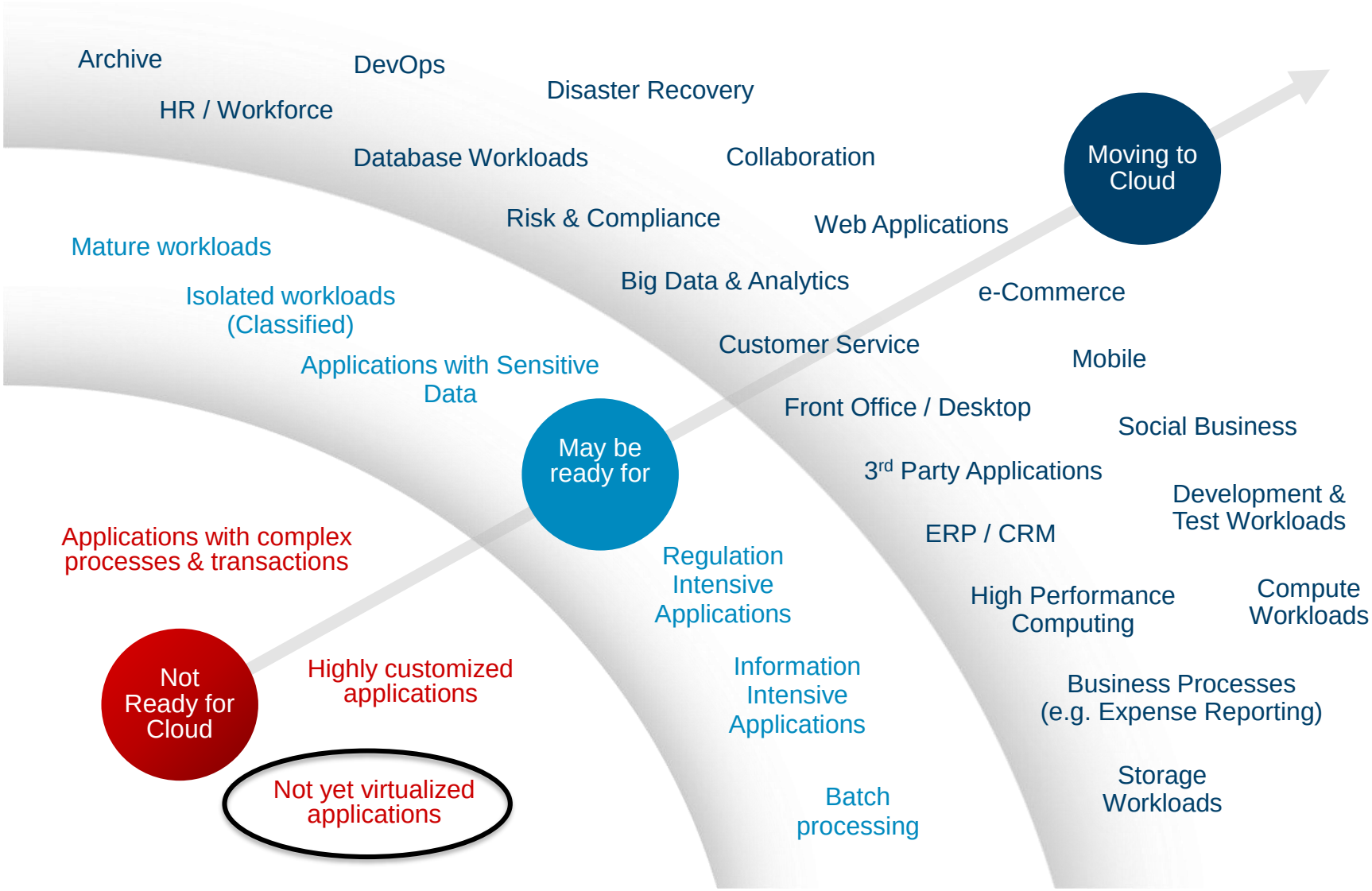
Additionally, more than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years, according to a 2015 analysis of numbers from the Bureau of Labor Statistics by Peninsula Press, a project of the Stanford University Journalism Program.
Source: http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#683b25157d27

Innovations – cloud, mobile, and IOT create unprecedented risks to organizations. 44% of security leaders expect a major cloud provider to suffer a significant security breach in the future. 33% of organizations don't even test their mobile apps. CISCO estimates that by 2020, there'll be 50 billion devices connected.
Sources: https://www-03.ibm.com/press/us/en/pressrelease/45326.wss; https://securityintelligence.com/mobile-insecurity/; http://blogs.cisco.com/diversity/the-internet-of-things-infographic

Advanced Attacks – more advanced than ever, with more than 80% involving cyber gangs, a global business that accounts for $400B+ a year.
Source: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Cloud Migration

Cloud adoption and business value is driven by workloads



 | *Decades of Cost Management Excellence*

Cloud Transition Estimating Process

As Is System

(User Data Cntr)

- Operate
- Sustain

Recurring Costs:
- Labor
- Materials
- Overhead
- ODCs
- Facilities
- PM/SE

Plan for Transition:

- *Business Case*
- *Change Mgmt*
- *Svc Level Agreement*

- What
- When
- Where To
- Security
- Access

Transition:

- Software
- Data
- Interfaces

Non-Recurring Costs:
- Modify/Refactor SW apps
- Prep data for migration
- Develop new middleware Interfaces
- Adapt to Cloud OS and Middleware Services
- PM/SE

Execute Plan:

- SW Porting
- *Data Migration*
- *User Training*

- Migrate
- Instantiate
- Test/Verify
- Parallel Ops
- Changeover
- Go Live

To Be System

(Cloud Host)

- IaaS
- PaaS
- SaaS

Recurring Costs:
- Fees
- Licenses
- Subscriptions

For:
- Infrastructure
- Run Time Env
- SW Services
- Access
- Cybersecurity
- PM/SE

Total Cost of Ownership Model

- Total Cost of Ownership (TCO) measures the direct and indirect costs of IT Infrastructure over the life cycle of systems

TCO = Capital Expenses	+ Operational Expenses	+ IT Governance/Sys Mgmt
(Direct)	(Direct + Indirect)	(Overhead/Admin)
(Infrastructure)	(Services)	(PM, FM, Cyber Mgmt)

With Transition to Cloud services:

- Change from a CAPEx focus to an OPEx focus
  - Introduces uncertainty since resource consumption is determined by workload
  - Difficult to estimate cost effective options and cost of bandwidth
- Impacts All Aspects of The Organization
  - Changes the acquisition model: infrastructure not procured
  - Changes the compliance / security model: provider security services
  - Changes the management model: provider systems management

In calculating TCO, organizations estimate and optimize cost based on workload

Evaluating the Cost Trade-Offs*

- The key cost-related question: how well the cloud performs in the context of real workloads and business requirements
  - It's not just price, but price- performance that matters
  - Analysis should take every cost driver into account
- What to Consider:
  - Capabilities: Innovation, Speed, Insight, Security
    - *What are the real requirements for applications, workloads, security and service levels?*
    - *Can the provider meet your requirements for security and compliance (Confidentiality, Availability, Integrity)?*
  - Performance: Flexibility to position workloads, Access new technology, Speed, Scalability
    - *Can the provider's cloud deliver the secure speed and throughput that individual workloads require?*
    - *Are secure choices available that deliver higher levels of performance and service?*
  - Economics of the solution: Choice of technologies, Cost/optimal ROI, Visibility and control
    - *How much will it cost to achieve the needed performance/security– initially, and in the future?*
    - *If upgrades are needed, what will they cost?*
    - *Are there hidden costs?*

**Cloud IT Economics, What you don't know about TCO can hurt you. IBM Corp., 2018*

Evaluating the Cost Trade-Offs

- Compare the most meaningful Measures
  - Web applications: Computer–intensive; response, throughput and scalability
    - *How many user requests are processed per second on average?*
    - *Do alternative environments deliver better price-performance for the required Confidentiality, Availability and Integrity required by the Application?*
  - Analytics: Storage-intensive; traditional business analytics, innovative cognitive apps
    - *How many input-output queries per hour can the cloud securely handle?*
    - *How costly is storage?*
  - Network-intensive workloads: Inter-application messaging; cloud-to-cloud, cloud-to-data center, data center-to-data center
    - *How much cost-of-security does a messaging-intensive workload add?*
    - *How cost-efficient is the cloud at securely moving data and workloads?*
  - Hosted cloud: move from on-premises to hosted cloud with speed and efficiency
    - *How much does it cost to migrate a virtual machine to the cloud?*

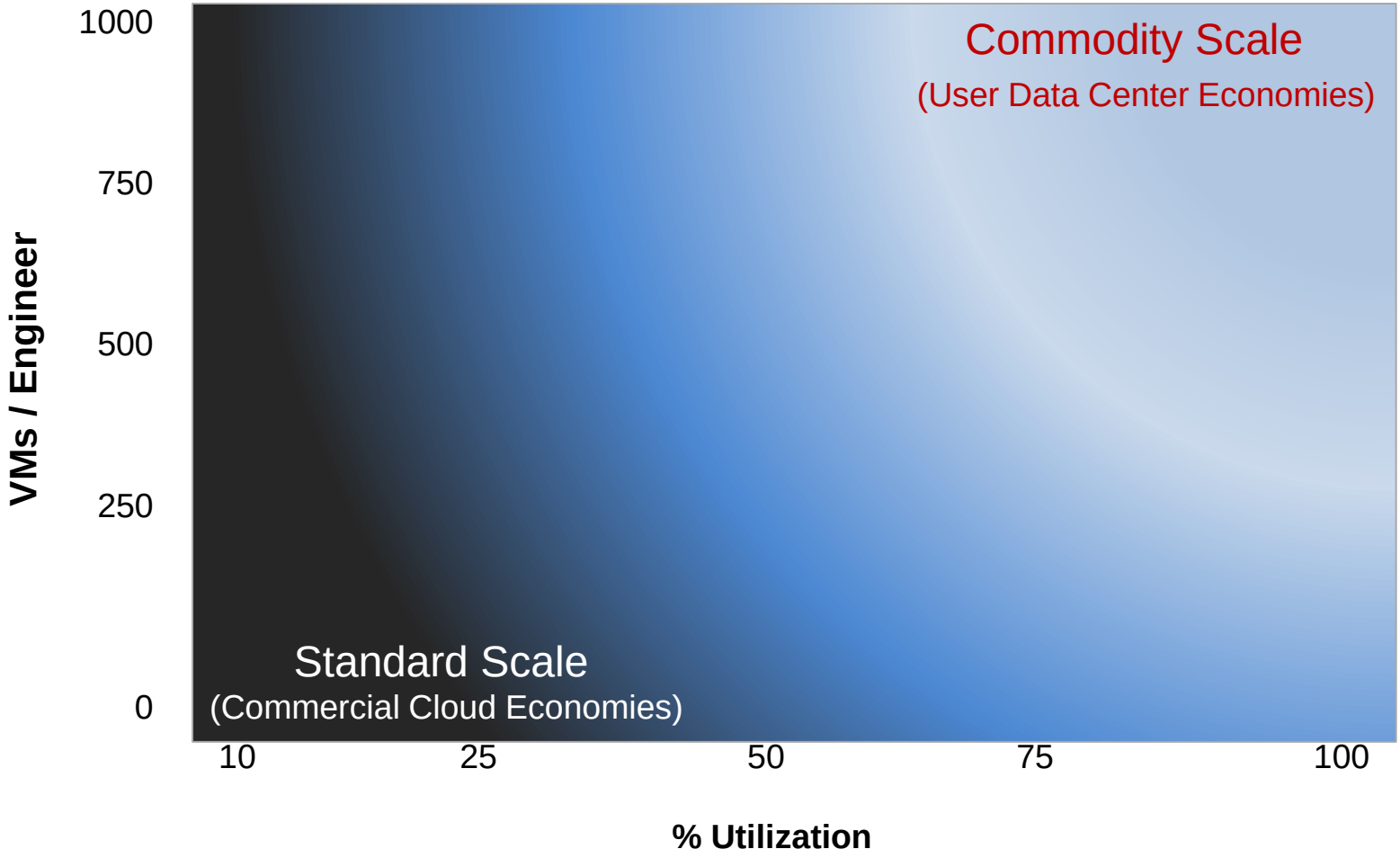
Evaluating the Cost Trade-Offs

- Another Approach - The "Cloud Price Index (pCPI)*: Support Labor vs Utilization of Capacity and Capability
- Derive the average price of a Cloud solution using a 'basket of goods' approach:
  - Consider the total cost of a bundle of hosting services, infrastructure, software and operating systems
  - Find the average "price per VM-hour" and "price per GB per month" for compute and storage requirements

- The unit cost of a virtual machine running on a user owned cloud comes down to two factors:
  - Labor efficiency and utilization. The greater the number of VMs an administrator can successfully manage (i.e., its labor efficiency), the lower the unit cost per resource.
  - The better-utilized the private cloud (i.e., its utilization), the lower the unit cost per resource.

** Total cost of ownership in private cloud: guidelines for buyers. O. Rogers and J. Atelsek, 451 Research, Sept 2017*

Cloud Price Index



 | *Decades of Cost Management Excellence*

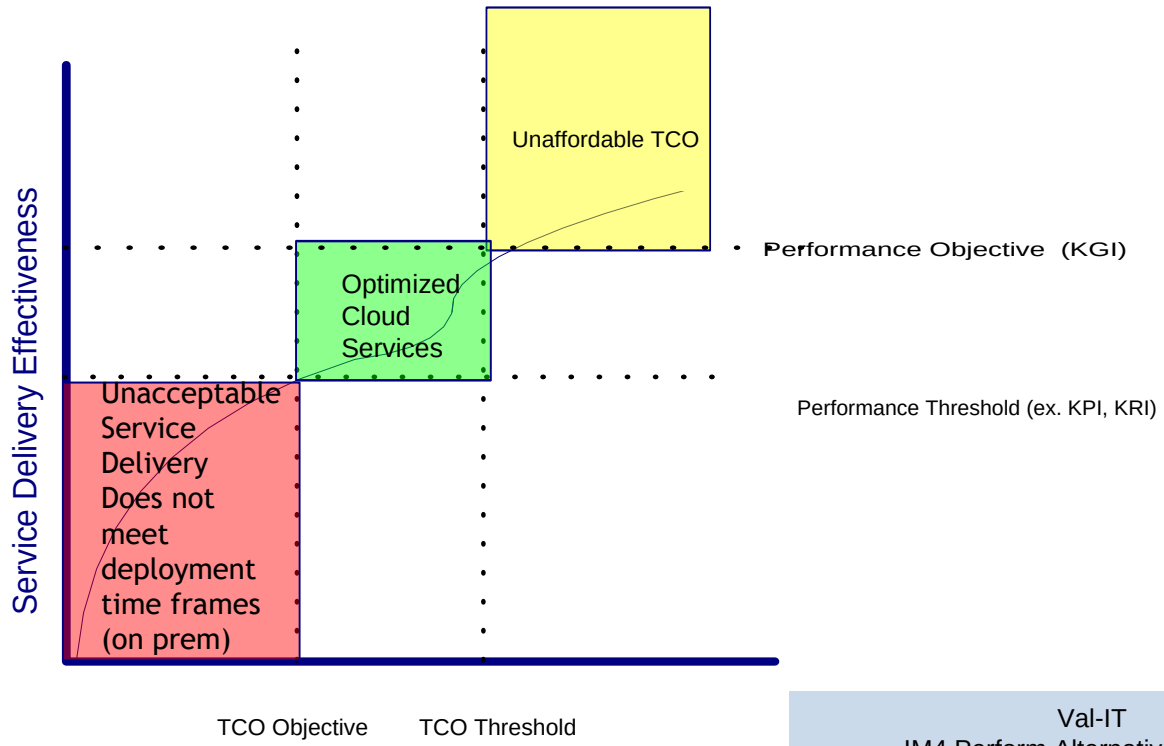
Optimized Cloud TCO Analysis Model

Extending CobiT* and Val-IT+ into a CAIV Framework

CobiT DS4 Ensure Continuous Service

Ensure that IT service and infrastructure can resist and

recover from failures…



Typical KPI

- Time to Market
- Patching (IAVA)
- SLA

Val-IT
IM4 Perform Alternative Analysis
IM7 Identify Full Life Cycle Costs and Benefits

**Control Objects for Information and Related Technologies*
+Value from IT Investments

The Optimized TCO provides the essential "best value" framework for the strategic decision process

Framework to Evaluate Cybersecurity Costs

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

Transition

To Be: XaaS
Fee for Svc
Virtual Domain

Analysis:
Metrics
Tools
Methods

Business System - Cyber Specific LCC
Capital Expenses
Cybersecurity Integration - Governance and Org
Custom Workload
Cybersecurity Services (SW)
Cyber End User Device (HW)
Cyber Data
System Level Technology
Dedicated Cyber Comm
Infrastructure Services
Systems Engineering (RMF)
Cyber Test and Evaluation
Operations Expenses
Cybersecurity Services - Governance and Org
System/Services Operations
Cybersecurity Services
Cyber Data Services
End User Device Support Services
Training Services Operations
System/Services Mgmt
Communications Services
Infrastructure Services
Cyber SW Maintenace/Modification
Managed Services Operations
Systems Engineering (RMF)
Recurring Cyber Tests

 | *Decades of Cost Management Excellence*

Additional Explanation

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

→ **Transition** →

To Be: XaaS
Fee for Svc
Virtual Domain

↔

Analysis:
Metrics
Tools
Methods

Business System - Cyber Specific LCC
Capital Expenses
Cybersecurity Integration - Governance and Org
Custom Workload
Cybersecurity Services (SW)
Cyber End User Device (HW)
Cyber Data
System Level Technology
Dedicated Cyber Comm
Infrastructure Services
Systems Engineering (RMF)
Cyber Test and Evaluation
Operations Expenses
Cybersecurity Services - Governance and Org
System/Services Operations
Cybersecurity Services
Cyber Data Services
End User Device Support Services
Training Services Operations
System/Services Mgmt
Communications Services
Infrastructure Services
Cyber SW Maintenace/Modification
Managed Services Operations
Systems Engineering (RMF)
Recurring Cyber Tests

Transition is a cooperative effort to identify, evaluate, implement and enforce security policies.

As organizations increasingly adopt cloud environments, they establish cloud-specific security policies that are often an extension of their corporate security policy.

To ensure a successful cloud adoption, both cloud service consumers and cloud service providers need to establish and follow their respective cloud security policies.

These security policies are often aligned to the cloud consumption and delivery model Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

 | *Decades of Cost Management Excellence*

Additional Explanation

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

Transition

To Be: XaaS
Fee for Svc
Virtual Domain

Analysis:
Metrics
Tools
Methods

Business System - Cyber Specific LCC
Capital Expenses
Cybersecurity Integration - Governance and Org
Custom Workload
Cybersecurity Services (SW)
Cyber End User Device (HW)
Cyber Data
System Level Technology
Dedicated Cyber Comm
Infrastructure Services
Systems Engineering (RMF)
Cyber Test and Evaluation
Operations Expenses
Cybersecurity Services - Governance and Org
System/Services Operations
Cybersecurity Services
Cyber Data Services
End User Device Support Services
Training Services Operations
System/Services Mgmt
Communications Services
Infrastructure Services
Cyber SW Maintenace/Modification
Managed Services Operations
Systems Engineering (RMF)
Recurring Cyber Tests

Cloud Security Transition Strategy:

Phase 1: Project Initiation: collect and review data; prepare transition team and assets

Phase 2: Assess the As Is Security Posture; catalog current cloud use; prepare assessment report for the client

Phase 3: Define the "target" To Be state; Analyze Requirements for the To Be Domain (Gap Analysis); present cloud security maturity framework

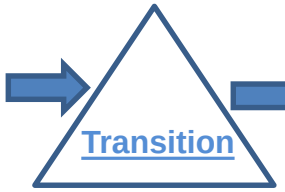
Phase 4: Recommend a Cloud Solution Roadmap and (potentially) a Business Case for the level of Cloud service

 | *Decades of Cost Management Excellence*

Additional Explanation

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration



To Be: XaaS
Fee for Svc
Virtual Domain

Analysis:
Metrics
Tools
Methods

Business System - Cyber Specific LCC
Capital Expenses
Cybersecurity Integration - Governance and Org
Custom Workload
Cybersecurity Services (SW)
Cyber End User Device (HW)
Cyber Data
System Level Technology
Dedicated Cyber Comm
Infrastructure Services
Systems Engineering (RMF)
Cyber Test and Evaluation
Operations Expenses
Cybersecurity Services - Governance and Org
System/Services Operations
Cybersecurity Services
Cyber Data Services
End User Device Support Services
Training Services Operations
System/Services Mgmt
Communications Services
Infrastructure Services
Cyber SW Maintenace/Modification
Managed Services Operations
Systems Engineering (RMF)
Recurring Cyber Tests

Cloud Security & Regulatory Compliance accelerators would:

- **Asses the maturity and effectiveness of the current security program in place at the client's organization**
- **Manage and govern information security more effectively and efficiently at all levels of the Cloud stack**
- **Identify and effectively manage security and regulatory compliance requirements while driving growth of programs**
- **Build a more risk aware culture through education and awareness**
- **Improve operational security for critical infrastructure (that would entail IaaS, PaaS and SaaS elements of the cloud embracement model)**

 | *Decades of Cost Management Excellence*

Map to a Common Program WBS

(Mil-Std-881D, App J)

Cost WBS (Mil-Std-881D, App J) →

Cybersecurity CES ↓

	1 Business System	1.1 Development/Procurement	1.1.1 Custom Application Development	1.1.1.1 Enterprise Services Elements	1.1.1.4 System Level Hardware	1.1.2 System Level Integration	1.1.3 Systems Engineering	1.1.3.1 Cyber Systems Engineering	1.1.4 Program Management	1.1.4.1 Cyber Program Management	1.1.5 Change Management	1.1.6 Data Management	1.1.7 System Test and Evaluation	1.1.7.1 Cybersecurity Test and Evaluation	1.1.12 Operational Site Infrastructure	1.1.12.1 Hardware	1.1.12.2 Software Licenses
Business System - Cyber Specific LCC				X	X	X		X		X	X	X		X	X	X	
Capital Expenses																	
Cybersecurity Integration - Governance and Org										X	X						
Custom Workload																	
Cybersecurity Services (SW)				X													X
Cyber End User Device (HW)					X												
Cyber Data												X					
System Level Technology																	
Dedicated Cyber Comm																X	
Infrastructure Services															X		
Systems Engineering (RMF)						X		X									
Cyber Test and Evaluation														X			

 | *Decades of Cost Management Excellence*

Map to a Common Program WBS

(Mil-Std-881D, App J)

Cost WBS (Mil-Std-881D, App J) →

Cybersecurity CES ↓

	1 Business System	1.2 Recurring Annual Business System Sustainment	1.2.1 Program Management	1.2.2 Systems/Sustainment Engineering	1.2.3 Change Management	1.2.4 Help Desk	1.2.5 Data Cleansing/Data Mgmt	1.2.6 System Data Base Admin	1.2.7 IT Infrastructure/Network Maintenance	1.2.7.3 Management	1.2.8 HW Tech Refresh	1.2.8.1 Cybersecurity Equipment	1.2.9 SW Licenses Refresh/Update	1.2.9.1 Cybersecurity SW License	1.2.10 Cybersecurity Maintenance Management	1.2.10.1 Compliane Operations and Tracking (RMF)	1.2.10.2 FOTE	1.2.10.3 Certification/Validation	1.2.11 Follow On User Training	1.2.13.2 Software (Includes Cybersecurity and IAVA)
Operations Expenses																				
Cybersecurity Services - Governance and Org																				
System/Services Operations			X		X	X														
Cybersecurity Services														X						
Cyber Data Services							X	X												
End User Device Support Services												X								
Training Services Operations																			X	
System/Services Mgmt																				
Communications Services																				
Infrastructure Services										X										
Cyber SW Maintenace/Modification																				
Managed Services Operations																				X
Systems Engineering (RMF)				X												X		X		
Recurring Cyber Tests																	X			

 | *Decades of Cost Management Excellence*

Trade-Offs by Cloud Model: IaaS

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

Transition

To Be: IaaS
Fee for Svc
Virtual Domain

Analysis:
Metrics
Tools
Methods

Business System - Cyber Specific LCC	As Is Total Cost of Ownership	As Is Total Cost of Ownership (IaaS)
Capital Expenses		
Cybersecurity Integration - Governance and Org	User Funded Program Mgmt (Governance)	
Custom Workload	Workload	Workload
Cybersecurity Services (SW)	User Owned/Managed App SW	
Cyber End User Device (HW)	User Owned/Managed App HW	Fee for Clouded Provided Domain Services
Cyber Data	User Owned Data Services	Fee for Clouded Provided Data Services
System Level Technology	Technology	Technology
Dedicated Cyber Comm	User Owned/Managed Comm	
Infrastructure Services	User Owned/Managed Infrastructure	Fee for Cloud Provided Virtual Capability
Systems Engineering (RMF)	User Funded Systems Engineering	
Cyber Test and Evaluation	User Funded Systems Test/Eval	
Operations Expenses		
Cybersecurity Services - Governance and Org	User Funded Program Mgmt (Governance)	
System/Services Operations	Workload Management and Operations	Workload Management and Operations
Cybersecurity Services	Data Center/Corporate Staff	
Cyber Data Services	Data Center/Corporate Staff	Fee for Cloud Data Service Mgmt and Ops
End User Device Support Services	Data Center/Corporate Staff	Fee for Cloud Virtual Domain Mgmt and Ops
Training Services Operations	Data Center/Corporate Staff	
System/Services Mgmt	Technology Management and Operations	Technology Management and Operations
Communications Services	Data Center/Corporate Staff	Fee for Cloud Provided/Managed Comm Svcs
Infrastructure Services	Data Center/Corporate Staff	Fee for Cloud Provided/Managed Infr Services
Cyber SW Maintenace/Modification	SW Maintenance and Modifications	
Managed Services Operations	User Owned/Managed SW Services	
Systems Engineering (RMF)	User Funded Systems Engineering	
Recurring Cyber Tests	User Funded Systems Test/Eval	

 | *Decades of Cost Management Excellence*

Trade-Offs by Cloud Model: PaaS

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

Transition

To Be: PaaS
Fee for Svc
Virtual Domain

Analysis:
Metrics
Tools
Methods

Business System - Cyber Specific LCC	As Is Total Cost of Ownership	As Is Total Cost of Ownership (PaaS)
Capital Expenses		
Cybersecurity Integration - Governance and Org	User Funded Program Mgmt (Governance)	
Custom Workload	Workload	Workload
Cybersecurity Services (SW)	User Owned/Managed App SW	Fee for Cloud Hosting of User Owned App SW
Cyber End User Device (HW)	User Owned/Managed App HW	Fee for Clouded Provided Domain Services
Cyber Data	User Owned Data Services	Fee for Clouded Provided Data Services
System Level Technology	Technology	Technology
Dedicated Cyber Comm	User Owned/Managed Comm	Fee for Cloud Provided Platform Services
Infrastructure Services	User Owned/Managed Infrastructure	Fee for Cloud Provided Virtual Capability
Systems Engineering (RMF)	User Funded Systems Engineering	Cloud Provided Systems Engineering
Cyber Test and Evaluation	User Funded Systems Test/Eval	
Operations Expenses		
Cybersecurity Services - Governance and Org	User Funded Program Mgmt (Governance)	
System/Services Operations	Workload Management and Operations	Workload Management and Operations
Cybersecurity Services	Data Center/Corporate Staff	Fee for Cloud Security Service Mgmt and Ops
Cyber Data Services	Data Center/Corporate Staff	Fee for Cloud Data Service Mgmt and Ops
End User Device Support Services	Data Center/Corporate Staff	Fee for Cloud Virtual Domain Mgmt and Ops
Training Services Operations	Data Center/Corporate Staff	Fee for Cloud Virtua Domain Training Svcs
System/Services Mgmt	Technology Management and Operations	Technology Management and Operations
Communications Services	Data Center/Corporate Staff	Fee for Cloud Provided/Managed Comm Svcs
Infrastructure Services	Data Center/Corporate Staff	Fee for Cloud Provided/Managed Infr Services
Cyber SW Maintenace/Modification	SW Maintenance and Modifications	
Managed Services Operations	User Owned/Managed SW Services	
Systems Engineering (RMF)	User Funded Systems Engineering	Cloud Provided Systems Engineering
Recurring Cyber Tests	User Funded Systems Test/Eval	

 | *Decades of Cost Management Excellence*

Trade-Offs by Cloud Model: SaaS

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

Transition

To Be: SaaS
Fee for Svc
Virtual Domain

Analysis:
Metrics
Tools
Methods

Business System - Cyber Specific LCC	As Is Total Cost of Ownership	As Is Total Cost of Ownership (SaaS)
Capital Expenses		
Cybersecurity Integration - Governance and Org	User Funded Program Mgmt (Governance)	Cloud Provided Program Mgmt (Governance)
Custom Workload	Workload	Workload
Cybersecurity Services (SW)	User Owned/Managed App SW	Fee for Cloud Provided/Owned App SW
Cyber End User Device (HW)	User Owned/Managed App HW	Fee for Clouded Provided Domain Services
Cyber Data	User Owned Data Services	Fee for Clouded Provided Data Services
System Level Technology	Technology	Technology
Dedicated Cyber Comm	User Owned/Managed Comm	Fee for Cloud Provided Platform Services
Infrastructure Services	User Owned/Managed Infrastructure	Fee for Cloud Provided Virtual Capability
Systems Engineering (RMF)	User Funded Systems Engineering	Cloud Provided Systems Engineering
Cyber Test and Evaluation	User Funded Systems Test/Eval	Cloud Provided Systems Test/Eval
Operations Expenses		
Cybersecurity Services - Governance and Org	User Funded Program Mgmt (Governance)	Cloud Provided Program Mgmt (Governance)
System/Services Operations	Workload Management and Operations	Workload Management and Operations
Cybersecurity Services	Data Center/Corporate Staff	Fee for Cloud Owned/Managed Cybersecurity
Cyber Data Services	Data Center/Corporate Staff	Fee for Cloud Data Service Mgmt and Ops
End User Device Support Services	Data Center/Corporate Staff	Fee for Cloud Virtual Domain Mgmt and Ops
Training Services Operations	Data Center/Corporate Staff	Fee for Cloud Virtual Domain Training Svcs
System/Services Mgmt	Technology Management and Operations	Technology Management and Operations
Communications Services	Data Center/Corporate Staff	Fee for Cloud Provided/Managed Comm Svcs
Infrastructure Services	Data Center/Corporate Staff	Fee for Cloud Provided/Managed Infr Services
Cyber SW Maintenace/Modification	SW Maintenance and Modifications	SW Maintenance and Modifications
Managed Services Operations	User Owned/Managed SW Services	Fee for Cloud Owned/Managed SW Services
Systems Engineering (RMF)	User Funded Systems Engineering	Cloud Provided Systems Engineering
Recurring Cyber Tests	User Funded Systems Test/Eval	Cloud Provided Systems Test/Eval

 | *Decades of Cost Management Excellence*

Conclusions / Wrap Up

- Cybersecurity related costs are included in a number of places in a system TCO Cost Element Structure: HW, SW, Infrastructure, Governance, Operations/Sustainment/Modifications
- Cost drivers are likely Labor costs for Systems Engineering and Security Management related to Risk Based Management of Cybersecurity requirements for the system's life cycle
- The optimal TCO solution is likely an affordable mix of user owned and managed applications that employ Cloud Infrastructure and Virtual Platforms
  - The User maintains responsibility for the Application Cybersecurity Assessment
  - The Cloud provider accepts responsibility and maintains authority for their Infrastructure and Virtual Domains
- Use of predictive analytics, combined with modeling approaches like CobiT, VAL-IT and cCPI provides a consistent framework to holistically and consistently calculate TCO on a lifecycle basis
- The process is a life cycle team effort supported by the User and by the Cloud Provider

David A. Cass
VP/CISO & Managing Partner, Global Cloud Security Services IBM

Contact:
M: (929) 237 – 6986
E: dcass@us.ibm.com
URL: www.ibm.com

Mr. Cass is the VP/CISO & Managing Partner, Global Cloud Security Services for IBM. He has global responsibility for all aspects of cloud security practices, processes, and policies across the IBM Cloud & Security Services Unit. Mr. Cass serves as a regulatory SME and an Executive Steering committee member for IBM's International Banking Customers. David is an active contributor to the FS-ISAC on Cloud Compliance and Security for financial services firms, and works closely with U.S., and International Regulators.

Previously Mr. Cass served as the SVP & Chief Information Security Officer for Elsevier. Where he lead an organization of experienced legal, risk and security professionals that provided data protection, privacy, security, and risk management guidance on a global basis for Elsevier.

David has extensive experience in IT security, risk assessment, risk management, business continuity and disaster recovery, developing security policies and procedures. He has played a key role in leading and building corporate risk & governance and information security organizations in the financial sector. As the Senior Director of Information Security Risk and Governance for Freddie Mac, David rebuilt the risk and governance function and developed a team to provide risk assessments, methodologies, tools, services, and training to improve the organization's capabilities and maturity. Prior to that he was Vice President of Risk Management for JPMorgan Chase, and was responsible for providing an accurate assessment of the current risk management state, contributing to the future direction of risk management, continuity and disaster recovery capabilities for the organization.

David has a MSE from the University of Pennsylvania, and a MBA from MIT. He is also a frequent speaker at high profile industry conferences, and serves on the Board of Directors for PixarBio Corporation.

 | *Decades of Cost Management Excellence*

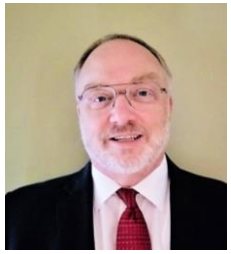
Zachary Jasnoff
VP Professional Services, PRICE Systems

Contact:
M: (856) 912.0974
E: Zachary.jasnoff@pricesystems.com
URL: www.pricesystems.com

Zachary Jasnoff is Vice President, Professional Services for PRICE Systems, LLC. Mr. Jasnoff has over 25 years' experience in Life Cycle Cost estimating on a wide range of defense programs and is an acknowledged expert in Affordability Management. Mr. Jasnoff began his career at the United States Government Accountability Office (GAO) where he was responsible for independent audits and investigations of defense acquisition programs.

Mr. Jasnoff then broadened his career in parametric lifecycle estimating while serving in various positions at Boeing and Lockheed-Martin. At Lockheed-Martin he was responsible for managing the Affordability Analysis group, and was the "Cost as an Independent Variable" (CAIV) author for the Littoral Combat Ship Proposal. Mr. Jasnoff also served as Vice President/Director of Business Resiliency at JPMorganChase. In this position, Mr. Jasnoff managed a staff responsible for developing best practices for measuring resiliency, value-at-risk and Total Cost of Ownership.

He has won several awards from the International Society of Parametric Analysts (ISPA) for various presentations on CAIV and advanced estimating methodologies. Mr. Jasnoff is also a firm believer in lifelong learning and, in August 2006, received his M.S.E in Technology Management from Penn Engineering and The Wharton School at the University of Pennsylvania. While at Wharton, Mr. Jasnoff was part of a team that developed intellectual property for the financial sector in Business Resiliency. He also holds an M.B.A from American University and B.A. from Villanova University



Richard D. Mabe
Solutions Consultant; Price Systems, LLC

Contact:
(856) 651-8567
richard.mabe@pricesystems.com

Mr. Mabe is a Senior Solutions Consultant within the Services Group of Price Systems, LLC. In this role, Mr. Mabe conducts research and develops modeling tools for a variety of programs within the federal government. Mr. Mabe also helps True Planning users develop custom solutions for life cycle cost estimates and other cost analysis products.

Mr. Mabe has over 40 years of experience as an operations analyst, focusing on logistics analysis and cost estimating for the Air Force and other government programs. Prior to his current position with Price Systems, LLC, Mr. Mabe was a Business Area Manager for Quantech Systems, Inc. at Hanscom AFB, managing a team of 20 analysts developing cost estimating products for Air Force C4I, Cyber and Networking system programs. Prior to his work at Quantech, Mr. Mabe was the Technical Advisor for the IT and Electronics Systems Division of the Air Force Cost Analysis Agency (AFCAA), providing cost research, databases and tailored tools to support independent cost estimates of AF acquisition programs. Mr. Mabe also supported several AF and DOD working groups focused on methods to apply industry best practices for SW development, cybersecurity and C4I systems integration to DOD programs.

Prior to working for AFCAA, Mr. Mabe provided cost estimating and cost analysis support to multiple C4I, Cyber and Networking programs at Hanscom AFB, MA, - for 2 years as a PEO level Cost Chief, and for 13 years as a Technical Expert for Tecolote Research, Inc. Many of these were Joint Service programs, sharing systems and equipment with Army and Navy C4I programs. Prior to working at Tecolote, Mr. Mabe spent 6 years with TASC in Reading, MA managing a team of systems engineers and logistics analysts developing readiness based supply and logistics models for the Air Force. Prior to TASC, Mr. Mabe was an Air Force supply and logistics officer, providing hands-on support to Air Force operations in the CONUS and in USAFE. He completed his active Air Force duties by serving as an Assistant Professor for Inventory Management at the Air Force Institute of Technology.

Mr. Mabe holds a BS Degree in Geology from Boise State University, and an MS in Logistics Management from AFIT. He received a Level 3 DAWIA certification in Business-Cost Estimating, and also a Level 3 DOD Financial Management certification in Cost. He is a recipient of the AF Outstanding Civilian Career Service Award.

Back-Up Slides

Evaluating the Cost Trade-Offs

- Predictive Analytics
  - Encompasses a variety of statistical techniques from modeling, machine learning, and data mining that analyze current and historical facts to make predictions about future, or otherwise unknown, events (Wikipedia 2015)
- Applied to Cloud Workloads – Industry Focus
  - Must take into account control requirements , technical issues and business risks (*Control Objectives for Information and Related Technology) (**CobiT**)*
  - Must take into account governance best practices for information technology-enabled business investments. *(value from IT investments) **VAL** IT*
- Best Practices – Cloud Workload Optimization Framework
  - Frameworks such as CobiT 5.0 and Val-IT 2.0 aligns IT Strategy to Business Strategy within a compliance, governance, operational risk management context
  - Extending CAIV best practices is a useful framework applied to cloud workloads.
  - Takes into account both TCO and Workload Performance Objectives and Threshold

Considerations using COBIT

In building an cloud workload optimization framework, it is important to select the aspects of CobiT that addresses the key elements of cloud workload optimization

- Minimizing service interruptions / continuous service
- Moving to cloud must insure availability and recoverability

- CobiT DS4 Ensure Continuous Service
  - The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilizing offsite backup storage and providing periodic continuity plan training.
  - An effective continuous service process minimizes the probability and impact of a major IT service interruption on key business functions and processes.

See more at: http://www.itgovernanceblog.com/ds4-ensure-continuous-service-250.htm#sthash.qH4Jf6Ar.dpuf

Considerations using VAL-IT

In building an cloud workload optimization framework, it is important to select the aspects of VAL-IT that addresses the key elements of cloud workload optimization

- Evaluate TCO over the full life cycle

- IM4 Develop full life-cycle costs and benefits.
  - Prepare a program budget based on full economic life-cycle costs. List all intermediate and business benefits in a benefits
  - Register, and plan how they will be realized. Identify and document targets for key outcomes to be achieved, including the
  - Method for measuring and the approach for mitigating non-achievement. Submit budgets, costs, benefits and associated plans for review, refinement and sign-off.

Importance of Understanding Difference between life cycle costs between Cloud and Traditional Approaches

