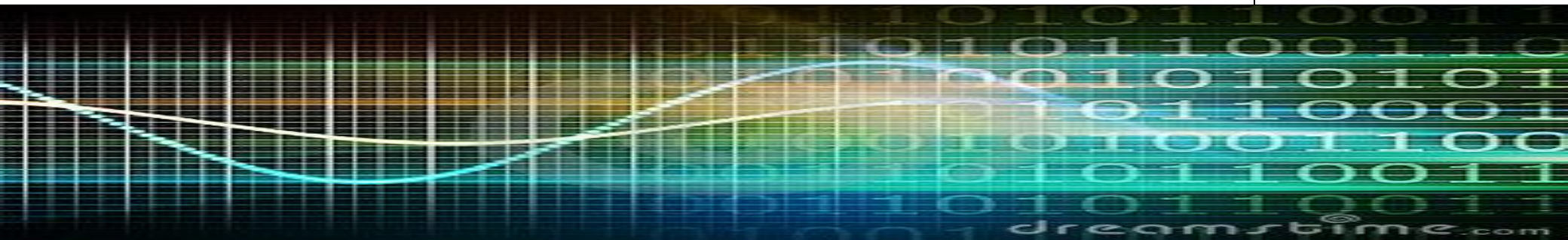


Roadmap for IT Modernization and Cyber Resilience



SEI Software Solutions Symposium 2017

- Dr. Ken Nidiffer, SEI, Moderator
- Robert Babiskin, JIE Chief Engineer/CTO Interop.
Clearinghouse Don Davidson, SL, OSD ATL
- Clarke Ansel, ITIL Foundations| Principal Analyst | IT-
AAC Fellow





Assuring IT Enabled Outcomes

exposing innovations & standards of Global IT market



❖ IT-AAC 501c3

- ✓ Consortia of Standards Bodies, Academia, Think Tanks and Non-Defense COIs.
- ✓ Greybeard Council
- ✓ Focus on sharing Commercial IT best practices and lessons learned
- ✓ Conduit to reaching over 20k innovative companies
- ✓ Reach core of \$3.77 Trillion Global IT Market
- ✓ Critical source for Open Architectures and Standards; SDN, SOA, Cloud, IA, Mobile, ITIL/COBIT, Internet of Things

❖ Interop. ClearingHouse (ICH)

- ✓ DOD Chartered research institute
- ✓ Focus on measures and metrics for **interoperability, security, service levels, commerciality & risk.**
- ✓ Resource for mentoring government transformation efforts
- ✓ Proven maturity model for Agile Acquisition, Tech Assessment and Business Case Analysis
- ✓ Superior source for risk based decision making
- ✓ Conflict free, no rice bowls



IT-AAC Communities of Practice

reaching over 108k innovators



IT - AAC Partners	Agile Methods	IT/Cloud Standards	Innovation Access	IT Risk Mgt	Industry Best Practices	Pilots & Contracts	IT Policy & Governance	Number of Companies (SMEs)
Aerospace Industry Association (AIA)			✓		✓		✓	325+
Open Network Foundation (ONF)					✓		✓	150+
Cloud Security Alliance (CSA)		✓	✓		✓	✓		48,000
Cloud Standards Customer Council (CSCC)	✓	✓			✓		✓	750+
Interoperability Clearinghouse (ICH)	✓		✓	✓	✓			360 SMEs
Intern'l Information Systems Security Certification Consortium (ISC2)		✓			✓			80,000+
Information Systems and Security Group (ISSA)		✓			✓		✓	10,000+
Object Management Group Industrial Internet Consortia	✓	✓	✓	✓	✓		✓	800+ 250+
AFCEA Ft Belvoir Chapter			✓	✓	✓	✓	✓	1,600+
IDC/IDG					✓		✓	1,100 SMEs
Consortium for IT SW Quality (CISQ)			✓	✓	✓	✓		600+
Telecommunication Industry Association (TIA)		✓	✓		✓		✓	290+
Financial Services Roundtable FS Round + FSTC)	✓		✓	✓	✓	✓	✓	100+



IT-AAC's Research Approach ***to Reforming and Assuring IT & Cyber***



- ☑ Repurposed over 40 existing body of evidence; DSB, DBB, BENS, GAO, HASC, CRS, NDIA, ACT/IAC, NAS, AF-SAB
- ☑ Recruited the best, most experienced thought leaders
- ☑ Partnered with over 20 leading industry COIs, avoid vested interests/status quo (SDOs, NGOs, EDUs)
- ☑ Conducted 60+ Leadership Workshops, reaching 3,000+
- ☑ Supported a dozen successful Agile Acquisition Pilots,...
proving that there is a better way to acquire time sensitive IT/Cyber Capabilities



State of Defense IT Acquisition

"a national security threat if not reformed"



Acquisition Lifecycle

- Long acquisition cycle-times
- Successive layers ... built over years
 - Limited flexibility and agility
- Risk Management is Deficient

Requirements

- Understanding and prioritizing requirements
- Ineffective role and comm in acquisitions

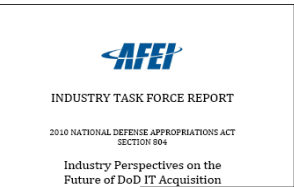
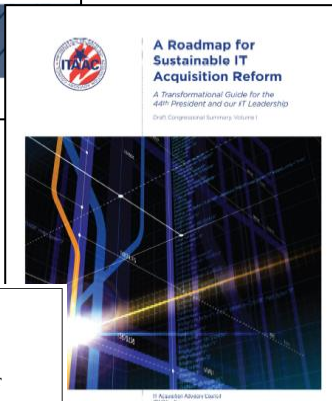
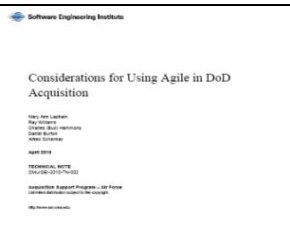
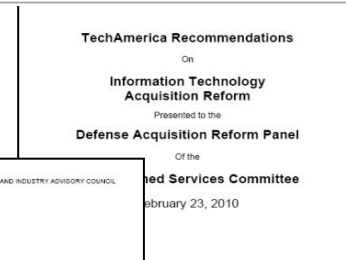
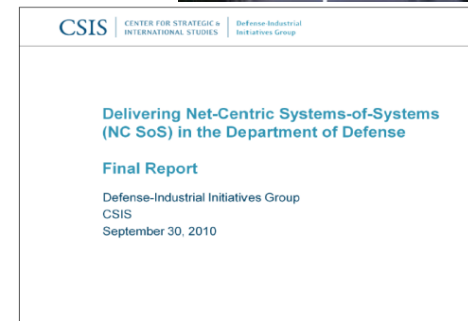
Test/Evaluation

- Testing is integrated too late and serially
 - Lack of automated testing

Funding & Governance

- Program-centric, not capability-centric
 - Overlapping decision layers (e.g., multiple review processes)
 - Lack of customer-driven metrics
- Funding inflexibility & negative incentives

"The inability to effectively acquire information technology systems is critical to national security. Thus, the many challenges surrounding information technology must be addressed if DOD is to remain a military leader in the future. The development of a new acquisition process, coupled with clear roles and responsibilities of key decision makers, and an experienced leadership and workforce, are important elements of the solution." Defense Science Board Report to Congress





Defense “Board” Conclusions

“ a national security threat if not addressed” DSB



HASC Defense Acquisition Panel 2010

- Only 16% of IT projects are completed on time and on budget.
- 31% are cancelled before completion.
- The remaining 53% are late and over budget, with the typical cost growth exceeding the original budget more than 89%.
- Of the IT projects that are completed, the final product contains only 61% of the originally specified features

Defense Business Board 2010: Current system hurts effective mission operations

- Architecture makes it nearly impossible to share critical data on a timely basis
- Proprietary systems and closed architecture make in-theatre upgrades difficult
- Lack of common standards make collaboration difficult
- Lack of portable ID forces individuals to be 'reinvented' with every change
- *Weak These are the final briefing slides as approved by the Defense*
- *Business Board in the public meeting held January 19, 2012.**
- Security creates need for more enclaves and dedicated networks

Defense Science Board 2009: Fixing the Defense IT Acquisition Process is a matter of national security

- Step back and figure out “what to buy” before focusing on the process of how to buy
- A “few good people” can help make the right decision and move on.
- The change order process is so common, it ensures contractors to bid low and plan to make money on the inevitable change orders
- Change the concept of “requirements” to “capabilities”



Unmet Congressional Directives

a forcing function needed to drive change



- ◆ **2010 NDAA Sec 804:** *“The Secretary of Defense shall develop and implement a new <agile> acquisition process for information technology systems. The acquisition process developed and implemented pursuant to this subsection shall, to the extent determined appropriate by the Secretary--*
 - *be designed to include– 1) early and continual involvement of the user; 2) multiple, rapidly executed increments or releases of capability; 3) early, successive prototyping to support an evolutionary approach; and 4) a modular, open-systems approach”*

- ◆ **2011 NDAA Sec 933:** *“ The Secretary of Defense, in consultation with the Secretaries of the military departments, shall develop a strategy to provide for the rapid acquisition of tools, applications, and other capabilities for cyber warfare for the United States Cyber Command and the cyber operations components of the military departments.*

- ◆ **2012 NDAA:** *"Migration of Defense data and government-provided services from Department-owned and operated data centers to cloud computing services generally available within the private sector that provide a better capability at a lower cost with the same or greater degree of security."*

- ◆ **2015 NDAA/FITARA:** *One of the requirements would be that the government develop a streamlined plan for its acquisitions.[2] The bill would increase the power of existing Chief Information Officers (CIO) within federal agencies so that they could be more effective.[3] Each agency would also be reduced to having only one CIO in the agency, who is then responsible for the success and failure of all IT projects in that agency.[4] The bill would also require the federal government to make use of private sector best practices.[3] The bill is intended to reduce IT procurement related waste.[5]*

- ◆ **2016 NDAA Agility in Acquisition Act:** *The bill would require all components conform to open interfaces in order to plug into the overall system. Module Open Systems Architecture (MOSA) will be based on consensus based standards (vs Milspec), and apply Evidenced Based Decision Making (a cornerstone of the Acquisition Assurance Method or AAM)*

Recommendations for Speeding IT Modernization and Cyber Resilience

What OMB, Congress and Industry Groups have concluded:

1. **INDUSTRIAL AGE IT ACQUISITION & ENGINEERING METHODS:** Waterfall design to spec frameworks (DODAF, JCIDS, LISI, NESI) obscures value of commercial IT standards and solution sets. Current approach results in 80% failure rates and significant cost overruns leading to FITARA.
2. **ILL-EQUIPED IT ACQUISITION ECOSYSTEM:** Government PMs and Acquisition Core lack expertise, experience and knowledge to deal with emerging Cyber Threats.
3. **DECISION AVOIDANCE vs RISK MGT :** Agencies lack mature Risk Based Decision Analytics Frameworks needed to model risks and guide modernization of legacy stove pipes. Emerging standards of practice are key to change.
4. **BARRIERS TO IT INNOVATIONS and BEST PRACTICES:** Decision makers lack access to commercial standards and innovations that drive a \$3.9 Trillion dollar global IT Market (of which the DIB represents less than ½ of 1%). This gap has lead to creation of Federal Innovation Labs (DHS, DIA, DoC, AF)



FITARA Scorecard

- ✓ Measurement and discussion in governance committees goes a long way to setting behavior
- ✓ You can only manage what you measure. Codify Gate controls that measure risk/value



Transform Acquisition Policy

- ✓ Transform IT Acquisition that enable continuous measurements of risk/value
- ✓ Require vendors to provide CISQ scores/certificate for each release
- ✓ Streamline processes that Mission Driven, Evidenced Based, and Agile



Service Level Management

- ✓ SLAs that treat software enhancements and maintenance as a service; track levels, penalties, credits
- ✓ Align SLAs with Mission Outcomes and Incentives



Acceptance criteria

- ✓ Measure and demand minimal set of acceptance criteria for any new development or modernized systems
- ✓ Modernize IT Infrastructure Services based on commercial design patterns (14 SOA Services)

Scorecard the Service Providers

Outsourcer	TQI	Reliability	Performance Efficiency	Security	Maintainability
VENDOR 1	2.59	3.16	2.34	3.01	1.99
VENDOR 2	2.81	2.78	2.78	3.12	2.34
VENDOR 3	2.59	1.67	3.54	2.98	1.76
VENDOR 4	3.06	3.12	3.11	2.79	3.11
VENDOR 5	2.83	2.56	2.88	3.03	2.56
VENDOR 6	2.90	3.76	2.89	2.97	2.55

Monitor Performance Over Time

TECHNICAL CODE QUALITY

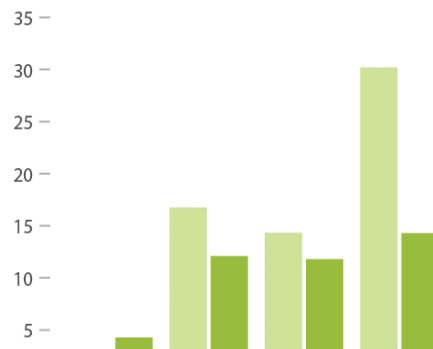
AVERAGE TQI
FEBRUARY 2012-JUNE 2014



Mean Time to Repair

QUALITY

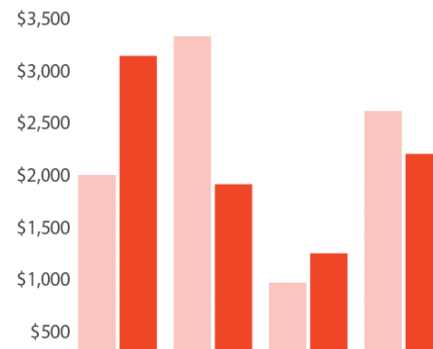
PRE-PRODUCTION
FEBRUARY 2012-JUNE 2014



Productivity

COST EFFECTIVENESS

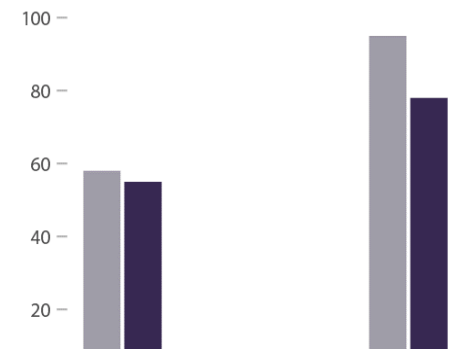
COST PER FUNCTION POINT / ENHANCEMENT
FEBRUARY 2012-JUNE 2014



Productivity

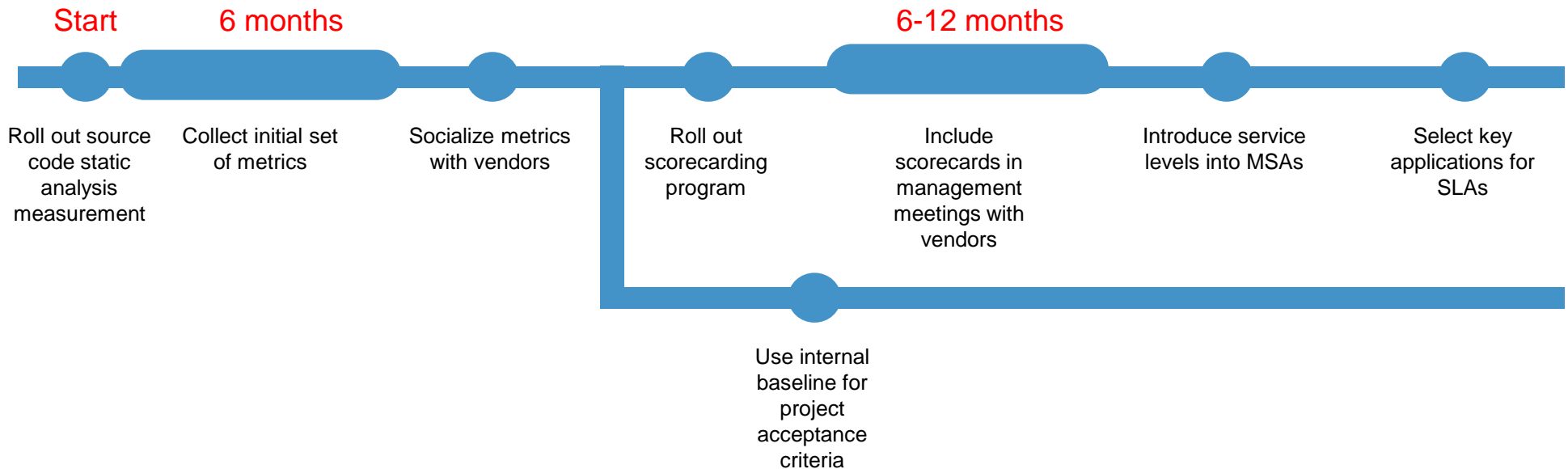
COST EFFECTIVENESS

COST PER FUNCTION POINT / MAINTAINED
FEBRUARY 2012-JUNE 2014



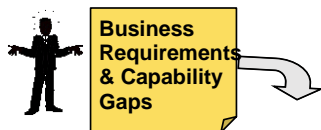
- Establish Evidenced Based COTS/OSS Assessment Processes
- Ensure you have access to vendor-delivered code
- Let your key sourcing partners know you're using CISQ and AAM analytics
- Partner with the IT-AAC and CISQ to introduce software analytics into contractual relationships

POTENTIAL DEPLOYMENT ROADMAP

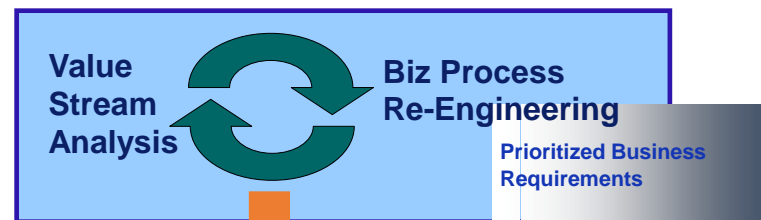


Acquisition Assurance Method (AAM)

Agile Acquisition Framework for Assured Outcomes



- Phase 1**
- Mission Needs: Value Stream Analysis:**
- Problem ID
 - Mission Rqts
 - Prioritization
 - Constraints
- Phase 2**
- Performance Management Assessment**
- Feasibility
 - Service Attributes
 - SLAs
 - Shared Services
- Phase 3**
- Solution Architecture Modeling:**
- Selection
 - Certification
 - Interop Spec
 - Openness



Measurable Outcomes
Business Metrics



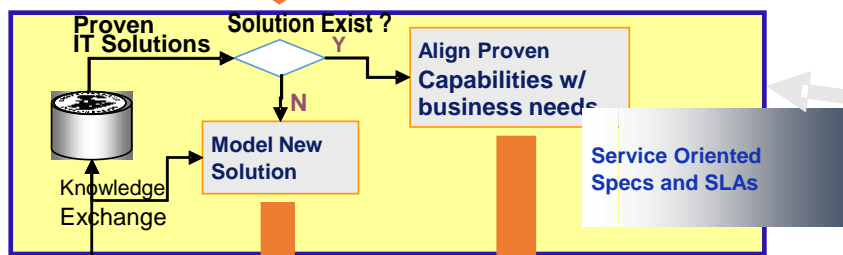
IT-AAC Communities of Practice



Evidence
Lessons Learned

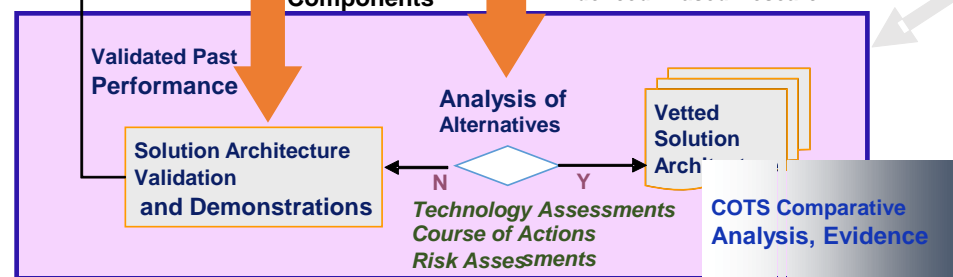
Innovations

Research,
Testing Results



Normalized SVC
Components

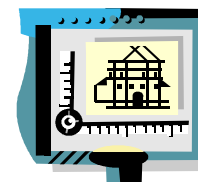
Solution Set
Evidenced -Based Research



Technology Assessments
Course of Actions
Risk Assessments

COTS Comparative
Analysis, Evidence

Validated Acquisition Strategy,
SLAs & Source Selection Criteria

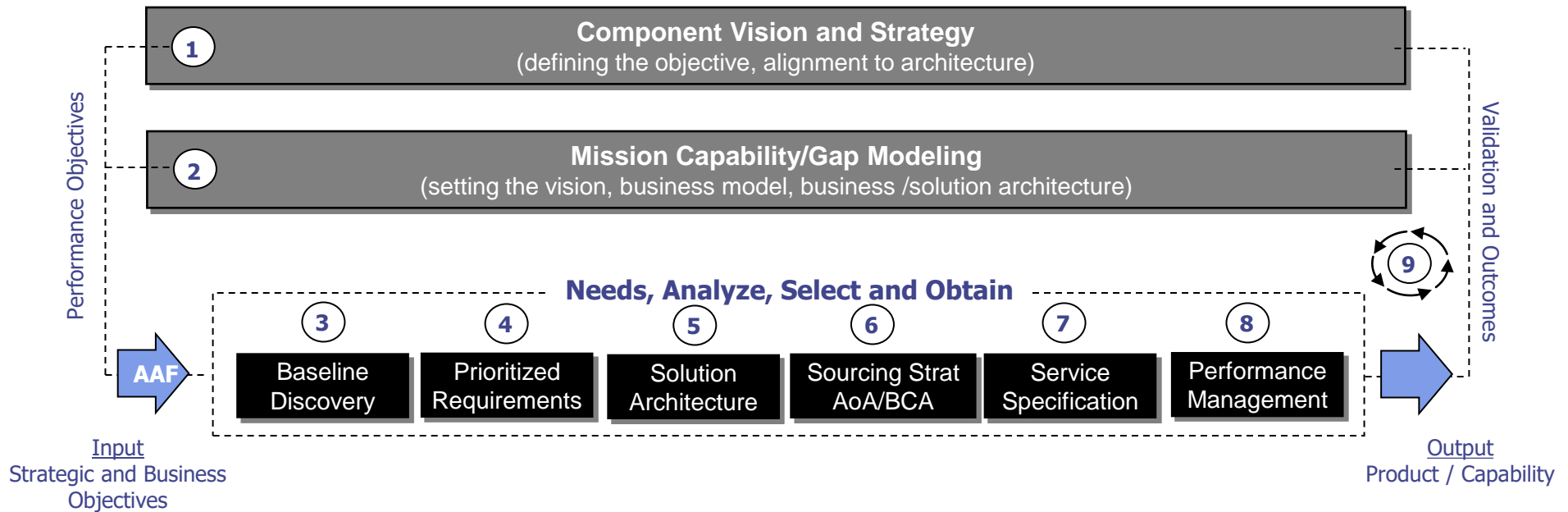


AAM Tools

Problem Statement	Capability Analysis	Solution Determination	Capability Prioritization	Feasibility Assessment	Economic Analysis	Roadmap	Risk Dashboard Assessment
-------------------	---------------------	------------------------	---------------------------	------------------------	-------------------	---------	---------------------------

An Agile Acquisition “Ecosystem” must consider needs of all stakeholders, and that IT comes in many forms

Pre-Acquisition Activities



Activities 4-7 become optional for several IT swim lanes including;

- Baseline Modernization
- Tech Insertion (taking advantage of new tech/upgrades)
- Reuse of existing service offering (E-Gov)
- Commodities; Desktop, Mobile, Storage, Networks, etc.

AAM's Fact Based & Data Driven Decision Analytics

Problem Statement

Mission Capability	No	High Level Capability
2	1	Reduce time to deploy infrastructure
1	2	Reduce infrastructure cost
1	3	Improve Reliability, Availability Survivability (RAS)
4	4	Work within current Security Management Posture
		Provide support for AF Use Cases
1	6	Support SBC storage strategy
2	7	Support Infrastructure Requirements
1	8	Improved Manageability
1	9	Provide the same user experience (irrespective of client; rich or thin client).

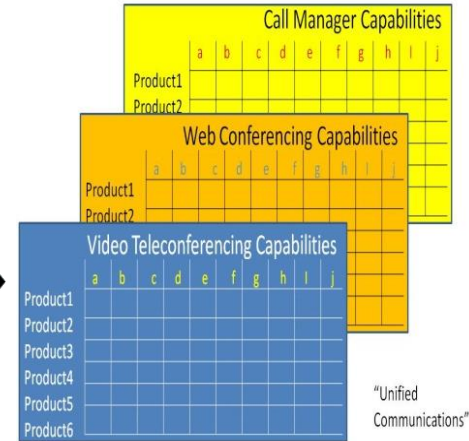
Builds On

Prioritized Capabilities

5e	Provide support for client type - Remote
5f	Provide support for client type - Unmanaged
125 6	Support SBC storage strategy
6a	Provide server-side storage of System data and/or system images
6b	Provide server-side storage of enterprise data
6c	Provide server-side storage of user data and/or system images
6d	Provide server-side storage of user application
6e	Provide server-side storage of enterprise data application
125 7	Support Infrastructure Requirements
7a	Maintain current bandwidth/network loads (min 10 GB to max 100GB user profiles, 100 MB to the desktop)
7b	Provide consistent capability, whether rich or thin, with differing capabilities based on Active Directory rights/groups
7d	Provide support for the Common Access Card (CAC)/DOD Public Key Infrastructure (PKI) logon
150 8	Improved Manageability
8a	Provide for remote manageability of desktop
8b	Provide support for all business and mission applications, including bandwidth sensitive applications
8c	Provide for a client computing environment solution that scales over the AF enterprise
8d	Allow use of a diverse mix of hardware end devices in a heterogeneous environment
8e	Increase IT service availability to the mobile/pervasive user
150 9	Provide the same user experience (irrespective of client; rich or thin client).

Builds On

Solution Determination Alternatives



Feasibility Assessments & Management Risks

Economic Analysis/TCO/ROI Tradeoff

Road Map

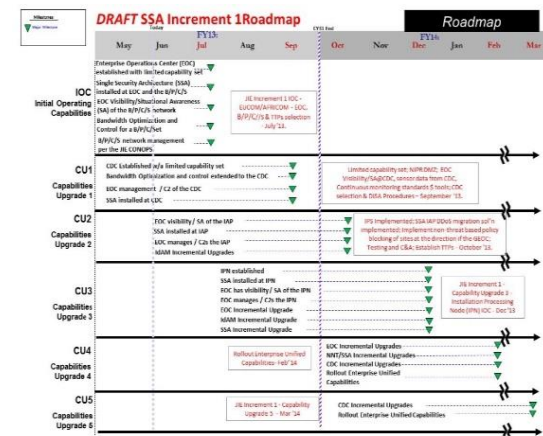
Value Factors	15%	15%	5%	5%	5%	13%	13%	15%	15%	Score
Reduce time to deploy infrastructure	1.67	3.00	3.40	1.50	0.75	1.40	1.00	1.56	1.00	1.67
Reduce infrastructure cost	2.33	3.15	3.40	3.00	1.53	1.40	1.33	2.11	2.00	2.28
Improve Reliability, Availability Survivability (RAS)	1.67	2.23	1.30	2.50	2.07	1.40	2.28	4.00	4.00	2.48
Work within current Security Management Posture	1.00	1.92	1.30	1.50	2.80	1.00	2.33	4.22	5.00	2.67
Provide support for AF Use Cases	1.67	2.23	1.30	2.50	2.07	1.40	2.00	2.78	4.00	2.88
Support SBC storage strategy	1.00	1.92	1.30	1.50	2.80	1.00	2.33	4.22	5.00	3.08
Support Infrastructure Requirements										
Improved Manageability										
Provide the same user experience (irrespective of client; rich or thin client).										

Overall Score on each Product

Blue = Essential	1-1.00
Green = Desirable	2-2.99
Yellow = Less Desirable	3-3.99
Red = Unacceptable	4-5.00

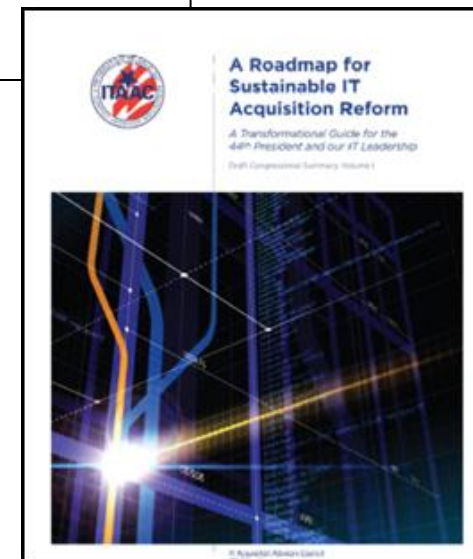
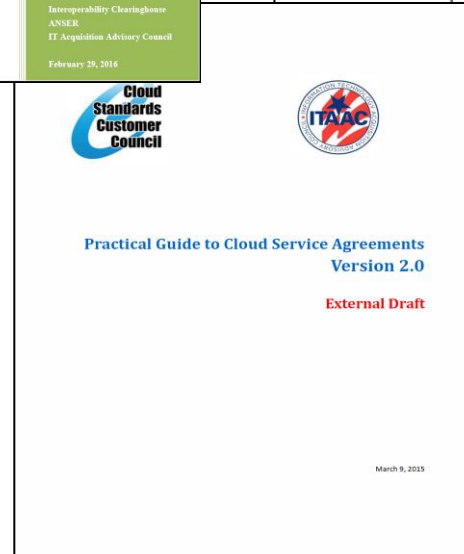
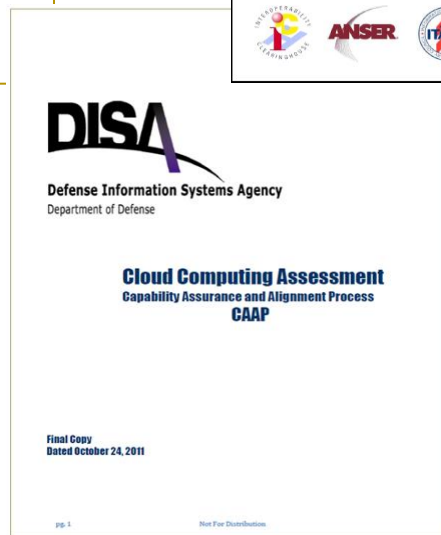
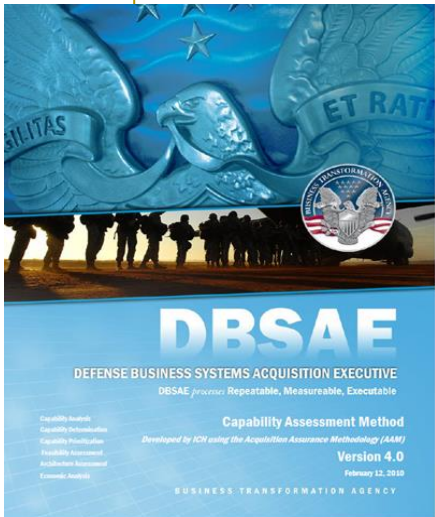
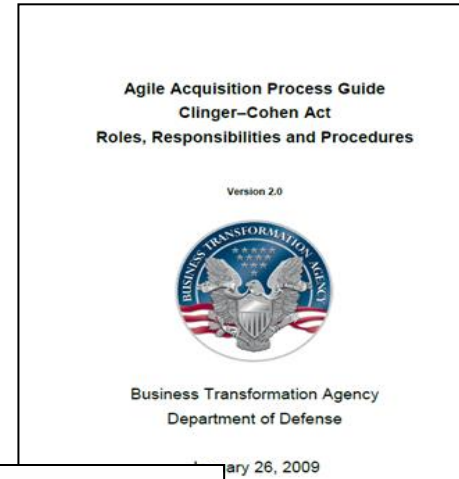
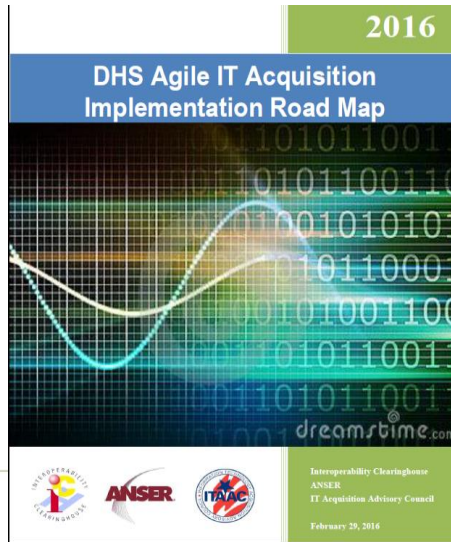
Units	250,000		
	Unmanaged PC	Managed PC	Thin Client
Direct Cost - 1 Unit	\$ 500	\$ 500	\$ 300
Direct Cost - 250K Unit	\$ 125,000,000	\$ 125,000,000	\$ 75,000,000
In-Direct Cost - 250K Unit	\$ 125,000,000	\$ 60,000,000	\$ 24,500,000
Migration Costs	\$ -	\$ -	\$ 24,500,000
TCO	\$ 420,500,000	\$ 289,250,000	\$ 147,720,000
per SBC	\$ 2,500	\$ 1,613	\$ 885

Investment
Return
TCO





Leverage Proven Processes ICH's Agile Mgt & Acquisition Playbooks





Past Performance = Assured Outcomes

Where AAM and IT-AAC have proven: better, faster, cheaper



<p>Navy: Assessment of AFLOAT Program – CANES SOA & Security Strategy Contact Value: \$350k Eliminated hi-risk Requirements by 23%, \$100Ms in potential savings</p>	<p>USAF: Streamlined COTS Acquisition Process. Applied to Server Virtualization. Contact Value: \$500k Established optimal arch with ROI of 450% & \$458 million savings</p>	<p>AFISRA: Applied AAM to conduct ISR Portfolio Risk Assessment (PRA) Contact Value: \$500K Guiding reorganization and restructure of ISR Portfolio</p>
<p>DISA CAE: DISN GSM-O Recompete Restructured performance metrics, acquisition strategy and SLAs to enable 30% savings on existing DISN Mgt Greatly Exceeded Forecasted Saving in both analysis and acquisition</p>	<p>GSA CFO: Financial Mgt System consolidation using AAM. Contact Value: \$500k Moved GSA FMS from OMB “red” to “green”. Eliminated duplicative investments that saved \$200M</p>	<p>BTA DBSAE: Transformed DOD’s Requirements and Agile process, with 2 successful pilots Contact Value: \$800k \$300 million in potential savings with minimal investment</p>
<p>Discovery Channel: Apply AAM to complete AoA and BCA for Enterprise Web Services/Tactical Cloud Contact Value: \$330k Provided actionable roadmap for world wide multi-media web services</p>	<p>GPO: Developed Acquisition Strategy for Future Digital System FDSys Contact Value: \$150k Led to successful acquisition and implementation on time, on budget and 80% cheaper than NARA RMS</p>	<p>DHS CIO: Agile Acquisition Roadmap Applying AAM to comply with NDAA/FITARA IT Reform Directives Partnered with DHS FFRDC to shift DHS away from failed weapon systems approach to IT acquisition</p>

“we believe that it is necessary to develop a comprehensive set of metrics to give transparency to program execution, avoid subjective judgment, and avoid the wasting of time in both executing commands and in oversight offices. This is consistent with the fundamental recommendations of the Packard Commission and Secretary Robert Gates’s initiative to eliminate inefficiency and waste.” PARCA-RAND Root Cause Analysis of Nunn-McCurdy Breaches



Case Study: Streamlining the DoD's IT Acquisition for Infrastructure



Challenge: Establish OSD BTA's Agile Acquisition Method for IT Infrastructure (SOA)

- ◆ Applied ICH's Acquisition Assurance Method (AAM) standard
 - Developed IT Business Systems lifecycle entry/exit criteria for great transparency
 - Established enhanced Clinger Cohen Act process guide for OSD BTA CIO
 - Developed Value Chain Capability Assessment Methodology (CAM)
 - Established IT Acquisition Advisory Council to overcome cultural impediments.
- ◆ Outcomes; IT Acquisition Reform we can believe in
 - Complemented Business Capability Lifecycle (BCL), providing analytical tools for framing decisions
 - Enabled actionable Clinger Cohen Act compliance that goes beyond check list
 - Enabled Component Acquisition Executive with means of judging business value of IT investments
 - Provided OSD BTA with alternative approach to DoD weapons systems style processes
 - Used to conduct Pre-milestone B "Hosting" AoA and Business Case Analysis in just 4 months. Projected Savings = \$350M over 5 years.

Office of the Secretary of Defense, DCIO (2001) *"Since the value of the ICH to our programs increases rapidly through results sharing, we encourage the defense community and IT industry to participate directly in the public service initiative in terms of sponsorship and lessons learned"*





Case Study: Streamlining the IT Acquisition process SAF CIO/AQ; AF Solution Assessment Process (ASAP)



Challenge: Establish a common and repeatable AF Wide COTS assessment/acquisition process

- ◆ **Integrated ICH Architecture Assurance Method into all major AF IT components**
 - Developed root cause of analysis of current weaknesses and deficiencies
 - Identified and integrated both AF and industry best practices into a common framework
 - Developed series of templates and input/exist criteria for each stage of the SDLC process
- ◆ **Outcomes: Increased traceability from requirements to acquisition, reducing “thrashii**
 - Provided a common, enterprise wide process designed for leveraging COTS
 - Augmented architecture process to address legacy and COTS capabilities
 - Reduce market research and analysis in a fraction of the cost and time by leveraging existing expertise and lessons learned of the market
 - Provided mechanisms for forcing adoption of 80% solution.



“We have put to practice the AF Solution Assessment Process (ASAP) at the Air Force Communications Agency (AFCA) with some well documented success. It was developed with Interoperability Clearinghouse (ICH) and provides a structured and measurable IT assessment process with the agility to provide decision-quality assessments ranging from quick-looks to more in-depth capability-focused technology assessments and lightweight business case analysis.” General Mike Peterson, AF CIO



Case Study: Validating SOA and Cross Domain Solutions Navy PMW 160 Consolidated Afloat Network Enterprise (CANES)



Challenge: Establish an enterprise ship board SOA infrastructure for all shipboard legacy systems

- ◆ **Establish an actionable solution architecture that leverages SOA & COTS implementation best practices**
 - Provide a standardized Solution Assessment Methodology to leverage best practices and mitigate deployment risk (compliment NESI).
 - Establishes a Solution Architecture standard and public/private research partnership that maximizes use of commercial trends (COTS/Open Source solutions) via an actionable Open Architecture (OA)
 - Enable Capability Based Acquisitions. Reveal Gaps in both requirement and industry offerings (define realm of the possible).
 - Establish SOA performance metrics and SLAs that reflect real world limitations and hold suppliers accountable.

- ◆ **Outcomes of ICH engagement (reduced requirements over specification by 23%);**
 - Proved out as a **standardized** IT Assessment & Solution Architecture process that will mitigate deployment risk.
 - AAM assessment products used:
 - Capability Determination and Metrics
 - Service Component Prioritization and Alignment and
 - Feasibility/Risk Assessment
 - Demonstrated the feasibility and viability of using GOTS/COTS/Open Source products within the CANES Architecture
 - Demonstrated a method and a plan to:
 - Assess SOA Service Components for CANES
 - Assess migration to Netcentric “need-to-share” systems
 - Produced a large body of artifacts that are important for the architecture phase





Case Study: World Largest Healthcare Agency OSD HA's Government Wide e-Healthcare program



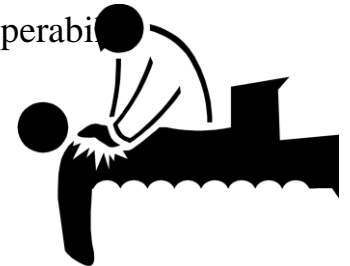
Challenge: Defense Agile Acquisition Framework & SOA E.H.R. Best Practices Guidance

Established Section 804 Agile Acquisition Framework for E.H.R Way Forward

- Developed source selection criteria for TMA Program Office
- Benchmarked SOA/Cloud Industry Best Practices and Lessons Learned with support from 10 Fortune 100 companies
- Built out a proven Agile Framework fully vetted by BTA (Acquisition Assurance Method)

Outcomes: Established SOA Roadmap that addressed stake holder needs

- Enabled award based on unambiguous design specs
- Augmented architecture process to address legacy and COTS SOA/ESB capabilities
- Was able to cycle through market research and analysis in a fraction of the cost and time of traditional efforts.
- Ensured viability of Solution Architecture in terms of; meeting HIPPA, security, and interoperability requirements



“The ICH repository data and analysis methodologies was very helpful in supporting a quick turn around for [Information Assurance] section of COTS security products. Highly detailed ICH technology domain and product evaluation data comprised over 60% of this urgently needed [architecture] report”. Northrop Grumman on ICH's support of their successful GCPR Pilot