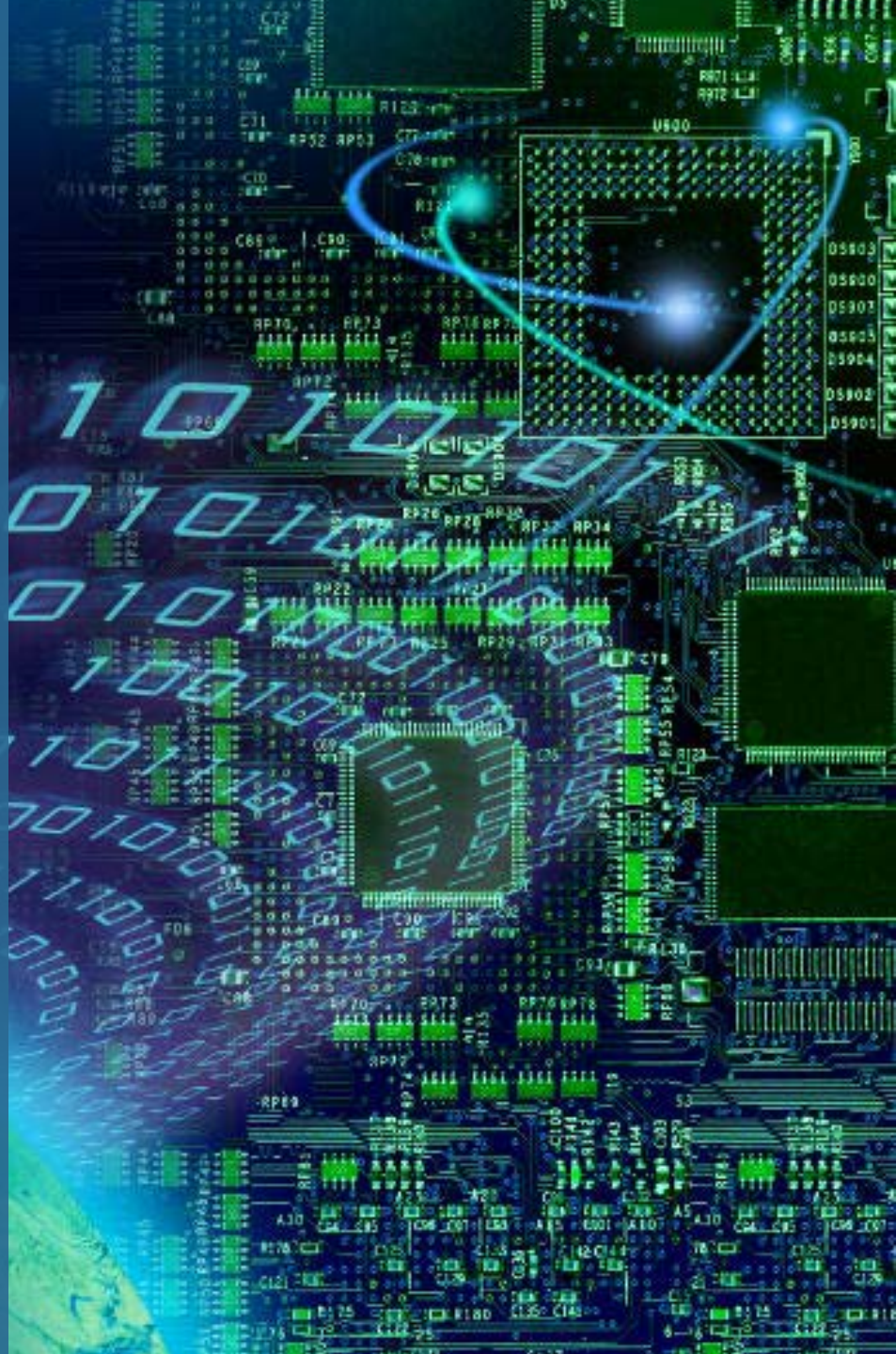
Cyber Resilience Summit
March 21, 2017
Handout



Consortium for IT Software Quality (CISQ)

- ✓ OMG® Managed Consensus Standards Body
- ✓ Adopted Top CWE and CVE identified by DHS, MITRE, SEI, DOD and NIST
- ✓ Set up to automate and assure s/w code quality and cyber assessments
- ✓ Proven model adopted by leading financial institutions, FFRDCs, and Federal Contractors
- ✓ Leading standard body IT S/W Quality and Risk Management

IT Acquisition Advisory Council (IT-AAC)

- ✓ Consortia of 22 Standards Bodies, Academia, Think Tanks and Non-Defense COIs.
- ✓ Leading architect of FITARA/NDAA Section 804
- ✓ Direct Conduit to Commercial IT best practices, innovations and lessons learned
- ✓ Just-in-Time SMEs close the knowledge and expertise gap
- ✓ Leading advocate for Agile Acquisition Maturity Model
- ✓ Critical source applied standards; Cyber, SDN, SOA, Cloud, IA, Mobile, ITIL/COBIT, Internet of Things

Cyber Resilience CSF

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 are 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)

CISQ
Consortium for IT Software Quality

State of Federal IT

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)

State of Federal IT/Cyber Ecosystem

CISQ Consortium for IT Software Quality

ITAAC Information Technology Advisory Council

IT Acquisition

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

Requirements

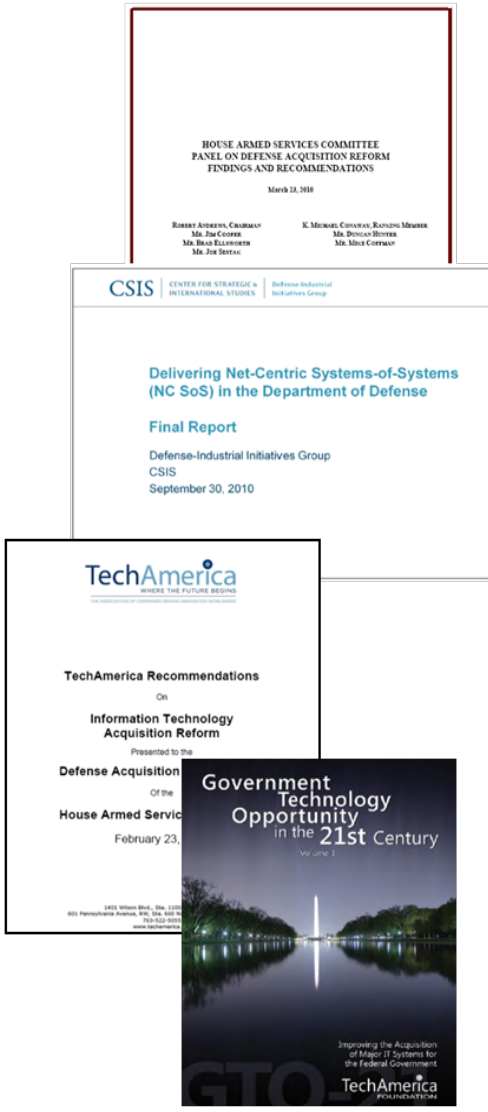
- Understanding and prioritizing IA/Cyber requirements
- Ineffective communications across SDLC

Test/Evaluation

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

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

Acquisition Assurance Method

CISQ Consortium for IT Software Quality

ITAAC

AAM Process

Business Requirements & Capability Gaps

Phase 1

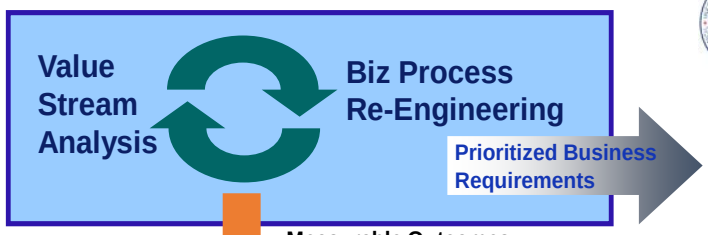
Mission Needs: Value Stream Analysis:
- Problem ID
- Mission Rqts
- Prioritization
- Constraints

Phase 2

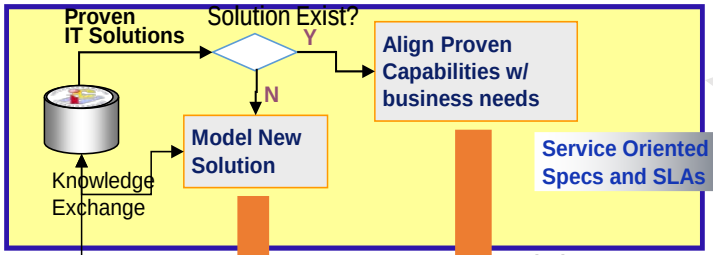
Performance Management Assessment
- Feasibility
- Service Attributes
- SLAs
- Shared Services

Phase 3

Solution Architecture Modeling:
- Selection
- Certification
- Interop Spec
- Openness

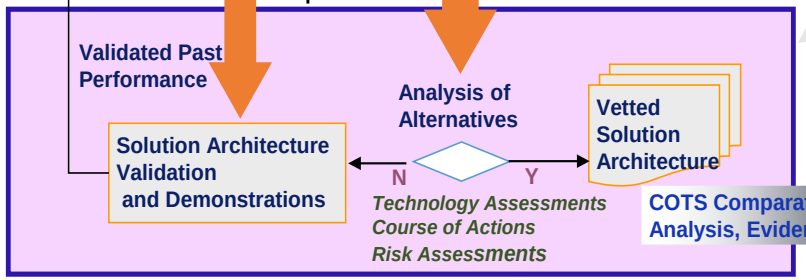


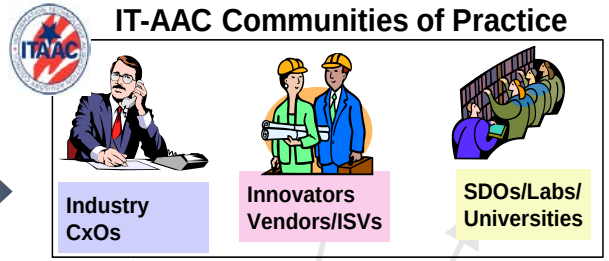
Measurable Outcomes
Business Metrics



Normalized SVC Components

Solution Set Evidenced-Based Research



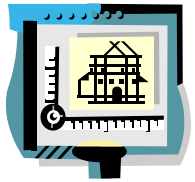


Evidence Lessons Learned

Innovations

Research, Testing Results

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

Acquisition Assurance Method

An Incremental Approach to IT Acquisition

Strategic Business Rqt's

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

Functional Capabilities

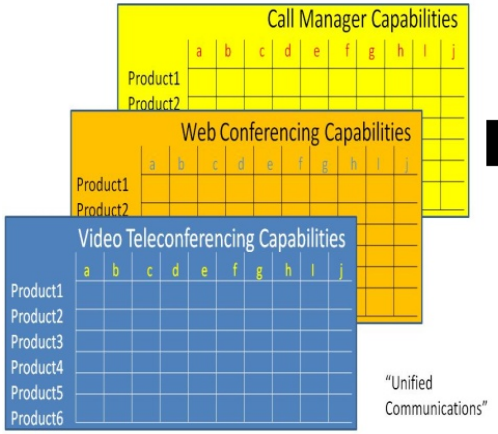
	5e	*Provide support for client type – Remote*
	5f	Provide support for client type – Unmanaged
125	6	**Support SBC storage strategy**
	6a	Provide server-side storage of System data and/or system images
	6b	Provide server-side storage of enterprise data
	6c	Provide server-side storage of user data and/or 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 bas 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

Capability Prioritization

	5e	*Provide support for client type – Remote*	*3*
	5f	Provide support for client type – Unmanaged	5
125	6	**Support SBC storage strategy**	
	6a	Provide server-side storage of System data and/or system images	1
	6b	Provide server-side storage of enterprise data	1
	6c	Provide server-side storage of user data and/or system images	1
	6d	Provide server-side storage of user application	1
	6e	Provide server-side storage of enterprise data application	1
125	7	**Support Infrastructure Requirements**	
	7a	Maintain current bandwidth/network loads (min 10 GB to max 100GB user profiles, 100 MB to the desktop)	1
	7b	Provide consistent capability, whether rich or thin, with differing capabilities based on Active Directory rights/groups	1
	7d	Provide support for the Common Access Card (CAC)/DOD Public Key Infrastructure (PKI) logon	1
150	8	**Improved Manageability**	
	8a	Provide for remote manageability of desktop	1
	8b	Provide support for all business and mission applications, including bandwidth sensitive applications	4
	8c	Provide for a client computing environment solution that scales over the AF enterprise	1
	8d	Allow use of a diverse mix of hardware end devices in a heterogeneous environment	1
	8e	Increase IT service availability to the mobile/pervasive user	2
150	9	**Provide the same user experience (irrespective of client; rich or thin client).**	1

Solution Determination



"Unified Communications"

Builds On

Feasibility Assessments

Value Factors	Reduce time to deploy infrastructure 15%	Reduce infrastructure cost 15%	Improve Reliability, Availability Survivability (RAS) 5%	Work within current Security Management Posture 5%	Provide support for AF Use Cases 5%	Support SBC storage strategy 13%	Support Infrastructure Requirements 13%	Improved Manageability 15%	Provide the same user experience (irrespective of client; rich or thin client) 15%	
Softgrid	1.67	3.00	3.40	1.50	0.73	1.40	1.00	1.56	1.00	1.67
Ardent	2.33	3.15	3.40	3.00	1.53	1.40	1.33	2.11	2.00	2.23
ClearCube	1.67	2.23	1.30	2.50	2.07	1.40	2.00	2.78	4.00	2.48
Wyse	1.00	1.92	1.30	1.50	2.80	1.00	2.33	4.22	5.00	2.67
CO/HP	1.67	2.23	1.30	2.50	2.07	1.40	2.00	2.78	4.00	2.83
Citrix	1.00	1.92	1.30	1.50	2.80	1.00	2.33	4.22	5.00	3.03

Overall Score on each Product

Blue = Essential	1 - 1.99
Green = Desirable	2 - 2.99
Yellow = Less Desirable	3 - 3.99
Red = Undesirable	4 - 5.00

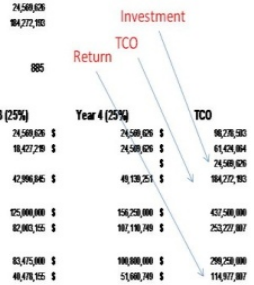
Builds On

Economic Analysis/TCO/ROI)

		Unmanaged PC	Managed PC	Thin Client
Units		250,000		
Direct Cost - 1 Unit	$	500	$ 504	$ 393
Direct cost - 250K Uni	$	125,000,000	$ 126,000,000	$ 98,278,593
In-Direct cost - 250K I	$	125,000,000	$ 69,300,000	$ 24,569,626
Migration Costs	$	-	$ -	$ 24,569,626
4 yr TCO	$	437,500,000	$ 290,250,000	$ 184,272,193
4 yr TCO per SBC Client	$	2,500	$ 1,613	$ 885

SBC		Year 1 (25%)	Year 2 (25%)	Year 3 (25%)	Year 4 (25%)	TCO
Direct Cost	$	24,569,626	$ 24,569,626	$ 24,569,626	$ 24,569,626	$ 98,278,503
In-Direct Cost	$	6,142,406	$ 12,284,813	$ 18,427,219	$ 24,569,626	$ 61,424,064
Migration Cost	$	24,569,626			$ -	$ 24,569,626
Annual Costs	$	55,281,658	$ 36,854,439	$ 42,996,845	$ 49,139,251	$ 184,272,193
Unmanaged PC						
Unmgd PC Annual	$	62,500,000	$ 93,750,000	$ 125,000,000	$ 156,250,000	$ 437,500,000
SBC Saving	$	7,218,342	$ 14,436,684	$ 21,655,026	$ 28,873,368	$ 72,183,421
Managed PC						
Managed PC Annual	$	40,825,000	$ 61,237,500	$ 81,650,000	$ 102,062,500	$ 285,775,000
SBC Saving	$	14,456,658	$ 28,913,316	$ 43,369,974	$ 57,826,632	$ 144,566,579

Breakeven Year is 2nd year
ROI 468% benefit/investment

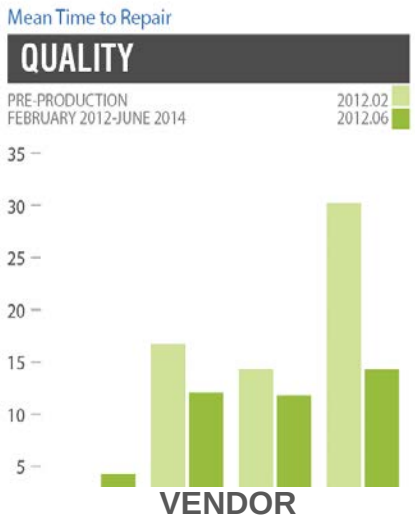


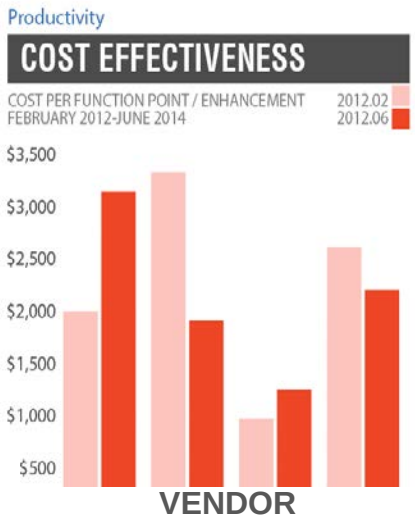
Standard, objective measurement creates visibility

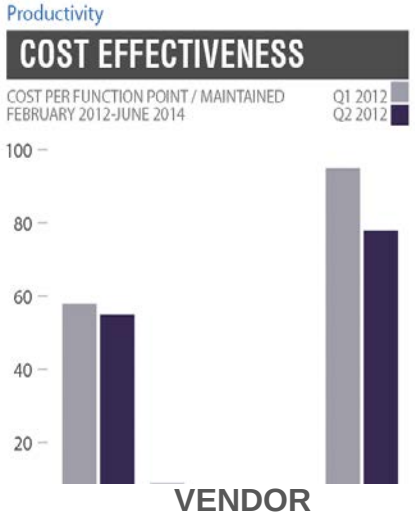
Scorecard the Service Providers

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







Critical Service Level Matrix

At Risk Amount and Allocation of Risk

Total Billing Per Release :	$1,000,000
Total At Risk Amount (10% of Bill) :	$100,000
Total Risk Pooler:	100%

10% is for example

Application Name	Tier 1 Metrics (Critical Service Levels)	At Risk Multiplier	Risk Allocation	At Risk Amount
OMS			30%	
	Total Quality Index	50%		$15,000
	Critical Violations	30%		$9,000
	Application Pain Violations	20%		$6,000
		100%		$30,000
CRM			10%	
	Total Quality Index	30%		$3,000
	Critical Violations	30%		$3,000
	Application Pain Violations	40%		$4,000
		100%		$10,000
AMSS			20%	
	Total Quality Index	50%		$10,000
	Critical Violations	30%		$6,000
	Application Pain Violations	20%		$4,000
		100%		$20,000
SDP			20%	
	Total Quality Index	50%		$10,000
	Critical Violations	30%		$6,000
	Application Pain Violations	20%		$4,000
		100%		$20,000
Enabler			20%	
	Total Quality Index	50%		$10,000
	Critical Violations	30%		$6,000
	Application Pain Violations	20%		$4,000
		100%		$20,000

Amount service provider has at risk on this individual Service Level is 30% * 50% * $100K = $15,000

- Anytime there is a default, the at risk amount will be applied
- Incentive is given to service provide equivalent to the at risk amount if they exceed the Expected Service Level by 5% of the delta between the then current Expected and Perfection
- Credits / Incentives are settled at the Annual Reset

Introducing Metrics for Performance-based Incentive Program

Client:

- Global financial service institution's Strategic Sourcing team rolled out voluntary program to all application managers
- Added service level clauses to contracts for 7 strategic ADM partners

Analysis perimeter:

- 125 applications analyzed monthly
- Applications selected based on criticality and spend

Performance-based service level implementation:

- Establish performance baseline over 6 months
- Subsequent months get measured
- Quality score cannot go down – penalty assessed if score deviates 10%
- Internal Delivery Leader can call an exception if appropriate to business
- Average TQI stabilizes over time
- Predictability of deliveries and improved SLA compliance

"We've done a very good job beating down the rate cards with our vendors, but we didn't feel we were getting the best value from our vendor partnerships. After putting this service level in place we noticed that the level of talent our key vendors were staffing on our projects got significantly better." - Head of ADM

Next Steps

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