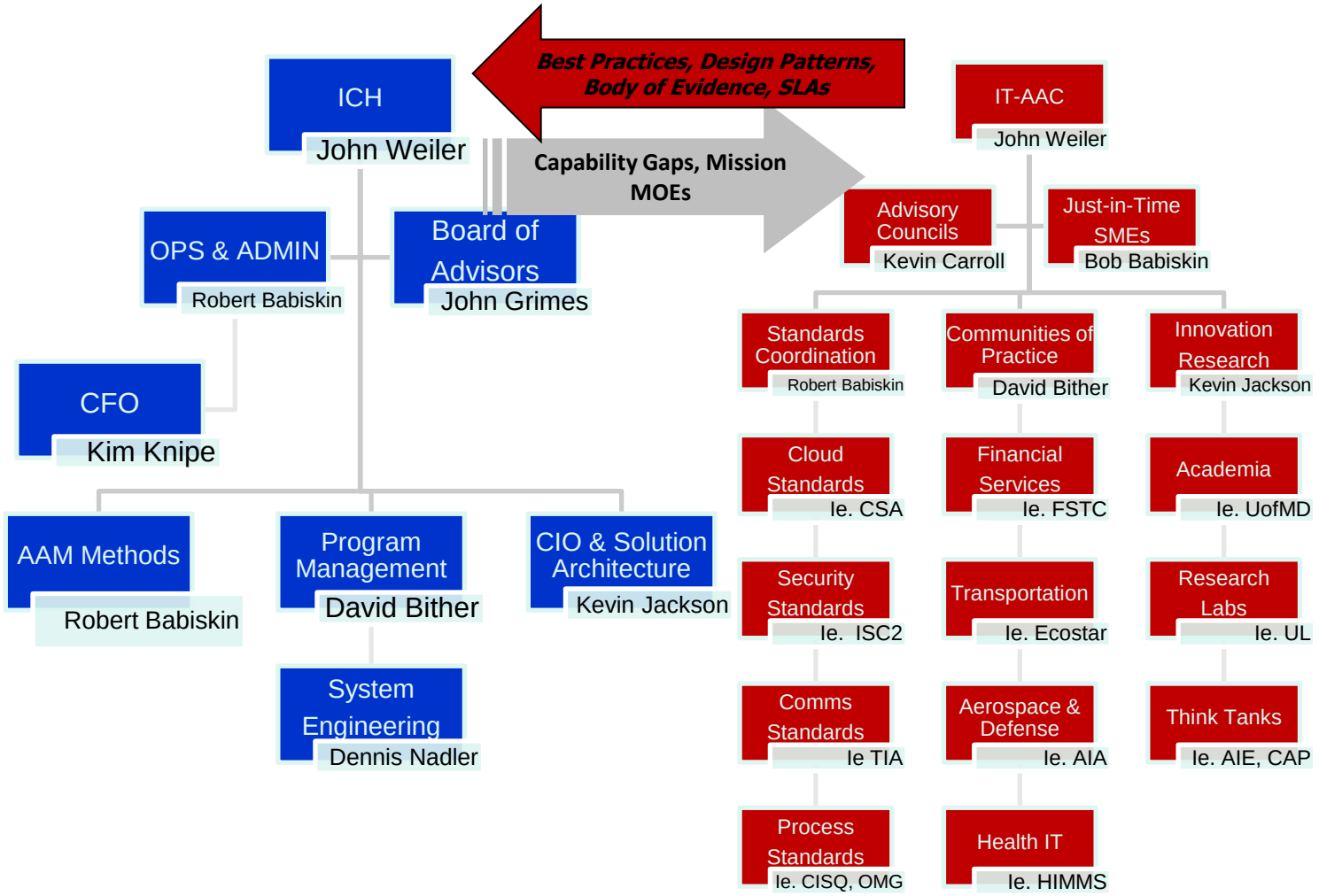
ICH and IT-AAC

FITARA Roadmap for Sustainable IT Reform

A decision analytics maturity model for measuring business value and risk of commercial IT

ICH and IT-AAC

Public/Private Partnership
Used on the Risk Assessment



2

IT-AAC Knowledge Exchange

Leveraging commercial IT standards of practices

IT -AAC Partners	Agile Methods	IT/Cloud Standards	Innovation Access	IT Risk Mgt	Industry Best Practices	Pilots & Contracts	IT Policy & Governance	IT Training & Mentoring
Aerospace Industry Association (AIA)			✓		✓		✓	
Center for American Progress (CAP)					✓		✓	
Cloud Security Alliance (CSA)		✓	✓		✓	✓		✓
Cloud Standards Customer Council (CSCC)	✓	✓			✓		✓	
Interoperability Clearinghouse (ICH)	✓		✓	✓	✓			✓
Intern'l Information Systems Security Certification Consortium (ISC2)		✓			✓			✓
Information Systems and Security Group (ISSA)		✓			✓		✓	✓
Object Management Group (OMG)	✓	✓	✓	✓	✓		✓	✓
University of Maryland (UofMD)			✓	✓	✓	✓	✓	✓
University of Tennessee (UofTN)					✓		✓	
Consortium for IT SW Quality (CISQ)			✓	✓	✓	✓		
Telecommunication Industry Association (TIA)		✓	✓		✓		✓	✓
Financial Services Technology Consortium (FSTC)	✓		✓	✓	✓	✓	✓	✓

Acquisition Assurance Method

Using Decision Analytics to Frame Risk/Value trade offs

Risk Assessments
Capability Assessments
Economic Assessment
Management Assessment

Acquisition Assurance Method (AAM)

a FITARA Agile Maturity Model for IT Acquisition Risk

AAM Process

Business Requirements & Capability Gaps

Phase 1

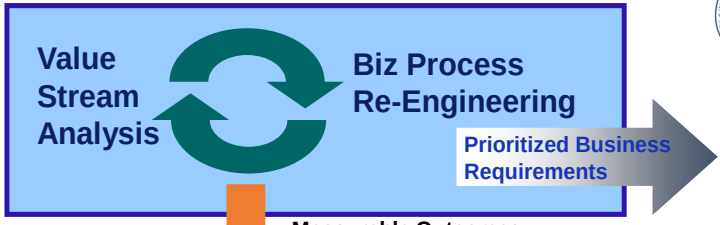
Mission Needs: Value Stream Analysis:
- Problem ID
- Mission Rqts
- Prioritization
- Constraints

Phase 2

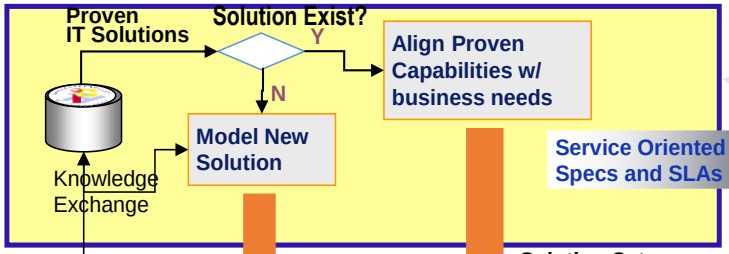
Performance Management Assessment
- Feasibility
- Service Attributes
- SLAs
- Shared Services

Phase 3

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

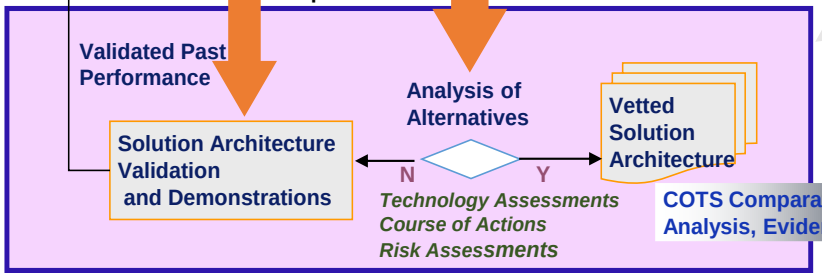


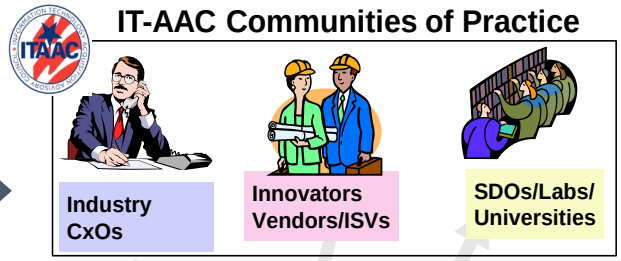
Measurable Outcomes
Business Metrics



Normalized SVC Components

Solution Set Evidenced-Based Research



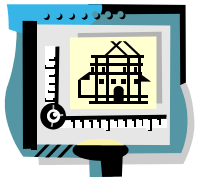


Evidence Lessons Learned

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

AAM

Value to Stake Holders

The **Acquisition Assurance Method** process is an enterprise approach for assessing technology Risk and Value as it applies to mission/business capabilities' improvements.

AAM is a methodology for achieving:

- ***Efficiency*** – of solution assessments and reduce redundant pre-acquisition operational activities
- Compliance with the Title 40 Clinger Cohen, DoD 5000.02 (JCIDS) and FITARA
- Alignment with the Agency Methods. Reduce the discovery time for business/technology artifacts while providing configuration management of those documents through the creation of knowledge libraries
- Streamline the technology assessment workflow process through standardized processes and methodology templates that will provide a clear understanding of the results and options of the assessment
- Standardize the capability assessment process of solution sets, including managerial processes to create an executable, measurable and sustainable process

AAM Process

Risk Based Decision Analytics

Repeatable, Executable, Measurable

Problem Statement - Risks

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

Risk Capability Risks

		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).**

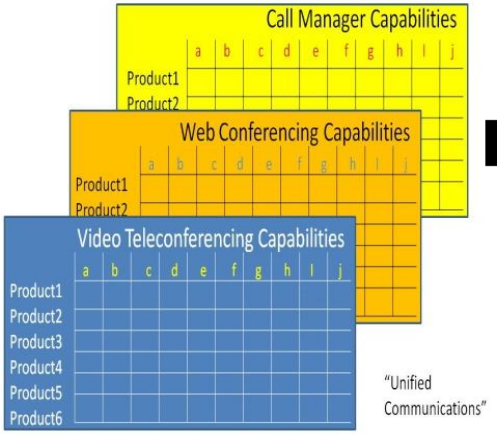
Builds On

Risk 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

Builds On

Solution Determination



"Unified Communications"

Builds On

Risk Feasibility Mitigation 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	1.55	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
CCIMP	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

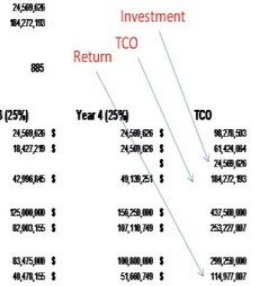
ROI

Units		250,000			
		Unmanaged PC	Managed PC	Thin Client	
Direct Cost - 1 Unit	$	500	$ 500	$ 393	
Direct cost - 250K Uni	$	125,000,000	$ 125,000,000	$ 98,278,500	
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	$ 299,250,000	$ 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	$ 14,895,561	$ 22,903,155	$ 31,110,749	$ 253,727,807
Managed PC						
Managed PC Annual	$	49,825,000	$ 66,150,000	$ 83,475,000	$ 100,800,000	$ 299,250,000
SBC Saving	$	(6,456,658)	$ 29,295,561	$ 40,478,155	$ 51,660,749	$ 114,977,807

Breakeven Year is 2nd year

ROI 468% benefit/investment



Case Study

How DISA applied AAM

DISA's CAAP Program

- **Single Security Architecture**
- **Unified Capability**
- **Secure Mobility**
- **Cloud Strategies**
- **MINIS ICD**

8

AAM

CONDUCTING THE RISK MANAGEMENT ASSESSMENT

(1) Risk Area Determination (RD)

- Risk Determination (RD)– is the process in the AAM, which defines "what" capability risks are to be evaluated as by "what" technologies/ solutions.

- The RD process breaks the capabilities into one or more solution sets to conduct an analytical technology assessment
  - This is a process that creates groupings (tables) of capability and technologies that satisfy the capabilities gaps that may be under risk.
  - All capabilities may not be solved by a single technology/product. This process breaks up the capability to classes of COTS products as "routers" while other capabilities may be solved by "mail systems".
  - CD is the process of turning a set of capability risks into a canonical form referred to as an Analysis Model

Risk Categories

Example – AF DCGS

From AF ISR Risk Assessment Project

Lack of:

- ❑ An Enterprise Methodology for AF DCGS.
- ❑ An Implementation Plan for Agility at AFISRA.
- ❑ A Management Plan for oversight of AF/A2 Staff through Metric.
- ❑ Technology Plan focused on Commercial Innovation.
- ❑ An Implementation Plan for a SPO.
- ❑ A Management Plan for oversight of AFISRA/SPO through a Dashboard
- ❑ Create an Agile Acquisition Strategy and Methodology.
- ❑ Design and Implementation of an AF/A2 and SAF/AQ Staffing Plan.
- ❑ Management Plan for Acquisition Approach. Shifting AF/A2/ SAF/AQ to an Agile
- ❑ Implementation Plan for Shifting SPO/PEP-EIS to an Agile Acquisition Approach.
- ❑ Change Management Plan.

Root-cause analyses of over 20 AF, congressional and oversight organizations documents and dozens of interviews.

Note: these Problems are common to most IT Programs

(2) Capability Risk Analysis

Capability Risk Analysis[1]

Risk Assessments require a specification of the risks required by the Program providing the Scope under which to operate:

- This may be determined in a formal requirements process within the agency or efforts internal to the Program.
- To start a Risk Assessment, a formal "trigger" must occur.
- A request must come from a sponsoring organization to assess a product, technology, process, or even a technical information enterprise solution.

[1]An ICH AAM Product not currently in the AFCA User Manual

Example: DCGS PROGRAM

(6) RISK AREAS Identified

Governance
Organization
Architecture
Technical
Process & Methodology
Return on Investment

13

Risks Assessment – 6 Major Risk Area

Example – AF DCGS

(1) Governance

- Sustainment procedures for IT-centri
  used to support modernization of ISR
- Authorities a
  program mar
  evaluation nc

(2) Organization

- Managing de
  discrete prog
- Managing AF
  sub-optimal f
  future increm

10

(3) Architecture

- Unclear and limited ar
  external system) -- nee
- The "To Be" architectu
- Enterprise Architectur
  Systems) oriented prog
  information architectu
- Lack of sensor integrat

(4) Technical

- The ability for AF DCGS portfolio programs to meet peek load requirements not verified
- Portfolio programs have not been fully vetted via application of cyber security Red Team or external denial of service and intrusion testing
- Reliability and availability performance requirements are incomplete for the programs within the portfolio
- Interface (I/F) artifacts do not support rapid (open) integration of sensor feeds and dissemination technology to meet interoperability (information sharing) requirements

(5) Process & Methodology

- Modification process being used ("1067 process") to address both urgent operational needs and functional requiements for critical ISR system
- Cost, schedule and technical performance requirements (baseline) for each program not established
- Process for managing (validating, verifying and prioritizing) capability-based requirements and functional/system level requirements not being used
- Limited application of formal configuration review and control process and lack of integration of CM into program management activities

(6) Return On Investment

- No metrics in place for measuring performance of portfolio/programs in terms of reducing infrastructure cost or delivering enhanced capability
- Weapon system sustainment funding authority and planning process being used for modernizing SoS IT enterprise
- Funding planning is conducted without direct traceability to verified and validated (capability needs-based) requirements
- Allocation of funds are not planned or tracked in terms of reduction of cost or greater capability

Risks Assessment – Decomposed to 51 Rusk Elements

Example – AF DCGS

	Risk Element	Mitigation	Govern	Acquistion	ROI-based	Risk based	Sensor Svcs	Incremental
RA4	Technical							
RE4.1	Sensor Integration	Service-Oriented Sensor Integration Method					✔	
RE4.2	Implementation Technology	Common Presentation Layer & Platform					✔	
RE4.3	Cybersecurity	Cybersecurity Test Scenarios and Conditions					✔	
RE4.4	Measures of Effectiveness	Technical Performance Goals Based on MOE (Measure of Effectiveness) Identified					✔	
RE4.5	Modernization Strategy	SW (Software) Maturity Assessment					✔	
RE4.6	Measure of Effectiveness	Technical Performance Goals Based on MOE (Measure of Effectiveness) Identified					✔	
RA5	Processes & Methodology							
RE5.1	Configuration Management	Integrated CM (Configuration Management) Process						✔
RE5.2	Migration Strategy	"To Be" SoS and Migration Strategy						✔
RE5.3	Sensor Integration	Service-Oriented Sensor Integration Method						✔
RE5.4	Modernization Strategy	PM Process for Risk Management, Baseline Management & I2 Capability Development						✔
RE5.5	SoS Management	I2 (Incremental & Iterative) Capability Development Process						✔
RE5.6	Modernization Strategy	MS (Integrated Master Schedule) with Critical Path						✔
RE5.7	Modernization Strategy	Functionality to Capability Trace Analysis						✔
RE5.8	Requirements Management	Requirements Identification, Validation and Prioritization Process						✔
RE5.9	Systems Engineering	Systems Engineering Plan						✔
RE5.10	IV&V	Formal IV&V (Independent Verification & Validation) process						✔
RE5.11	Baseline Management	Baseline Establishment & Management Method						✔
RE5.12	Joint Interoperability	Implementing an Information Support Plan (ISP)						✔
RE5.13	Program Management	PM Process for Risk Management, Baseline Management & I2 Capability Development						✔
RA6	Return-On-Investment (ROI)							
RE6.1	Modernization Strategy	Enterprise Portfolio Management Plan			✔			
RE6.2	Migration Strategy	Migration Funding Requirements			✔			
RE6.3	Capability Traceability	Capability-based Requirements to Cost Tracing			✔			
RE6.4	Funding Allocation	Sustainment and New Capability Funding Allocation & Ratio			✔			
RE6.5	Capability Traceability	Baseline Performance Requirements to Cost Tracing			✔			
RE6.6	Funding Allocation	Sustainment and New Capability Funding Allocation & Trend Analysis			✔			
RE6.7	Capability Traceability				✔			
RE6.8	Performance Metrics	Funding Execution Metrics & Performance Monitoring			✔			

(3) Capability Risk Prioritization (CRP)

- All risks are not equal
- Each must be assessed as to its overall contribution or value to the solution being assessed
- Conducted with the key stake-holder to create an analytical measure of the value of the risk to the enterprise/program/project
- CRP is an input tool in assessing how a capability can be met based on the availability of existing (COTS/GOTS) technology
- Goal is to look at the value of each capability/objective in the environment and assign numerical priorities representing the importance of each individual capability
- The outcome is an agreed-upon prioritization of the risk values
- Prioritization can be reused as weighted evaluation factors in other acquisitions

(4) Solution Determination (SD)

Multiple Strategies to Solve Risk Elements

- The SD process, first, produces a capability description and an analysis plan which breaks the capability risks into one or more course of action sets:
  - A simple solution set is a set of capabilities evaluated by a technology assessment (TA) referred to as an analysis group
  - A complex solution set may require several analysis groups which can be constructed by use-cases or by subsets of capabilities defined by a set of products
- Second the SD produces the Risk AoA options
  - AoA's for the same problem statement
  - AoA's for a segments of problem statement (e.g., evolutionary)
  - AoA's that are product oriented
  - AoA's that are Architectural
  - AoA's the are process and operationally oriented

17

Scoring the Risk
Calculating the Risk

- In this example, capabilities are rated on a scale of one to five in which a value of 1 indicates almost no risk to satisfy while a 5 represents a high risk
- The team members use a group jury-style approach discussing why particular scores are assigned, defending their position until there is a convergence of the entire team (group normalization)
- If multiple groups are used, they will have to go through the normalization process among each other

CAPABILITY	VALUE
No Risk	1
Moderate Risk	2
Manageable Risk	3
Significant Risk	4
High Risk	5

Evaluating risk

Severity \ Likelihood	1 Remote	2 Unlikely	3 Possible	4 Likely	5 Certain
1 Trivial	1	2	3	4	5
2 Minor	2	4	6	8	10
3 Lost time	3	6	9	12	15
4 Major	4	8	12	16	20
5 Fatal	5	10	15	20	25

(5) Risks Assessment – Scoring the Risk

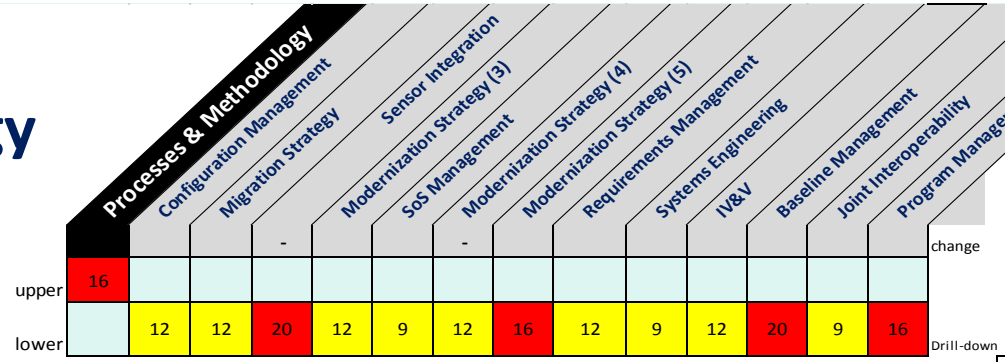
Under AAM Feasibility Assessment

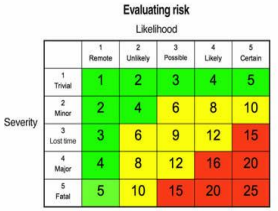
SAMPLE – AF DCGS

Processes & Methodology

DCGS PRA Dashboard

Portfolio View





Elements	Processes & Methodology	Description	Descriptors: Critical Pat	Cost	Schedule	Technical	Impact	Probability	Overall
RE5.1	Configuration Management	Limited application of formal configuration review and control process and lack of integration of CM into program management activities	No	No	Yes	Yes	HM	H	H
RE5.2	Migration Strategy	Modernization activities are being conducted without an AF DCGS modernization migration strategy and defined "To Be" SoS.	No	Yes	Yes	No	HM	H	H
RE5.3	Sensor Integration	Attempting to integrate new ISR sensors without a formal integration and engineering process for new sensors	No	Yes	Yes	No	HM	HM	HM
RE5.4	Modernization Strategy (3)	Program management process employed from AF DCGS program management directive (PMD) not applicable to management and modernization of SoS IT enterprise	Yes	No	Yes	Yes	M	M	M
RE5.5	SoS Management	Block release methodology used for SoS IT enterprise instead of Iterative & Incremental capability delivery process	Yes	No	Yes	Yes	HM	HM	HM
RE5.6	Modernization Strategy (4)	System modernization and development activities being conducted without use of program IMS (Integrated Master Schedule)	Yes	No	Yes	Yes	M	HM	HM
RE5.7	Modernization Strategy (5)	Modification process being used ("1067 process") to address both urgent operational needs and functional requirements for critical ISR system	No	Yes	Yes	Yes	H	H	H
RE5.8	Requirements Management	Process for managing (validating, verifiying and prioritizing) capability-based requirements and functional/system level requirements not being used	No	No	Yes	Yes	HM	H	H
RE5.9	Systems Engineering	No apparent process for developing and approving SEP (Systems Engineering Plan) for planned enhancements	No	No	Yes	No	HM	HM	HM
RE5.10	IV&V	IV&V (Independent Verfiication & Validation) process not being used	No	Yes	Yes	Yes	H	HM	H
RE5.11	Baseline Management	Cost, schedule and technical performance requirements for each program not established	Yes	Yes	Yes	Yes	H	H	H
RE5.12	Joint Interoperability	Level of joint interoperability not easily decerned - lack of artifact or docuemented planning (e.g. Information Support Plan)	No	Yes	Yes	Yes	H	HM	H
RE5.13	Program Management	Critical path needs to be established for all programs in the portfolio	No	Yes	Yes	Yes	H	H	H

Sample Consumer Report

For Analysis of Alternative

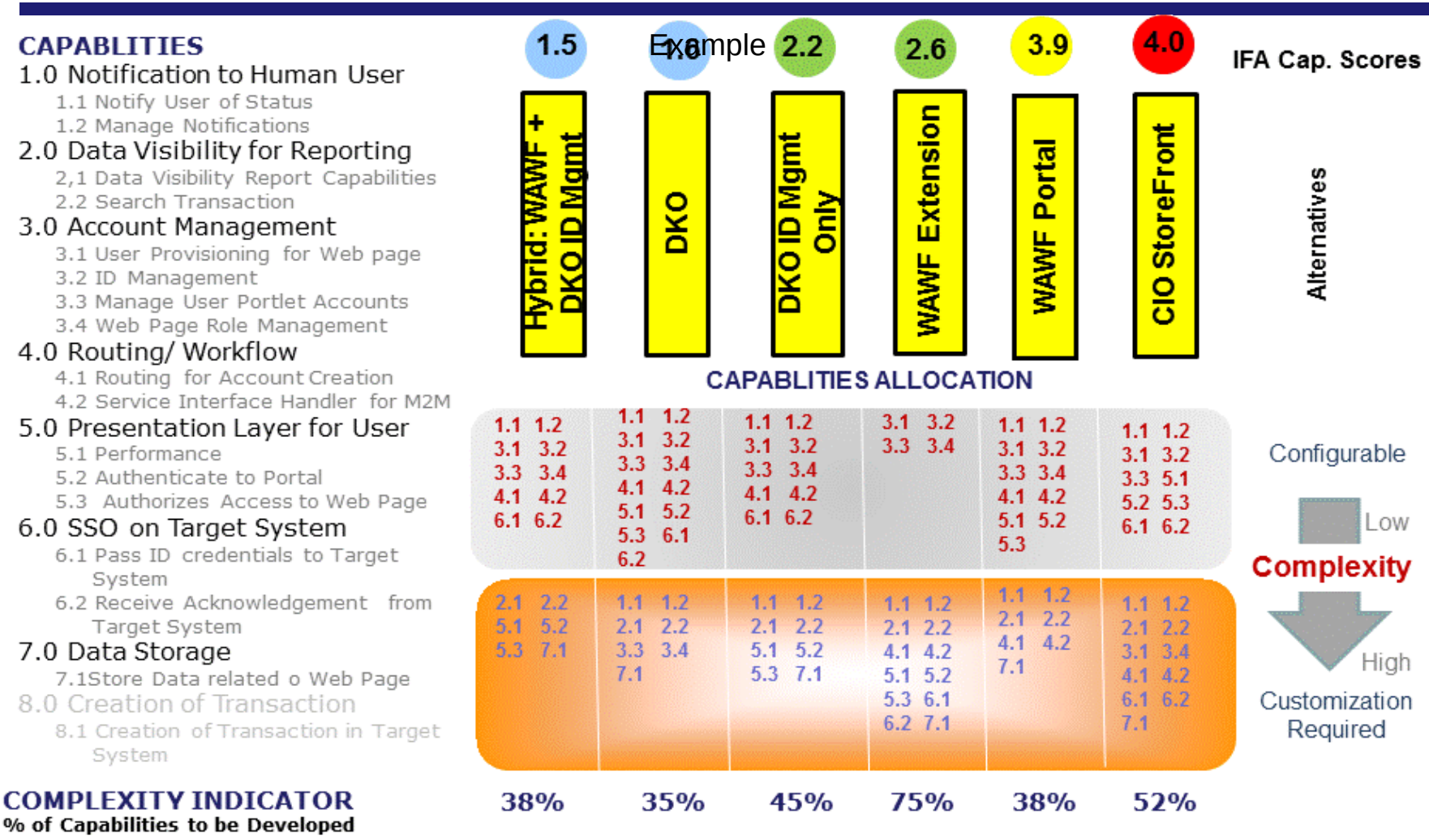
	Reduce time to deploy infrastructure	Reduce infrastructure cost	Improve Reliability, Availability Survivability (RAS)	Work within current Security Management Posture	Provide support for AF Use Cases	Support SBC storage strategy	Support Infrastructure Requirements	Improved Manageability	Provide the same user experience (irrespective of client; rich or thin client).	Score
Value Factors	**15%**	**15%**	**5%**	**5%**	**5%**	**13%**	**13%**	**15%**	**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
CCI/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

This process may not be a selection but shows sufficient COTS/GOTS products availability for a Procurement rather than development – FAR Compliance

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

Risk Assessment Alternative

Example Function Point Analysis



Risks Assessment – Recommendations

Sample – AF DCGS (1 of 6)

Recommendation 1 - Apply a governance structure and process that provides a clear delineation of portfolio and program-level functions and unambiguous responsibilities for key activities and resources.

DECRIPTION: **Currently, AF DCGS shares many of the executive, management, engineering and support responsibilities across disparate organizations within the enterprise. This has the effect of limiting agility for making decisions and committing resources in support of requirements validation, systems integration, quality control, testing, and other management functions. This also impacts the ability to respond to high-priority or changing operational requirements.**
To achieve maximum agility, prime responsibilities are assigned for requirements management, program management, solution and technical development, test and evaluation, operations support and executive oversight for each program in the portfolio. In addition, responsibility for key management and engineering processes and tools are aligned within each functional area. These include program baseline development, system configurations and CMB (Configuration Management Board), requirements prioritization, transition planning and risk management.

DESIRED OUTCOME

By identifying and specifying executive and management roles and responsibilities, programmatic decisions will be made in a responsive manner in support of critical and short-suspense warfighter requirements. Published artifacts allow management and support personnel to unambiguously understand AF DCGS governance methodology and supporting process.

ACTIONS

1. Develop and promulgate an integrated management process for AF DCGS that reflects key events and flow of information in support of the governance structure. This includes the processes, inputs, outflows and artifacts needed to manage requirements, program baselines, functional verification and validation and executive oversight at the portfolio-level.
2. Develop policy and implementation plans that establish roles and responsibilities for AF DCGS management COI (Community of Interest). Specified executive oversight responsibilities include approving program baseline, setting entrance and exit criteria for development phases, and acceptable risk standards for fielding decisions.
3. Develop a management matrix that aligns program milestones, events, processes and artifacts and documentation with the responsible agent within the AF DCGS management COI.

Past Performance = Assured Outcomes

Where AAM eliminated critical architecture decision risks

Navy: Assessment of AFLOAT Program – CANES SOA & Security Strategy
Contact Value: $350k
Eliminated hi-risk Requirements by 23%, $100Ms in potential savings

USAF: Streamlined COTS Acquisition Process. Applied to Server Virtualization.
Contract Value: $500k
Established optimal arch with ROI of 450% & $458 million savings

NRO: NRO ISP Transformation Roadmap
Contract Value: $450K
Comprehensive benchmark of industry best practices in just 4 months.

USMC: Solution Architecture, AoA and BBA for Cross Domain, Thin Client
Contract Value: $300k
Greatly Exceeded Forecasted Saving in both analysis and acquisition

GSA: Financial Mgt System consolidation using AAM.
Contract Value: $500k
Moved FMS from OMB "red" to "green". Eliminated duplicative investments that saved $200M

BTA: Build out of AAM to create BTA's Agile Requirements and BCA Method, with two completed Pilots
Contract Value: $500k
Reduced IT Requirements, EoA, BCA and Metrics development by 70%

BTA: Apply AAM to complete AoA and BCA for DoD SOA Project
Contract Value: $250k
Reduced pre-acquisition cycle time and cost of Analysis by 80% (4 months vs 18)

GPO: Developed Acquisition Strategy for Future Digital System FDSys
Contract Value: $150k
Led to successful acquisition and implementation on time, on budget and 80% cheaper than NARA RMS

AF ISR Agency: Portfolio Risk Assessment and Risk Mgt Dashboard (DCGS)
Contract Value: $450k
Identified 6 major Risk Areas and 50 risk incidences with Dashboard for tracking remediation and metrics