Understanding SwA Supply and Demand (Development)

SwA Working Groups June 22, 2010

Michele Moss, Booz Allen Hamilton

Ed Wotring, Information Security Solutions

- Overview Of Challenges In The Implementation Of SwA Practices
- Understanding Practice Implementation (A Self Assessment Approach)
- Leveraging The Practice Implementation Self Assessment During Acquisition

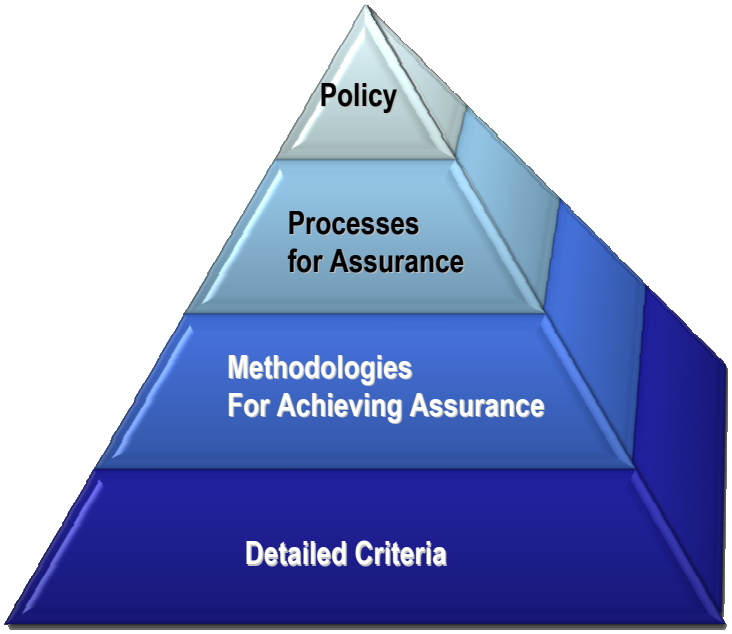
- Capture and discuss community of practices software assurance issues
- Share best practices
- Provide community input to and comments on:
  - DHS and DoD Guidebooks relating to Software Assurance
  - National and International Software Assurance Standards
  - DHS and DoD Policy Guidance on System and Software Assurance

Homeland Security

- In support of acquisition, management, and engineering and practices for software and systems assurance:
  - Community consensus standards for addressing assurance concerns throughout the system and software life cycles
  - Process benchmarking tools for assessing organizational capability with respect to assurance
  - Practice guidebooks providing compendiums of best practices and lessons learned
  - Community input to acquisition policy and guidance

Homeland Security

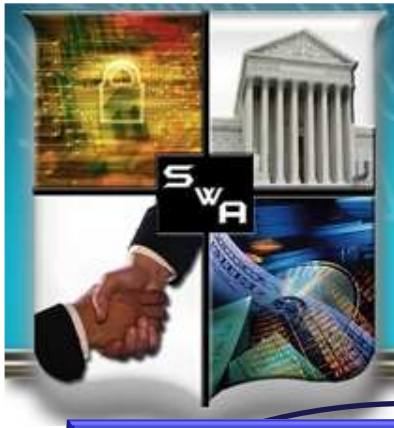
Project leadership and team members need to know where and how to contribute



- Assurance PRM defines the goals and practices needed to achieve SwA
- Assurance for CMMI ® defines the Assurance Thread for Implementation and Improvement of Assurance Practices that are assumed when using the CMMI-DEV

Understanding gaps helps suppliers and acquirers prioritize organizational efforts and funding to implement improvement actions

https://buildsecurityin.us-cert.gov/swa/procresrc.html



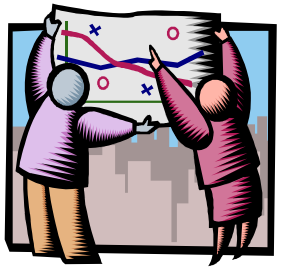
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Process Improvement Lifecycle - A Process for Achieving Assurance

Mission/Business Process

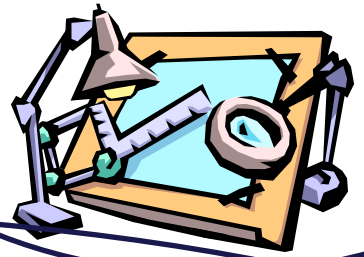
Understand Your Business Requirements for Assurance



Measure Your Results

Information System

Build or Refine and Execute Your Assurance Processes



Understand Assurance-Related Process Capability Expectations

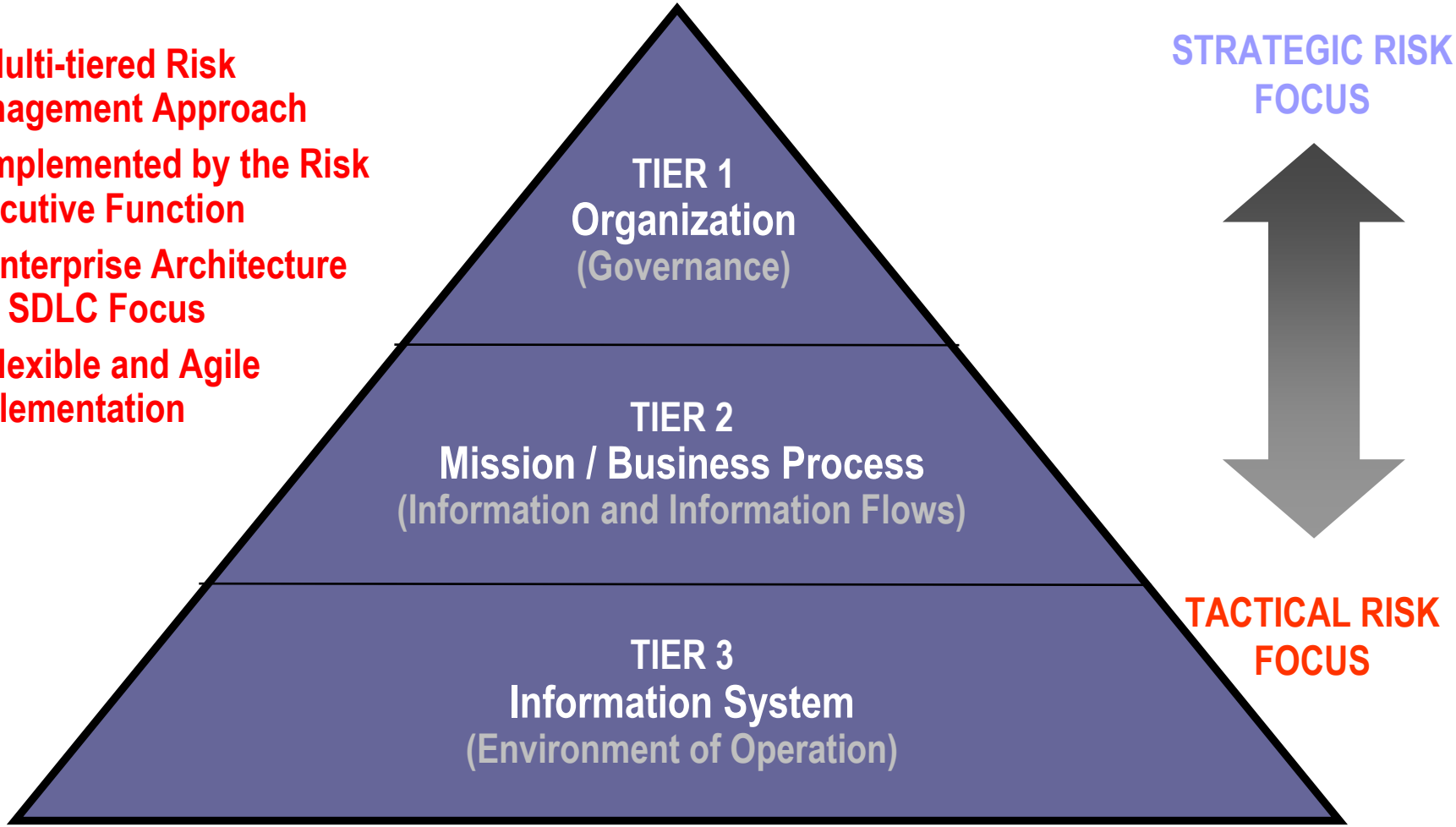
Organization Support

Look to Standards for Assurance Process Detail

Adapted from: Paul Croll, Computer Sciences Corporation, August 2007

Enterprise-Wide Risk Management

- **Multi-tiered Risk Management Approach**
- **Implemented by the Risk Executive Function**
- **Enterprise Architecture and SDLC Focus**
- **Flexible and Agile Implementation**



FISMA 2010 and Beyond
Strategic and Tactical Risk Management and the Role of Software Assurance
Ron Ross, NIST
Software Assurance Workshops
June 21, 2010

- Overview Of Challenges In The Implementation Of SwA Practices
- Understanding Practice Implementation (A Self Assessment Approach)
- Leveraging The Practice Implementation Self Assessment During Acquisition

- Analyzed freely available models to determine how various models address similar goals and practices
- Identified the intersections of the common practices amongst the models regardless of the intended audience and levels of granularity
- Intended to support “Getting Started” by increasing awareness of improving software assurance by:
  - Learning how multiple models address similar assurance goals
  - Selecting practices from these models
- Provides a means for selecting models and practices that are best suited for the individual needs of various organizations

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Mappings Of The Common Practices

SwA Common Practices Consolidation

	Governance			Knowledge			Verification			Deployment			Supplier Management		
	Strategy & Metrics	**Policy & Compliance**	**Training & Guidance**	**Threat Assessment**	**Security Requirements**	**Secure Design**	**Architecture Analysis**	**Code Analysis**	**Risk-Based Security Testing**	**Penetration Testing**	**Vulnerability Management**	**Environment Hardening**	**Agreement Requirements**	**Evaluation & Selection**	**Agreement Management**
Practices:	Establishes Security Plan; communicates and provides training for the plan	Identifies and monitors relevant compliance drivers	Conducts security awareness training regularly	Builds and maintains list of application-specific attack models	Documents, analyzes, and manages functional security requirements	Develops list of preferred frameworks and security features; explicitly applies security principles to design	Reviews design against security requirements	Develops list of top bugs and creates review checklists from security requirements	Performs edge / boundary value condition testing in QA process	Performs external penetration testing on production software with latest techniques and mitigates	Identifies point of contact for incident response; creates incident response team	Maintains operational environment specification	Identifies and prioritizes supplier dependencies; identifies, assesses, and mitigates risks associated with supplier dependencies	Establishes, reviews, and distributes solicitation package	Formalizes supplier relationships and executes supplier agreement
BSIMM	SM1.1	CP1.1	T1.1	AM1.1	SR1.1	SFD1.1	AA1.1 - AA1.3	CR1.1	ST1.1 - ST1.2	PT1.1 - PT1.2	CMVM2.1	SE1.1	SR3.1	-	-
	-	CP1.2	T3.4	AM1.4	-	SFD1.2	SFD3.1	-	-	-	-	SE1.2	-	-	-
CMMI-ACQ	PP SG2 - SG3	OPF SG1	OT SG2	RSKM SG1 - SG2	ARD SG1, SG3	ATM SG2	ATM SG1	AVER SG3	AVER SG3	AVER SG3	CAR SG1	CM SG2 - SG3	RSKM SG2-SG3	SSAD SG1	AM SG1
	-	-	-	-	REQM SG1	AVAL SG2	AVAL SG1 - SG2	-	-	CAR SG1 - SG2	OPD SG1	-	PP SG1	-	SSAD SG3
OSAMM	SM1B	PC1A	EG1A	TA1A	SR1A	SA1A	DR1B	CR1A	ST2B	ST1B	VM1A	EH1A	-	-	-
	-	PC1B	-	-	SR2B	SA1B	-	-	-	-	VM1B	-	-	-	-
PRM	SG 2.1	SG 3.1	SG 1.3	SG 3.2	SG 3.1	SG 3.2	SG 3.4	SG 3.4	SG 3.4	SG 3.4	SG 4.3	SG 4.3	SG 2.3	SG 2.3	SG 2.3
	SG 1.3	-	-	-	-	-	-	-	-	-	-	-	SG 3.1	-	-
RMM	RTSE:SG2 - SG3	COMP:SG2	OTA:SG1 - SG2	RISK:SG1 - SG4	RRD:SG1 - SG3	RTSE:SG1 - SG2	-	VAR:SG2	RTSE:SG3	RTSE:SG3	VAR:SG1	ADM:SG3	EXD:SG1 - SG2	EXD:SG3	EXD:SG3
	MON:SG1	MON:SG1 - SG2	-	KIM:SG6	RRM:SG1	KIM:SG2, SG6	-	KIM:SG6	-	-	MON:SG1	KIM:SG5	RISK:SG3 - SG6	-	-
Practices:	Collects and tracks security plan metrics based upon risk	Establishes policies and procedures for compliance with security plan and other compliance requirements	Conducts role-based advanced application security training	Identifies potential attacker profiles	Documents, analyzes, and manages non-functional security requirements	Builds secure frameworks, security services, and security design patterns	Makes design reviews available for projects	Uses automated code analysis tools; requires code analysis as part of development	Integrates black box security testing tools into QA of software releases	Performs periodic internal white box pen testing	Develops consistent incident response process	Monitors baseline environment configuration changes	Establishes enterprise and assurance requirements for supplier agreement	Evaluates solicitation responses	Monitors and corrects supplier processes and performance
BSIMM	SM1.5	CP1.3	T2.1	AM1.3	SR1.3	SFD2.1	AA2.1	CR1.4	ST2.1	PT2.1 - PT2.3	CMVM1.1	SE1.1	SR2.1, SR2.5	-	-
	SM2.1	CP3.2	-	-	-	SFD2.3	AA2.3	CR2.3	-	-	-	-	-	-	-
CMMI-ACQ	MA SG1 - SG2	OPF SG2 - SG3	OT SG2	RSKM SG1 - SG2	ARD SG1, SG3	ATM SG2	AVAL SG1	AVER SG3	AVER SG3	AVER SG3	CAR SG1	CM SG2 - SG3	REQM SG1	SSAD SG2	AM SG1
	PMC SG1	-	-		REQM SG1	AVAL SG2	PMC SG1 - SG2	-	-	-	OPD SG1	-	ARD SG2	-	REQM SG1
OSAMM	SM1B	PC2A	EG2A	TA1B	SR1B	SA2A	DR2A	CR2A	ST1B	ST1A	VM2A	EH2B	SR3A	-	-
	-	-	EG3B	-	-	SA2B	DR2B	CR2B	-	ST1B	-	-	-	-	-
PRM	SG 1.1	SG 1.2	SG 1.3	SG 3.2	SG 3.1	SG 3.2	SG 3.4	SG 3.4	SG 3.4	SG 3.4	SG 4.3	SG 4.3	SG 3.1	SG 2.3	SG 2.3
	SG 2.2	-	-	-	-	-	-	-	-	-	-	-	-	-	SG 3.5
RMM	MA:SG2	RTSE:SG2	OTA:SG3 - SG4	RISK:SG1 - SG4	COMP:SG2	RTSE:SG3	-	RTSE:SG3	RTSE:SG3	RTSE:SG3	VAR:SG1	ADM:SG3	EXD:SG3	EXD:SG3	EXD:SG4
	MON:SG2	COMP:SG1	-	KIM:SG6	RRM:SG1	-	-	-	-	-	MON:SG1	KIM:SG5	RRD:SG2 - SG3	-	RRM:SG1
Practices:	Drives budgets based upon analysis from metrics collections	Measures project compliance at specific checkpoints	Provides security resources for coaching / learning	Builds and maintains abuse cases and attack patterns	Builds repository of well written testable and reusable security requirements	Requires use of approved security platforms and architectures	Builds standard architectural patterns from lessons learned	Tailors code analysis for application-specific concerns	Employs risk-driven automated security and regression testing in QA process	Performs extensive penetration testing customized with organizational knowledge	Conducts root cause analysis for incidents, fixes all occurrences of bugs	Identifies and deploys relevant operations and protection tools; performs code signing	Establishes supplier agreement	Negotiates and selects supplier	Evaluates and accepts supplier work products
BSIMM	SM1.5	CP2.3	T1.3 - T1.4	AM2.1	SR1.2	SFD3.2	AA3.2	CR3.1	ST3.1	PT3.1 - PT3.2	CMVM3.1 - 3.2	SE2.3	CP2.4	-	-
	-	CP3.3	T2.4 - T2.5	AM 2.2	SR2.3	-	-	-	-	-	-	-	CP3.2	-	-
CMMI-ACQ	PMC SG2	OPP SG1	OT SG2	RSKM SG2	-	CM SG1	AVAL SG2	AVER SG3	AVER SG3	AVER SG3	CAR SG1 - SG2	OID SG1 - SG2	SSAD SG3	SSAD SG2	AM SG1
	-	-	-	-	-	-	-	-	-	-	-				PPQA SG1
OSAMM	SM3A	PC3A	EG1B - EG2B	TA2A	SR2A	SA3A	DR3A	CR3A	ST1A	ST1B	VM3A	EH3A	-	-	-
	SM3B	-	EG3A	-	-	SA3B	-	-	ST2A	-	-	OE3B	-	-	-
PRM	SG 3.1	SG 4.1	SG 1.3	SG 3.1	-	SG 3.2	SG 3.4	SG 3.4	SG 3.4	SG 3.4	SG 4.2	SG 4.3	SG 2.3	SG 2.3	SG 2.3
	-	-	-	-	-	-	-	-	-	-	SG 3.5	-	-	-	-
RMM	RTSE:SG3.SP1	RTSE:SG2	OTA:SG2	RISK:SG1 - SG4	KIM:SG6	KIM:SG2	KIM:SG6	RTSE:SG2	RTSE:SG3	RTSE:SG3	VAR:SG2 - SG4	RISK:SG5	EXD:SG3	EXD:SG3	EXD:SG4
	MON:SG2	COMP:SG3 - SG4	OTA:SG4	KIM:SG6	-	-	-	RTSE:SG3	-	-	MON:SG2	-	-	-	RRM:SG1

Assurance PRM	SAFEcode	MS SDL	Open SAMM	BSIMM
•Establish and maintain the strategic assurance training needs of the organization •Ensure resources have the training needed to do their job	1. Foundational (everyone) 2. Advanced (secure coding and testing practices) 3. Specialized (role-based)	1. Basic Concepts 2. Common Baseline 3. Custom Training	1. Technical Security Awareness training 2. Role specific guidance 3. Comprehensive security training and certifications	1. Create the software security satellite 2. Make customized, role-based training available on demand 3. Provide recognition for skills and career path progression

Source: SwA Benchmarking and Implementation, Moss, SSTC 2010

- Organizations must be able to understand and become aware of risk throughout the supply chain.
  - What assurance goals are being met?
  - What practices are being implemented?
  - Who are the suppliers and how are they managing risk?
- Organizations need to be able to quantify and baseline assurance and risk management activities to ensure rugged software and software services are being developed and acquired.
- Supply chain partners must achieve increased awareness and communication to effectively understand risk throughout the software supply chain.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

SwA Self-Assessment (High Level)

Role	Goal	Expected Practice	Activities	Source	BSIMM	CMMI-ACQ	OSAM M	RMM	MS SDL	Developer Considerations	Acquirer Considerations	Practice Implementation Level	Notes
DEV	SG 3.1 Establish assurance requirements.	SP 3.1.1 Understand the operating environment and define the operating constraints for assurance within the environments of system deployment.	Identify the system assurance context. Identify the system vulnerabilities with each operating environment defined for the system. Identify applicable assurance laws, policies, and constraints.	AF RD SP 1.1		PP SG1	EH1A	EF SG1 - SG2					
		SP 3.1.2 Develop customer assurance requirements.		AF RD SP 1.2	SR1.1	ARD SG1, SG3	SR1A	RRD:SG1 - SG3					
					SR1.2	REQM SG1	SR1B	COMP:SG 2					
					SR1.3		SR2A	KIM:SG6					
					SR2.3		SR2B	RRM:SG1					
		SP 3.1.3 Define product and product component assurance requirements		AF SP 2.1	SFD3.2	CM SG1	SA3A	KIM:SG2	P7				
							SA3B		P2				
		SP 3.1.4 Identify operational concepts and associated scenarios for intended and unintended use and associated assurance considerations.		AF RD SP3.1	AM1.1	RSKM SG1 - SG2	TA1A	RISK:SG1 - SG4					
					AM1.3		TA1B	KIM:SG6					
					AM1.4		TA2A						
					AM2.1								
					AM2.2								
		SP 3.1.5 Analyze assurance requirements.	Ensure established assurance requirements for the product flow to lower level solutions. Verify requirements against assurance objectives	AF RD SP 3.5	SR1.3	ARD SG3	SR1B	RRD:SG3					
		SP 3.1.6 Balance assurance needs against cost benefits.		AF SP 3.4	SM1.5	ARD SG3	SM3A - SM3B	FRM:SG4 - SG5, RRD:SG3					
		SP 3.1.7 Obtain Agreement of risk for Assurance level.			SM2.4	RSKM SG2	SM1A	RISK SG4, KIM SG3					
DEV	SG 3.2 Architect a solution for assurance.	SP 3.2.1 Develop alternative solutions and selection criteria for assurance.	Identify assurance defects and effectiveness of corrective actions in relevant products/systems/operations and apply lessons learned to alternative solutions; Understand the assurance capabilities of other products similar to the one under development that have been developed	TS SP 1.1	SFD1.1	ATM SG2	SA1A	RTSE:SG1 - SG2					
					SFD1.2	AVAL SG2	SA1B	KIM:SG2, SG6					
		SP 3.2.2 Architect for assurance.	Ensure the assurance of the product from the end-user's perspective; Ensure the customer's assurance responsibilities are specified; Identify resources and trust	AF TS SP2.1	SFD2.1	ATM SG2	SA2A	RTSE:SG3	P7				
					SFD2.3	AVAL SG2	SA2B						
		SP 3.2.3 Design for assurance.	Understand threat related design issues for design alternatives Emphasize potential design issues related to threat models or risk scenarios when considering design	AF TS SP 2.1	SFD2.1				P7				
		SP 3.2.4 Implement the assurance designs of the product components.		AF TS SP 3.1	AA3.2		SA1B						
		SP 3.2.5 Identify deviations from assurance coding standards. Implement appropriate mitigation to meet defined assurance objectives.		AF TS SP 3.1	CR1.4	AVER SG3	CR2A	RTSE:SG2					
					CR2.3		CR2B	RTSE:SG3					
					CR3.1		CR3A						

- Overview Of Challenges In The Implementation Of SwA Practices
- Understanding Practice Implementation (A Self Assessment Approach)
- Leveraging The Practice Implementation Self Assessment During Acquisition

- Post the Updated Assurance Process Reference Model (PRM) Goals and Practices for comment
- Validate Mappings with authors of the common practices
- Expand the Assurance PRM to include operations
  - Collaborate with MAEC efforts
- Expand the mappings to include additional references and ensure alignment with emerging efforts
  - NIST Pubs (i.e. IR 7622, Risk Management, Developmental Security, Security Controls)
  - Cyber Scope
  - SAFECode
  - Work items and standards from ISO (others?)
  - Other efforts that would inform the SwA Self-Assessment
- Continue discussions at future SwA events
- Understanding the synergies with the SwA Self Assessment and efforts to inform Acquisition Decisions

What should we consider from the acquisition community's perspective as we move forward?