



Benchmarking Software Assurance Implementation

Michele Moss
SSTC Conference
May 18, 2011

Report Documentation Page

Form Approved
OMB No. 0704-0188

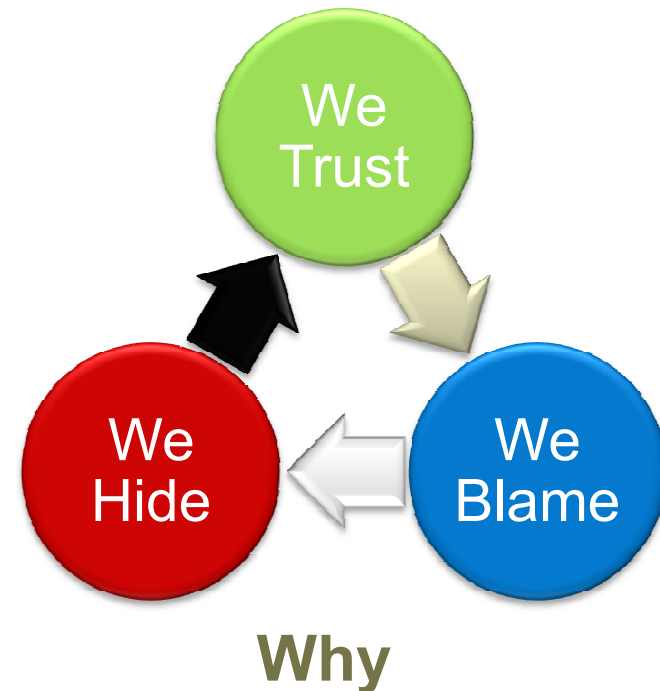
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE 18 MAY 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Benchmarking Software Assurance Implementation				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Booz Allen Hamilton ,8283 Greensboro Drive,McLean,VA,22102				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented at the 23rd Systems and Software Technology Conference (SSTC), 16-19 May 2011, Salt Lake City, UT. Sponsored in part by the USAF. U.S. Government or Federal Rights License					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	unclassified	unclassified	Same as Report (SAR)	20	

100 Apps Written By 100 Developers At 100 Companies

What CIOs Get

- ▶ 83 apps have serious vulnerabilities
- ▶ 72 apps have cross site scripting
- ▶ 40 apps have SQL Injection
- ▶ 100 apps contain code of unknown origin
- ▶ 90 apps use un-patched libraries with known flaws
- ▶ 5 apps have had a scan or pentest
- ▶ 1 app has had a manual security code review
- ▶ 0 apps provide any visibility into security



- ▶ 1 company has a responsible appsec program
- ▶ 1 developer has any security training

Adapted from: The Open Web Application Security Project, Jeff Williams, Aspect Security, SWA Forum Sept 2010

Process Improvement Best Practices Are Key To Addressing Cyber Challenges

▶ Who

- Specialists (i.e. SwA SMEs)
- Practitioners (Developers)

▶ What

- Measure progress
- Internal policy

▶ When

- During product development process
- During Leadership discussions
- As part of development and acquisition reviews

▶ Where

- IT Development Organizations
- IT Acquisition Organizations
- IT Integrator Organizations

Courtesy of September 2010 SwA Panel SwA Practices
– Getting to Effectiveness in Implementation

▶ Why

- Customer pressure
- Reaction to an incident

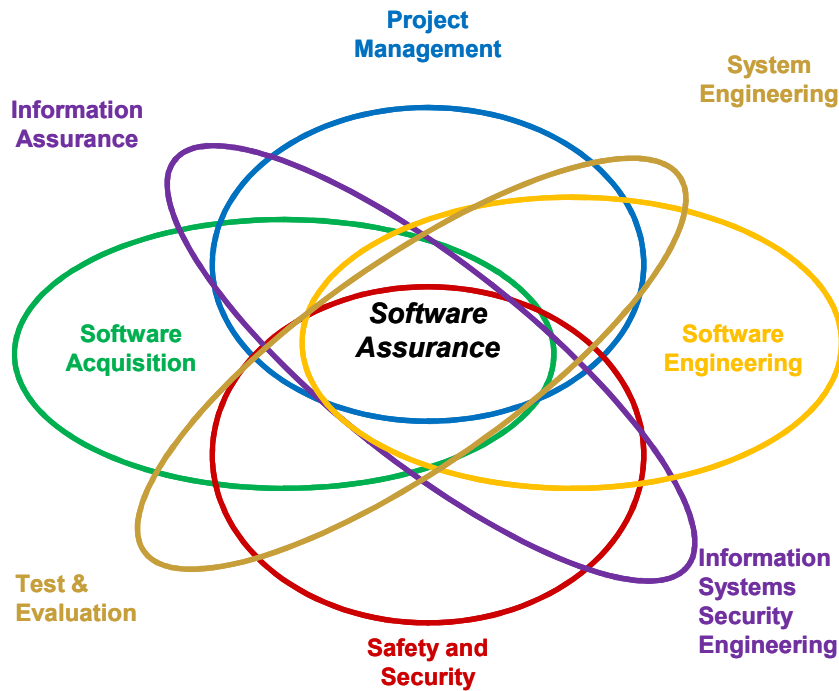
▶ Why Not

- Software security is not an explicit requirement in development contracts or acquisition processes
- Secure software training is not given to developers and architects

▶ How

- Executive leadership commitment
- Translate ROI to project manager vocabulary (cost, schedule, quality)
- Start small and build
- Use standards (i.e. coding standards)
- Avoid creating a new language
- Leverage what is already known
- Increase automation of menial tasks

SwA requires multi-disciplinary collaboration

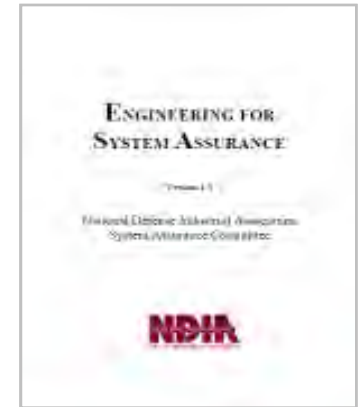
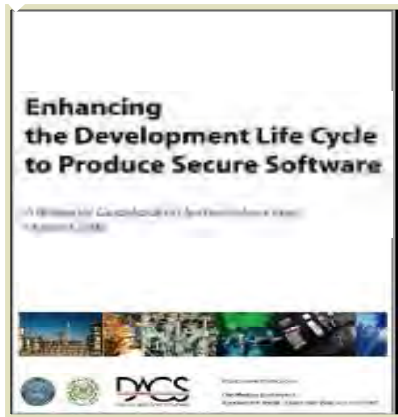


Communication Challenges	
▶ Vocabulary	▶ Experience
▶ Reserved Words	▶ Objectives
▶ Priorities	▶ Drivers
▶ Perspective	▶ Risks

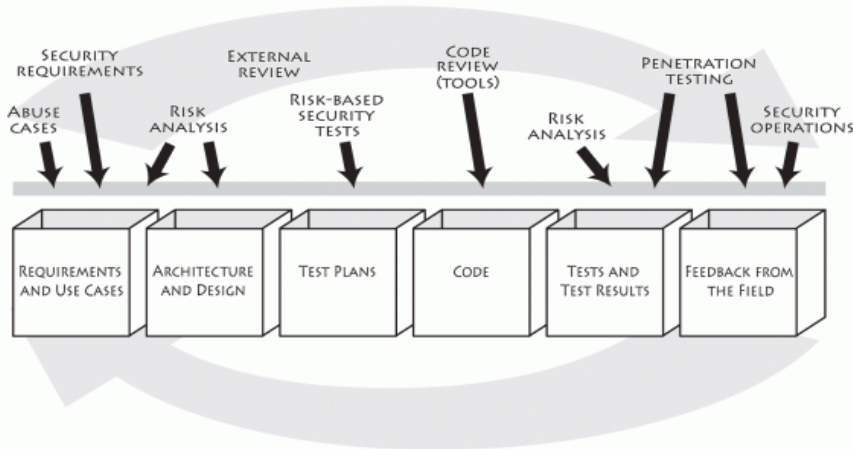
Source: <https://buildsecurityin.us-cert.gov/swa/procesrc.html>

Without a common language we cannot communicate across disciplines

Until recently, SwA communication tools focused on developer-centric audiences



Assurance for CMMI®



Different types of benchmarks exist – process and product

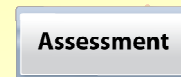
▶ *The chicken.... (a.k.a. Process Focused Assessment)*

- *Management Systems (ISO 9001, ISO 27001, ISO 2000)*
- *Capability Maturity Models (CMMI, Assurance PRM, RMM, Assurance for CMMI)*
- *Lifecycle Processes (ISO/IEEE 15288, ISO/IEEE 12207)*
- *COBIT, ITIL, MS SDL, OSAMM, BSIMM*

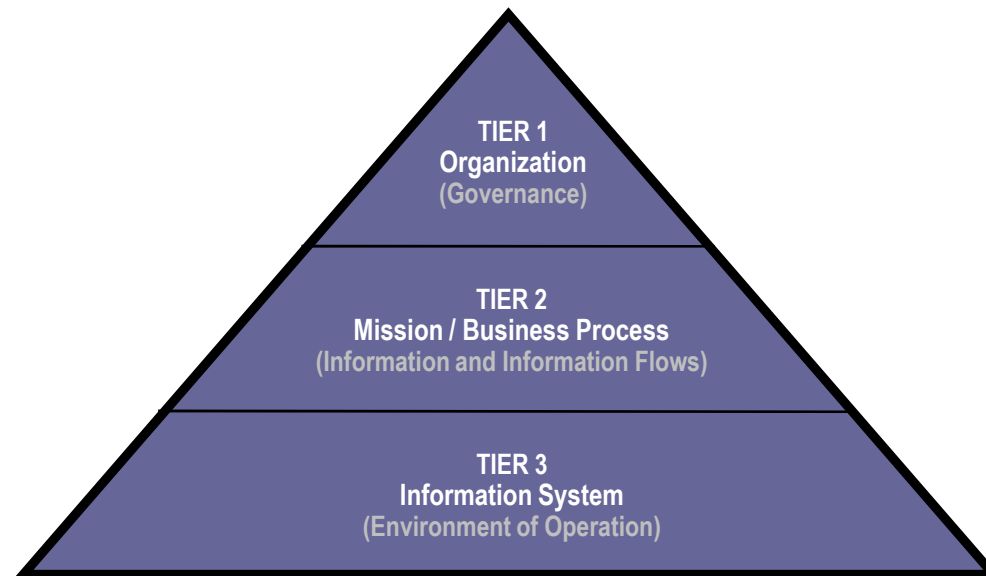


▶ *The egg ... (a.k.a Product Focused Assessments)*

- *SCAP - NIST-SCAP*
- *ISO/OMG W3C – KDM, BPMN, RIF, XMI, RDF*
- *OWASP Top 10*
- *SANS TOP 25*
- *Secure Code Check Lists*
- *Static Code Analysis*
- *Pen Test Results*



To effectively produce better code, SwA needs to translate to organizational and mission/ business-focused stakeholders



Source: NIST 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach

- ✓ **Applicable in diverse contexts – e.g., Defense, National Security, Finance, Health care, Aviations, Telecommunications**
- ✓ **Become a source of market differentiator rather than a source of liability or misunderstanding in acquisition decisions**

Executives want to understand the benefits to their organization

Executive Vocabulary

- ▶ Contributions to the bottom line
- ▶ Alignment with business strategy/plan
- ▶ Financial return for investing

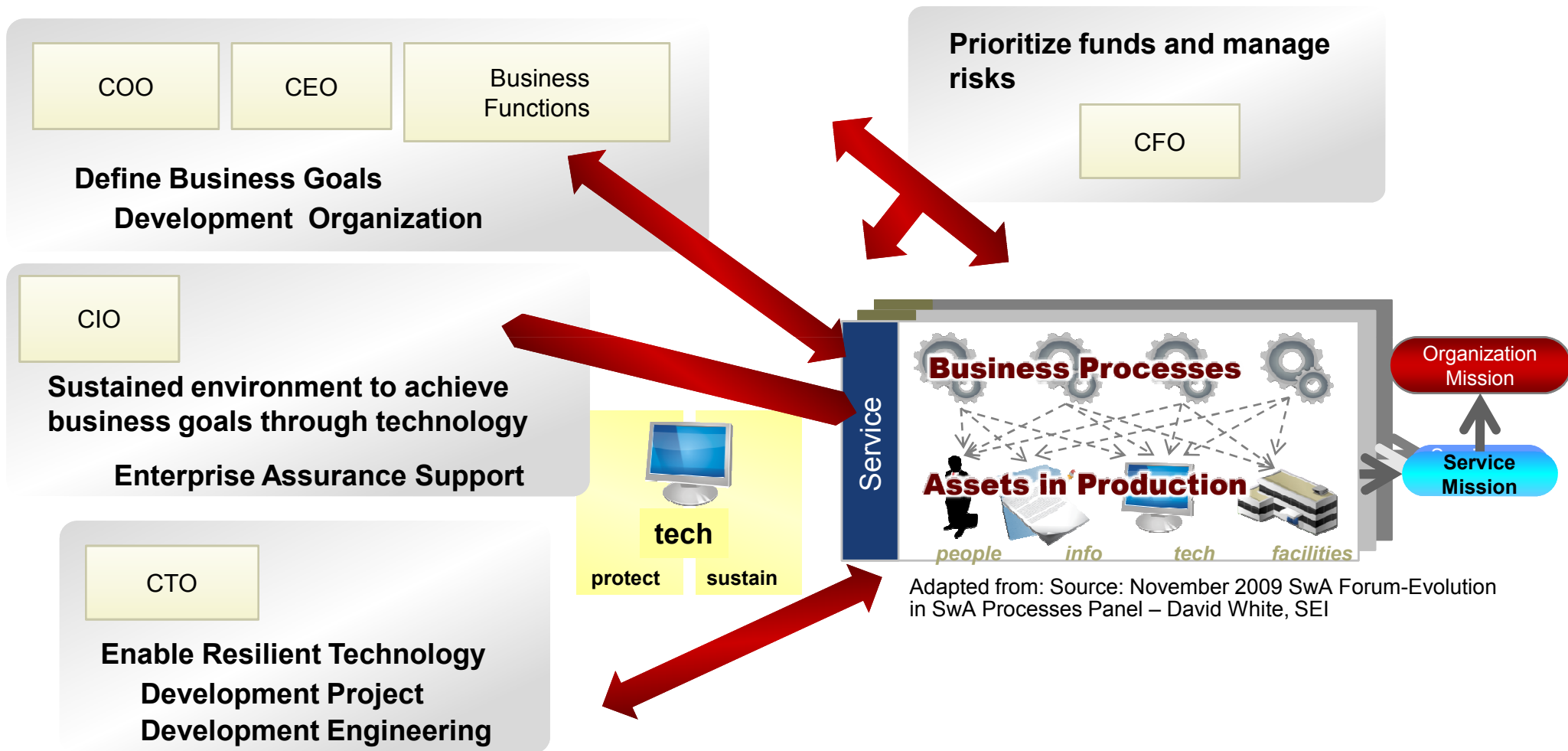
Payback Period
Net Present Value
Benefit/Cost Ratio
Return on Investment

Application Security Gaps

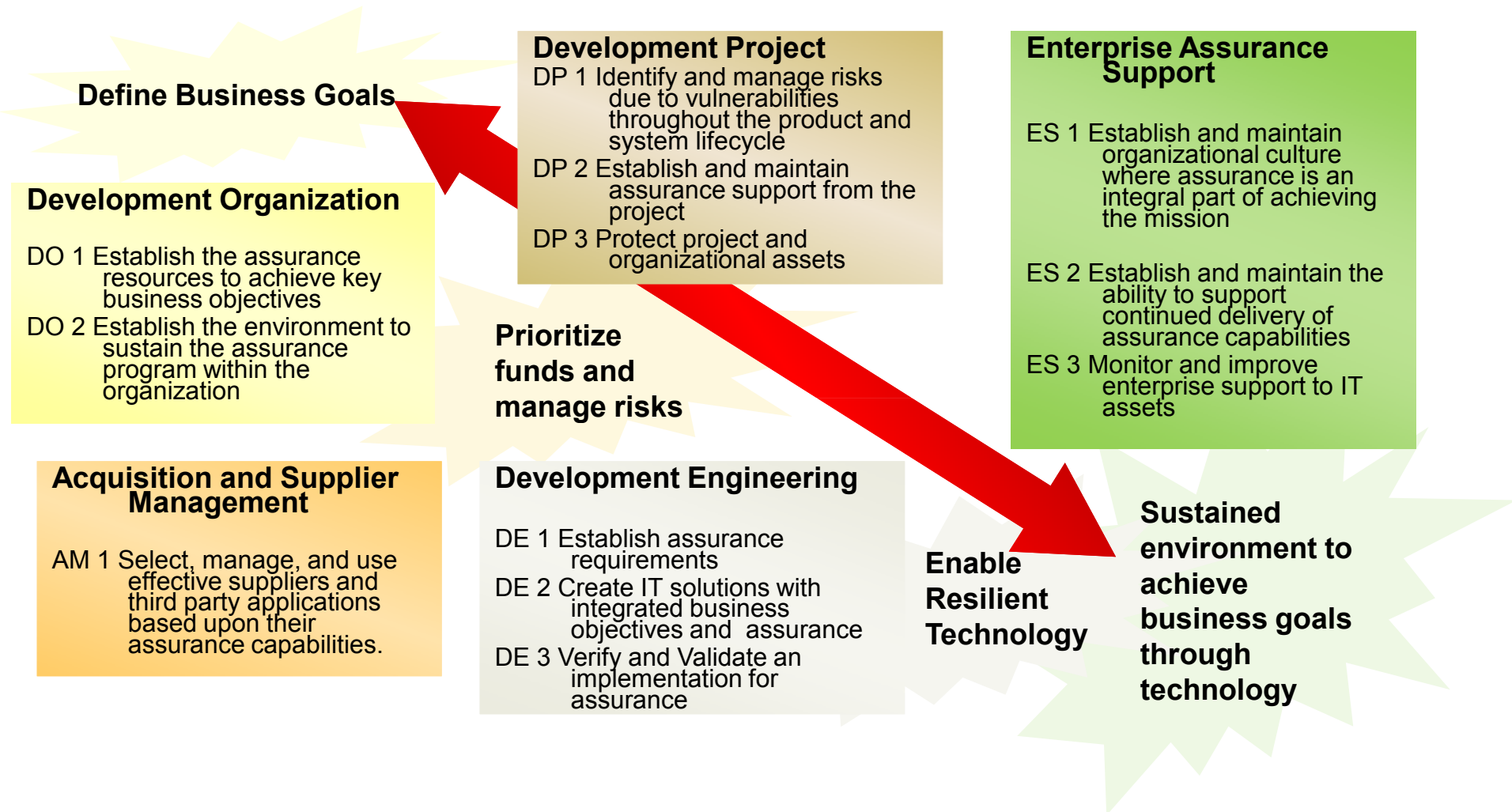
- ▶ Explicitly connect with business strategy and mission
- ▶ Address accomplishments
- ▶ Connect the dots at the enterprise level

It is a long term management process that may take time to demonstrate measurable results

Resiliency Management Model provides a framework for presenting our problem in executive terms

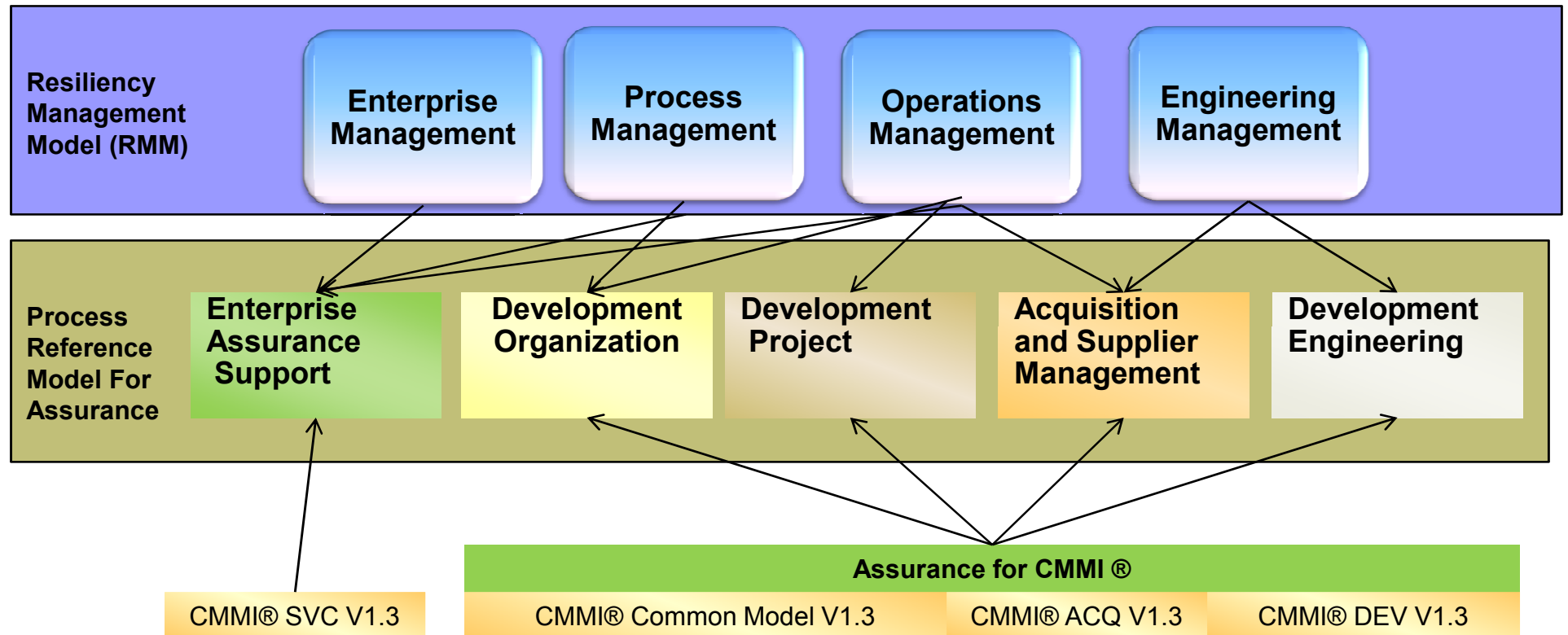


Assurance PRM provides a “vertical slice” that addresses assurance from executive to developer



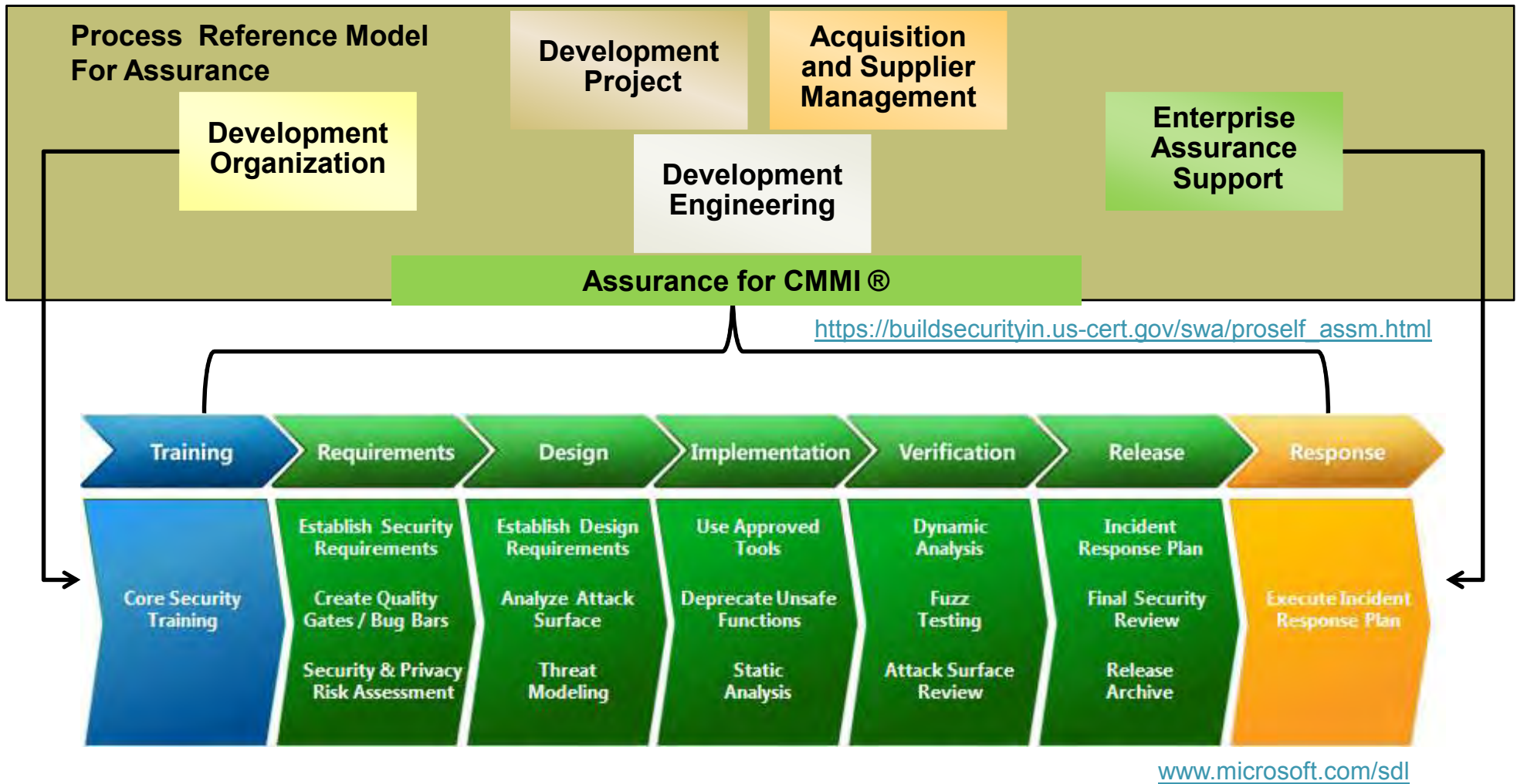
https://buildsecurityin.us-cert.gov/swa/proself_assm.html

Assurance PRM holistically connects executive-focused RMM and more detailed CMMI frameworks



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

The MS SDL Provides Ready To Use Resources For Application Security



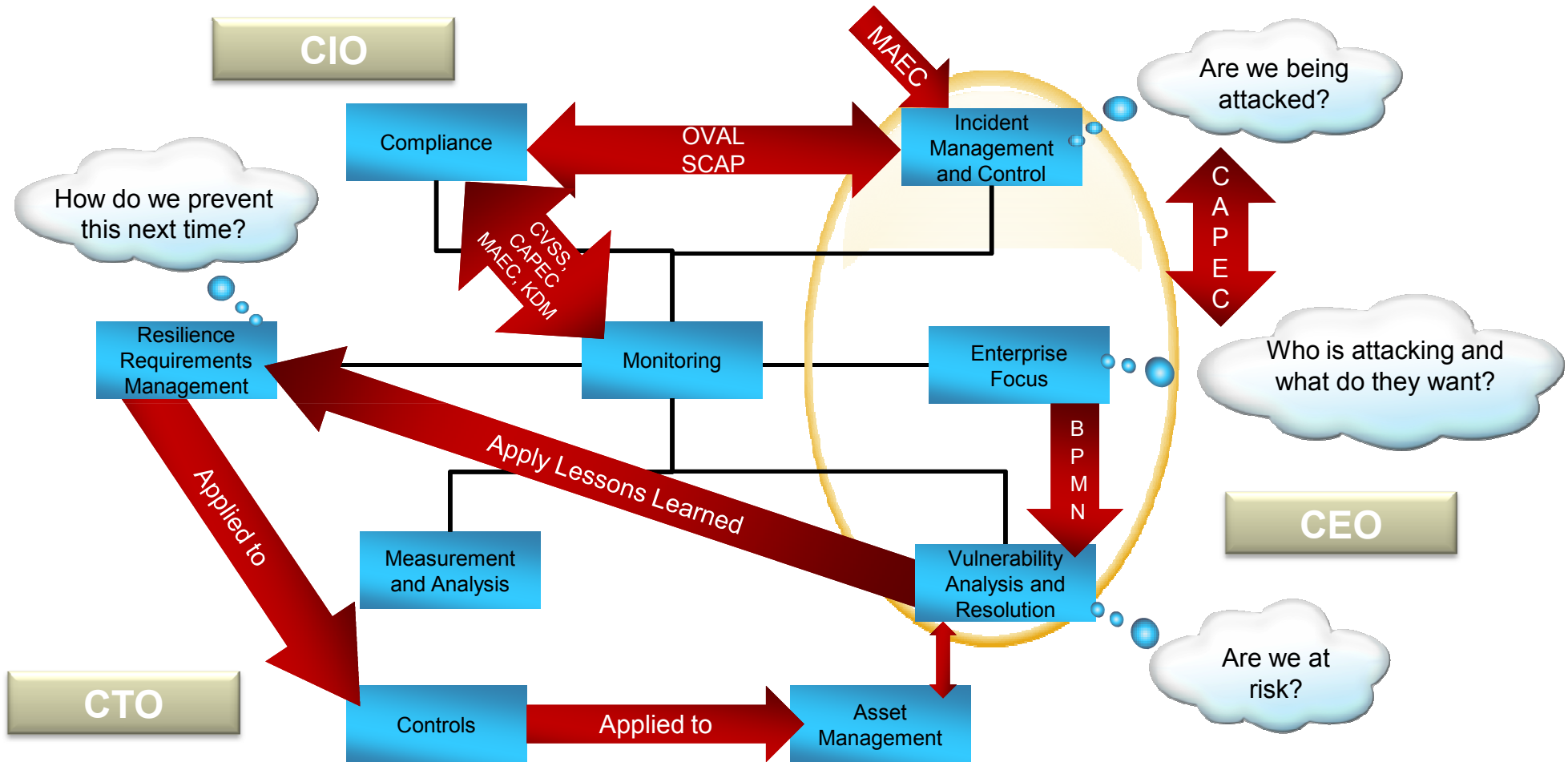
Multiple tools exist for measuring the implementation of SwA practices

Assessment Tool	Overview	Perspective
Capability Maturity Model Integration (CMMI)	Defines the “What” for systems and software development, services, and acquisition	Development, services, acquisition, and associated organizational elements
Resiliency Management Model (RMM)	Defines the “What” for converging security, business continuity, and IT operations in support of operational risk management	Enterprise Operations
Assurance Process Reference Model (PRM)	Defines the “What”-level practices for addressing assurance in the context of software/system, development, operations, and enterprise	Development and associated organizational and enterprise elements
Assurance for CMMI	Defines the “What”-level practices for addressing assurance in the context of software/system, development,	Development /integration in the context of CMMI
Microsoft Secure Development Lifecycle (SDL)	Detailed example of “How” for implementation of engineering efforts	Development
Open Software Assurance Maturity Model (SAMM)	Example of “How” from the context of software assurance with many examples portable to security architecture	Development, operations, and enterprise
Build Security In Maturity Model (BSIMM)	Example of “How” from the context of real world examples primarily from large product vendors and financial services organizations	Development, operations, and enterprise

Software Assurance Maturity Models identify pre-defined paths for implementing SwA



Understanding investment *impact* across the organization requires analysis and interpretation of diverse measures



Adapted from September 2010 SwA Forum, CERT RMM for Assurance , Lisa Young, SEI

To be effective, benchmarks should address all stakeholders and all relevant considerations

Process and Organization

- ▶ Process-based gap analysis or “SCAMPI-like” assessment
- ▶ Capability maturity benchmarks
- ▶ Expectations for repeatable results

Specific Practices

- ▶ Industry defined SwA program implementations
- ▶ Specific implementation paths
- ▶ Explicit milestones for tracking progress

- ▶ Resiliency Management Model (RMM)
- ▶ Assurance Process Reference Model (PRM)
- ▶ Assurance for CMMI
- ▶ Capability Maturity Model Integration (CMMI)

- ▶ Open Software Assurance Maturity Model (SAMM)
- ▶ Microsoft Secure Development Lifecycle (SDL) Optimization Model
- ▶ Build Security In Maturity Model (BSIMM)

We need to use a toolbox to be successful

- ▶ Very little of this is rocket science, however, it may be tedious and not exciting at times
- ▶ Both Process and Product assessments are valuable within specific contexts – we need to explicitly decide on our objectives to use them right
- ▶ There are LOTS of ways to communicate – no single way speaks to all audiences NOR it is effective by itself
- ▶ We are ALL trying to say the same things – we just use different words
- ▶ There is plenty of resources out there on how to develop better code
- ▶ There are also resources out there on how to demonstrate value

Benchmarking is possible today by using the wealth of the available content and applying it to the problem!!!

Nadya Bartol
Senior Associate

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
One Preserve Parkway
Rockville, MD 20852
Tel (301) 922-9537
bartol_nadya@bah.com

Michele Moss
Lead Associate

Booz | Allen | Hamilton

Booz Allen Hamilton Inc.
8283 Greensboro Dr
McLean, VA 22102
703-377-1254
moss_michele@bah.com

Back-up

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

The DHS SwA Processes and Practices Working Group has synthesized the contributions of leading government and industry experts into a set of high-level goals and supporting practices (an evolution of the SwA community's Assurance Process Reference Model)

The goals and practices are mapped to specific industry resources providing additional detail and real world implementation and supporting practices

- Assurance Focus for CMMI
- Building Security In Maturity Model
- Open Software Assurance Maturity Model
- CERT® Resilience Management Model
- CMMI for Acquisition
- CMMI for Development
- CMMI for Services
- SwA Community's Assurance Process Reference Model –Initial Mappings
- SwA Community's Assurance Process Reference Model - Self Assessment
- SwA Community's Assurance Process Reference Model – Mapping to Assurance Models

Other valuable resources that are in the process of being mapped include

- NIST IR 7622: DRAFT Piloting Supply Chain Risk Management Practices for Federal Information Systems
- NDIA System Assurance Guidebook
- Microsoft Security Development Lifecycle
- SAFECode