



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Processes and Practices Working Group

Paul Croll, CSC
Michele Moss, BAH

March 10, 2009



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

P&P WG Mission and Goals

- 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
- Share best practices
- Capture and discuss software assurance issues



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

DHS and DoD guidebooks relating to software assurance

- Enhancing the Development Life Cycle to Produce Secure Software, v2.0
 - https://www.thedacs.com/techs/enhanced_life_cycles/
- Engineering for System Assurance, v1.0
 - <http://www.acq.osd.mil/sse/ssa/docs/SA-Guidebook-v1-Oct2008.pdf>
 - http://www.ndia.org/Template.cfm?Section=NDIA_Divisions_Page&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=3&ContentID=677

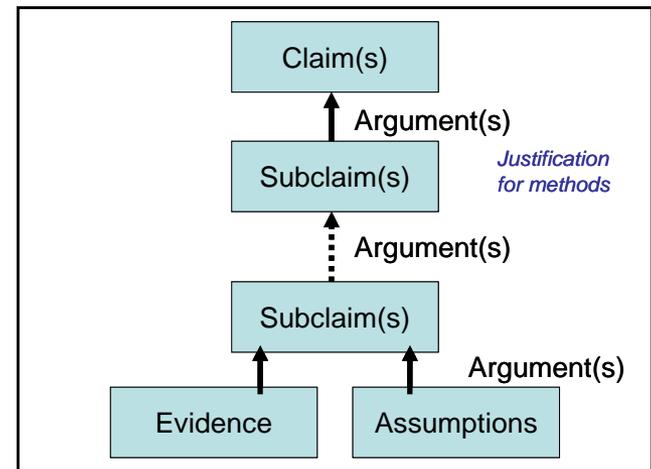


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

National and international software assurance standards - SC7

- The goal of 15026 is to provide a set of generic hooks:
 - To the life cycle process standards of SC 7
 - For use by specialty engineering disciplines
- Centerpiece is an “assurance case”
- *The assurance case itself is an element of the system.*



Planned Parts:

- 15026-1: Concepts and vocabulary (initially a TR2 and then revised to be an IS) [2009]
- 15026-2: Assurance case (including planning for the assurance case itself) [2009]
- 15026-3: System integrity levels (a revision of the 1998 standard)
- 15026-4: Assurance in the life cycle (including project planning for assurance considerations)



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

***National and international software assurance standards –
SC27***

- A variety of standards in progress related to SwA including
 - ISO/IEC 27034 – Application Security (multipart)
 - ISO/IEC 29147 – Responsible Vulnerability Disclosure
- A variety of proposed standards related to SwA
 - Guidelines for Security of Outsourcing
 - Information Security Governance Framework
 - Secure System Engineering Principles and Techniques



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

National and international software assurance standards – SC22

Outline of Current Draft of ISO/IEC 24772 Vulnerability Template

- Scope
- References
- Terms and Definitions
- Vulnerability Issues
- Programming Language Vulnerabilities
 - (Currently 48 of them)
- Application Vulnerabilities
 - (Currently 18 of them, selected because of relationship to languages)



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

P&P WG Mission and Goals

- 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
- Share best practices
- Capture and discuss software assurance issues



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Share Best Practices

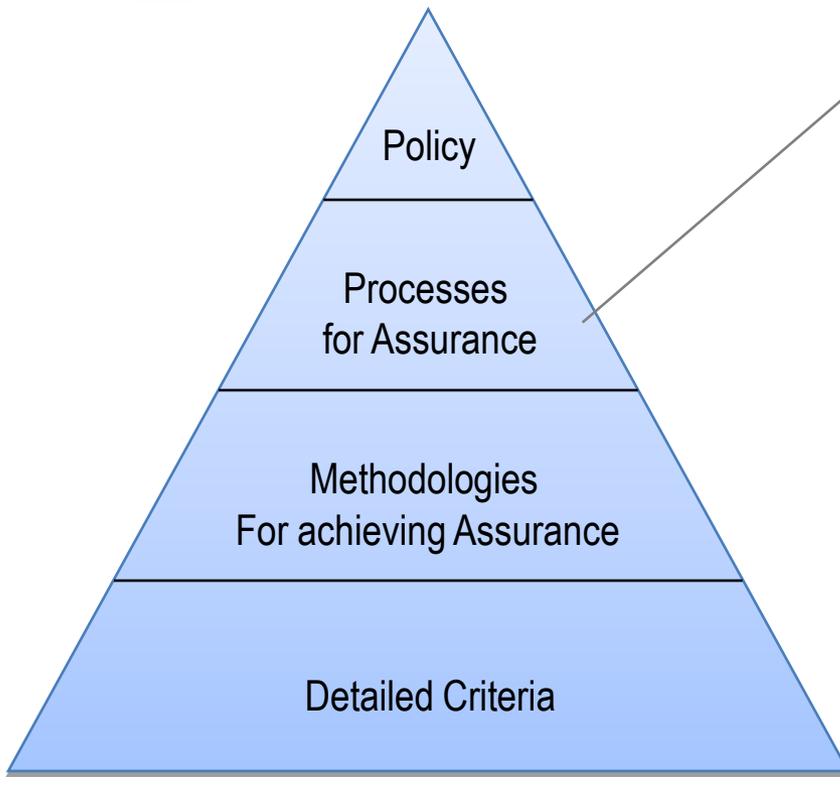
- Updating the Processes and Practices portion of the Software Assurance Community Resources and Information Clearinghouse (CRIC)
- Developing Pocket Guides as resources for users



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance for CMMI®



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

Focus Topic: Assurance for CMMI® defines the Assurance Thread for Implementation and Improvement of Assurance Practices

Gap analysis can be used to help organizations

- Gain knowledge of assurance practices and risks
- Identify process gaps and risks
- Prioritize organizational efforts and funding
- Define and plan improvement actions



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Progress Update

- March 2007: SEPG Birds of a Feather
- August 7, 2007: Industry Assurance for CMMI ® Meeting
- September 2007: Motorola, Lockheed Martin and Booz Allen form Assurance Working Group
- October 2007 – present: Assurance Harmonization Working Group
- January 2008 – present: Assurance Focus Topic Working Group
- July 16, 2008: Gained CMMI ® Steering Group approval to create Focus Topic for Assurance
- Today
 - Working with CMMI ® Architecture Team to develop a Focus Topic that documents the assurance thread through the CMMI ®
 - Refining practices and mapping to CMMI ® as necessary
 - Collecting feedback on use of draft materials
 - Submitted CRs for inclusion of content in CMMI-DEV V1.3



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Change Request for CMMI-DEV 1.3 Model Content

Requested Change

- Expand the current informative material in CMMI - DEV v1.2 to more specifically address assurance activities that enable predictable execution and trustworthiness of products and services. Assurance practices have been harmonized and are articulated in a format compatible with the CMMI. The latest work products from this effort are available at <https://buildsecurityin.us-cert.gov/swa/procwg.html>

Rational

- Growing considerations related to globalization, systems of systems, system survivability, and cyber issues have resulted in an increasing number of organizations evolving the approach to address software and systems assurance in their products and services. Many of these organizations are formulating and implementing best practices and standards covering security, safety and reliability in the context of CMMI-DEV practices. Incorporating informative information in select CMMI-DEV practices will enable more streamlined planning, implementation, evaluation, and improvement of practices used to create and maintain products and services



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Change Request for CMMI-DEV 1.3 Appraisal Method

Requested Change

- Establish a mechanism to enable use of the CMMI constellations and SCAMPI method with other frameworks and models deployed by organizations. Examples of other frameworks would include ISO 9000 and the Focus Topic for Assurance. The mechanism established should facilitate integration of the other frameworks/models with CMMI for both process improvement and appraisal. When other frameworks/models are used in conjunction with SCAMPI, they should be documented in the ADS. Given the challenges associated with integrating CMMI with other frameworks and models, consideration should be given to initially integrating those that more easily align architecturally with CMMI (e.g, CMMI Focus Topics) and those for which there is high user interest/need for alignment (e.g, in the assurance arena).

Rational

- Establish a mechanism to enable use of the CMMI constellations and SCAMPI method with other frameworks and models deployed by organizations. Examples of other frameworks would include ISO 9000 and the Focus Topic for Assurance. The mechanism established should facilitate integration of the other frameworks/models with CMMI for both process improvement and appraisal. When other frameworks/models are used in conjunction with SCAMPI, they should be documented in the ADS. Given the challenges associated with integrating CMMI with other frameworks and models, consideration should be given to initially integrating those that more easily align architecturally with CMMI (e.g, CMMI Focus Topics) and those for which there is high user interest/need for alignment (e.g, in the assurance arena).



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

P&P WG Mission and Goals

- 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
- Share best practices
- Capture and discuss software assurance issues



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Processes and Practices December Session

- ISO Standards Update - *Jim Moore, Mitre; Nayda Bartol, BAH; and Robert Seacord, SEI*
- Software Assurance SMARTS (Skills Measuring Assessment and Reinforced Training Solutions) - *Mano Paul, SecuRisk Solutions*
- SwA Business Case Effort - *Carol Woody, CMU*
- Update on the Assurance for CMMI Practices - *Michele Moss, BAH; Margaret Nadworny*
- SwA Pocket Reference Guide Proposal Review- *Pedro Vales, CTC*
- Panel on Overcoming the Barriers to Adoption of Assurance Practices -
Moderator: Carol Woody, SEI; Rama Moorthy, CEO, Hatha Systems; Robert Seacord, Secure Coding Team Lead, CERT/SEI; Dan Reddy, Consulting Product Manager Information Security, EMC²; Dr. Linda Wilbanks, Chief Information Officer, National Nuclear Security Administration
- Brainstorm: Reaching a Broader Audience - *Paul Croll, CSC & Michele Moss, BAH*



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

What can you do?

- *Leverage existing resources to get started*
- *Watch for updates <https://buildsecurityin.us-cert.gov/swa/progresrc.html>*
- *Share your Lessons Learned (swawg-process @ cert.org)*
- *Attend the Summer Working Group Sessions and contribute to discussions on using available resources*



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

For More Information . . .

Paul R. Croll
CSC
17021 Combs Drive
King George, VA 22485

Phone: +1 540.644.6224
Fax: +1 540.663.0276
e-mail: pcroll@csc.com

Michele Moss
Booz Allen Hamilton
8283 Greensboro Drive
McLean, VA 22102

Phone: +1 703.377.1254
Fax: +1 703.902.3595
e-mail: moss_michele@bah.com