



SOFTWARE ASSURANCE FORUM

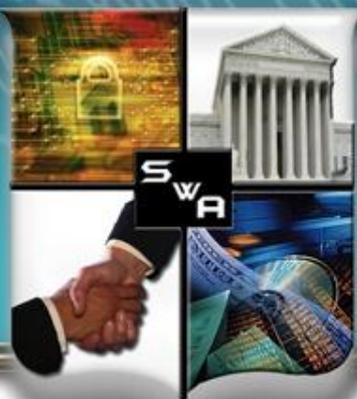
BUILDING SECURITY IN

Leveraging SwA Automation throughout the SDLC

SwA Working Groups June 26, 2012

Michele Moss, Booz Allen Hamilton

Paul Croll, CSC



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

DHS Software Assurance (SwA) Community

Through public-private collaboration promotes security and resilience of software throughout the lifecycle; focused on reducing exploitable software weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient software products. Collaboratively advancing software-relevant rating schemes

... encourage the production, evaluation and acquisition of better quality and more secure software through targeting

People

Developers and users education & training

Processes

Sound practices, standards, & practical guidelines for secure software development

Technology

Security test criteria, diagnostic tools, common enumerations, SwA R&D, and SwA measurement

Acquisition

Software security improvements through due-diligence questions, specs and guidelines for acquisitions/ outsourcing

* SwA Forum is part of the Cross-Sector Cyber Security Working Group (CSCSWG) established under auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) that provides legal framework for participation.



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Processes & Practices Goals

- 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



SOFTWARE ASSURANCE FORUM

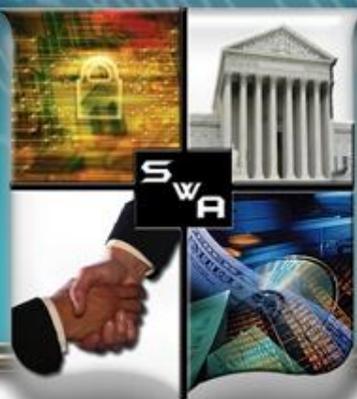
BUILDING SECURITY IN

Processes & Practices Expected Outcomes

- 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

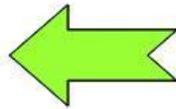
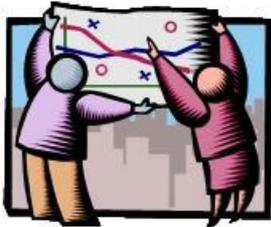


SOFTWARE ASSURANCE FORUM

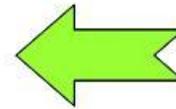
BUILDING SECURITY IN

Achieving System and Software Assurance (the early years)

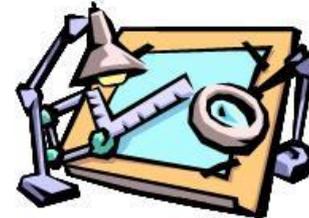
1. Understand Your Business Requirements for Assurance



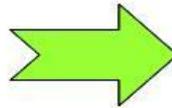
5. Measure Your Results - Modify Processes as Necessary



4. Build or Refine and Execute Your Assurance Processes



2. Look to the CMMI® for Assurance-Related Process Capability Expectations



3. Look to Standards for Assurance Process Detail

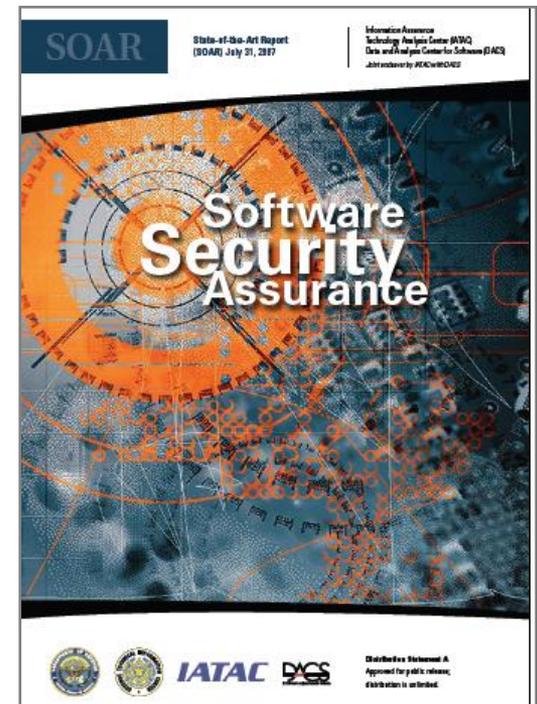




SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Software Security Assurance: A State of the Art Report

- Describes numerous methodologies, best practices, technologies, and tools currently being used to specify, design, and implement software that will be less vulnerable to attack, and to verify its attack-resistance, attack-tolerance, and attack-resilience;
- Offers a large number of available print and online resources from which readers can learn more about the principles and practices that constitute Software Security Assurance;
- Provides observations about potentials for success, remaining shortcomings, and emerging trends across the S/W Security Assurance landscape.



<http://iac.dtic.mil/iatac/download/security.pdf>



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Toward an Organization for Software System Security

Principles and Guidelines

0. Introduction

- 0.1/0.2 Purpose / Scope
- 0.3 Reasoning Underlying The Organization
- 0.4 Organization Of Remainder Of Document

1. The Adverse

- 1.1. Limit, Reduce, Or Manage Violators
- 1.2. Limit, Reduce, Or Manage Benefits To Violators Or Attackers
- 1.3. Increase Attacker Losses
- 1.4. Increase Attacker Uncertainty

2. The System

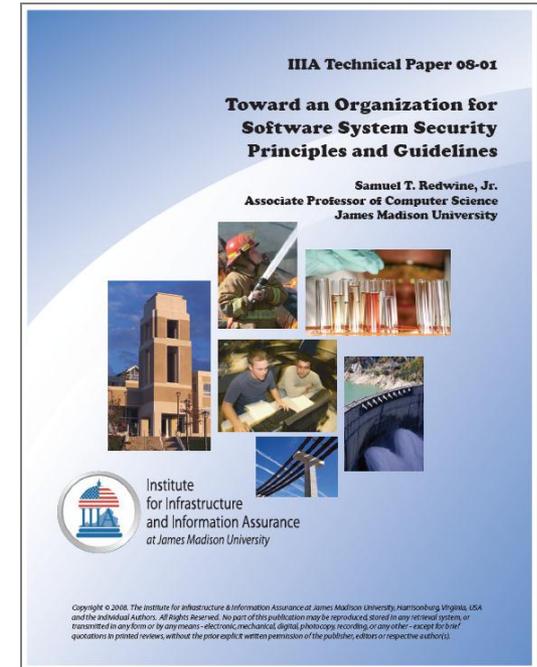
- 2.1. Limit, Reduce, Or Manage Violations
- 2.2. Improve Benefits Or Avoid Adverse Effects On System Benefits
- 2.3. Limit, Reduce, Or Manage Security-related Costs
- 2.4. Limit, Reduce, Or Manage Security-related Uncertainties

3. The Environment

- 3.1. Nature Of Environment
- 3.2. Benefits To And From Environment
- 3.3. Limit, Reduce, Or Manage Environment-related Losses
- 3.4. Limit, Reduce, Or Manage Environment-related Uncertainties

4. Conclusion

- 5. Appendix A: Principles Of War
- 6. Appendix B: Purpose-condition-action-result Matrix
- 7/8. Bibliography / Acknowledgements



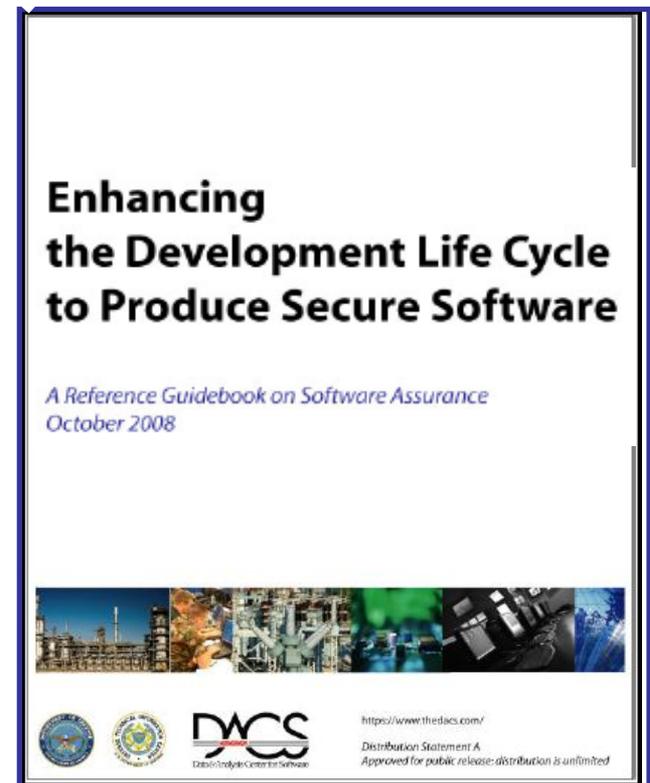


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

*Enhancing the Development Life Cycle to
Produce Secure Software, v2.0*

- Does provide information to help readers understand, assess, and choose from among the growing number of security-enhancing SDLC processes, methodologies, practices, techniques, and supporting tools
- Does not espouse a specific approach or philosophy.
- Does not attempt to evaluate or critique security-enhancement approaches



https://www.thedacs.com/techs/enhanced_life_cycles/



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Software Project Management for Software Assurance: DACS State-of-the-Art Report

- The primary audience for this report is software project managers
- Information on how the need for software assurance affects software project management
- Tools and resources for quantifying the effects of software assurance on software development, both in terms of planning (cost estimation and budgeting), and in terms of overall cost-effectiveness and return on investment
- DACS Report Number 347617

**Software Project Management
for
Software Assurance**

A DACS State-of-the-Art Report
DACS Report Number 347617
Contract Number SP0700-98-D-4000
(Data & Analysis Center for Software)

30 September 2007

PREPARED FOR:
Air Force Research Laboratory
AFRL/IFT
525 Brooks Road
Griffiss AFB, NY 13441-5700

PREPARED BY:
Elaine Feitchak
Thomas McGibbon
Robert Vienmeau

ITT Advanced Engineering and Sciences
775 Dardarian Drive
Rome, NY 13441

Distribution Statement A
Approved for public release; distribution is unlimited



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Engineering for System Assurance, v1.0

- NDIA/DoD guidebook providing process and technology guidance to increase the level of system assurance.
- Intended primarily to aid program managers (PMs) and systems engineers (SEs) who are seeking guidance on how to incorporate assurance measures into their system life cycles.

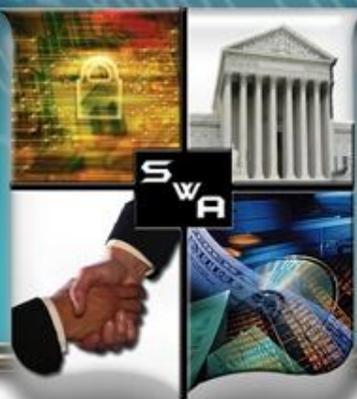
ENGINEERING FOR SYSTEM ASSURANCE

Version 1.0

National Defense Industrial Association
System Assurance Committee



<http://www.acq.osd.mil/sse/ssa/docs/SA-Guidebook-v1-Oct2008.pdf>



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Microsoft Security Development Lifecycle (SDL)

Delivering secure software requires:

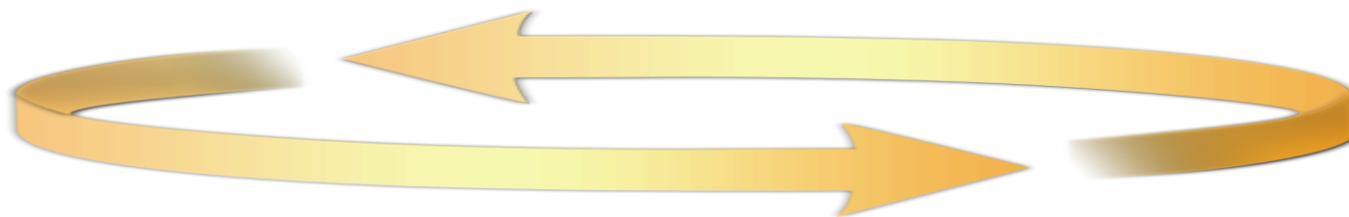
Executive commitment → SDL a mandatory policy at Microsoft since 2004



Education

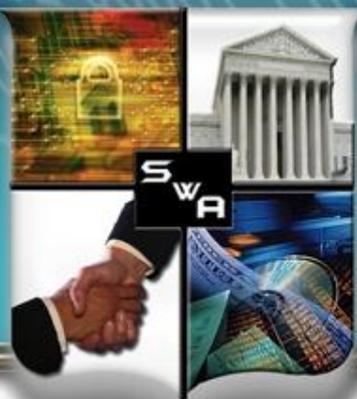
Technology and Process

Accountability



Ongoing Process Improvements → 6 month cycle

<http://www.microsoft.com/sdl>

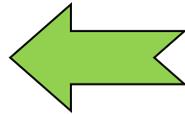


SOFTWARE ASSURANCE FORUM

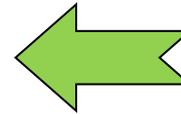
BUILDING SECURITY IN

Achieving System and Software Assurance (the early years)

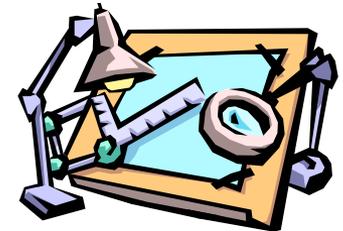
1. Understand Your Business Requirements for Assurance



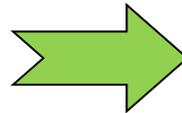
5. Measure Your Results - Modify Processes as Necessary



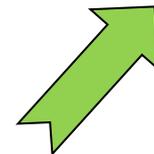
4. Build or Refine and Execute Your Assurance Processes

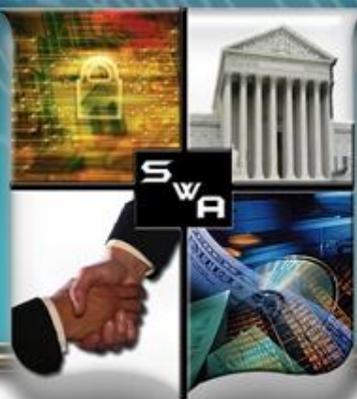


2. Use Assurance-Related Process Capability Expectations



3. Look to Standards for Assurance Process Detail



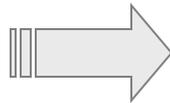


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Addressing the Relationship between Quality and Assurance

Requirements



What is wanted

What is created

Unmet requirements

Extra Requirements

Quality - Does the result meet the requirements?

Assurance -

- What other features are enabled?
- How do these other features impact the original requirements?

**It isn't about Quality OR Assurance ...
It is about Quality AND Assurance**

Courtesy of Margaret Nadworny and Michele Moss



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Addressing Assurance Capability

- June 2007 – SwA P&P Working Group initiated efforts to collaborate with industry (SEI and ISSEA) to integrate security in capability based process improvement and capability benchmarking
- 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: Assurance Harmonization Working Group
- January 2008: Assurance Focus Topic Working Group
- July 16, 2008: Gained CMMI ® Steering Group approval to create Focus Topic for Assurance
- February 27, 2009: Submitted Change Requests for consideration in CMMI v 1.3
- Updating Assurance PRM practices with refined practices, revised CMMI mapping, and industry LL



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Industry Concerns with Security Benchmarks

- If there is a one size fits all solution, it must be at a level of detail that the context is applicable in diverse contexts (Defense, National Security, Finance, Health care, Aviations, Telecommunications)
- Discomfort in using assurance for acquisition decisions
 - Potential source of liability – false sense of assurance
 - Integrity of appraisals – exaggerated claims
 - Potential misinterpretation of appraisal results - Cannot ensure that any product is secure
- Implementation of the current model is costly – cognizant of increased size/scope of model
- We don't need another certification!
- Assurance must be built in



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

August 7, 2007 “Assurance” Workshop

- Objectives
 - Discuss “Best Practices” for Assurance
 - Identify sources of best practices for assurance
 - Understand Lessons Learned associated with use of assurance processes and practices
 - Understand stakeholder views for deploying practices and addressing assurance in CMMI®
- Participants
 - Government, Industry, Academia
 - Acquirers, vendors, developers, standards organizations, test labs, and research

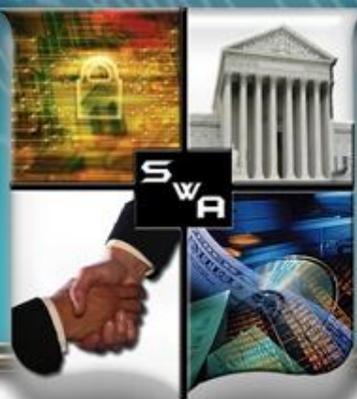


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Challenges in Creating an Assurance Capability Framework

- Key references were in “draft” or a presentation/discussion
- The practices were not codified in a standard
- Solutions were being identified through “Research” and pilots
- The acquisition community was not requesting the practices – no demand
- Relied on assumptions that were not valid (raise awareness and they will act)
- Outreach efforts resulted – “So what do you want me to do?”
- Existing documentation was in SwA Community speak



SOFTWARE ASSURANCE FORUM

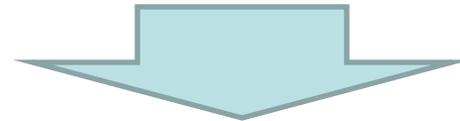
BUILDING SECURITY IN

Our Assurance Capability Framework Enables Communication

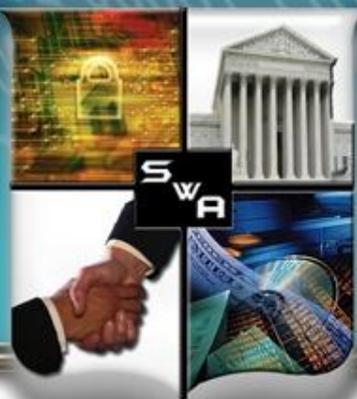
Project leadership and team members need to know where and how to contribute



- 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

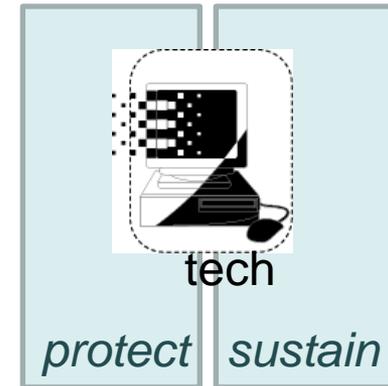


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Resiliency Begins At The Asset Level

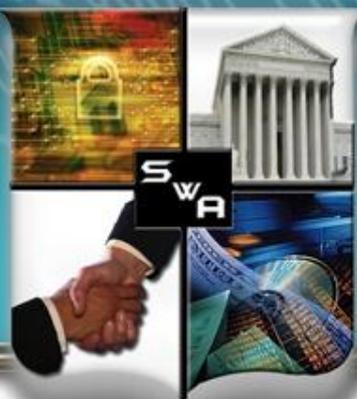
- Resiliency requirements form basis for protection and sustainment of an asset
- Resiliency requirements are informed by
 - Organization's mission and strategy
 - Role of the asset in the service
 - Asset interdependencies
- Resiliency requirements must be addressed in development & acquisition of new software assets



CERT® Resiliency Management Model (RMM) is a process improvement model that addresses

Convergence of security, business continuity, and IT operations to manage operational Risk and establish operational resiliency

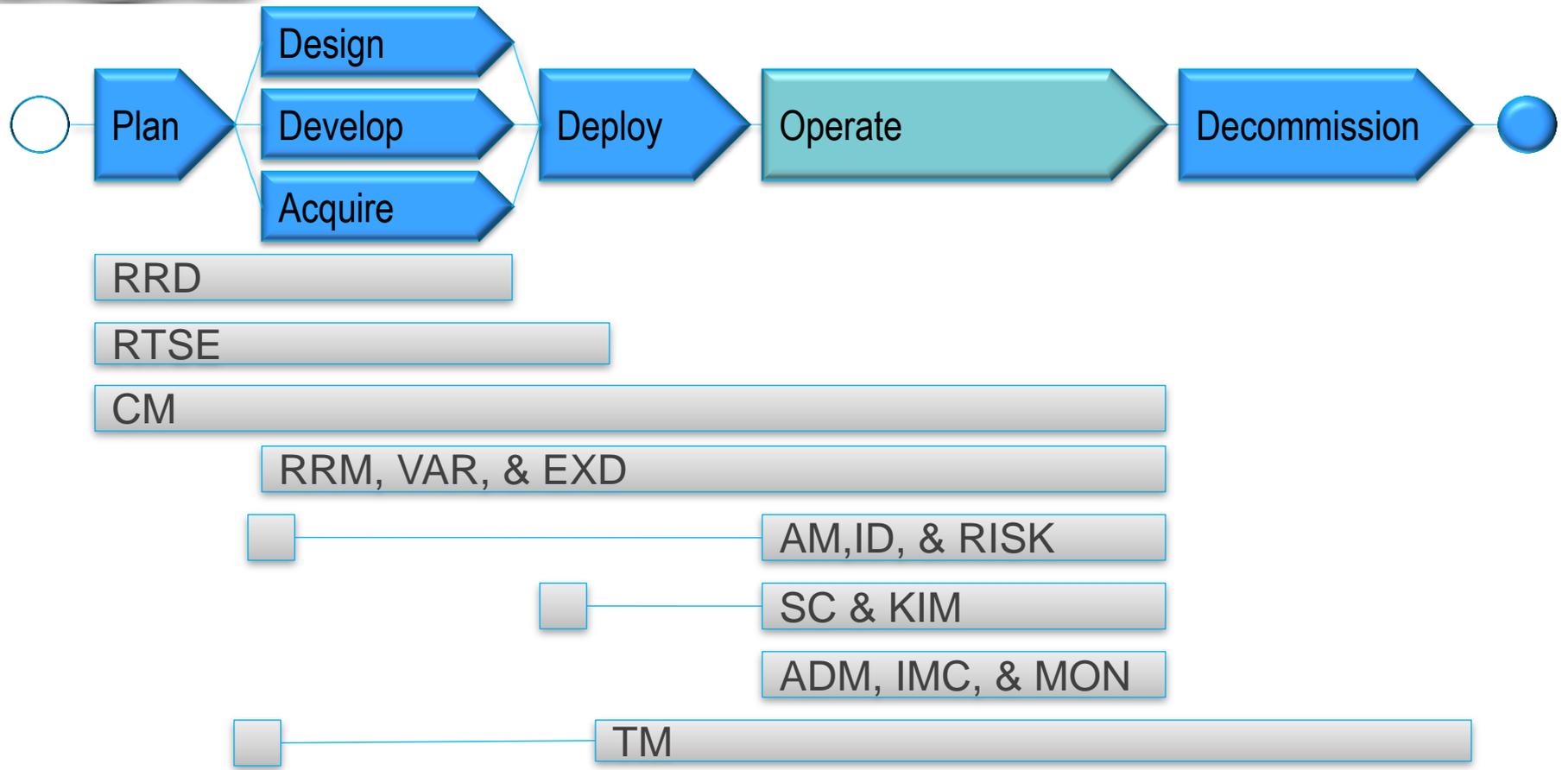
<http://www.cert.org/resiliency/rmm.html>

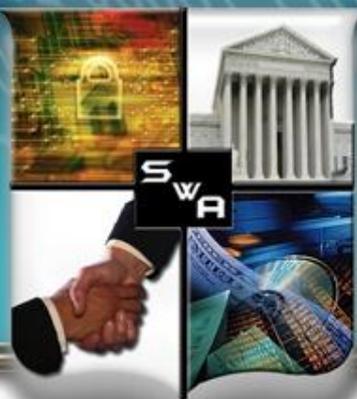


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

RTSE: Software Assurance View





SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

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

Define Business Goals

Development Organization

- DO 1 Establish the assurance resources to achieve key business objectives
- DO 2 Establish the environment to sustain the assurance program within the organization

Acquisition and Supplier Management

- AM 1 Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities.

Development Project

- DP 1 Identify and manage risks due to vulnerabilities throughout the product and system lifecycle
- DP 2 Establish and maintain assurance support from the project
- DP 3 Protect project and organizational assets

Prioritize funds and manage risks

Development Engineering

- DE 1 Establish assurance requirements
- DE 2 Create IT solutions with integrated business objectives and assurance
- DE 3 Verify and Validate an implementation for assurance

Enterprise Assurance Support

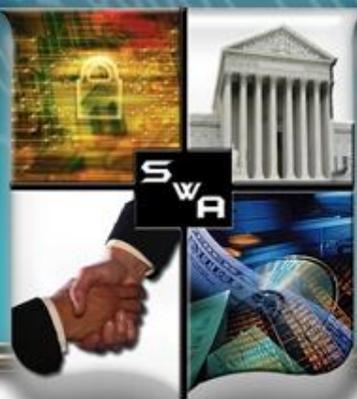
- ES 1 Establish and maintain organizational culture where assurance is an integral part of achieving the mission
- ES 2 Establish and maintain the ability to support continued delivery of assurance capabilities
- ES 3 Monitor and improve enterprise support to IT assets

Enable Resilient Technology

Sustained environment to achieve business goals through technology

The Assurance PRM Is A Holistic Framework that connects CMMI and RMM to facilitate communication

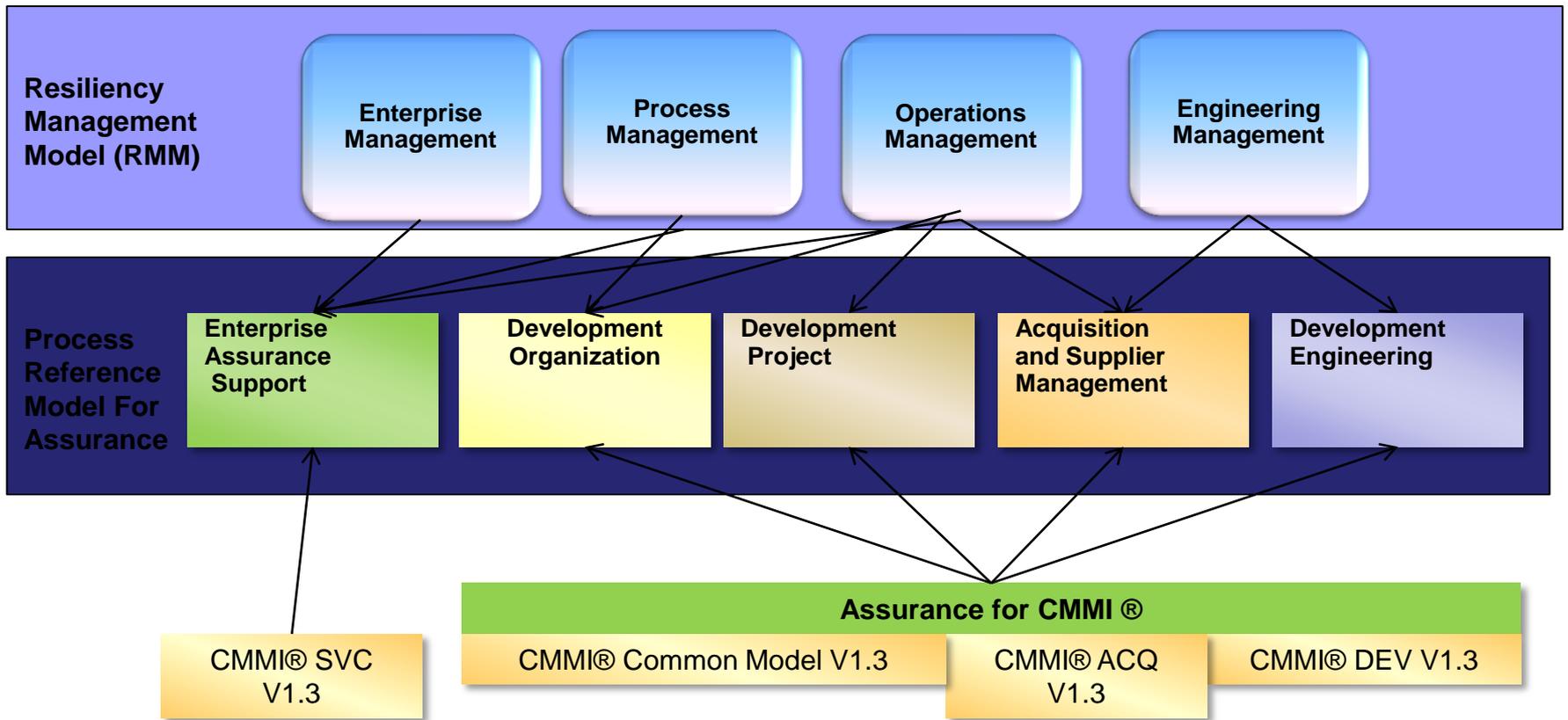
https://buildsecurityin.us-cert.gov/swa/proself_assm.html

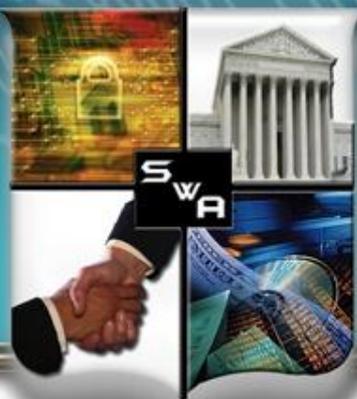


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

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





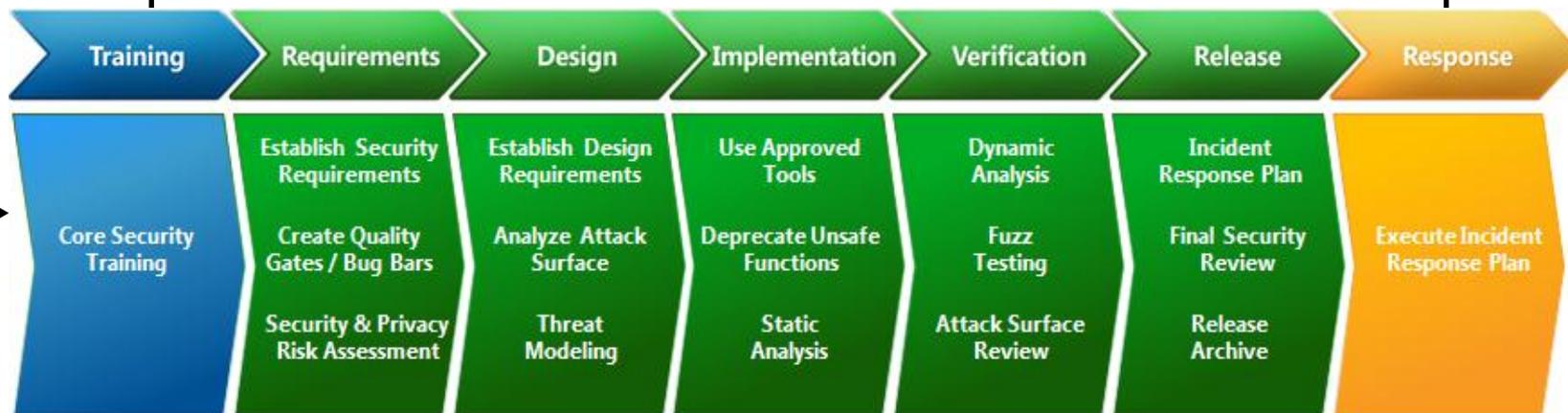
SOFTWARE ASSURANCE FORUM

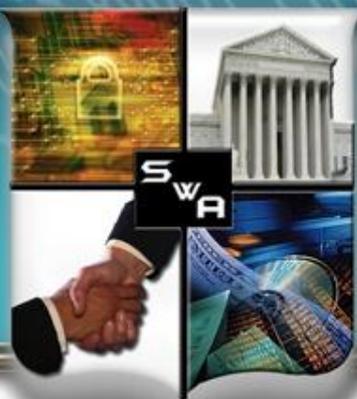
BUILDING SECURITY IN

The MS SDL Provides Ready To Use Resources For Application Security



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



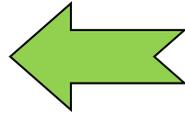


SOFTWARE ASSURANCE FORUM

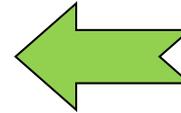
BUILDING SECURITY IN

Achieving System and Software Assurance (the early years)

1. Understand Your Business Requirements for Assurance



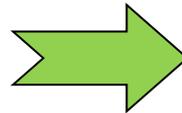
5. Measure Your Results - Modify Processes as Necessary



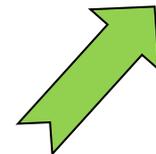
4. Build or Refine and Execute Your Assurance Processes

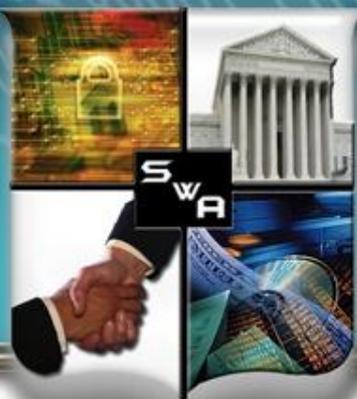


2. Use Assurance-Related Process Capability Expectations



3. Look to Standards for Assurance Process Detail





SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Software Security Engineering: A Guide for Project Managers



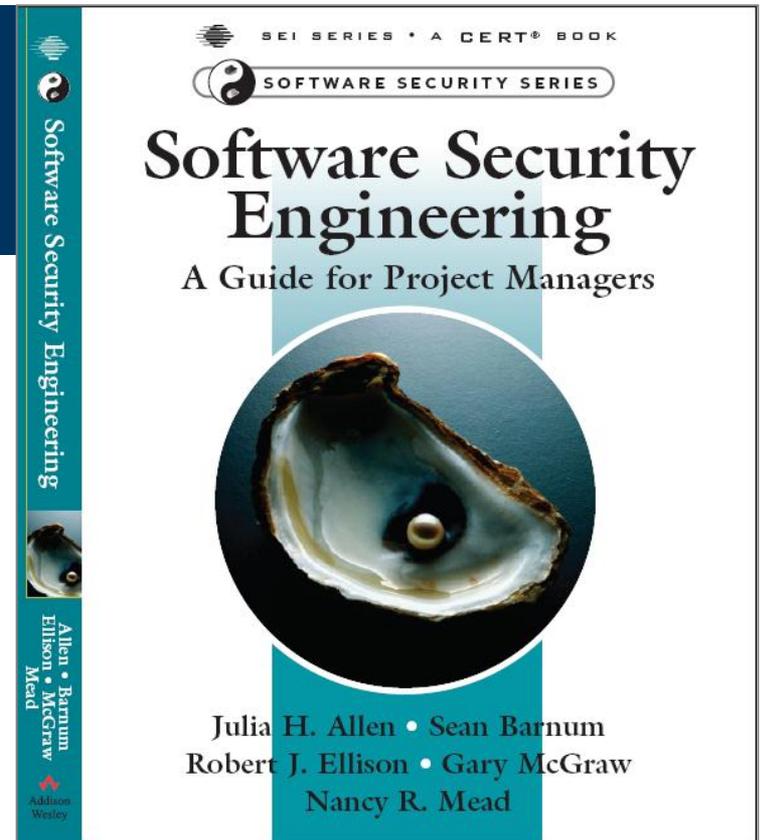
Build Security In

Setting a Higher Standard for Software Assurance

Sponsored by DHS National Cyber Security Division



- Organized for Project Managers
 - Derives material from DHS SwA “Build Security In” web site
 - <https://buildsecurityin.us-cert.gov>
 - Provides a process focus for projects delivering software-intensive products and systems
- Published in May 2008



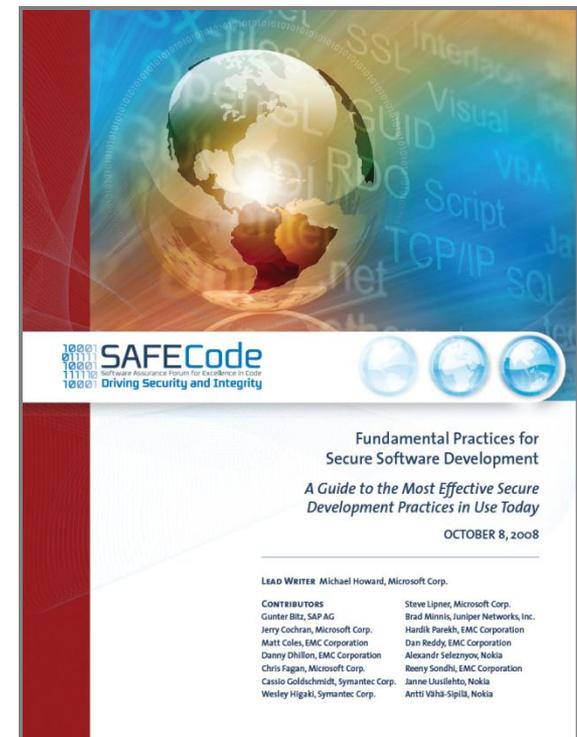


SOFTWARE ASSURANCE FORUM

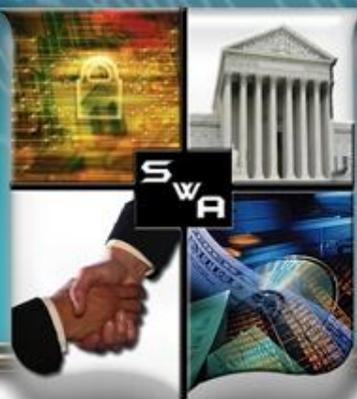
BUILDING SECURITY IN

SAFECode

- Fundamental Practices for Secure Software Development: Guide to the Most Effective Secure Development Practices in Use Today, Oct 8, 2008
 - Common security-related elements of software development methodologies
 - Secure Programming practices:
 - Test to validate robustness and security
 - Code Integrity and Handling
 - Documentation (about software security posture & secure configurations)



http://www.safecode.org/publications/SAFECode_Dev_Practices1008.pdf



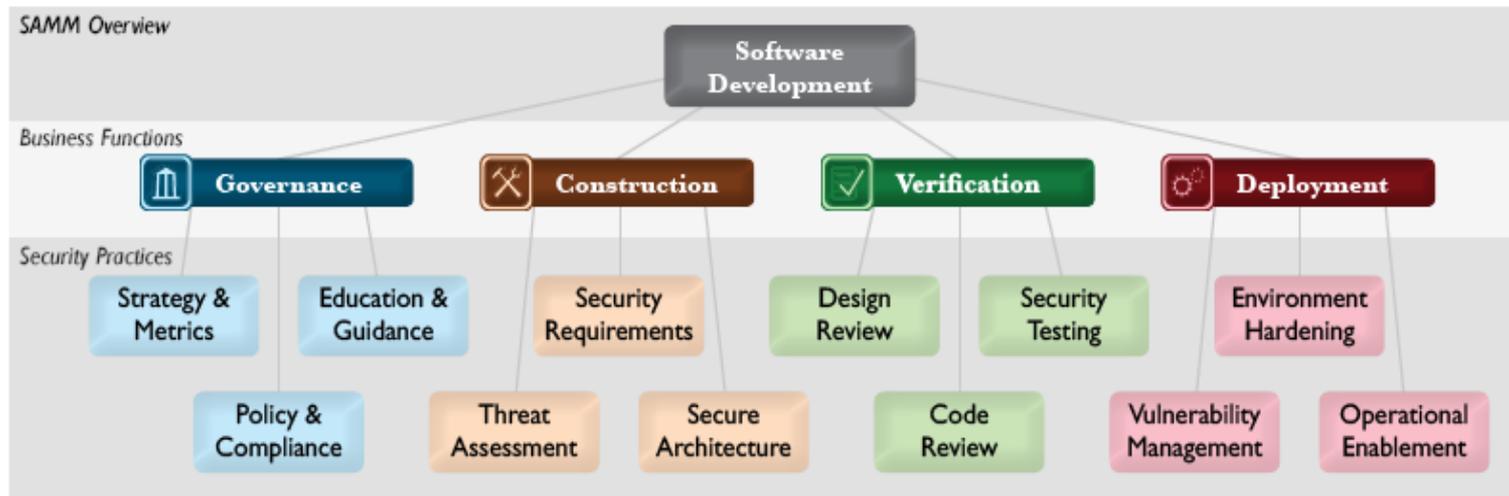
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

OPEN SAMM

– Open Software Assurance Maturity Model (SAMM)

- ▶ <http://www.opensamm.org/>
- ▶ Open framework to help organizations formulate and implement a strategy for software security tailored to specific risks



<http://www.opensamm.org/downloads/SAMM-1.0.pdf>



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN *BSIMM*

– Building Security In Maturity Model (BSIMM)

- ▶ <http://www.bsimm2.com/>
- ▶ Is designed to help understand and plan a software security initiative
- ▶ BSIMM was created through a process of understanding and analyzing real-world data from nine leading software security initiatives
- ▶ BSIMM uses a Software Security Framework (SSF), to provide a conceptual scaffolding for the model
- ▶ Properly used, BSIMM can help determine where your organization stands with respect to real-world software security initiatives and what steps can be taken to make your approach more effective.

– BSIMM

- ▶ Not a complete "how to" guide for software security, nor is it a one size fits all model
- ▶ It is a collection of good ideas and activities that are in use today



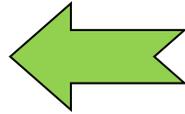
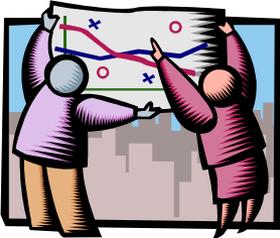


SOFTWARE ASSURANCE FORUM

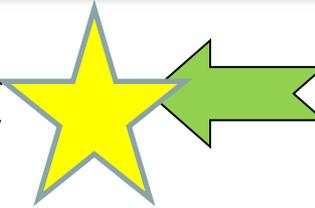
BUILDING SECURITY IN

Achieving System and Software Assurance (the early years)

1. Understand Your Business Requirements for Assurance



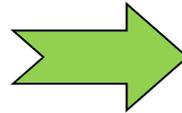
5. Measure Your Results - Modify Processes as Necessary



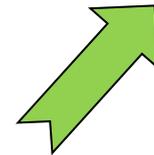
4. Build or Refine and Execute Your Assurance Processes

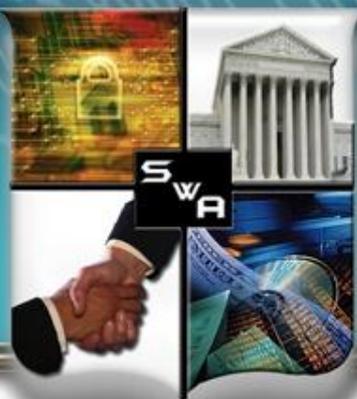


2. Use Assurance-Related Process Capability Expectations



3. Look to Standards for Assurance Process Detail

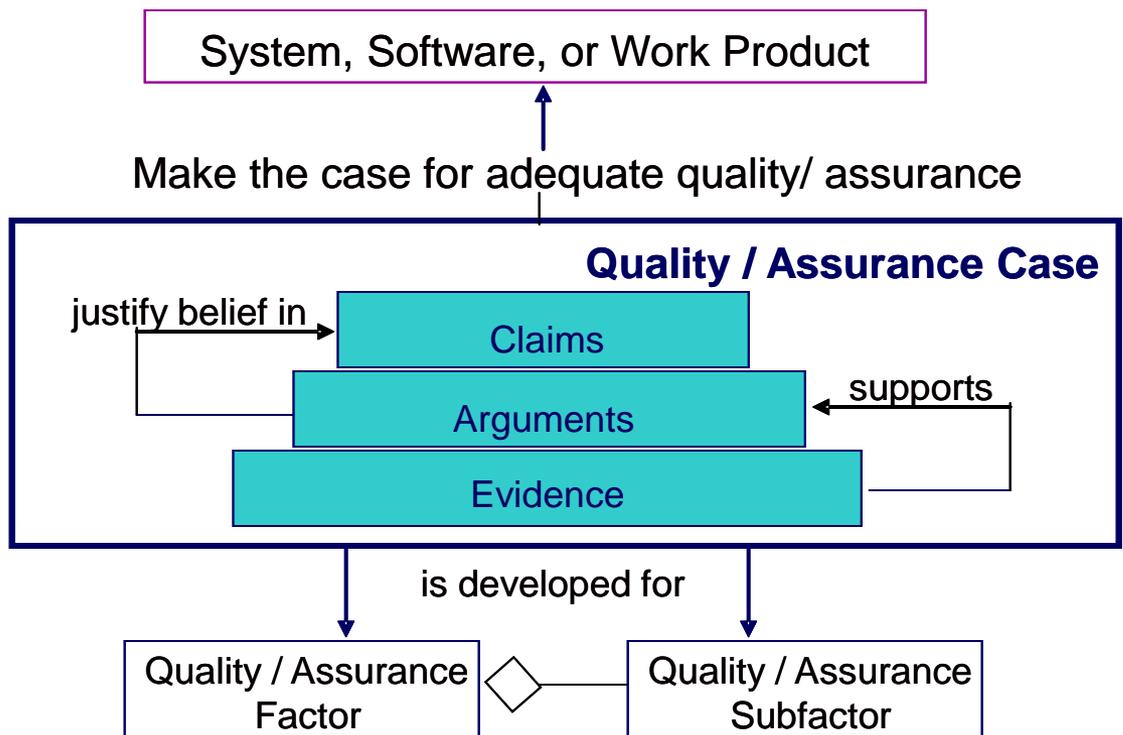




SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

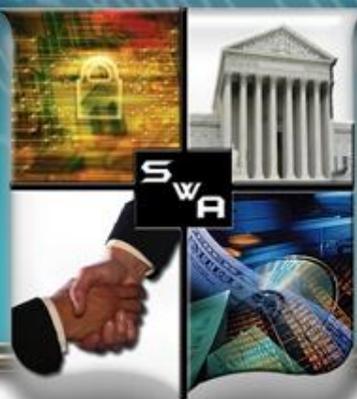
An Assurance Case



Attributes

- Clear
- Consistent
- Complete
- Comprehensible
- Defensible
- Bounded
- Addresses all life cycle stages

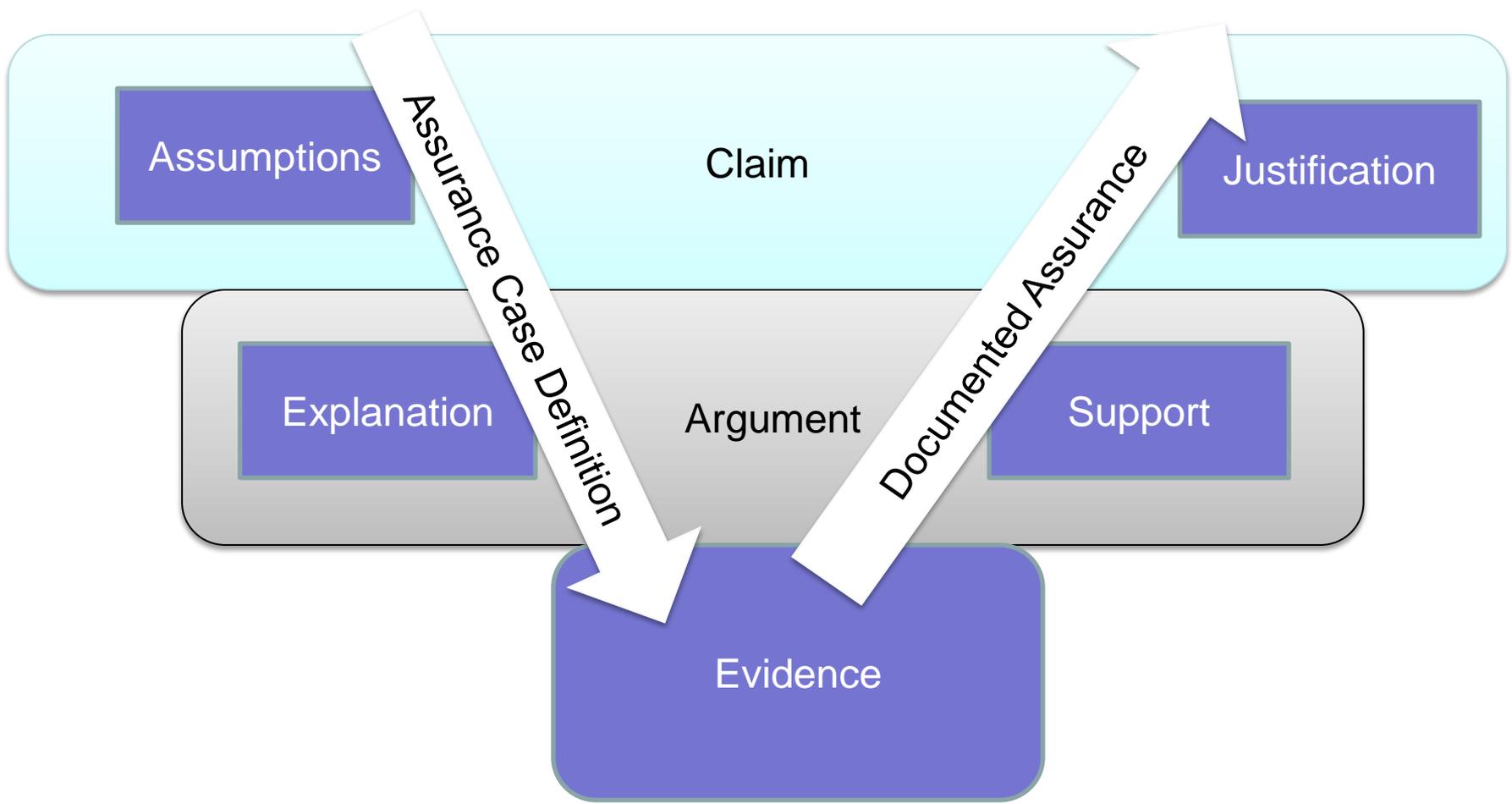
Adapted from a slide by Joe Jarzombek who, in turn, credited IEEE CS alternative proposal for 15026 and CMU SEI QUASAR tutorial by Donald Firesmith, March 2007



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Creating An Assurance Case





SOFTWARE ASSURANCE FORUM

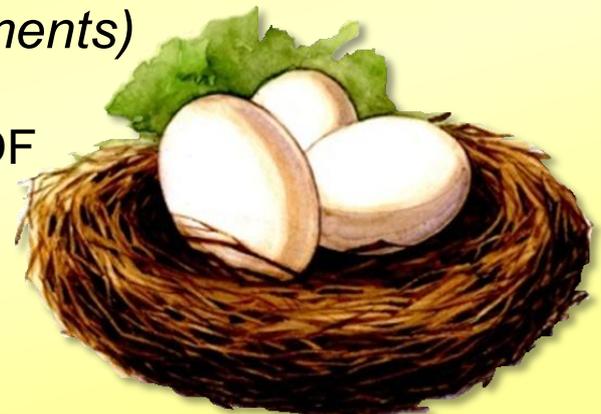
BUILDING SECURITY IN

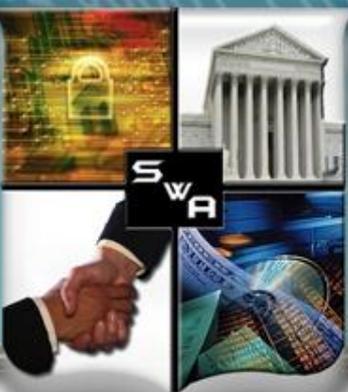
The Solution Requires A Balance Of Benchmarks

- *The chicken.... (a.k.a. Process Focused Assessment)*
 - *Management Systems (ISO 9001, ISO 27001, ISO 2000)*
 - *Capability Maturity Models (CMMI, RMM, SSE-CMM)*
 - *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*





SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

SwA Measurement Working Group

Trend of CVEs with high CVSS scores against maturity levels indicates a relationship between maturity level and CVSS scores

CVEs present on the system with CVSS score above 7

EAL Rating

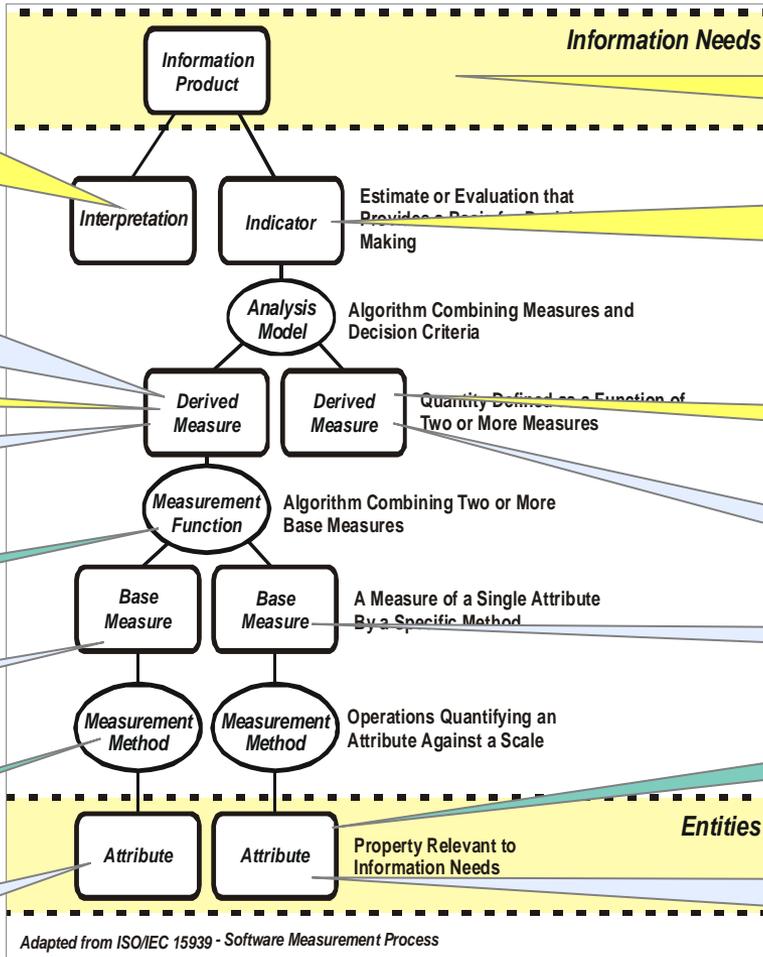
Number of or CWEs per set number of lines of code

Measurement Process

Number of CVEs or CWEs

Measurement

Line of code



Understand the impact of improved assurance practices

Comparison of CVEs with CVSS scores above 7 compared with project's Maturity Level

CMMI Maturity Level

CVSS Score

Number of lines of code

MOF Element

Measured Artifact

CVE/CWE/defect

Adapted from ISO/IEC 15939 - Software Measurement Process



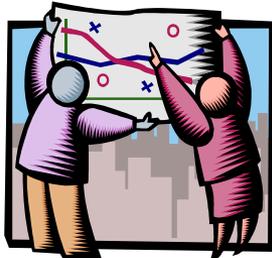
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Process Improvement Lifecycle - A Process for Achieving Assurance (Today)

Mission/Business Process

Understand Your Business Requirements for Assurance



Measure Your Results



Information System

Build or Refine and Execute Your Assurance Processes



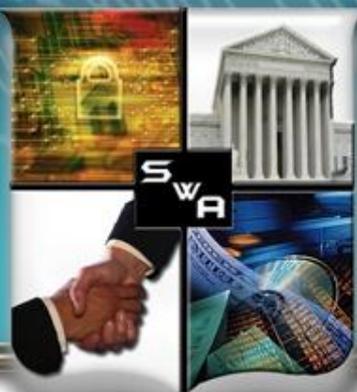
Understand Assurance-Related Process Capability Expectations



Organization Support

Look to Standards for Assurance Process Detail





SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Acquirers of IT products and services trust that suppliers are addressing cyber security without validating

Prepare for the acquisition

Advertise the acquisition and select the supplier

Initiate an agreement

Monitor the agreement

Accept the product or service

Product Development and Maintenance

Requirements Management

Design/Develop

Test

47% **do not** perform acceptance testing of third-party code

30% **do not** use static analysis/manual code

27% **do not** practice secure design

19% **do not** carry out security requirement definition

46% use own development method, rather than SDL or CMM/CMMI

15% follow SDL

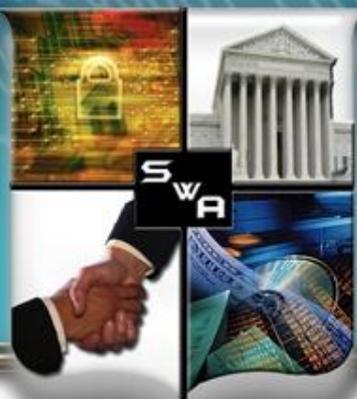
20% follow CMM/CMMI®

61% had **no** special incentive program to get developers and testers to work together

More than 70% **do not** measure developers with security related metrics

ROI was greater for those who employed a coordinated, prescriptive approach

Source: Forrester, "State of Application Security," January 2011



SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Achieving System and Software Assurance

1. Understand Your Business Requirements for Assurance



2. Use Assurance-Related Process Capability Expectations



5. Measure Your Results - Modify Processes as Necessary



3. Look to Standards for Assurance Process Detail



4. Build or Refine and Execute Your Assurance Processes





SOFTWARE ASSURANCE FORUM

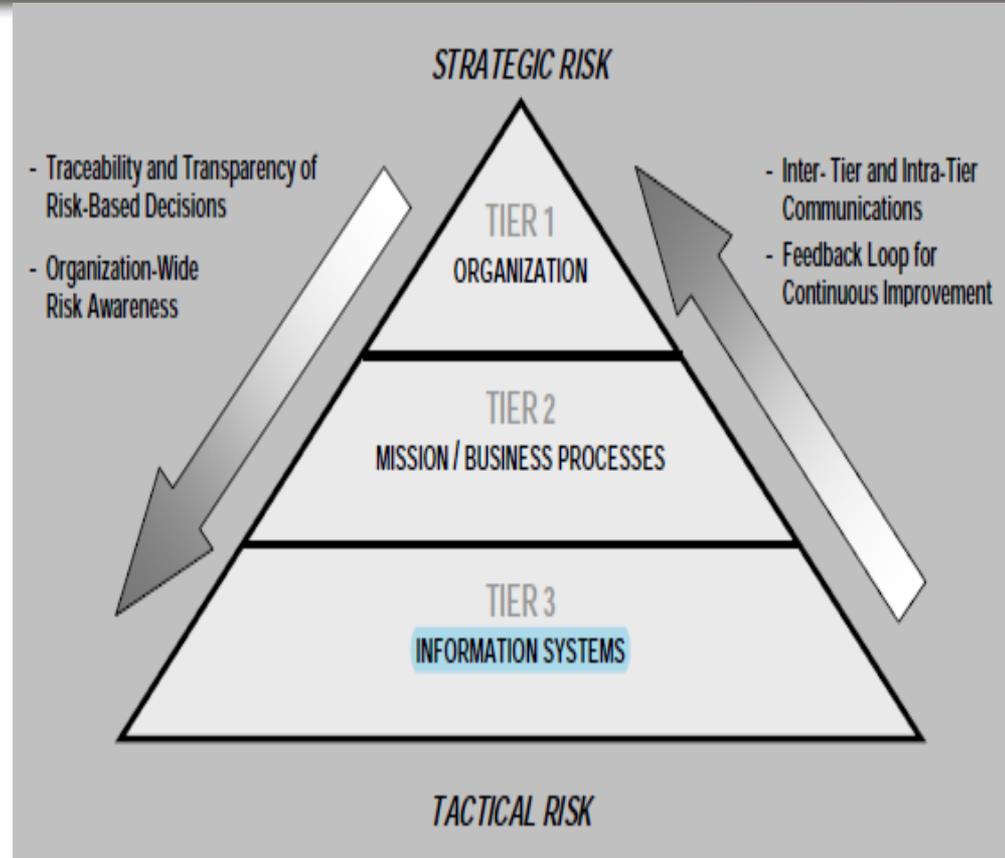
BUILDING SECURITY IN

Software Assurance Challenges

Businesses trust that cyber threats are being addressed

When Business do address the SwA problem it is compliance driven

Tactical approaches for swa are being used and as a result do not tie directly to strategic business efforts and SwA does not contribute to business ROI





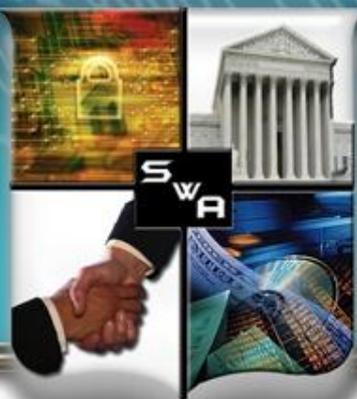
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Draft NIST SP 800-53 rev 4 has SwA controls for low, moderate, and high systems

- AT-3 Security Training
- CM-7 Least Functionality
- SA-3 System Development Life Cycle
- SA -4 Acquisition Process
- SA -11 Developer Security Testing
- SA -15 Development Process, Standards, and Tools
- SA – 16 Developer-Provided Training
- SA – 17 Developer Security Architecture and Design

PRELIMINARY



SOFTWARE ASSURANCE FORUM BUILDING SECURITY IN

Join us at the SwA Working Groups

Paul R. Croll
CSC
5166 Potomac Drive
King George, VA 22485-5824

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

