Assurance for CMMI®: A Toolbox for Multiple Cyber Challenges

9th Annual CMMI® Technology Conference
17 November 2009

Michele Moss, Booz Allen Hamilton
Debbie McCoy, Booz Allen Hamilton

©CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.
Agenda

- Setting the Stage
- Assurance for CMMI®
- Code Vulnerabilities
- Global Supply Chain
- Organizational Cyberspace
- Next Steps
• Dependencies on technology are greater than ever
• Possibility of disruption is greater than ever because software is vulnerable
• Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities

Adapted from: Jarzombek, Mitigating Risks to the Enterprise through Development and Acquisition, SEPG 2009
Gaps Exist In The Intended Audience For SwA Literature

Distribution of Literature
(Percentage of literature by Intended Audience)

- Academia: 21.3%
- Academia and Practitioners: 17.0%
- Development Community: 13.3%
- Practitioners: 13.6%
- Middle Management: 1.8%
- Government (other): 0.6%
- Executive Decision Makers: 0.6%
- Government (Defense): 1.2%
- Programmers: 4.8%
- Software Assurance Community: 13.1%
- Software Project Managers: 0.3%
- Standards Community: 0.4%
- Acquisition Community: 0.1%
Agenda

• Setting the Stage
• Assurance for CMMI®
• Code Vulnerabilities
• Global Supply Chain
• Organizational Cyberspace
• Next Steps
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.

https://buildsecurityin.us-cert.gov/swa/procrsresc.html
The purpose of Organizational Training (OT) is to develop the skills and knowledge of people so they can perform their roles effectively and efficiently. [1, p. 275]

Addressing an organization’s assurance training needs increases the likelihood that qualified and appropriately trained resources are performing the necessary integrated assurance activities on the project.

The use of the Focus Topic as described throughout this document creates a natural inclusion of assurance activities for the following practices within the OT process area: SP1.2, SP1.4, SP2.1, SP2.2, and SP2.3.

SG 1. A training capability, which supports the organization’s management and technical roles, is established and maintained.

SP 1.1 Establish and maintain the strategic training needs of the organization.

Understanding the capabilities needed to achieve the strategic business objectives of an organization provides the foundation for planning and executing the necessary assurance skills within the organization.

AF 1.1.1 Establish and maintain the assurance training needs of the organization [2, SP1.3.3]

Specialized skills are necessary to achieve project and organizational assurance objectives. Assurance objectives included in the organization’s strategic business objectives and process improvement plan contribute to the identification of potential future training needs.

Examples of categories of training needs for assurance include (but are not limited to) the following:

- Assurance (general awareness, organizational considerations, stakeholder considerations, legal implications, missions needs, abuse/misuse analysis, secure coding, testing, etc)
- Workforce credentials and certification maintenance requirements (i.e. Project Management Professional (PMP), Certified Information Systems Security Professional (CISPP))

Supporting examples, sub practices, etc that clarify the Assurance practice

Typical Work Products:

- Assurance Training Needs
- Assurance Assessment Analysis

Context of Assurance for the PA

Assurance practice aligned with existing CMMI® Specific practice
Setting the Stage
Assurance for CMMI®
Code Vulnerabilities
Global Supply Chain
Organizational Cyberspace
Next Steps
• 64% of the vulnerabilities in NVD in 2004 are due to programming errors*
  – 51% of those due to classic errors like buffer overflows, cross-site-scripting, injection flaws*
• Probability of serious vulnerabilities is 52.3% (Capers Jones Overview of the US software Industry, April 2008)
• 27% of development effort is devoted to defect removal, repair, and rework (Capers Jones Overview of the US software Industry, April 2008)
• 67% percent of the attacks in 2007 were "for profit" motivated, ideological hacking came second (Web Application Security Consortium Annual 2007 Report)

* courtesy of Robert Seacord
Technology:
Static Analysis, CWE, CVE, CVSS

People:
Project manager
Security analyst
Developer

Assurance for CMMI® Practice
TS AF 3.1.2
Identify deviations from assurance coding standards

Secure Coding Roadmap
## Secure Coding Practice Implementation

<table>
<thead>
<tr>
<th>SDLC Activity</th>
<th>Assurance for CMMI</th>
<th>BSIMM</th>
<th>TSP Secure *</th>
</tr>
</thead>
<tbody>
<tr>
<td>Code Review Checklists</td>
<td><strong>OPD AF 1.1.1 Establish and maintain organizational processes to achieve the assurance business objectives.</strong>&lt;br&gt;<strong>TS AF 3.1.2 Identify deviations from assurance coding standards.</strong></td>
<td><strong>SR Level 1: Provide easily accessible security standards and (compliance-driven) requirements</strong></td>
<td>CERT SCI provides language specific secure coding guidelines for C, C++, and Java.&lt;br&gt;To claim compliance with a standard, software developers must be able to produce on request documentation as to which systematic and specific deviations have been permitted during development.</td>
</tr>
<tr>
<td>Static Analysis Tools</td>
<td><strong>IPM AF 1.3.1 Establish and maintain assurance of the project’s work environment based on the organization’s work environment standards.</strong></td>
<td><strong>CR Level 2: Enforce standards through mandatory automated code review and centralized reporting</strong>&lt;br&gt;<strong>CR Level 3: Build an automated code review factory with tailored rules</strong></td>
<td>Automatable guidelines are identified by WG14/N1393. Remaining guidelines are enforced through manual inspection. The CERT Source Code Analysis Laboratory certifies conformance to standards.</td>
</tr>
</tbody>
</table>

* courtesy of Robert Seacord
Agenda

- Setting the Stage
- Assurance for CMMI®
- Code Vulnerabilities
- Global Supply Chain
- Organizational Cyberspace
- Next Steps
• Deliberately embedded malicious functionality
• Theft to intellectual property
• Fake or counterfeit products
• Exploitable IT/software unintentionally produced by suppliers with poor security practices
• Lack of developer and acquirer awareness of associated risks

Increased Vigilance Is Critical To Reducing IT Risks From The Supply Chain

**Technology:**
- Automated Penetration Testing Tools
- Network Vulnerability Scanners

**People:**
- Project manager
- Security analyst
- Developer

**Assurance for CMMI® Practice:**

- **TS AF 2.1.1** Architect for assurance.
- **TS AF 2.1.2** Design for assurance.
- **TS AF 3.1.1** Implement the assurance designs of the product components.
- **VAL AF 2.2.1** Analyze the results of assurance validation activities.
- **VER AF 3.2.1** Analyze the results of assurance verification activities.
Established Design Principles

- **Chain of Custody**: The confidence that each change and handoff made during the source code’s lifetime is authorized, transparent and verifiable.
- **Least Privilege Access**: Personnel can access critical data with only the privileges needed to do their jobs.
- **Separation of Duties**: Personnel cannot unilaterally change data, nor unilaterally control the development process.
- **Tamper Resistance and Evidence**: Attempts to tamper are obstructed, and when they occur they are evident and reversible.
- **Persistent Protection**: Critical data is protected in ways that remain effective even if removed from the development location.
- **Compliance Management**: The success of the protections can be continually and independently confirmed.
- **Code Testing and Verification**: Methods for code inspection are applied and suspicious code is detected.

Agenda

- Setting the Stage
- Assurance for CMMI®
- Code Vulnerabilities
- Global Supply Chain
- Organizational Cyberspace
- Next Steps
Technology:
Process, Measurement, and Artifact Repositories
Social Media

People:
Executive Sponsors
Project Managers
Project Teams

Assurance for CMMI® Practice
OPF AF 1.1.1 Establish and maintain the description of the assurance context and objectives for the organization.

OPD AF 1.1.1 Establish and maintain organizational processes to achieve the assurance business objectives.

OT AF 1.1.1 Establish and maintain the strategic assurance training needs of the organization
“It is the policy of Motorola to offer security solutions designed to protect the confidentiality, integrity and availability of information and other assets appropriate to their value to Motorola, and to service providers (and their customers) using Motorola products.” (source: Motorola Secure Software Development Model (MSSDM) Lessons Learned, Margaret Nadworny, August 10, 2007)

Establish and maintain organizational processes to achieve the assurance business objectives. Identify deviations from assurance coding standards. (Source: Assurance for CMMI® March 2009)

BSIMSR Level 1: Provide easily accessible security standards and (compliance-driven) requirements. Safecode Whitepaper - Fundamental Practices for Secure SW Development (section on Programming)

TSP Secure CERT SCI provides language specific secure coding guidelines for C, C++, and Java. To claim compliance with a standard, software developers must be able to produce on request documentation as to which systematic and specific deviations have been permitted during development.
**Plan and Prepare for Appraisal**

- Analyze Requirements
- Develop Appraisal Plan
- Select and Prepare Appraisal Team
- Prepare for Collection of Objective Evidence

**Conduct Appraisal**

- Obtain and Analyze Initial Objective Evidence
- Examine Objective Evidence
- Verify and Validate Objective Evidence
- Document Objective Evidence

**Generate Appraisal Results**

- Generate Appraisal Results

**Report Results**

- Package and Archive Appraisal Assets
- Deliver Appraisal Results

---

**SCAMPI**

- SCAMPI is a service mark of Carnegie Mellon University

---

**Incorporate Assurance Focus Practices**

- SM SCAMPI is a service mark of Carnegie Mellon University
Agenda

• Setting the Stage
• Assurance for CMMI®
• Code Vulnerabilities
• Global Supply Chain
• Organizational Cyberspace
• Next Steps
What can you do?

• Use “Draft Practices” to identify gaps in your assurance practices [https://buildsecurityin.us-cert.gov/swa/progresrc.html](https://buildsecurityin.us-cert.gov/swa/progresrc.html)

• Measure and improve your assurance practices

• Share your lessons learned (swawg-process @ cert.org)
References for Integrating Assurance

- DHS Software Assurance Working Groups
  - https://buildsecurityin.us-cert.gov
  - http://www.us-cert.gov/swa/
- IATAC /DACS
  - http://iac.dtic/iatac
  - https://www.thedacs.com
  - Enhancing the Development Life Cycle to Produce Secure Software
  - State of the Art Report on Software Security Assurance
- NIST
  - http://csrc.nist.gov/
- NDIA
  - Systems Engineering Division
  - System Assurance Guidebook
- SANS
  - http://www.sans.org/
- International Organization for Standardization (ISO)
  - http://www.iso.org
- Software Security Engineering
  - http://www.softwaresecurityengineering.com/
Contact Information

- Michele Moss, CISSP, CSSLP
  Booz Allen Hamilton
  Co-Chair DHS SwA Processes and Practices Working Group
  moss_michele@bah.com

- Debbie McCoy, SCAMPI® B/C Team Lead, Introduction to CMMI® Instructor
  Booz Allen Hamilton
  mccoy_debbie@bah.com