

Lessons Learned From Applying An Assurance Focus to CMMI

*SEPG Conference
March 2009*

Session ID:2223

® Capability Maturity Model, Capability Maturity Modeling, and CMM are registered in the U.S. Patent & Trademark Office.

SM SCAMPI is a service mark of Carnegie Mellon University

Agenda

Assurance And Quality

Assurance Working Group

Improving Product Quality

Evaluating Assurance Practices

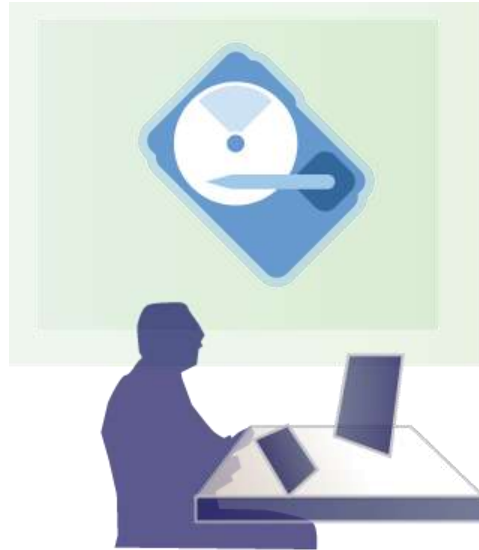
Summary

Today's Reality Requires Increased Confidence In Our IT Products and Services

- ▶ Dependencies on technology are greater than ever
 - Rapid advances
 - Enhancement of quality of life
 - Increased interdependencies
- ▶ Possibility of disruption is greater than ever because software is vulnerable
 - Way of life may be impacted when systems are not available or compromised
 - Missions of health, safety, finance, communications, transportation are at risk
- ▶ Loss of confidence alone can lead to stakeholder actions that disrupt critical business activities

Assurance Is Confidence Our Needs Are Met

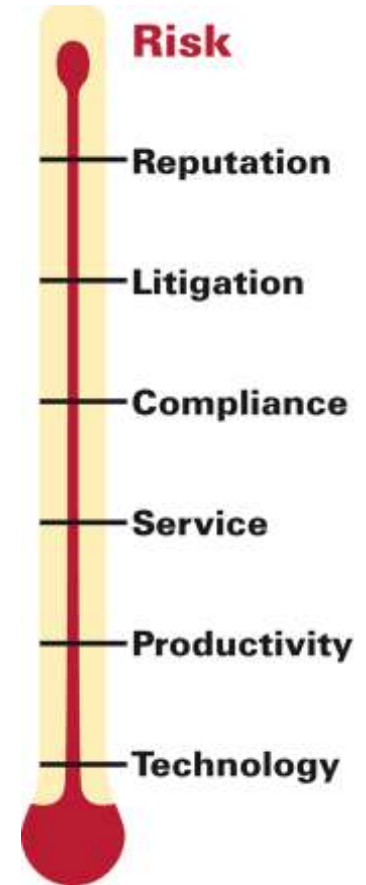
- ▶ Software Assurance – The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its life cycle, and the software functions in the intended manner. [CNSSI 4009]



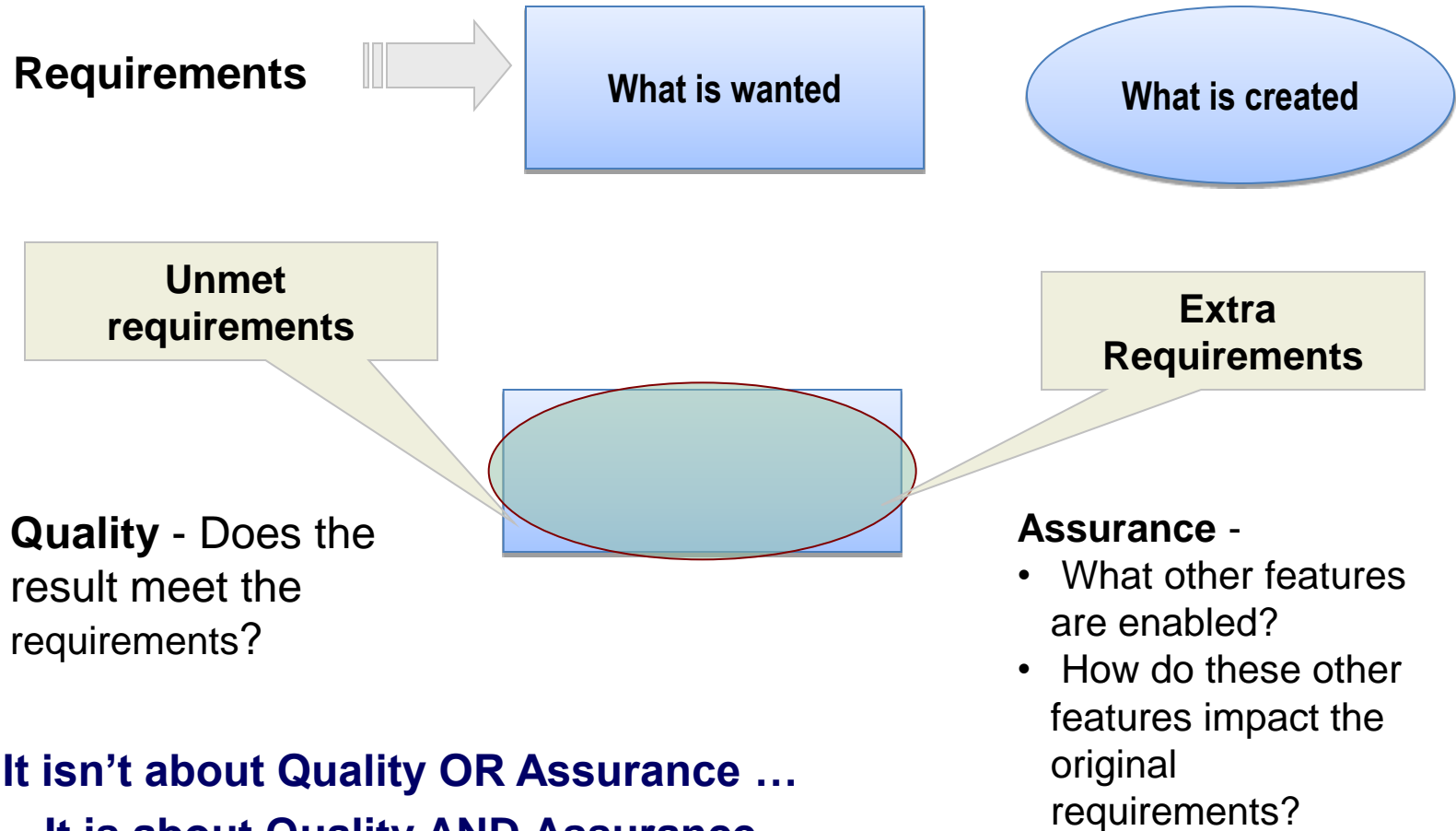
Assurance is a property of software or systems that ensures the security, safety, and reliability of the product.

Assurance Risks and Software Quality

- ▶ 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)



The Relationship between Quality and Assurance



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

Agenda

Assurance And Quality

Assurance Working Group

Improving Product Quality

Evaluating Assurance Practices

Summary

Assurance Working Group - Incorporating Assurance in Quality Frameworks

- ▶ 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
- ▶ December 2007 - Create Process Reference Model (PRM) for Assurance
 - Motorola Secure Software Development Model (MSSDM)
 - SSE-CMM
- ▶ May 2008 - Create mapping of PRM to CMMI®
- ▶ July 16, 2008: Gained CMMI® Steering Group approval to create Focus Topic for Assurance
- ▶ Working with CMMI® Architecture Team to develop a Focus Topic that documents the assurance thread through the CMMI®
- ▶ Preparing a formal change request for consideration by the CMMI® – DEV Project Team

Process Reference Framework for Assurance - Overview

Assurance Process Management

- Achieve key business objectives
- Establish an environment to sustain assurance
- Deploy assurance capabilities and features across the organization that achieve the business assurance goals

Assurance Project Management

- Manage assurance against plans
- Manage assurance support activities
- Select and Manage Suppliers based upon assurance capabilities

Assurance Engineering

- Establish assurance requirements
- Architect a solution for assurance
- Verify and validate the product assurance
- Identify and manage risks due to existence of vulnerabilities

Assurance Support Activities

- Perform product assurance audits
- Determine root causes of assurance defects
- Protect project and organizational assets
- Identify and manage risks due to existence of vulnerabilities

Agenda

Assurance And Quality

Assurance Working Group

Improving Product Quality

Evaluating Assurance Practices

Summary

Practical Example – Sample Code

```
#include <stdlib.h>

#define BUFSIZE 100

void foo(char *bar) {

    char BUF[BUFSIZE];
    strcpy(BUF, bar);
    printf("%s\n", BUF);

}

int main() {
    char *baz;
    baz = getenv("HOME");
    foo(baz);
    exit(0);
}
```

1. Allocate a buffer

2. Copy bar into BUF

3. Print BUF

4. Retrieve pointer
to HOME

5. Print out HOME

Practical Example - Validation

```
#include <stdlib.h>

#define BUFSIZE 100

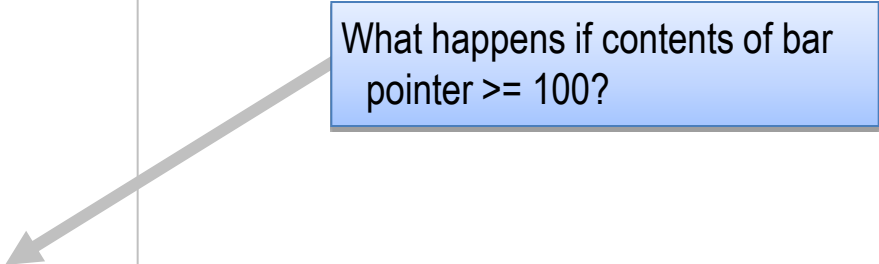
void foo(char *bar) {

    char BUF[BUFSIZE];
    strcpy(BUF, bar);
    printf("%s\n", BUF);

}

int main() {
    char *baz;
    baz = getenv("HOME");
    foo(baz);
    exit(0);
}
```

What happens if contents of bar pointer ≥ 100 ?



Practical Example - Defect Identified!



**System crash is the good news!
=> You know you have a problem.**

**If the system doesn't crash, how
does this situation manifest itself?
=> Non reproducible error that is very
difficult/costly to debug**

Practical Example - Assurance Exploit

- ▶ Start out with “excessive” input values
 - Increase until a system crash
 - Denial of Service Attack
 - Back off until the system does not crash
 - Insert new return values and new code
 - Take over the application or service
- ▶ Leave little evidence you have taken over the application or what damage has been caused

Practical Example - Improving Security and Code Quality Through Process

```
#include <stdlib.h>

#define BUFSIZE 100

void foo(char *bar) {

    char BUF[BUFSIZE]; strncpy(BUF, bar,
    BUFSIZE);
    BUF(BUFSIZE-1)=NULL;

    printf("%s\n", BUF);

}

int main() {
    char *baz;
    baz = getenv("HOME");
    foo(baz);
    exit(0);
}
```

1. Use safe functions, i.e. strncpy.

2. Make sure item being copied does not exceed size of the destination

3. Make sure BUF array ends properly.

Enhanced Coding Standards for Developers

- ▶ Train the development team
- ▶ Checklists for code reviews
- ▶ Static analysis tools
 - Activate security flags
- ▶ False / True
 - Positive / Negative
- ▶ Address unresolved issues w/security experts
- ▶ Document unresolved issues

1. Use safe functions, I.e. strncpy.

2. Make sure item being copied does not exceed size of the destination

3. Insert NULL characters in arrays

<https://www.securecoding.cert.org/confluence/display/seccode/CERT+C+Secure+Coding+Standard>

Automate Code Inspections – Know your Static Analysis Tool

- ▶ Simple test cases generated for coding standards which could be automated
- ▶ Motorola experience
 - Approximately 25% covered by tool
- ▶ Work with your vendor for customized enhancement capability
- ▶ Consider alternative tools
 - A different 25% may be covered
- ▶ Know what your vendor(s) can/cannot do
 - YES - Buffer Overflows
 - NO - Detection of uninitialized complex variables
- ▶ Emphasize negative cases in code reviews
- ▶ False/True Positive/Negative

Process Reference Framework for Assurance – Contributing practices

Assurance Process Management

- **Achieve key business objectives**
- Establish an environment to sustain assurance
- Deploy assurance capabilities and features across the organization that achieve the business assurance goals

Assurance Project Management

- **Manage assurance against plans**
- **Manage assurance support activities**
- **Select and Manage Suppliers based upon assurance capabilities**

Assurance Engineering

- **Establish assurance requirements**
- Architect a solution for assurance
- Verify and validate the product assurance
- **Identify and manage risks due to existence of vulnerabilities**

Assurance Support Activities

- **Perform product assurance audits**
- Determine root causes of assurance defects
- **Protect project and organizational assets**
- **Identify and manage risks due to existence of vulnerabilities**

Agenda

Assurance And Quality

Assurance Working Group

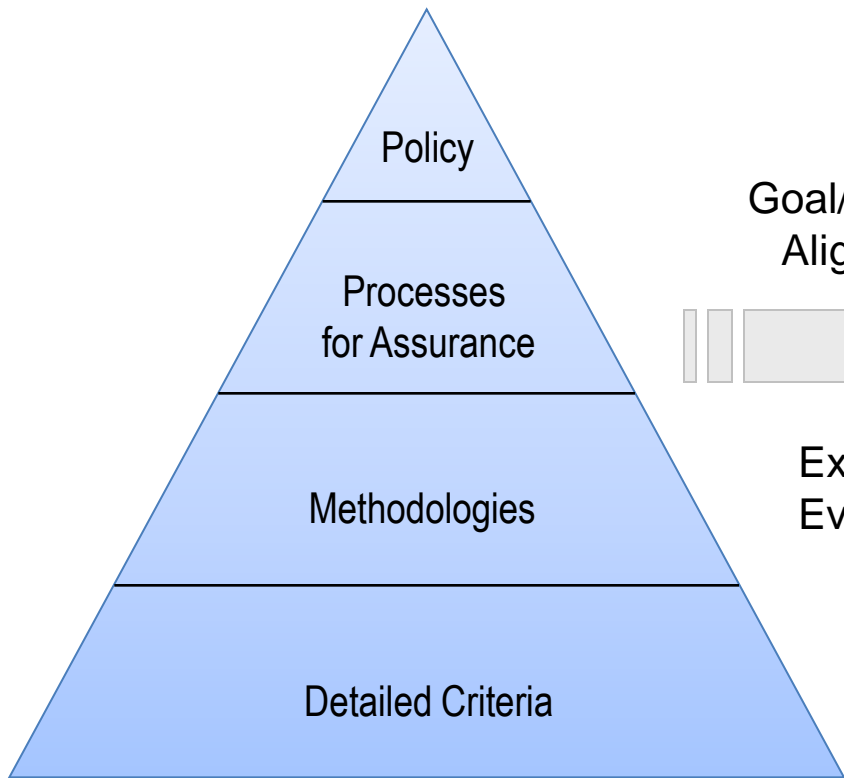
Improving Product Quality

Evaluating Assurance Practices

Summary

Assurance Focus For CMMI® – A tool for assessing the integration of assurance practices

Governance Framework



Goal/Process
Alignment



Expected
Evidence

Process Capability Assessment Results

Process Gap Analysis

Or

CMMI® SCAMPISM

Plan and Prepare for Appraisal

Conduct Appraisal

Report Results

Leverage the SCAMPISM Feedback Loop for Assurance Practices

▶ Why?

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

▶ How?

- Integrate assurance capability assessments in existing CMMI® activities
- Leverage existing PIID data and interviews to characterize practices relevant to CMMI® PAs and report as a part of appraisal and results

- ▶ Word of Caution: SCAMPISM demonstrates that an organization is more likely to produce a product that meets quality or assurance objectives

Lessons Learned from Integrated Appraisals

- ▶ Implementation of the current CMMI® model is already costly!
 - Manageable Assurance Foot Print
 - Ease of Use Assurance Models
- ▶ Booz Allen's experience in internally and externally led integrated SCAMPISM
 - Coordination with Industry is needed to create a more effective and scalable approach
 - Consistent understanding and interpretation of results (assurance in products is increased NOT guaranteed)

Assurance Focus For CMMI® Simplifies Integrated Improvement and Appraisals

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 (CISSP))

Typical Work Products:

- Assurance Training Needs
- Assurance Assessment Analysis

Context of Assurance for the PA

Assurance practice aligned with existing CMMI® specific practice

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

Typical Work Products

Alignment of CMMI® and Assurance Practices

- ▶ Establish and maintain the strategic training needs of the organization. (OT SP 1.1)
 - Assurance Thread -Establish and maintain the assurance training needs of the organization
 - Typical Work Product - Assurance Training Needs (may be part of Organizational Training Needs)
- ▶ Determine which training needs are the responsibility of the organization and which will be left to the individual project or support group. (OT SP 1.2)
- ▶ Establish and maintain an organizational training tactical plan. (OT SP 1.3)
- ▶ Establish and maintain training capability to address organizational training needs. (OT SP 1.4)

Focus Topic Contributions to Process Improvement and Integrated Appraisals

- ▶ Provides way to capture evidence and evaluate integration of assurance capabilities at the organizational level
- ▶ Defines uniquely aligned assurance practices for CMMI® Goals and Specific Practices reducing the need for another model
- ▶ Allows characterization of assurance practices
- ▶ Informative material provides additional detail on the assurance practice that provides clarification of the practice and can be the foundation for training
- ▶ Informative material on assurance focus through the CMMI® practices facilitates identification of assurance evidence while evaluating CMMI® specific practices

Agenda

Assurance And Quality

Assurance Working Group

Improving Product Quality

Evaluating Assurance Practices

Summary

Summary

- ▶ Assurance can improve your quality
- ▶ Use “Draft PRM for Assurance” or “Draft Assurance Focus for CMMI®” to identify gaps in your Assurance Practices
- ▶ Watch for updates <https://buildsecurityin.us-cert.gov/swa/procesrc.html>
- ▶ Share your Lessons Learned (swawg-process @ cert.org)

Contact Information

Michele Moss
Associate

Booz | Allen | Hamilton

8283 Greensboro Drive
McLean, VA 22102
Tel (703) 377-1254
moss_michele@bah.com

Margaret Nadworny

76 Armijo Road
Silver City, NM 88061

Telephone: 512-947-4317
Margaret.Nadworny@yahoo.com