Assurance Process Reference Model for use with CMMI and Measurement for Software Assurance and Cyber Security

PSM June 2009

Michele Moss, CISSP, ISSPCS, CSSLP
Co-Chair, DHS SwA Processes and Practices Working Group
Booz Allen Hamilton

Joe Jarzombek, PMP, CSSLP
Director for Software Assurance
National Cyber Security Division
Office of the Assistant Secretary for Cyber Security and Communications
US Department of Homeland Security

* The Software Assurance (SwA) Forum and Working Groups are co-sponsored by DHS, DoD, and NIST to enable public-private collaboration in advancing software security and resiliency
• With today’s global software supply chain, Software/Systems Engineering, Quality Assurance, Testing and Project Management must explicitly address security risks posed by exploitable software.
  – Traditional processes do not explicitly address software-related security risks that can be passed from projects to using organizations.
  – Internationally recognized standards are needed to support processes and provide transparency for more informed decision-making for mitigating enterprise risks.
  – Many suppliers use CMMs to guide process improvement & assess capabilities; yet many CMMs do not explicitly address safety and security as normative material
  – ‘Assurance’ needs to be explicitly addressed in standards & capability benchmarking models for organizations involved with security/safety-critical applications.

• Mitigating Supply Chain Risks requires an understanding and management of Suppliers’ Capabilities, Products and Services
  – Enterprise risks stemming from supply chain are influenced by suppliers and acquisition projects
  – IT/Software Assurance processes/practices span development/acquisition.
  – Derived (non-explicit) security requirements should be elicited/considered.

• More comprehensive security measurement and diagnostic capabilities are needed to support processes and provide transparency for more informed decision-making for mitigating risks to the enterprise

Free resources are available to assist personnel in security-enhancing contracting, outsourcing and development activities (see https://buildsecurityin.us-cert.gov/swa)
Agenda

• Setting the stage
• A practical example
• Leveraging Process Capability Benchmarks
• Summary
“Supply chain introduces risks to American society that relies on Federal Government for essential information and services.”

30 Sep 2005 changes to Federal Acquisition Regulation (FAR) focus on IT Security

Focuses on the role of contractors in security as Federal agencies outsource various IT functions.

Enterprise Processes for deploying capabilities: Increasingly Distributed and Complex

New Considerations for Quality & Security

Development Process

- Company Employees
- Contractors
- Open Source
- 3rd Party Libraries
- Offshore
- US Dev. Center A
- Developed In-house
- Enterprise Employees
- Foreign Contractors
- Foreign Sub-Contractors

Procurement Process

- ISV Employees
- Foreign Contractor
- License 3rd Party Libraries
- Open Source
- ISV (COTS)
- Purchased
- Outsource Partner A
- Outsourcer Employees
- Indian Contractor
- Chinese Contractor
- License 3rd Party Libraries

Source: SwA WG Panel presentations, 2008
• Dependencies on technology are greater than ever
  – Rapid advances
  – Enhancement of quality of life
  – Increased interdependencies

• Possibility of disruption is now greater 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

Source: Moss Nadworny, “Lessons Learned From Applying An Assurance Focus to CMMI”, SEPG 2009
What CIOs want

- Reliably software that functions as promised
- Software free from security vulnerabilities and malicious code
- Ease of Integration & Configuration
- Software conforms to Requirements & Industry Standards
- Convenience & Ease of Use
- Rich Feature Set
- Other

https://www.cioexecutivecouncil.com October 11, 2006 Press Release
• **Assurance** – Grounds for confidence that an entity meets its security objectives. [ISO/IEC 15408-1: 2005-10-01].

• **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 system that makes us more comfortable with relying on that system.**

Source Bartol, Jarzombek, Moss, "Mitigating Risks to the Enterprise through Development and Acquisition", SEPG 2009
## Software Assurance Forum & Working Groups*

... 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

### Products and Contributions

| Build Security In - https://buildsecurityin.us-cert.gov and SwA community resources & info clearinghouse |

---

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

- TMB
  - Risk Mgmt Vocabulary

- ISO
  - Advisory Group on Security

- IEC

- TC176
  - Quality Mgmt

- JTC1 Information Technology

- TC56
  - Dependability

- TC65
  - Safety

- SC7
  - SW & System Engineering

- SC27
  - IT Security

- SC22
  - Programming Languages

* DHS NCSD has membership on SC7, SC27 & IEEE S2ESC leveraging Liaisons in place or requested with other committees
The Assurance Problem Space

- Large-scale systems and systems of systems represent a complex supply chain integrating
  - Proprietary and open-source software
  - Legacy systems
  - Hardware and Firmware

- These systems are sourced from multiple suppliers who employ people from around the world

- Most systems depend upon software for their functionality

- Technologies to build reliable and secure software are inadequate
  - Our ability to develop software has not kept pace with hardware advances
  - Can’t construct complex software-intensive systems for which we can anticipate performance

- Assurance is a full life cycle problem
DoD-Related Guidance For Systems Assurance

**National Defense Industrial Association Guidebook on Engineering for System Assurance**

- Correspondence with Existing Documentation, Policies, and Standards
  - Executive Policy, Services Standards, NIST/NSA (NIAP) Standards, GEIA, AIA, IEEE, ISO/IEC Standards, Best Practice (e.g., DHS/DOD SwA CBK)

- Intended to supplement the knowledge of systems (and software) engineers who have responsibility for systems for which there are assurance concerns
  - General Guidance mapped to ISO/IEC 15288, System Life Cycle Processes
  - DoD Specific Guidance
    - Anti-Tamper
    - DAG Lifecycle Framework
    - Technology Development Phase
    - System Development & Demonstration Phase
    - Production, Deployment, Operations, & Support Phases
    - Supporting Processes
    - Periodic Reports
    - Supplier Assurance
    - Mappings
NDIA/DoD System Assurance Guidebook – Mapped To ISO/IEC/IEEE 15288

- Agreement Processes
  - Acquisition
  - Supply

- Project Processes
  - Project Planning
  - Project Assessment
  - Project Control
  - Decision-making
  - Risk Management
  - Configuration Management
  - Information Management

- Technical Processes
  - Stakeholder Requirements Definition
  - Requirements Analysis
  - Architectural Design
  - Implementation
  - Integration
  - Verification
  - Transition
  - Validation
  - Operation
  - Maintenance
  - Disposal

- Assurance Case Process

- Enterprise Processes
  - Enterprise Environment Management
  - Investment Management

- Enterprise Processes
  - System Life Cycle Process Management
  - Resource Management [including human resource training]
  - Quality Management
ISO/IEC JTC1 SC7 Software and Systems Engineering:
ISO/IEC 15026 “Systems and Software Assurance”

“System and software assurance focuses on the management of risk and assurance of safety, security, and dependability within the context of system and software life cycles.”

Terms of Reference changed: ISO/IEC JTC1/SC7 WG7, previously “System and Software Integrity” SC7 WG9
ISO/IEC/IEEE 15026, System and Software Assurance

A four-part standard
- 15026-1: Concepts and vocabulary
  - Initially a Technical Report
- 15026-2: Assurance case
  - Includes requirements on the assurance case content and the life cycle of the assurance case itself as well as an informative clause on planning for the assurance case itself
- 15026-3: System integrity levels (a revision of the 1998 standard)
  - Relates integrity levels to the assurance case and includes related requirements for their use with and without an assurance case
- 15026-4: Assurance in the life cycle
  - Addresses concurrent development and maintenance of the product and the assurance case including project planning for assurance considerations
ISO/IEC/IEEE 15026 Assurance Case

Set of structured assurance claims, supported by evidence and reasoning (arguments), that demonstrates how assurance needs have been satisfied.
- Shows compliance with assurance objectives
- Provides an argument for the safety and security of the product or service.
- Built, collected, and maintained throughout the life cycle
- Derived from multiple sources

Sub-parts
- A high level summary
- Justification that product or service is acceptably safe, secure, or dependable
- Rationale for claiming a specified level of safety and security
- Conformance with relevant standards & regulatory requirements
- The configuration baseline
- Identified hazards and threats and residual risk of each hazard / threat
- Operational & support assumptions

Attributes
- Clear
- Consistent
- Complete
- Comprehensible
- Defensible
- Bounded
- Addresses all life cycle stages
### Drivers
- Need to demonstrate the value of SwA
- Decreasing funding and increasing accountability for it
- Calls for quantifiable ROI and risk exposure
- Need for data to support decisions and substantiate assurance claims

### Benefits
- Supports business case for assurance
- Provides quantifiable information to support decision making and accountability
- Quantifies SwA improvements
- Helps demonstrate regulatory compliance
- Helps demonstrate value to executives
- Motivates stakeholder to change behavior

### Response
- Developed Practical measurement Framework for Software Assurance and Information Security
  - Is harmonized with common system and software and security measurement methodologies
  - Provides an approach for quantifying achievement of SwA goals and objectives within the context of individual projects, programs, or enterprises
  - Provides a framework for the organizations to integrate SwA measurement in their overall measurement efforts in a cost-effective and a seamless manner
• ISO/IEC 15939, Practical Software and System Measurement (PSM)
• CMMI Measurement and Analysis Process Area
• CMMI Goal, Question, Indicator, Measure (GQIM)
• NIST SP 800-55 Rev1, Performance Measurement Guide for Information Security
• ISO/IEC 27004, Information Security Management Measurement

Existing measurement methodologies can be applied to SwA and supply chain
<table>
<thead>
<tr>
<th>PSM</th>
<th>CMMI® (Measurement and Analysis Process Area)</th>
<th>CMMI® GQ(I)M</th>
<th>ISO/IEC 27004</th>
<th>NIST SP 800-55 Revision 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 15939</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• ISO/IEC 15939, Practical Software and System Measurement (PSM)
• CMMI Measurement and Analysis Process Area
• CMMI Goal, Question, Indicator, Measure (GQIM)
• NIST SP 800-55 Rev1, Performance Measurement Guide for Information Security
• ISO/IEC 27004, Information Security Management Measurement

-----------------------------------------------

• Practical Measurement Framework for Software Assurance and Information Security
• CIS Security Metrics
• Measuring Cyber Security and Information Assurance

Existing measurement methodologies can be applied to SwA and supply chain
SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN

Stakeholders

Organizations

Supplier

Acquirer

People

Executive

Practitioner

Stakeholders
Measurement Process

Create/Update Measures
- State goals
- Identify data sources and elements
- Analyze how goals and data elements relate
- Create a series of measures

Collect Data
- Gather data from available data sources

Store Data
- Document/store data in an appropriate repository

Analyze and Compile Data
- Analyze collected data
- Compile and aggregate into measures
- Interpret data
- Identify causes of findings

Report Measures
- Document measures in appropriate reporting formats
- Report measures to stakeholders

Use Measures
- Support decisions
- Allocate resources
- Prioritize improvements
- Communicate to executives and external stakeholders

Continuous Improvement
- Refresh measures to ensure they are still relevant to the project, program, or organization
- Train measurement staff
Security Control Measures

- Percent of new systems that have completed certification and accreditation (C&A) prior to their implementation (NIST SP 800-53 Control: CA-6: Security Accreditation)
- Percent of employees who are authorized access to information systems only after they sign an acknowledgement that they have read and understood rules of behavior (NIST SP 800-53 Controls – PL-4: Rules of Behavior and AC-2: Account Management)
- Percent of the agency’s information system budget devoted to information security (NIST SP 800-53 Controls – SA-2; Allocation of Resources)

*Security Control Measures address compliance with the end state of the system, but not the underlying processes, structures, and code*
SwA Measures address transparency of processes and product properties
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

Source: Moss Nadworny, "Lessons Learned From Applying An Assurance Focus to CMMI", SEPG 2009
Making Security Measurable

MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through enumerating baseline security data, providing standardized languages as means for accurately communicating the information, and encouraging the sharing of the information with users by developing repositories.

The other activities and initiatives listed here have similar concepts or compatible approaches to MITRE's. Together all of these efforts are helping to make security more measurable by defining the concepts that need to be measured, providing for high-fidelity communications about the measurements, and providing for sharing of the measurements and the

| Measurable security pertains at a minimum to the following areas: |
| --- | --- | --- | --- |
| Vulnerability Management | Asset Security Assessment | Configuration Guidance | Malware Response |
| Intrusion Detection | Asset Management | Patch Management | Threat Analysis |
| Incident Management | |

<table>
<thead>
<tr>
<th>Enumerations</th>
<th>Languages</th>
<th>Repositories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CVE</strong> Common Vulnerabilities and Exposures (CVE®) - common vulnerability identifiers</td>
<td><strong>OVALL</strong> Open Vulnerability and Assessment Language (OVALL) - standard for determining vulnerability and configuration issues</td>
<td><strong>OVAL Repository</strong> - community-developed OVAL Vulnerability, Compliance, Inventory, and Patch Definitions</td>
</tr>
<tr>
<td><strong>CWE</strong> Common Weakness Enumeration (CWE™) - list of software weakness types</td>
<td><strong>CRF</strong> Common Result Format (CRF™) - standardized assessment result format for conveying findings based on common names and naming schemes</td>
<td><strong>National Vulnerability Database (NVD)</strong> - U.S. vulnerability database based on CVE that integrates all publicly available vulnerability resources and references</td>
</tr>
<tr>
<td><strong>CAPEC</strong> Common Attack Pattern Enumeration and Classification (CAPEC™) - list of common attack patterns</td>
<td><strong>CEE</strong> Common Event Expression (CEE™) - standardizes the way computer events are described, logged, and exchanged</td>
<td><strong>NIST Security Content Automation Protocol (SCAP)</strong> - security content for automating technical control compliance activities, vulnerability checking, and security measurement</td>
</tr>
</tbody>
</table>
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

CVSS Score

MOF Element

Measured Artifact

CMMI Maturity Level

CVE/CWE/defect

Adapted from ISO/IEC 15939 - Software Measurement Process
Agenda

• Setting the stage
• A practical example
• Leveraging Process Capability Benchmarks
• Conclusion
```c
#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

April 1999, Evan Thomas, CS student, University of British Columbia

http://www.cosc.brocku.ca/~cspress/HelloWorld/1999/04-apr/attack_class.html

Source: Moss Nadworny, “Lessons Learned From Applying An Assurance Focus to CMMI”, SEPG 2009
#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);
}
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

April 1999, Evan Thomas, CS student, University of British Columbia
http://www.cosc.brocku.ca/~cspress/HelloWorld/1999/04-apr/attack_class.html

Source: Moss Nadworny, "Lessons Learned From Applying An Assurance Focus to CMMI", SEPG 2009
• 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

Source: Moss Nadworny, “Lessons Learned From Applying An Assurance Focus to CMMI”, SEPG 2009
• Setting the stage
• A practical example
• Leveraging Process Capability Benchmarks
• Summary
Governance Framework

- Policy
- Processes for Assurance
- Methodologies
- Detailed Criteria

Process Capability Feedback and Improvement

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 (The “what” not the “how”)

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

SM SCAMPI is a service mark of Carnegie Mellon University.
Many suppliers use CMMs to guide process improvement & assess capabilities; yet many CMMs do not explicitly address safety and security.

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

Focus Topic: Assurance for Capability Maturity Model Integration (CMMI)® defines the Assurance Thread for Implementation and Improvement of Assurance Practices

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


Other Assurance Maturity Models have been released in 2009:
The Building Security In Maturity Model (BSIMM) helps organizations plan software security initiatives http://www.bsi-mm.com/
The Software Assurance Maturity Model (SAMM) which is an open framework to help organizations formulate and implement a strategy for software security that is tailored to specific risks facing the organization http://www.opensamm.org/
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
SAM is in the Project Management Category

CMMI Model Foundation (CMF)


- Supplier Agreement Management
- Requirements Development
- Technical Solution
- Validation
- Verification
- Product Integration
- Integration Verification
Assurance For CMMI Identifies
The Assurance Thread for CMMI-DEV

Process Area

Specific Goals

Generic Goals

Specific Practices

Assurance Focus for Goal

Generic Practices

Assurance Focus for practice
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 areas: SP1.1, SP1.4, SP1.2, 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 the 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 [1, SPI.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 plans 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, mission needs, abstract 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**
The purpose of Measurement and Analysis (MA) is to develop and sustain a measurement capability that is used to support management information needs.

**SG 1 Align Measurement and Analysis Activities**

*Measurement objectives and activities are aligned with identified information needs and objectives.*

- **SP 1.1** Establish and maintain measurement objectives that are derived from identified information needs and objectives.
- **SP 1.2** Specify measures to address the measurement objectives. *In order to support a project’s assurance activities, creation of measures related to the assurance of a product or service may be required for internal and external stakeholders.*
- **SP 1.3** Specify how measurement data will be obtained and stored.
- **SP 1.4** Specify how measurement data will be analyzed and reported.
AF 1.2.1 Define and improve project assurance measures.

Description

Stakeholder organizations interested in assurance have identified information assurance needs and objectives. Based upon these assurance objectives, measures are defined to monitor and track the success the project team has in meeting those objectives. It is expected that the measures collected will evolve over time from advances in the assurance capabilities as well as changes in organizational and product assurance objectives. A subset of these measures may become a formal part of the product or service that provides updates on the assurance of the product or service over time.

Typical Work Products:
- Specification of base and derived assurance measures
- Updated sets of assurance measures
SG 2  Provide Measurement Results

*Measurement results, which address identified information needs and objectives, are provided.*

SP 2.1  Obtain specified measurement data.

SP 2.2  Analyze and interpret measurement data.

SP 2.3  Manage and store measurement data, measurement specifications, and analysis results.

Data related to the assurance of the product contains information about potentially exploitable weaknesses in a product or service. In the form of an assurance case, this data becomes part of the product or service. Improper access or use of the data may cause potential harm. Proper management and storage of this information is important to maintain the controlled access and ensure that the information is not lost or damaged.

SP 2.4  Report results of measurement and analysis activities to all relevant stakeholders.
AF 2.3.1 Store assurance measures appropriately.

Description

Due to the sensitivity of the data, additional care must be given to identify the appropriate audiences for the various assurance measures. For audiences such as the project team, more detailed views may be desired and needed for effective use of the data. Conversely, executives or other stakeholders may only need a summary that can be used for justification of assurance practices or decision making based on a summary view of the data. The assurance data that is part of the assurance case becomes an important artifact and part of the product or service.

**Typical Work Products:**
- Stored assurance measurement data inventory.
- Assurance data protection mechanisms
- Assurance case
<table>
<thead>
<tr>
<th>SDLC Activity</th>
<th>What</th>
<th>How</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>Fundamental Practices for Secure SW Development (section on Programming)</strong></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>Fundamental Practices for Secure SW Development (section on Programming)</strong></td>
</tr>
<tr>
<td>SDLC Activity</td>
<td>What</td>
<td>How</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Assurance for CMMI</td>
<td>SafeCode</td>
</tr>
<tr>
<td>Train Developers</td>
<td>OT AF 1.1.1 Establish and maintain the strategic assurance training needs of the organization</td>
<td>“Fundamental Practices for Secure SW Development” (section on Requirements)</td>
</tr>
<tr>
<td>Manage Project Risks</td>
<td>PMC AF 1.3.1 Monitor Assurance Risk</td>
<td>Not specifically identified</td>
</tr>
<tr>
<td>Identify Policy</td>
<td>OPF AF 1.1.1 Establish and maintain the description of the assurance context and objectives for the organization.</td>
<td>Not specifically identified</td>
</tr>
<tr>
<td>SDLC Activity</td>
<td>What</td>
<td>How</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Follow a process</td>
<td><strong>Assurance for CMMI</strong>&lt;br&gt;OPD AF 1.1.1 Establish and maintain organizational processes to achieve the assurance business objectives&lt;br&gt;OPD AF 1.3.1 Establish and maintain the tailoring criteria and guidelines for assurance in the organization’s set of standard processes</td>
<td><strong>SafeCode</strong>&lt;br&gt;Not specifically identified</td>
</tr>
</tbody>
</table>
• Setting the stage
• A practical example
• Leveraging Process Capability Benchmarks
• Summary
Summary

- Assurance is critical for enterprise operations
- Assurance and Quality are complementary
- Assurance for CMMI® is a critical piece that will help integrate Assurance concerns into system and software development processes
- Measurement is needed to demonstrate that the risks have been addressed
- Behaviors and organizational processes must change to make this happen
- Use “PRM for Assurance” or “Assurance Focus for CMMI®” draft material (now available) to identify gaps in any organization’s Assurance Practices
- Watch for updates [https://buildsecurityin.us-cert.gov/swa/procresrc.html](https://buildsecurityin.us-cert.gov/swa/procresrc.html)
- Share your Lessons Learned (swawg-process @ cert.org)
- Use the “Practical Measurement Framework for Software Assurance and Information Security”
- Share your Lessons Learned (swawg-measure @ cert.org)
- Watch for updates [https://buildsecurityin.us-cert.gov/swa/measwg.html](https://buildsecurityin.us-cert.gov/swa/measwg.html)
• Michele Moss, CISSP, CSSLP
  Co-Chair, SwA Processes and Practices Working Group
  moss_michele@bah.com

• Nadya Bartol, CISSP, CEGIT
  Co-Chair, SwA Measurement Working Group
  bartol_nadya@bah.com

• Joe Jarzombek, PMP
  Director for Software Assurance
  National Cyber Security Division
  US Department of Homeland Security
  Joe.Jarzombek@dhs.gov

* The Software Assurance (SwA) Forum and Working Groups are co-sponsored by DHS, DoD, and NIST to enable public-private collaboration in advancing software security and resiliency