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

SSTC April 2009
Michele Moss

Homeland Security

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Agenda

- Setting the stage
- A practical example
- Understanding the processes
- Using measurement for decision making
- Summary

- Dependencies on technology are greater then 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

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

- **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

Requirements

What is wanted

What is created

Unmet requirements

Extra Requirements

Quality - Does the result meet the requirements?

Assurance -

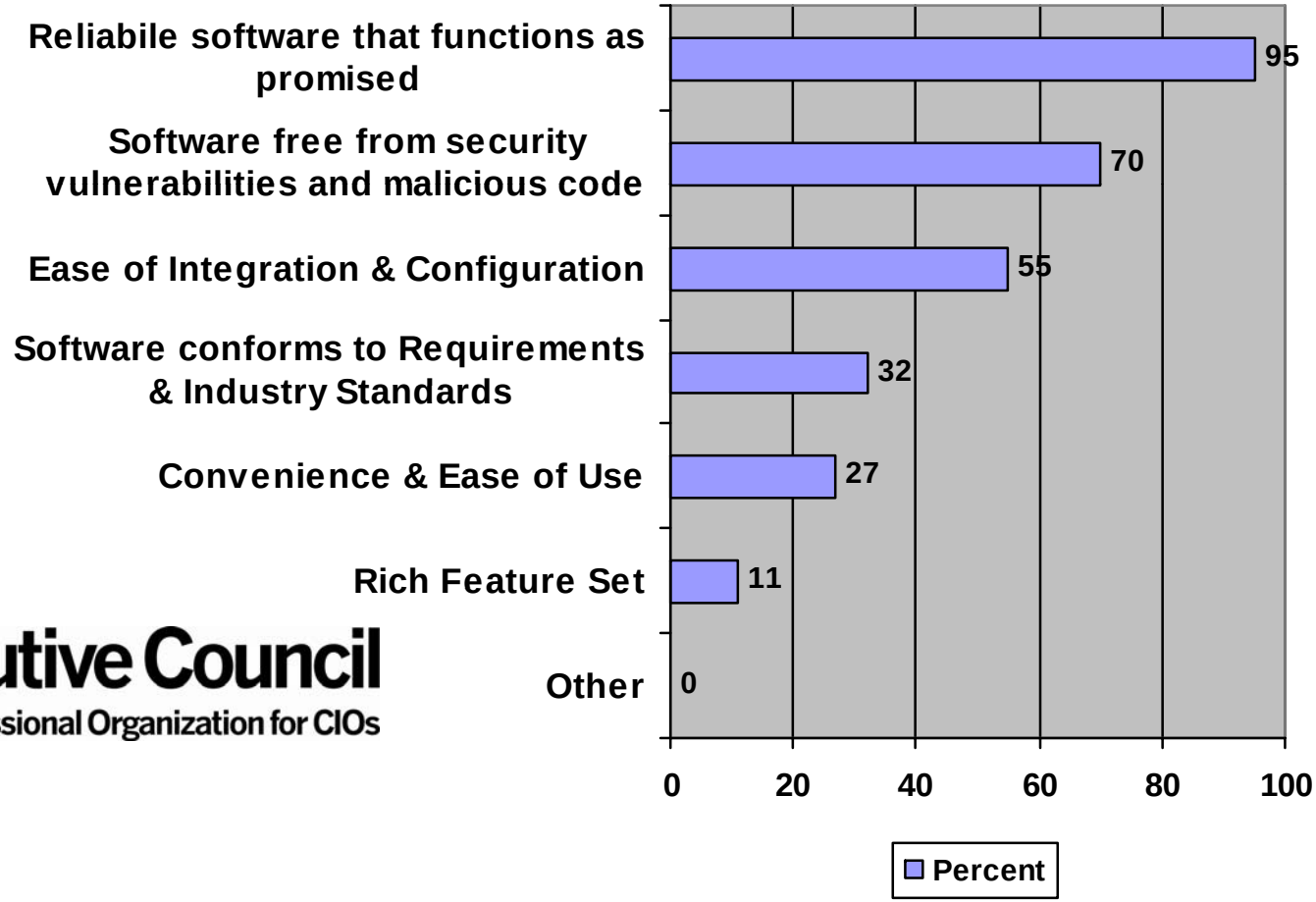
- What other features are enabled?
- How do these other features impact the original requirements?

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

What CIOs want



CIO Executive Council
The Professional Organization for CIOs

https://www.cioexecutivecouncil.com *October 11, 2006 Press Release*

- Setting the stage
- A practical example
- Understanding the processes
- Using measurement for decision making
- Conclusion


```
#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

What happens if contents of bar pointer >= 100?

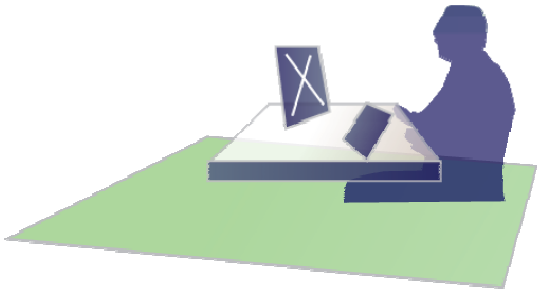
```
#include <stdlib.h>
#define BUFSIZE 100
void foo(char *bar) {
  char BUF[BUFSIZE];
   strcpy(BUF, bar);
   printf("%s\n", BUF);
  }
int main() {
   char *baz;
   baz = getenv("HOME");
   foo(baz);
   exit(0);
   }
```

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

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

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

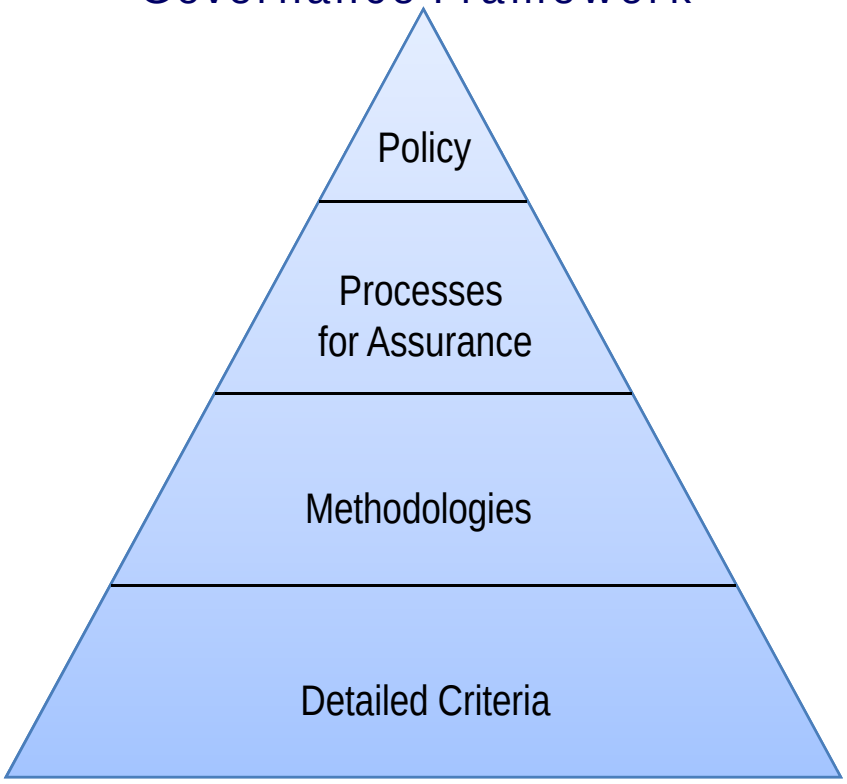
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Agenda

- Setting the stage
- A practical example
- Understanding the processes
- Using measurement for decision making
- Summary

Governance Framework



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/procresrc.html

SM SCAMPI is a service mark of Carnegie Mellon University.

- DHS SwA Working Groups http://www.us-cert.gov/swa/
- Build Security In https://buildsecurityin.us- cert.gov
- DACS https://www.thedacs.com
  - Enhancing the Development Life Cycle to Produce Secure Software
- NDIA (www.ndia.org)
  - System Assurance Guidebook
- NIST (http://csrc.nist.gov/)
- SANS (http://www.sans.org/)
- International Organization for Standardization (ISO) (http://www.iso.org)
- SAFECODE (http://www.safecode.org/)
- The Building Security In Maturity Model (http://www.bsi-mm.com/)

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Practices That Contribute To Secure Coding (1 of 3)

Illustrative

SDLC Activity	What	How	
	Assurance for CMMI	SafeCode	BSIMM
Code Review Checklists	*OPD AF 1.1.1 Establish and maintain organizational processes to achieve the assurance business objectives.* *TS AF 3.1.2 Identify deviations from assurance coding standards.*	Fundamental Practices for Secure SW Development (section on Programming)	SR Level 1: Provide easily accessible security standards and (compliance-driven) requirements
Static Analysis Tools	*IPM AF 1.3.1 Establish and maintain assurance of the project's work environment based on the organization's work environment standards.*	Fundamental Practices for Secure SW Development (section on Programming)	CR Level 2: Enforce standards through mandatory automated code review and centralized reporting CR Level 3: Build an automated code review factory with tailored rules

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Practices That Contribute To Secure Coding(2 of 3)

Illustrative

SDLC Activity	What	How	
	Assurance for CMMI	SafeCode	BSIMM
Train Developers	OT AF 1.1.1 Establish and maintain the strategic assurance training needs of the organization	Fundamental Practices for Secure SW Development (section on Requirements) White paper on Training currently under development	T Level 1: Create the software security satellite T Level 2: Make customized, role-based training available on demand
Manage Project Risks	PMC AF 1.3.1 Monitor Assurance Risk	Not specifically identified	SM Level 3: Practice Risk-Based portfolio management
Identify Policy	OPF AF 1.1.1 Establish and maintain the description of the assurance context and objectives for the organization.	Not specifically identified	[CP1.2] Create Policy

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Practices That Contribute To Secure Coding(3 of 3)

Illustrative

SDLC Activity	What	How	
	Assurance for CMMI	SafeCode	BSIMM
Follow a process	OPD AF 1.1.1 Establish and maintain organizational processes to achieve the assurance business objectives OPD AF 1.3.1 Establish and maintain the tailoring criteria and guidelines for assurance in the organization's set of standard processes	Not specifically identified	[SM1.1] Publish Process

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Agenda

- Setting the stage
- A practical example
- Understanding the processes
- Using measurement for decision making
- Summary

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

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

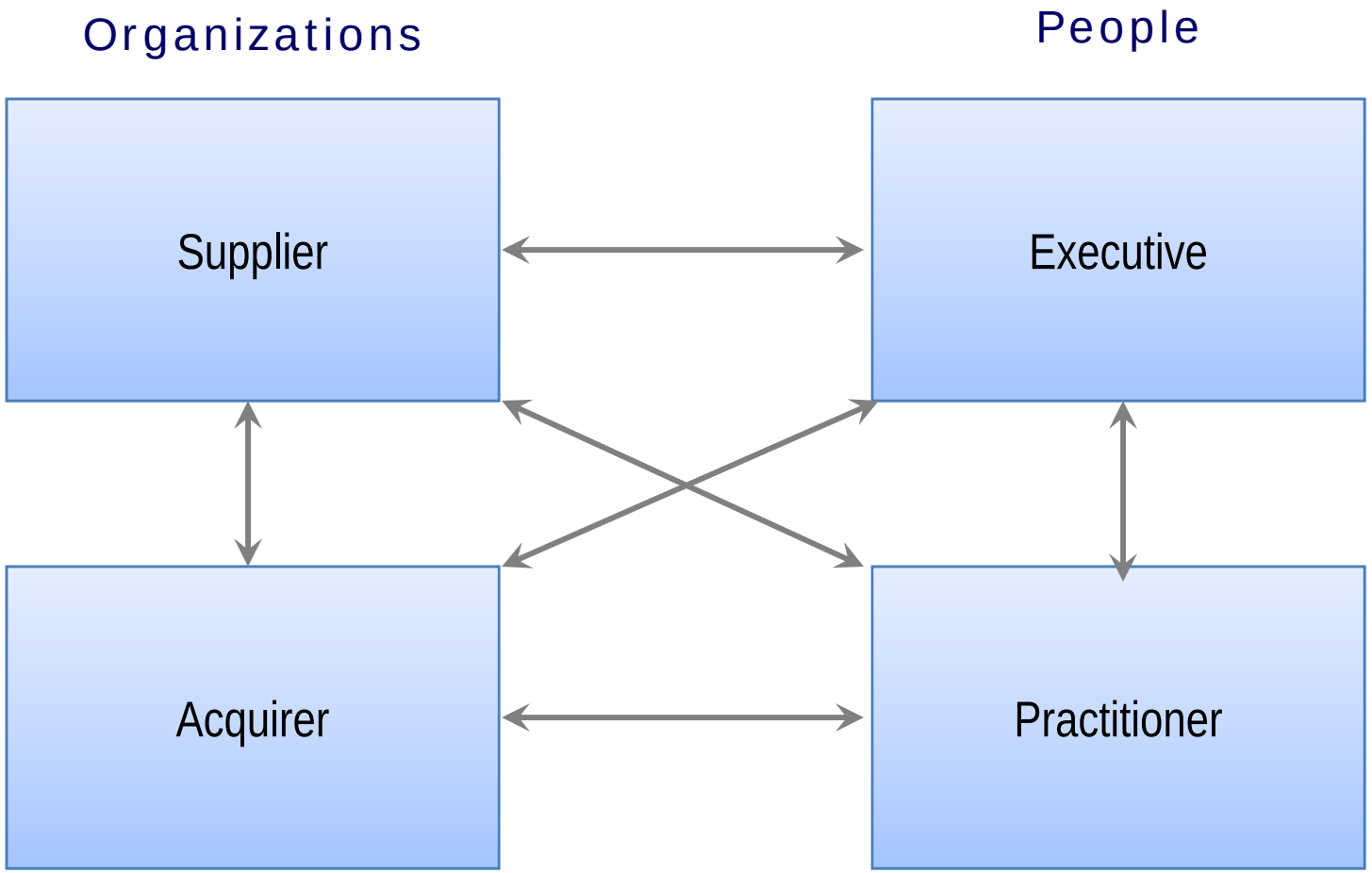
Response

- Developing Practical measurement Framework for Software Assurance and Information Security that
  - 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
- http://www.psmsc.com/Downloads/TechnologyPapers/SwA%20Measurement%2010-08-8.pdf

- 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


SOFTWARE ASSURANCE FORUM
BUILDING SECURITY IN
Stakeholders


Organizations
People
Supplier
Executive
Acquirer
Practitioner

Create/ Update Measures	Collect Data	Store Data	Analyze and Compile Data	Report Measures	Use Measures
• State goals • Identify data sources and elements • Analyze how goals and data elements relate • Create a series of measures	• Gather data from available data sources	• Document/ store data in an appropriate repository	• Analyze collected data • Compile and aggregate into measures • Interpret data • Identify causes of findings	• Document measures in appropriate reporting formats • Report measures to stakeholders	• 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

- 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

- Acquisition
  - Number and percent of acquisition discussions that include SwA representative
  - Number and percent of contracting officers who received training in the security provisions of the FAR
  - Percent of documented Supplier claims verified through testing, inspection, or other methods
  - Number and percent of relevant high impact vulnerabilities (CVEs) present in the system
- Testing
  - Number and percent of tests that evaluate application response to misuse, abuse, or threats
  - Number and percent of tests that attempt to subvert execution or work around security controls
  - Percent of untested source code related to security controls and SwA requirements

SwA Measures address transparency of processes and product properties

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Agenda

- Setting the stage
- A practical example
- Understanding the processes
- Using measurement for decision making
- Summary

- Assurance is critical for your enterprise's 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 "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/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

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

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