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

Security-Enhanced Capabilities: Mitigating Enterprise Risks

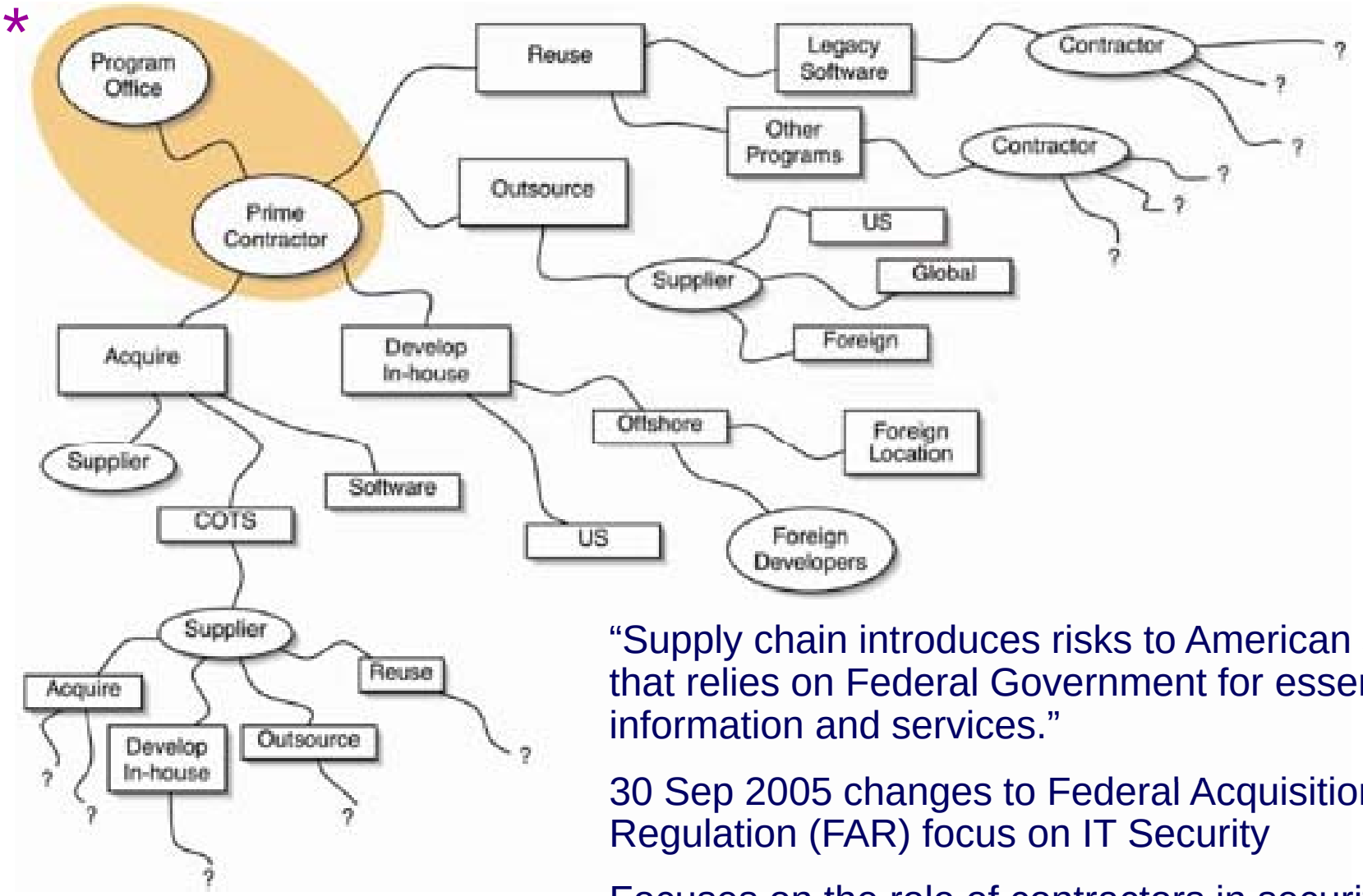
- With today's global software supply chain, Software/Systems Engineering, Quality Assurance, Testing and Project Management must explicitly address security risks posed by exploitable software.
  - Traditional processes do not explicitly address software-related security risks that can be passed from 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

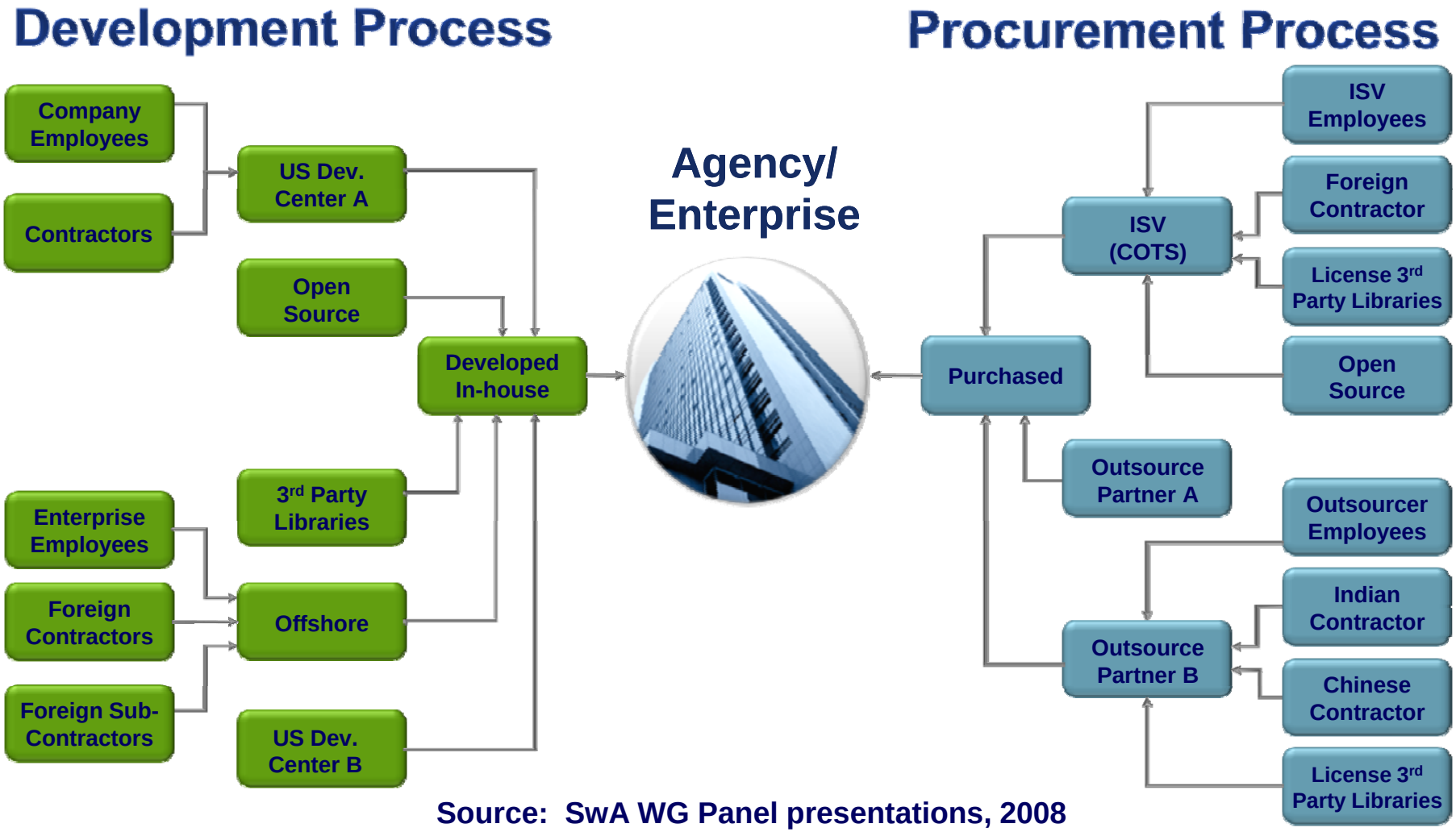
Focuses on the role of contractors in security as Federal agencies outsource various IT functions.

Homeland Security

"Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"

Enterprise Processes for deploying capabilities: Increasingly Distributed and Complex

New Considerations for Quality & Security

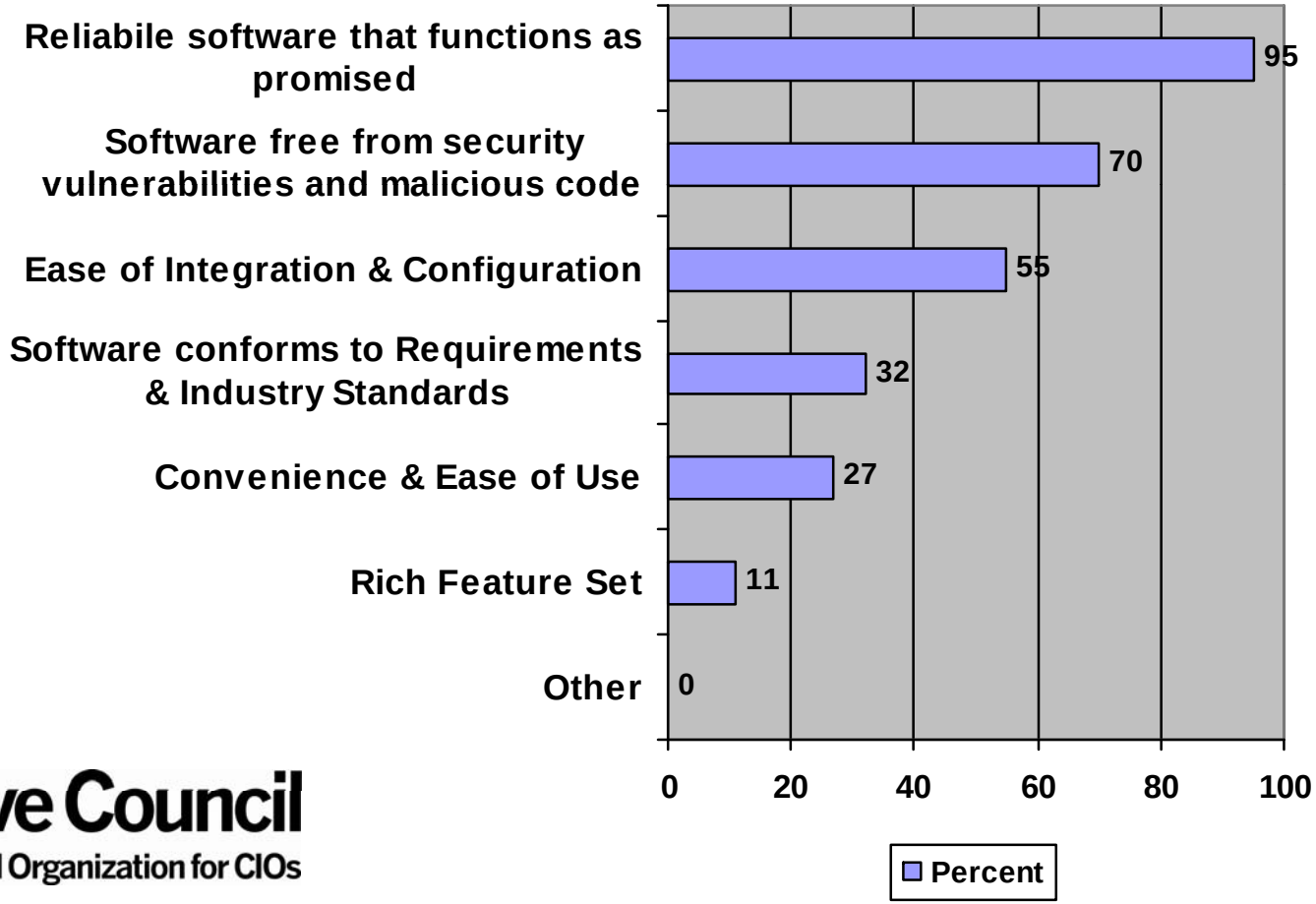


Source: SwA WG Panel presentations, 2008

- Dependencies on technology are greater then 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



CIO Executive Council
The Professional Organization for CIOs

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

What Is Assurance

- **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	Processes	Technology	Acquisition
Developers and users education & training	Sound practices, standards, & practical guidelines for secure software development	Security test criteria, diagnostic tools, common enumerations, SwA R&D, and SwA measurement	Software security improvements through due-diligence questions, specs and guidelines for acquisitions/ outsourcing

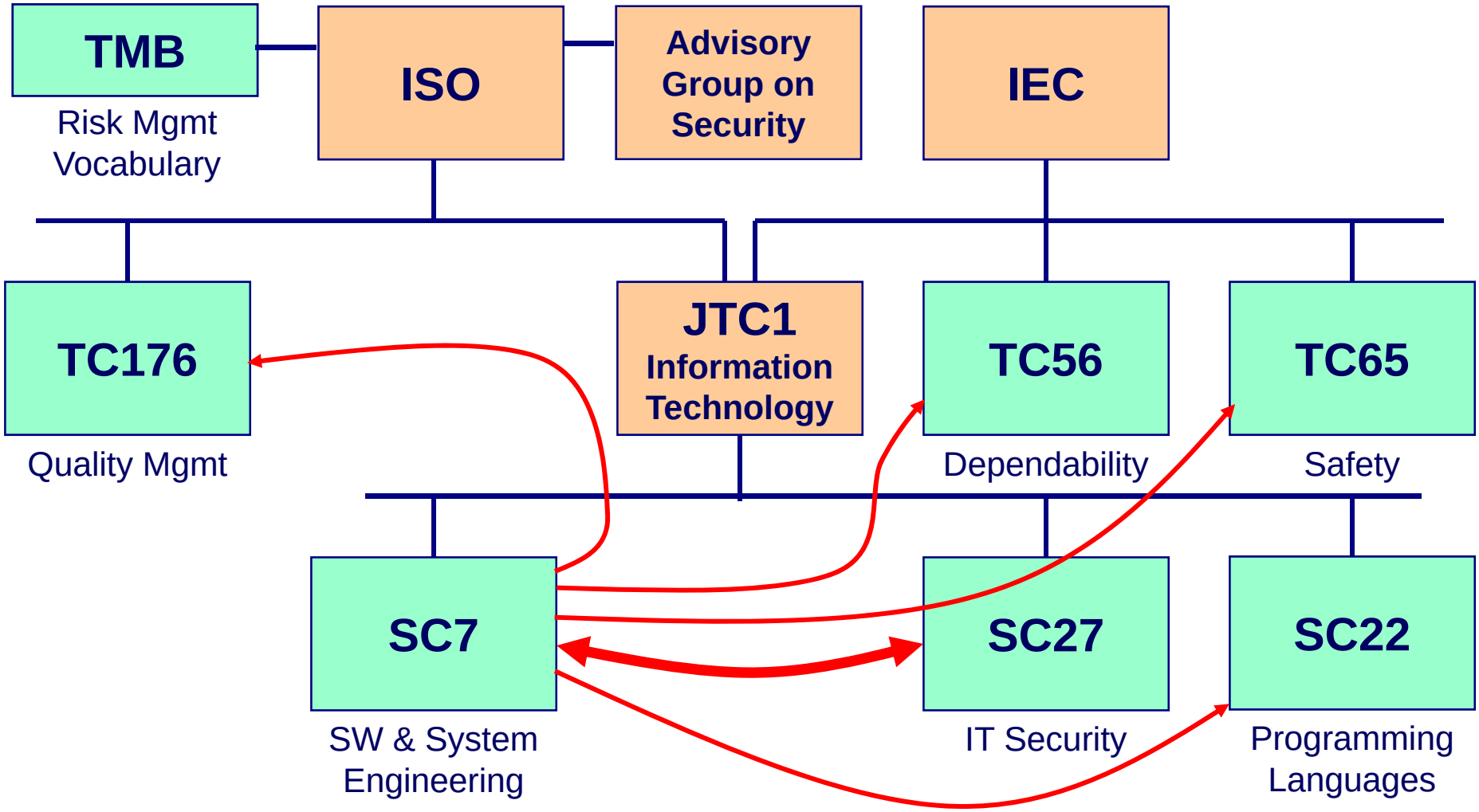
Products and Contributions

Build Security In - https://buildsecurityin.us-cert.gov and SwA community resources & info clearinghouse	Practical Measurement Framework for SwA/InfoSec Making the Business Case for Software Assurance
SwA Common Body of Knowledge (CBK) & Glossary Organization of SwSys Security Principles/Guidelines SwA Developers' Guide on Security-Enhancing SDLC	SwA Metrics & Tool Evaluation (with NIST) SwA Ecosystem w/ DoD, NSA, NIST, OMG & TOG NIST Special Pub 500 Series on SwA Tools
Software Security Assurance State of the Art Report Systems Assurance Guide (via DoD and NDIA)	Common Weakness Enumeration (CWE) dictionary Common Attack Pattern Enumeration (CAPEC)
SwA-related standards – ISO/IEC JTC1 SC7/27/22, IEEE CS, OMG, TOG, & CMM-based Assurance	SwA in Acquisition: Mitigating Risks to Enterprise Software Project Management for SwA SOAR

Homeland Security

* 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



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

Homeland Security

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

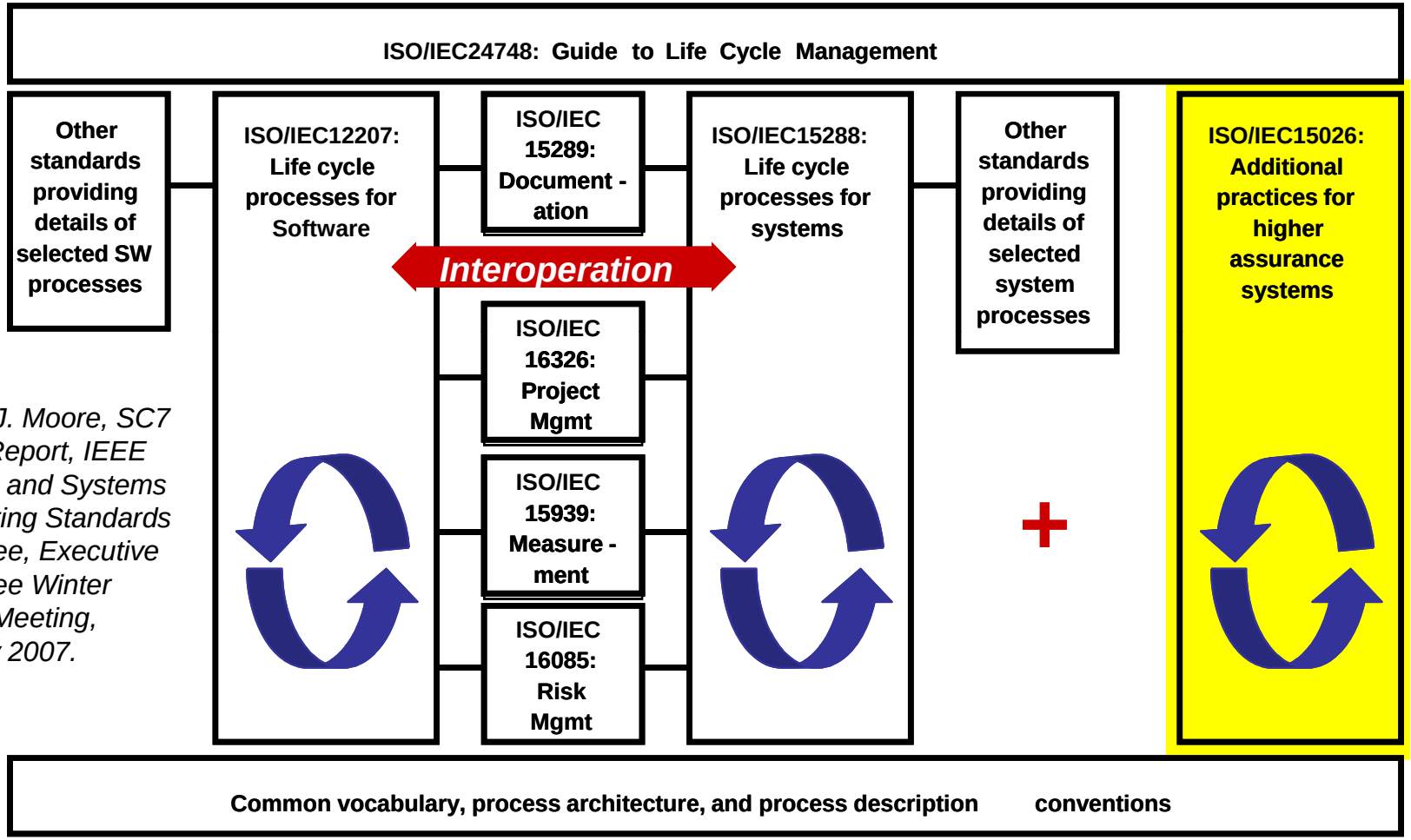
NDIA/DoD System Assurance Guidebook – Mapped To ISO/IEC/IEEE 15288

- Agreement Processes
  - Acquisition
  - Supply
- Project Processes
  - Project Planning
  - Project Assessment
  - Project Control
  - Decision-making
  - Risk Management
  - Configuration Management
  - Information Management
- **Assurance Case Process**

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

- Enterprise Processes
  - Enterprise Environment Management
  - Investment Management
  - 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"



Source: J. Moore, SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Winter Plenary Meeting, February 2007.

"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."

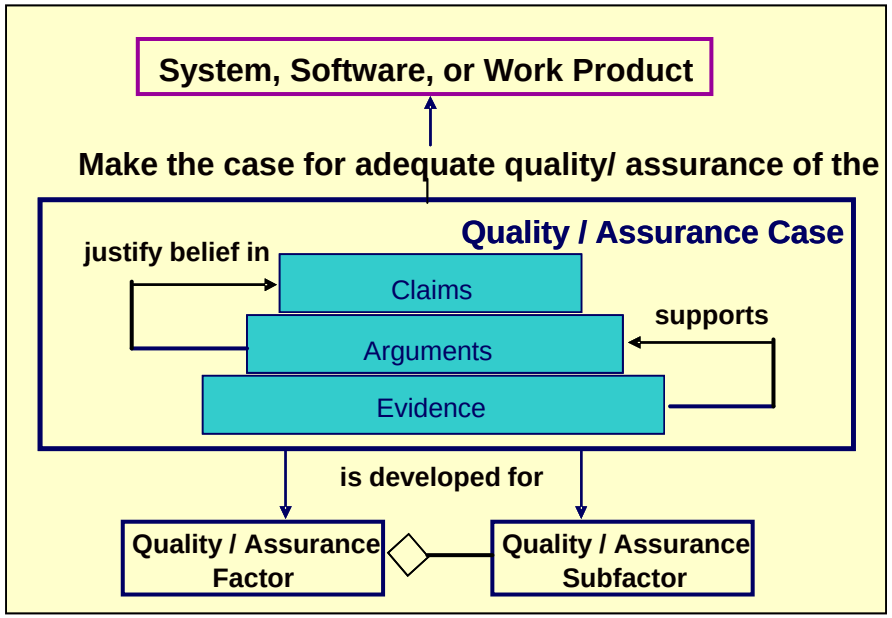
Terms of Reference changed: ISO/IEC JTC1/SC7 WG7, previously "System and Software Integrity" SC7 WG9

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

SwA Measurement

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

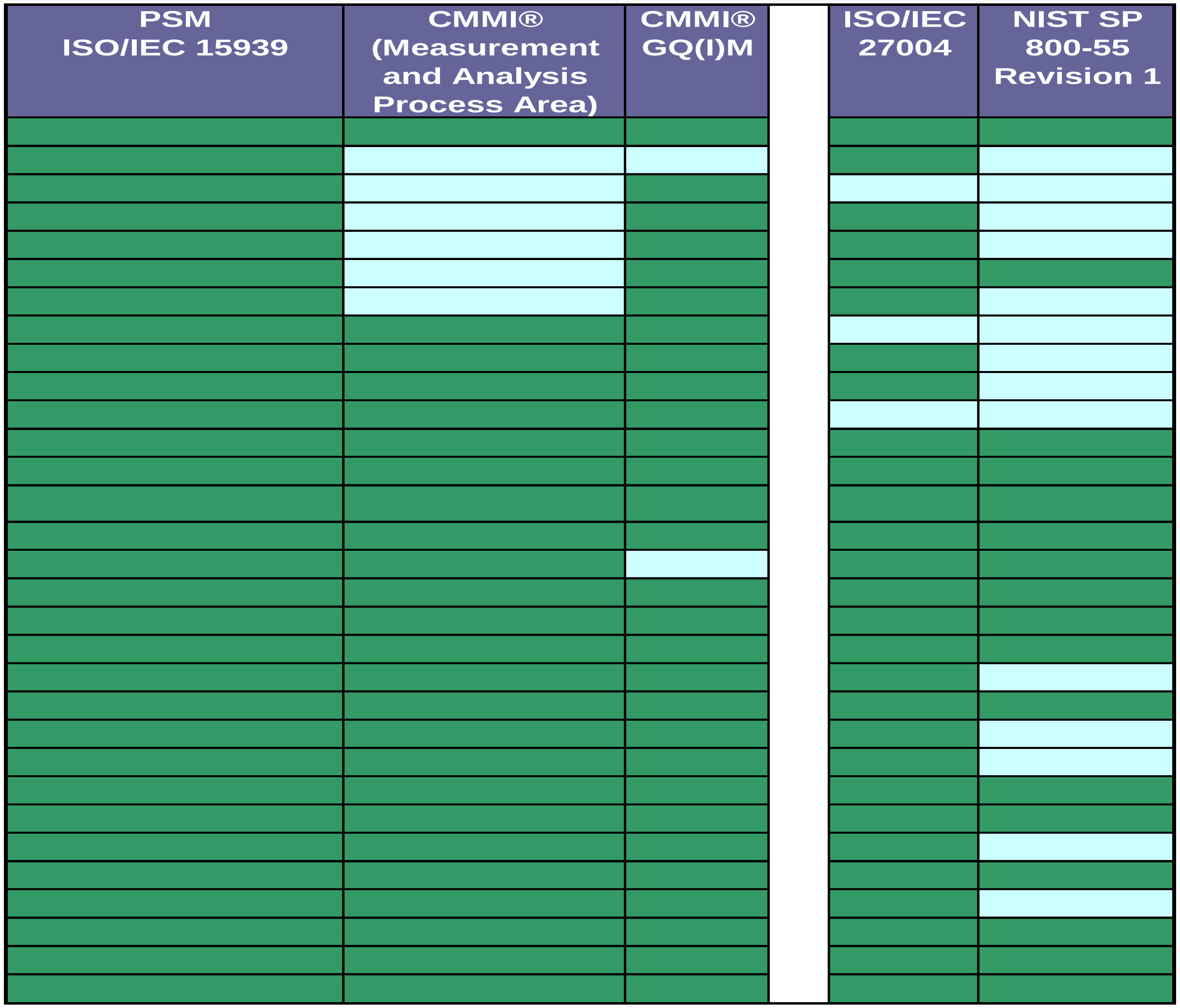
- Developed Practical measurement Framework for Software Assurance and Information Security
  - Is harmonized with common system and software and security measurement methodologies
  - Provides an approach for quantifying achievement of SwA goals and objectives within the context of individual projects, 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
- http://www.psmsc.com/Downloads/TechnologyPapers/SwA%20Measurement%2010-08-8.pdf

Base Methodologies

- 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

Measurement Framework



PSM ISO/IEC 15939	CMMI® (Measurement and Analysis Process Area)	CMMI® GQ(I)M		ISO/IEC 27004	NIST SP 800-55 Revision 1
🟩	🟩	🟩		🟩	🟩
🟩	🟦	🟦		🟩	🟦
🟩	🟦	🟩		🟦	🟦
🟩	🟦	🟩		🟩	🟦
🟩	🟦	🟩		🟩	🟦
🟩	🟦	🟩		🟩	🟩
🟩	🟦	🟩		🟩	🟦
🟩	🟩	🟩		🟦	🟦
🟩	🟩	🟩		🟩	🟦
🟩	🟩	🟩		🟩	🟦
🟩	🟩	🟩		🟦	🟦
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟦		🟩	🟩
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟦
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟦
🟩	🟩	🟩		🟩	🟦
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟦
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟦
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟩
🟩	🟩	🟩		🟩	🟩

Base Methodologies

- 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

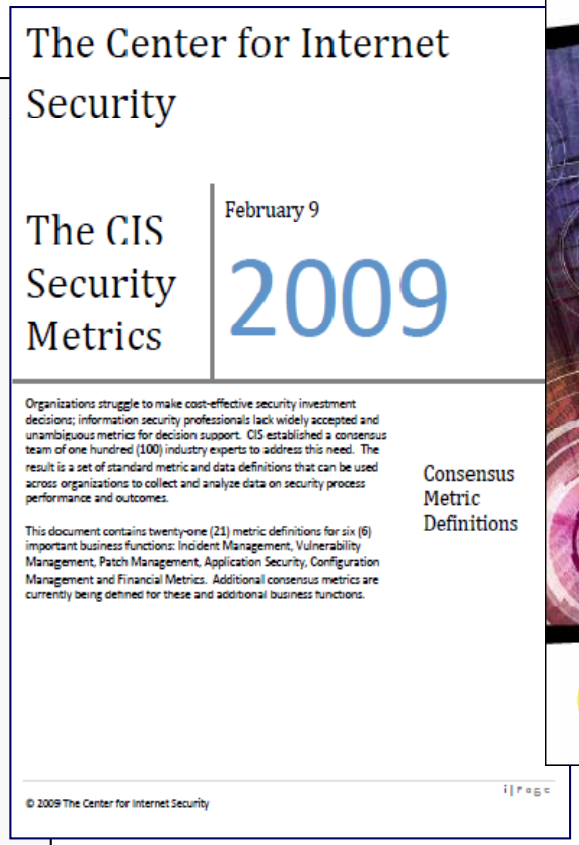
SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Security Measurement Resources

Practical Measurement Framework for Software Assurance and Information Security

Oct 2008



The Center for Internet Security

The CIS Security Metrics

February 9

2009

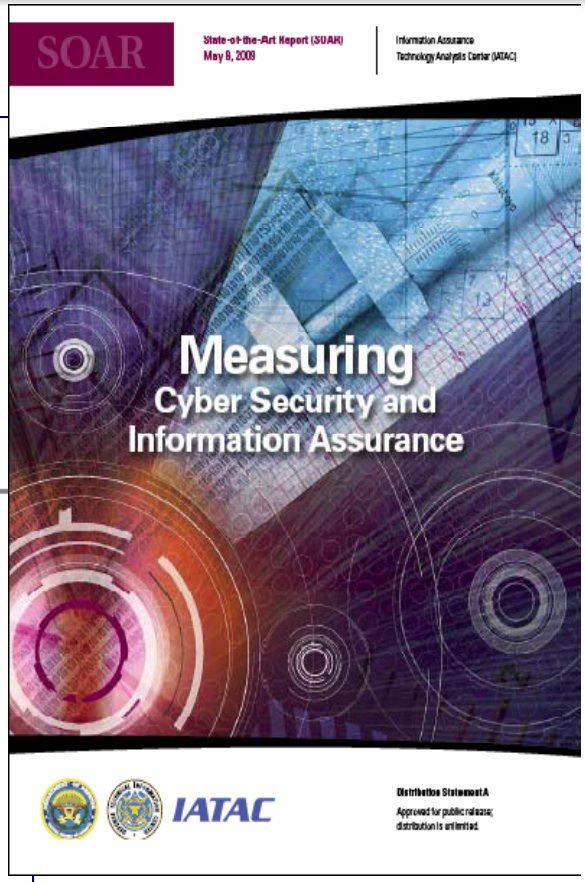
Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS established a consensus team of one hundred (100) industry experts to address this need. The result is a set of standard metric and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes.

This document contains twenty-one (21) metric definitions for six (6) important business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management and Financial Metrics. Additional consensus metrics are currently being defined for these and additional business functions.

Consensus Metric Definitions

© 2009 The Center for Internet Security

i | Page



SOAR

State-of-the-Art Report (SOAR)
May 8, 2009

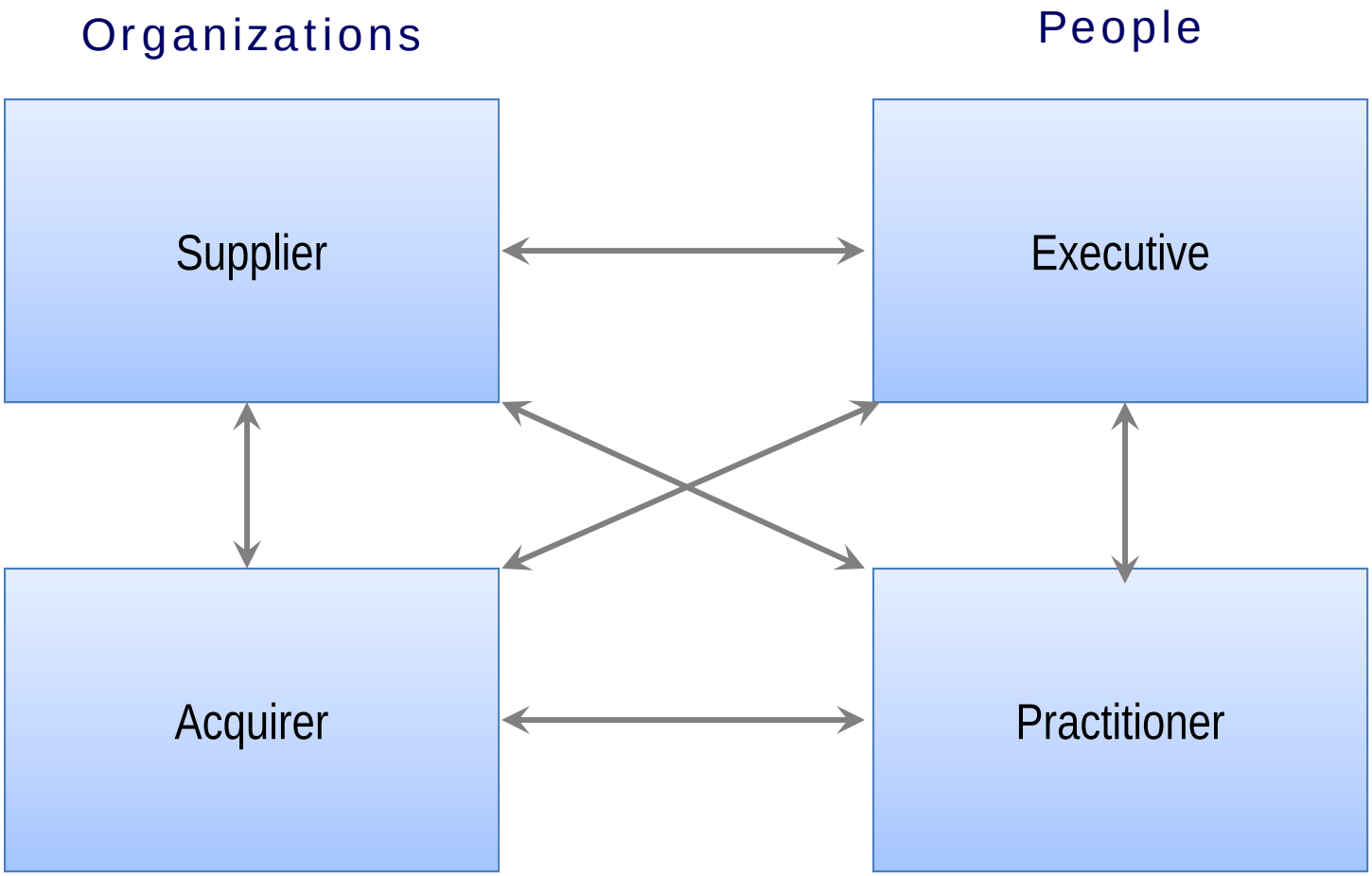
Information Assurance Technology Analysis Center (IATAC)

Measuring Cyber Security and Information Assurance

IATAC

Distribution Statement A
Approved for public release; distribution is unlimited.

Stakeholders



Measurement Process

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

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

- 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

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

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

makingsecuritymeasurable.mitre.org

Making Security Measurable™

A Collection of Information Security Community Standardization Activities and Initiatives

Home | About | Current Collection | Feedback Requested

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:

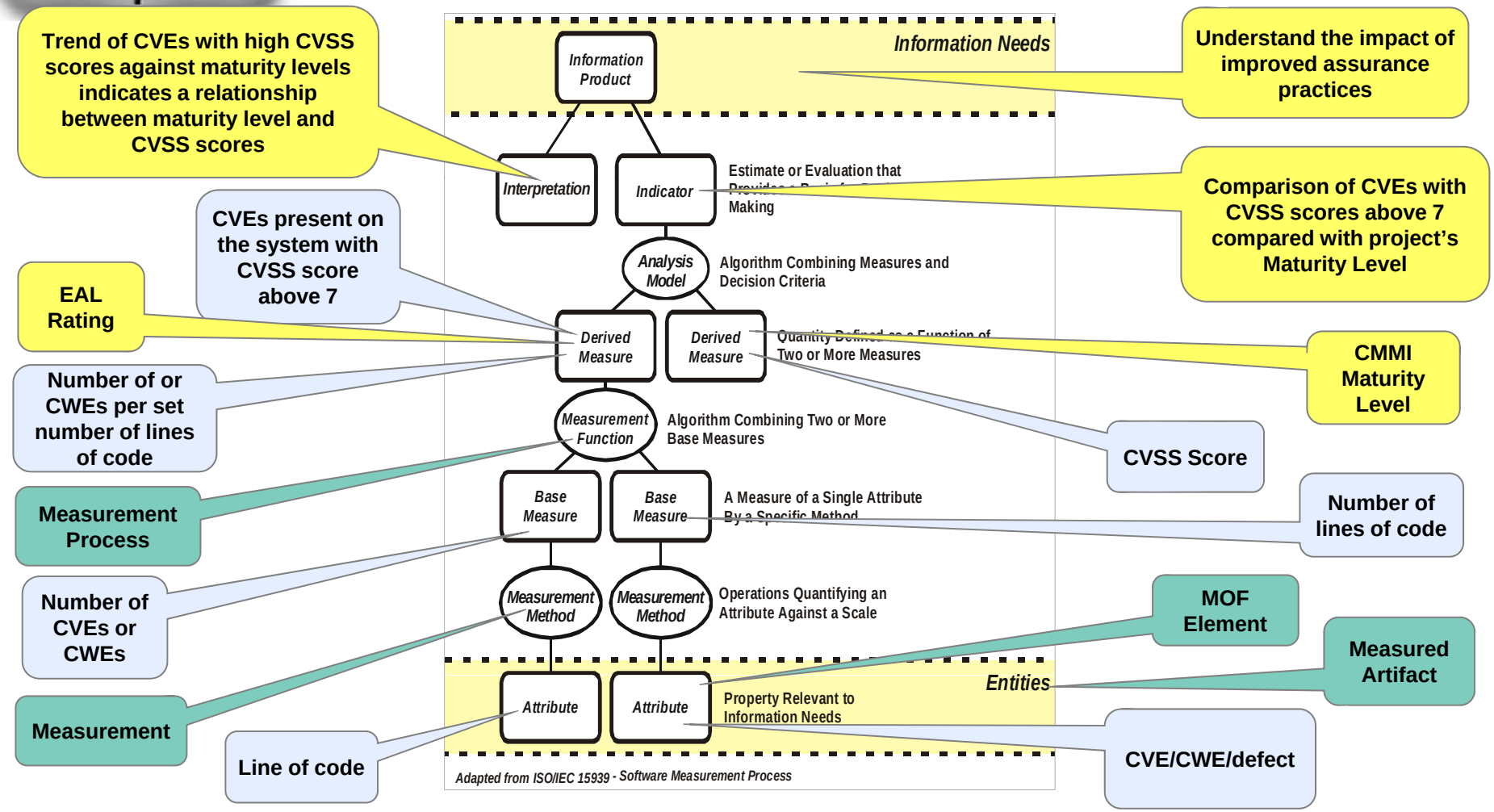
- Vulnerability Management
- Asset Security Assessment
- Configuration Guidance
- Malware Response
- Threat Analysis
- Intrusion Detection
- Asset Management
- Patch Management
- Incident Management

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

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

SwA Measurement Working Group



Agenda

- Setting the stage
- A practical example
- Leveraging Process Capability Benchmarks
- Conclusion

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

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 - Validation

What happens if contents of bar pointer >= 100?

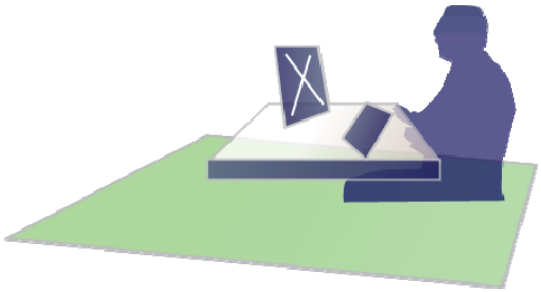
```
#include <stdlib.h>
#define BUFSIZE 100
void foo(char *bar) {
  char BUF[BUFSIZE];
   strcpy(BUF, bar);
   printf("%s\n", BUF);
  }
int main() {
   char *baz;
   baz = getenv("HOME");
   foo(baz);
   exit(0);
   }
```

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

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

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

Agenda

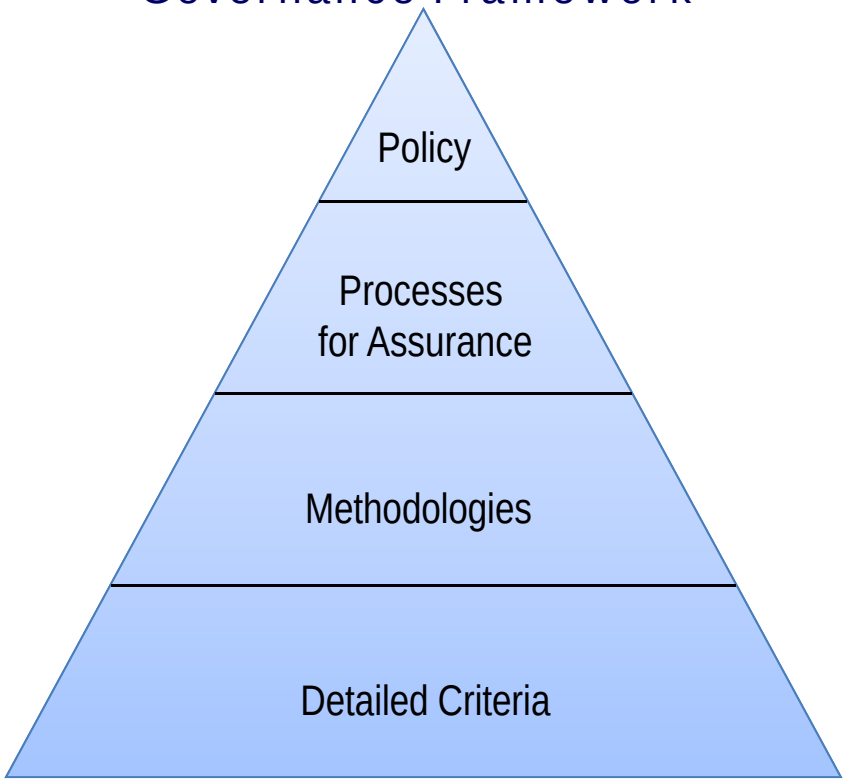
- Setting the stage
- A practical example
- Leveraging Process Capability Benchmarks
- Summary

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Integrate And Improve Assurance Practices In The SDLC

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”)

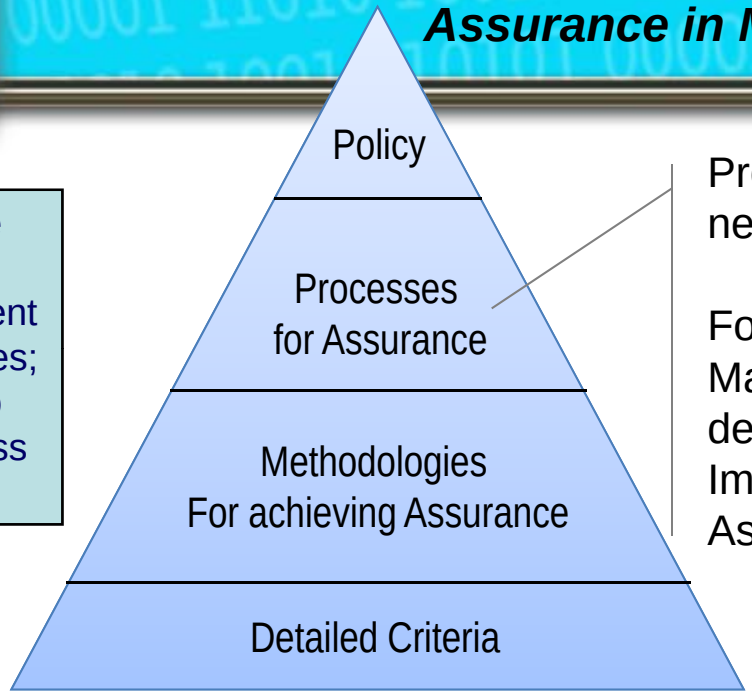
https://buildsecurityin.us-cert.gov/swa/procresrc.html

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Assurance in Maturity Models

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

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

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

Experience gained for "Assurance" enhanced processes in *U.S. DoD and FAA joint project on Safety and Security Extensions for Integrated Capability Maturity Models, September 2004,* at SwA Community Resources and Information Clearinghouse - see https://buildsecurityin.us-cert.gov/swa/downloads/SafetyandSecurityExt-Sep2004.pdf

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/

Process Reference Model - 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

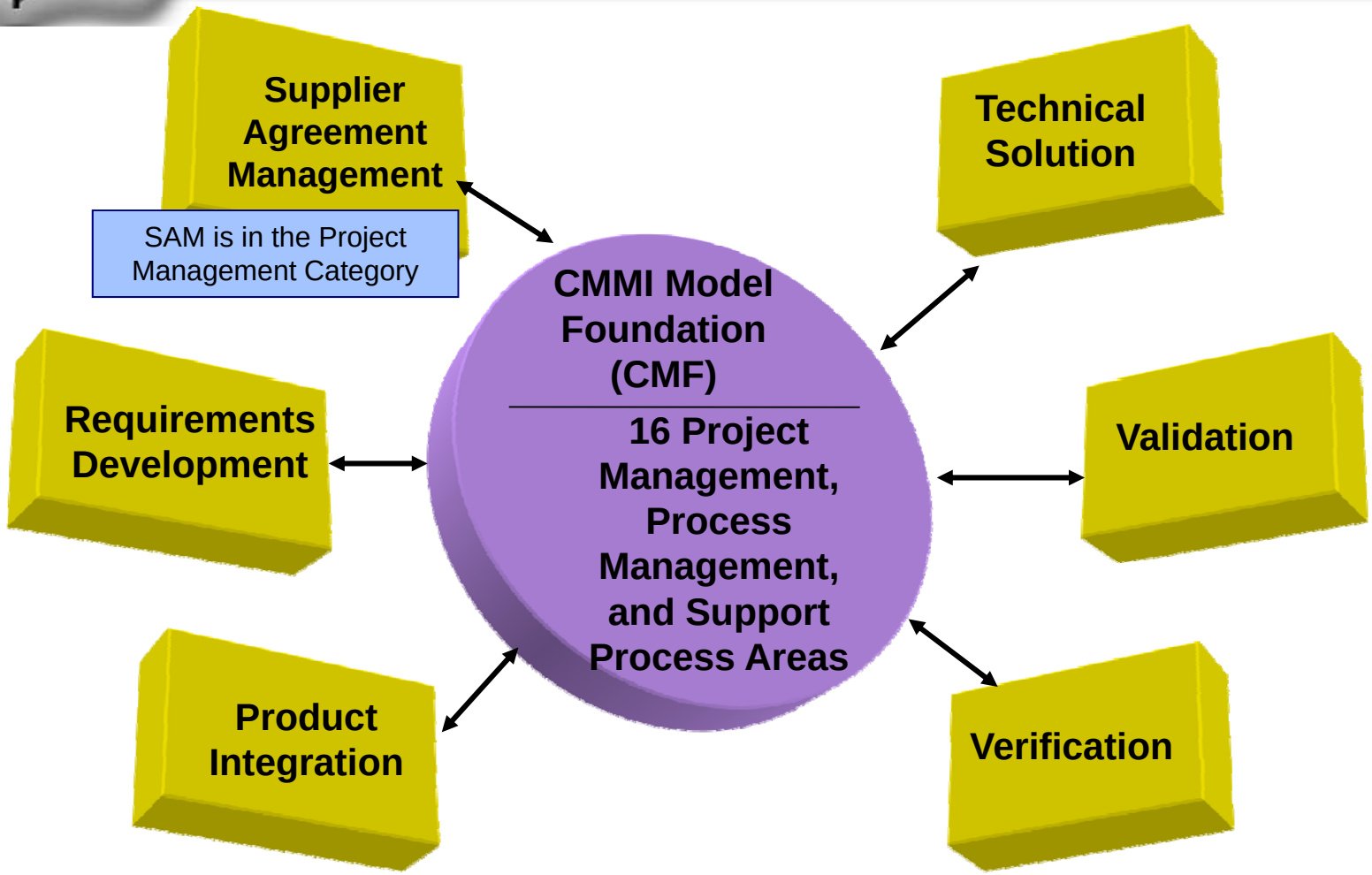
Assurance Engineering

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

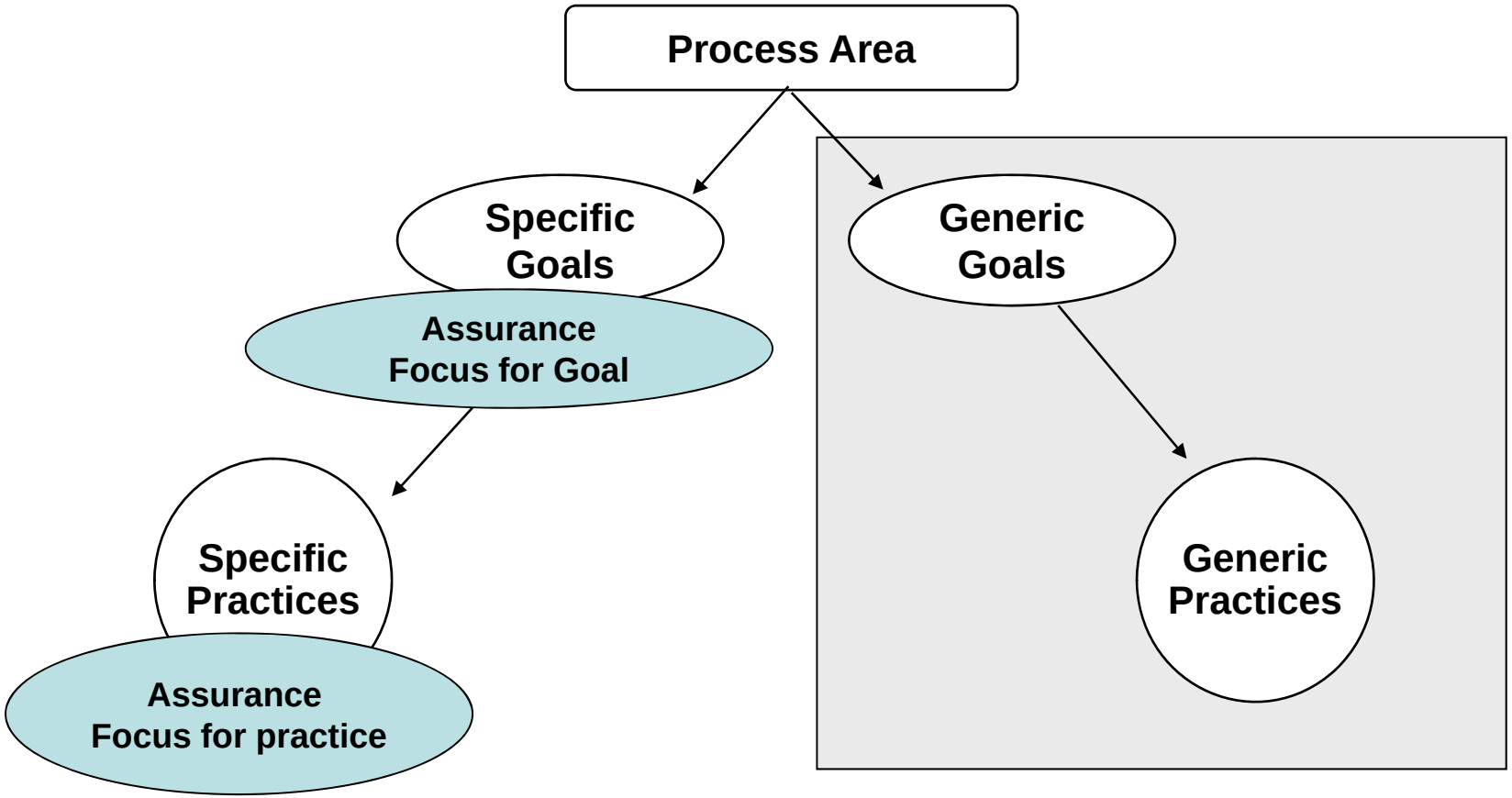
Assurance Support Activities

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

CMMI-DEV v1.2


Supplier Agreement Management
SAM is in the Project Management Category
Technical Solution
CMMI Model Foundation (CMF)
16 Project Management, Process Management, and Support Process Areas
Requirements Development
Validation
Product Integration
Verification

Assurance For CMMI Identifies The Assurance Thread for CMMI-DEV



Assurance Focus For CMMI®

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

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.

MA SP 1.2

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

Measurement and Analysis Specific Goal 2

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

MA SP 2.3

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

Measurable Practices for 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

Measurable Practices for Secure Coding (1 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) "Security Engineering Training" whitepaper	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

Measurable Practices for Secure Coding (1 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

Agenda

- 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
- 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

Contact Info

- 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