Practices Make Perfect – Leveraging Your Engineering and Management Practices To Meet the Software Assurance Challenge

Paul R. Croll

Computer Sciences Corporation
pcroll@csc.com

Industry Co-Chair, NDIA Systems Assurance Committee

Co-Chair, DHS Software Assurance Forum Working Group on Processes and Practices

Past Convener, ISO/IEC JTC1/SC7 WG9, System and Software Assurance

Topics

- System Assurance Defined
- The System Assurance Problem Space
- Software As A Root Cause Problem
- The Systems Engineering Challenge
- The CMMI® and Assurance
- Bang-For-The-Buck CMMI-DEV® Process Areas
- Guidance For Systems Assurance
- Standardization In Support Of Assurance
- Summary

System Assurance Defined

- The level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.
  - *CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006*
- Grounds for confidence that an entity meets its relevant needs, goals or objectives for safety, security and dependability or other characteristics deemed to be critical, and possesses the related required properties.
  - *ISO/IEC CD 15026, 2007, Systems and Software Assurance*

System Assurance Problem Space

- Large-scale systems and systems of systems represent a complex supply chain integrating
  - Proprietary and open-source software
  - Legacy systems
  - Hardware
  - Firmware
- These systems are sourced from multiple suppliers who employ people from around the world
- Most systems depend upon software for a good portion of 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 systems-level problem**

Software As A Root Cause Problem

- Risk has dramatically increased due to the simultaneous growth in software vulnerabilities and in threat opportunities
- Risk management processes inadequately address these threats and risks
- Threats presented by suppliers of software products and services are not adequately identified and analyzed
- Development and acquisition processes inadequately address software security
- There is a fundamental lack of both the scientific understanding of software risks and the capabilities to effectively diagnose and mitigate in the in a timely manner

Source: J. Jarzombek. DOD Software Assurance Initiative: Mitigating Risks Attributable to Software. DOD Software Assurance Forum, July 2004.

Or, More Succinctly . . .

- There is a failure to assure correct, predictable, safe, secure execution of complex software in distributed environments
- Inadequate attention is given to the total life cycle issues, including impacts on life cycle cost and risk associated with the use of commercial or reused products and components

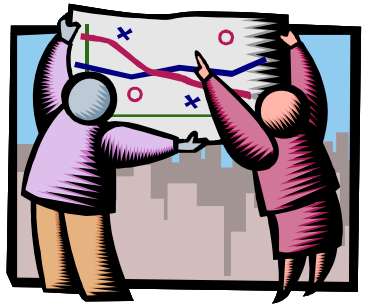
Source: G. Draper (ed.), Top Software Engineering Issues Within Department of Defense and Defense Industry. National Defense Industrial Association, Arlington, VA, August 2006.

The Systems Engineering Challenge

- Integrating a heterogeneous set of globally engineered and supplied proprietary, open-source, and other software; hardware; and firmware; as well as legacy systems; to create well-engineered integrated, interoperable, and extendable systems whose security, safety, and other risks are acceptable – or at least tolerable.

Achieving System and Software Assurance Through CMMI®-Compliant Processes

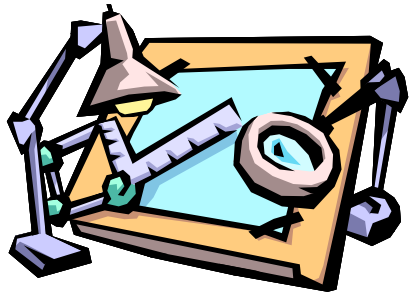
1. Understand Your Business Requirements for Assurance



2. Look to the CMMI® for Assurance-Related Process Capability Expectations

3. Look to Standards for Assurance Process Detail

4. Build or Refine and Execute Your Assurance Processes



5. Measure Your Results - Modify Processes as Necessary

CMMI®- DEV Assurance Shortfalls

- Inconsistent treatment of safety and security concerns
- Insufficient assurance detail in required and expected components
  - Specific goals
  - Specific practices
- Insufficient traceability to assurance source standards

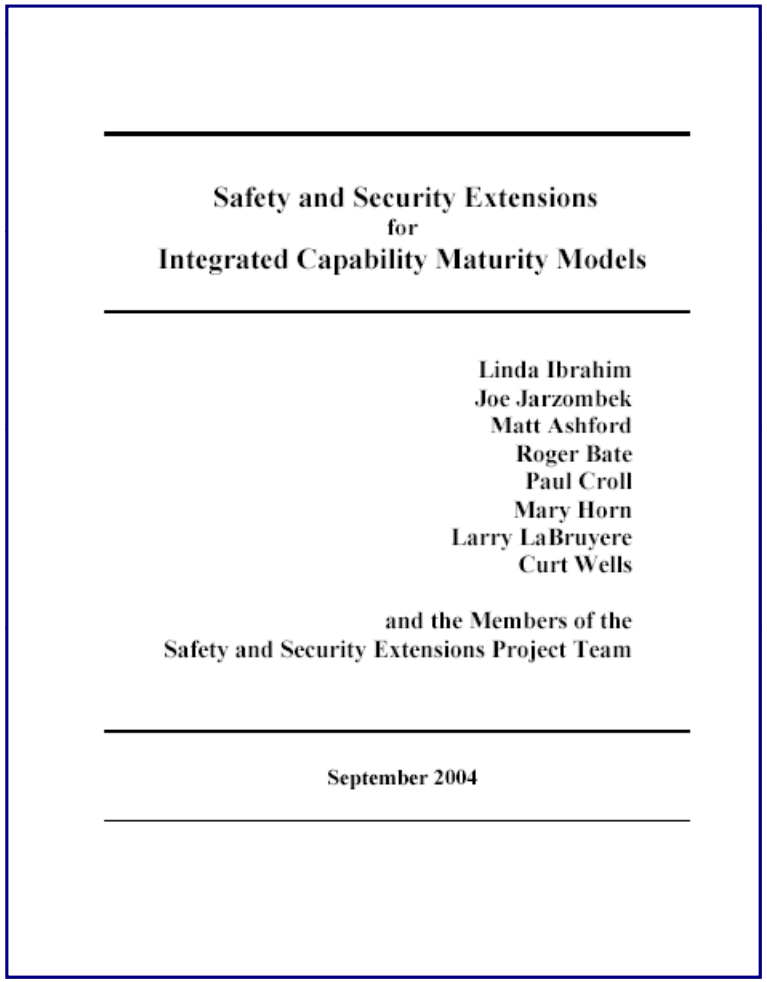
CMMI® – DEV Process Areas and Assurance

Name	*Abbr*	*Safety*	*Security*
Requirements Management	REQM	√	√
Project Planning	PP	√	√
Project Monitoring and Control	PMC		√
Supplier Agreement Management	SAM		√
Measurement and Analysis	MA		√
Process and Product Quality Assurance	PPQA		
Configuration Management	CM	√	√
Requirements Development	RD	√	√
Technical Solution	TS	√	√
Product Integration	PI	√	√
Verification	VER		
Validation	VAL		
Organizational Process Focus	OPF		
Organizational Process Definition +IPPD	OPD +IPPD	√	√
Organizational Training	OT	√	√
Integrated Project Management +IPPD	IPM +IPPD	√	√
Risk Management	RSKM	√	√
Decision Analysis and Resolution	DAR	√	
Organizational Process Performance	OPP		
Quantitative Project Management	QPM		
Organizational Innovation and Deployment	OID		
Causal Analysis and Resolution	CAR	√	

Source: CMMI® for Development, Version 1.2, CMU/SEI-2006-TR-008, August 2006

Safety and Security Extensions for Integrated Capability Maturity Models – Take 1

1. **Ensure Safety and Security Competency**
2. **Establish Qualified Work Environment**
3. **Ensure Integrity of Safety and Security Information**
4. **Monitor Operations and Report Incidents**
5. **Ensure Business Continuity**
6. **Identify Safety and Security Risks**
7. **Analyze and Prioritize Risks**
8. **Determine, Implement, and Monitor Risk Mitigation Plan**
9. **Determine Regulatory Requirements, Laws, and Standards**
10. **Develop and Deploy Safe and Secure Products and Services**
11. **Objectively Evaluate Products**
12. **Establish Safety and Security Assurance Arguments**
13. **Establish Independent Safety and Security Reporting**
14. **Establish a Safety and Security Plan**
15. **Select and Manage Suppliers, Products, and Services**
16. **Monitor and Control Activities and Products**



Safety and Security Extensions
for
Integrated Capability Maturity Models

Linda Ibrahim
Joe Jarzombek
Matt Ashford
Roger Bate
Paul Croll
Mary Horn
Larry LaBruyere
Curt Wells

and the Members of the
Safety and Security Extensions Project Team

September 2004

Source: United States Federal Aviation Administration, Safety and Security Extensions for Integrated Capability Maturity Models, September 2004 (http://www.faa.gov/about/office_org/headquarters_offices/aio/documents/media/SafetyandSecurityExt-FINAL-web.pdf)

Source Standards

Safety

- **Defence Standard 00-56**, Safety Management Requirements for Defence Systems, Ministry of Defence, United Kingdom, December 1996.
- **IEC 61508**, Functional Safety of electrical/electronic/programmable electronic safety-related systems, International Electrotechnical Commission, 1997.
- Military Standard System Safety Program Requirements, **MIL-STD-882C**, United States Department of Defense, January 1993.
- Standard Practice for System Safety, **MIL-STD-882D**, United States Department of Defense, February 2000.

Security

- **ISO/IEC 21827**, Systems Security Engineering Capability Maturity Model®, SSE-CMM®, Model Description Document, Version 3.0, June 15, 2003.
- **ISO/IEC 15408:1999**, Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, Version 2.1, 1999.
- **ISO/IEC 17799:2000(E)**: Information technology – Code of practice for information security management, International Organization for Standardization, First edition 2000-12-01.
- Risk Management Guide for Information Technology Systems, **National Institute of Standards and Technology, Special Publication 800-30, 2001**.

Source: United States Federal Aviation Administration, Safety and Security Extensions for Integrated Capability Maturity Models, September 2004 (http://www.faa.gov/about/office_org/headquarters_offices/aio/documents/media/SafetyandSecurityExt-FINAL-web.pdf)

Security Extensions for Integrated Capability Maturity Models – Take 2

- Workshop on Assurance with CMMI®, August 7, 2007
  - Relationships between Models and Standards
  - Industry experiences in extending models for assurance
    - Motorola's Secure Software Development Model
    - Lockheed Martin's Software Safety and Security Certification Best Practices
    - Booz Allen Hamilton's experience with multiple models
  - Community of interest feedback on security extensions to the CMMI®
- Security Model Harmonization Working Group
  - Harmonization of key security capability maturity models including but not limited to the **SSE-CMM** and the **Motorola Secure Software Development Model (MSSDM)**
  - Draft Process Reference Model for Assurance
  - Assurance beginning with Security in Phase I adding Safety and Dependability in Phase II

Process Reference Model for Assurance

PA1 - Assurance Process Management

SG1.1 Determine the assurance improvement opportunities to achieve key business goals.

SG1.2 Establish the infrastructure to sustain the assurance program within the organization.

SG1.3 Establish and maintain an assurance culture for requirements, analysis, architecture, development, integration, and test.

PA2 - Assurance Project Management

SG2.1 Manage assurance activities against plans. All assurance aspects of the technical effort are planned.

SG2.2 Establish and maintain an assurance infrastructure for the project.

SG2.3 Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities.

PA3 - Assurance Engineering

SG3.1 Establish assurance requirements.

SG3.2 Architect a solution for assurance.

SG3.3 Implement a solution for assurance.

SG3.4 Verify and Validate the product assurance.

SG3.5 Identify and manage risks throughout the product and system lifecycle.

PA4 - Assurance Support Management

SG4.1 Provide clear evidence that the work products meet the customer's assurance needs.

SG4.2 Protect project and organizational assets.

Bang-For-The-Buck CMMI®-DEV Project Management Process Areas

$$$	RSKM	– **Identify, Evaluate, Categorize, and Prioritize Assurance Risks** – **Develop assurance risk mitigation strategies**
$$	PP	– Determine a technical approach for the project that supports the assurance requirements – Determine the level of security required for tasks, work products, hardware, software, personnel, and work environment
$$	PMC	– Monitor significant changes in risk status – Monitor the security environment
$$$	SAM	– **Evaluate COTS products for compliance with assurance requirements** – **Evaluate the trustworthiness of the supplier**

Bang-For-The-Buck CMMI-DEV® Process Management Process Areas

$$$

OT

- Establish and maintain training capability to address assurance-related training needs
- **Provide training necessary to ensure the competency of individuals required to perform assurance-related roles effectively**

Bang-For-The-Buck CMMI-DEV® Engineering Process Areas

$$$	RD	– **Identify customer expectations for assurance** – **Define product assurance attributes**
$$$	TS	– **Identify and analyze alternative solutions based on proposed product architectures that address critical product qualities** – Ensure that the detailed design adheres to applicable assurance standards and criteria
$$	VER	– Select verification methods based on their ability to demonstrate that the work product properly reflects the specified assurance requirements – Establish and maintain the environment needed to support validation, including test tools and simulations
$$	VAL	– Select validation methods based on their ability to demonstrate that customer expectations for assurance are satisfied – Establish and maintain the environment needed to support validation, including test tools and simulations

Bang-For-The-Buck CMMI-DEV® Support Process Areas

$$$ **CM**

- Create a baseline that can be changed only through formal change control procedures
- Perform reviews to ensure that changes have not compromised the safety, security, or dependability

$$ **PPQA**

- Objectively evaluate the work products against the applicable assurance process descriptions, standards, and procedures

DoD-Related Guidance For Systems Assurance

- ***National Defense Industrial Association System Assurance Guidebook***
  - An NDIA guidebook 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
    - Correspondence with Existing Documentation, Policies, and Standards
      - Executive Policy, Services Standards, NIST/NSA (NIAP) Standards, GEIA, AIA, IEEE, ISO Standards, Best Practice (e.g., DHS/DOD SwABOK)

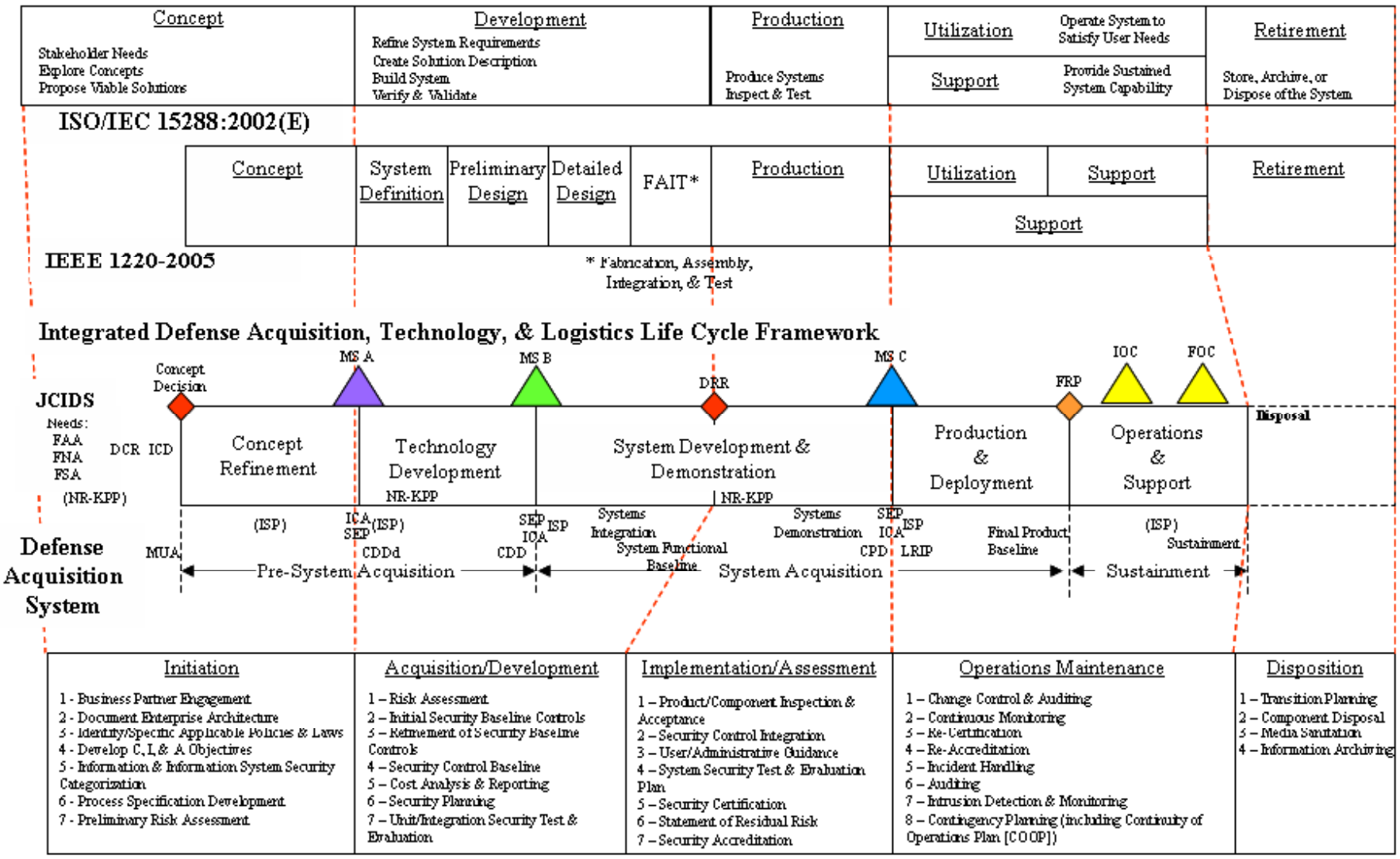
NDIA/DoD System Assurance Guidebook – Mapped To ISO/IEC/IEEE 15288

- 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

Alignment of Standards In The Guidebook



NIST Information Security and the System Development Life Cycle

Other Guidance For Systems Assurance

- ***State of the Art Report on Software Security Assurance***
  - An IATAC/DACS report identifying and describing the current state of the art in software security assurance
- ***Secure Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software***
  - A DHS guidebook intended as a framework to identify workforce needs for competencies and leverage standards and best practices to guide software-related curriculum development
- ***Security in the Software Life Cycle: Making Software Development Processes – and the Software Produced by Them – More Secure***
  - An DHS report providing a compendium of methodologies, life cycle process models, sound practices, and supporting technologies that would, if adhered to, increase software security
- ***Software Assurance in Acquisition: Mitigating Risks to the Enterprise***
  - A DHS report intended to provide guidance on enhancing supply chain management through improved risk mitigation and contracting for secure software

Standardization In Support Of Assurance

- ISO/IEC SC22 – OWG: Vulnerabilities (OWGV)
  - Project 22.24772: Guidance for Avoiding Vulnerabilities through Language Selection and Use
- ISO/IEC SC 27 IT Security Techniques
  - ISO/IEC 15408, Common Criteria for IT Security Evaluation
  - ISO/IEC 15443, FRITSA
    - Part 1: A framework for IT security assurance
    - Part 2: Assurance methods
    - Part 3: Analysis of assurance methods
  - ISO/IEC 21827, System Security Engineering Capability Maturity Model (SSE CMM) revision
  - ISO/IEC 27000 series – Information Security Management System (ISMS)
- IEC SC 65A, Functional Safety
  - IEC 61508, Functional Safety Of Electrical/ Electronic/Programmable Electronic Safety-related Systems
- ISO/IEC JTC1/SC7, Software and Systems Engineering
  - ISO/IEC/IEEE 15026, System and Software Assurance

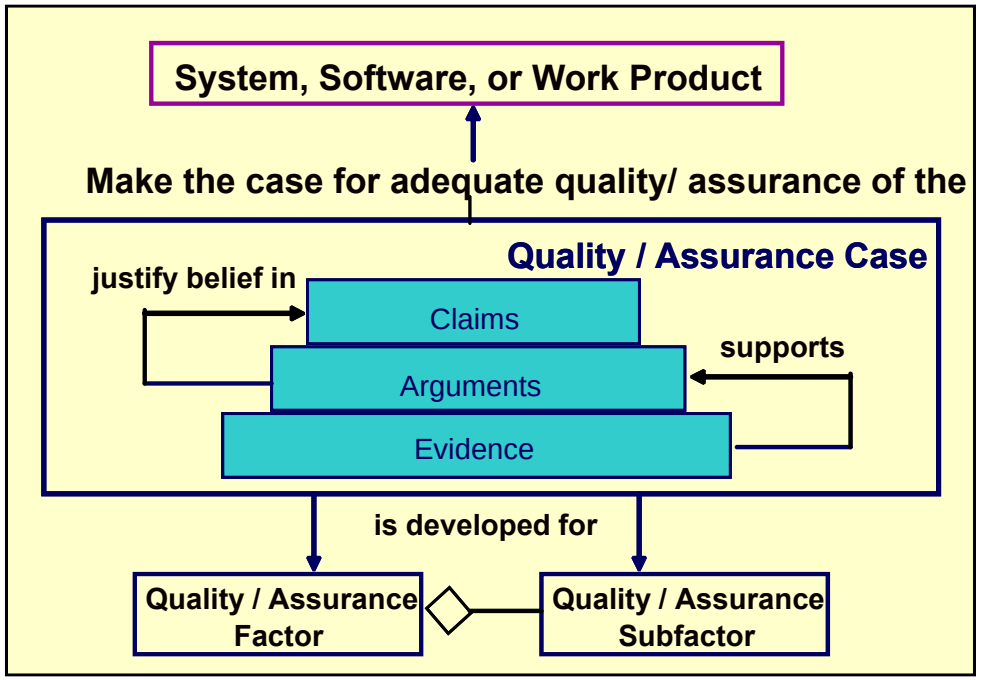
Federal Information Security Management Act (FISMA)[1] Implementation

- **FIPS Publication 199**, Standards for Security Categorization of Federal Information and Information System
- **FIPS Publication 200**, Minimum Security Requirements for Federal Information and Federal Information Systems
- **NIST Special Publication 800-30, Revision 1**, Risk Assessment Guideline)
- **NIST Special Publication 800-37**, Guide for the Security Certification and Accreditation of Federal Information Systems
- **NIST Special Publication 800-39**, NIST Risk Management Framework
- **NIST Special Publication 800-53 Revision 1**, Recommended Security Controls for Federal Information Systems
- **NIST Special Publication 800-53A**, Guide for Assessing the Security Controls in Federal Information Systems
- **NIST Special Publication 800-59**, Guide for Identifying an Information System as a National Security System
- **NIST Special Publication 800-60**, Guide for Mapping Types of Information and Information Systems to Security Categories

[1]*Federal Information Security Management Act of 2002*
Source: http://csrc.nist.gov/sec-cert/ca-proj-phases.html

The ISO/IEC/IEEE 15026 Assurance Case

- **Set of structured assurance claims, supported by evidence and reasoning, 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 and regulatory requirements
  - The configuration baseline
  - Identified hazards and threats and residual risk of each hazard and threat
  - Operational and support assumptions

Attributes

- Clear
- Consistent
- Complete
- Comprehensible
- Defensible
- Bounded
- Addresses all life cycle stages

Summary

- **The challenge**
  - Integrating a heterogeneous set of globally engineered and supplied proprietary, open-source, and other software; hardware; and firmware; as well as legacy systems; to create well-engineered integrated, interoperable, and extendable systems whose security, safety, and other risks are acceptable – or at least tolerable.

    Source: G. Draper (ed.), Top Software Engineering Issues Within Department of Defense and Defense Industry. National Defense Industrial Association, Arlington, VA, August 2006.
- **Your engineering and management practices can help meet the software assurance challenge**
  - Understand your business requirements for assurance
  - Use process benchmarks like the CMMI-DEV® to help focus process capability with respect to assurance
  - Use standards and other guidance documents to help elaborate process details
  - Assess how well your processes are supporting your business requirements for assurance, and improve as necessary

References

CMMI® for Development, Version 1.2, CMU/SEI-2006-TR-008, Software Engineering Institute, Carnegie Mellon University, August 2006

G. Draper (ed.), *Top Software Engineering Issues Within Department of Defense and Defense Industry*. National Defense Industrial Association, Arlington, VA, August 2006.

K. Goertzel (ed.), *State of the Art Report on Software Security Assurance, Draft*. DOD Information Assurance Technical Assistance Center (IATAC) and the DOD Data and Analysis Center for Software (DACS), March 2007.

K. Goertzel (ed.), *Security in the Software Life Cycle: Making Software Development Processes – and the Software Produced by Them – More Secure, Draft 1.1*. U.S. Department of Homeland Security, July 2006.

J. Jarzombek. *DOD Software Assurance Initiative: Mitigating Risks Attributable to Software*. DOD Software Assurance Forum, July 2004.

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

J. Moore, *Proposed Revision of ISO/IEC 15026: Status Report, IEEE Software and Systems Engineering Standards Committee*, Executive Committee Summer Plenary Meeting, July 2007

National Defense Industrial Association Systems Assurance Guidebook. *Version .89*. National Defense Industrial Association, Arlington, VA, February, 2008.

S. Redwine (ed.), Secure *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software*, *Draft 1.1*. U.S. Department of Homeland Security, September 25 2006.

Software Assurance in Acquisition: Mitigating Risks to the Enterprise, Draft 1.0. U.S. Department of Homeland Security, March 2007.

For More Information . . .

Paul R. Croll
Computer Sciences Corporation
5166 Potomac Drive
King George, VA 22485-5824

Phone: +1 540.644.6224
Fax: +1 540.663.0276
e-mail: pcroll@csc.com