Standards And Guidance For Engineering Secure Systems

Paul Croll
IEEE Computer Society
VP for Technical and Conference Activities

CSC Fellow

SSTC 2012
Salt Lake City, UT
April 24, 2012

IEEE computer society

CSC

IEEE

Topics

- System and Software Assurance vs. Information Assurance
- The System and Software Assurance Problem
- The Governance Context for Assurance
- Governance in the Engineering Life Cycle
- Standards for System and Software Assurance
- Additional Guidance For Systems and Software Assurance
- Rationalizing Governance, Engineering Practice, and Engineering Economics

System and Software Assurance vs. Information Assurance

- System assurance is the justified confidence that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.

- Software assurance is 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.

Source: Committee on National Security Standards. CNSS Instruction No. 4009, National Information Assurance Glossary, Ft. Meade, MD, Revised 2010..

- Information Assurance consists of measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Source: Committee on National Security Standards. CNSS Instruction No. 4009, National Information Assurance Glossary, Ft. Meade, MD, Revised 2010..

The System and Software Assurance Engineering Problem

The Assurance Problem Space

- System Integration Complexity
  - Proprietary and open-source software
  - Legacy systems
  - Hardware
  - Firmware
- Sourcing/Supply Chain
  - Multiple suppliers who employ people from around the world
- Reliance on Software Functionality
  - Most systems depend upon software for much of their functionality
  - Technologies to build reliable and secure software are in many cases inadequate
  - Difficult to construct complex software-intensive systems for which we accurately predict behavior

Assurance is a full life cycle problem

Software As A Root Cause Problem

- Software risk has dramatically increased due to the simultaneous growth in software vulnerabilities and in threat opportunities
- Software 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.

The Scope of The Problem

Size in FP	Civilian Government Projects	Military Projects	*Average*
1	1	1	*1*
10	5	4	*5*
100	29	14	*24*
1,000	155	55	*120*
10,000	832	209	*600*
100,000	4,467	794	*3,031*
1,000,000	23,988	3,020	*15,412*
Average	*4,211*	*585*	*2,742*

Figure 1. Estimated Number of Security Vulnerabilities in Software Applications. Source: Capers Jones © 2008

Size in FP	Civilian Government Projects	Military Projects	*Average*
1	25.00%	5.00%	*11.29%*
10	35.00%	15.00%	*26.00%*
100	45.00%	20.00%	*33.57%*
1,000	62.00%	30.00%	*54.57%*
10,000	80.00%	35.00%	*74.00%*
100,000	87.00%	40.00%	*80.14%*
1,000,000	92.00%	45.00%	*86.29%*
Average	*60.86%*	*27.14%*	*52.27%*

Figure 2. Probability of Serious Security Vulnerabilities in Software Applications. Source: Capers Jones © 2008

- For military projects, as one approaches systems the size of typical large combat systems (expressed as function points), the estimated number of security vulnerabilities rises to above 3000 and the probability of serious vulnerabilities rises to over 45%
- The statistics are much worse for civilian systems. As we move more and more into COTS and open source software for our combat systems, one might expect that the true extent of vulnerabilities in our systems would lie somewhere between those of military and civilian systems.

Software Assurance Engineering Shortfalls

- Current techniques for specifying, building, demonstrating, and verifying assured components with well understood properties are not cost-effective or scalable
- Cannot easily infer the assurance properties of a system, or systems of systems, from component level assurance information
- Don't know enough about composability problems and emergent behavior when components are interconnected in large-scale systems and systems of systems
- Exhaustive testing to rule out vulnerabilities is generally not feasible due to the size and complexity of our systems of interest

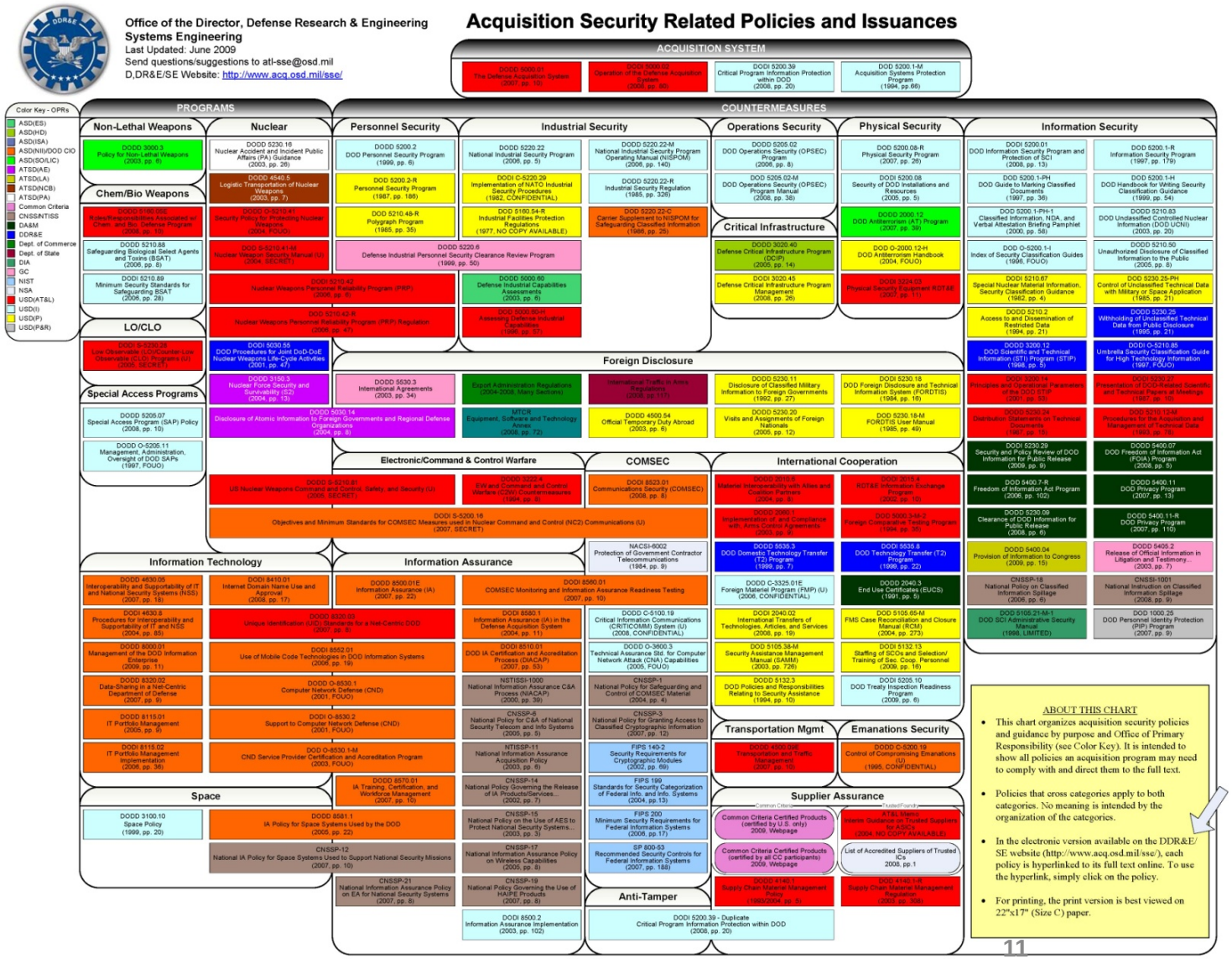
Source: G. Draper (ed.), Top Software Engineering Issues Within Department of Defense and Defense Industry. National Defense Industrial Association, Arlington, VA, August 2006.

Governance for System and Software Assurance

The Governance Context for Assurance

- In the U. S. Federal marketplace alone, there are over two hundred governance documents related to system and software assurance
  - An example for the US DoD is provided on the next slide
- A recent U. S. Congressional Budget Office review estimated the cost of implementing the Federal Information Security Act of 2008 (FISMA) alone, designed to improve information security throughout the federal government, at US $40 million in 2009 and about US $570 million over the 2009-2013 period.
- These external governance requirements drive internal governance structures that must be both responsive and cost-effective, while providing value to all stakeholders

Example: US DoD Compilation of Security-Related Policy and Guidance

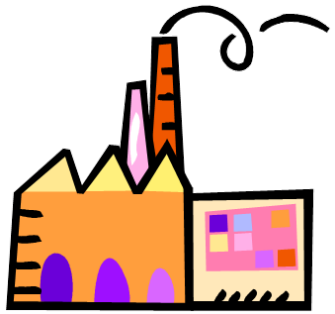


Source: Acquisition Security Related Policies and Issuances, Office of the Director, Defense Research & Engineering Systems Engineering, http://www.acq.osd.mil/se/docs/acq-security-policy-tool/index.html

IEEE computer society

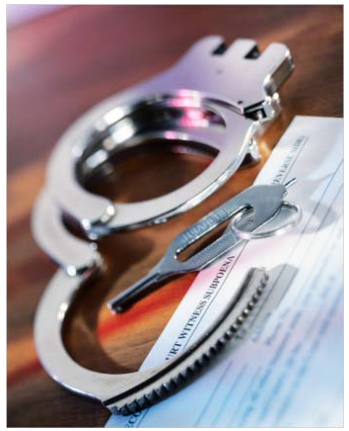
Governance Classes

- In performing the engineering trades associated with system and software assurance, governance documents of various classes define compliance and conformance requirements that may constrain the trade space. These may include:
  - Legal and regulatory requirements
  - Industry standards
  - Client-imposed requirements
  - Internal guidelines

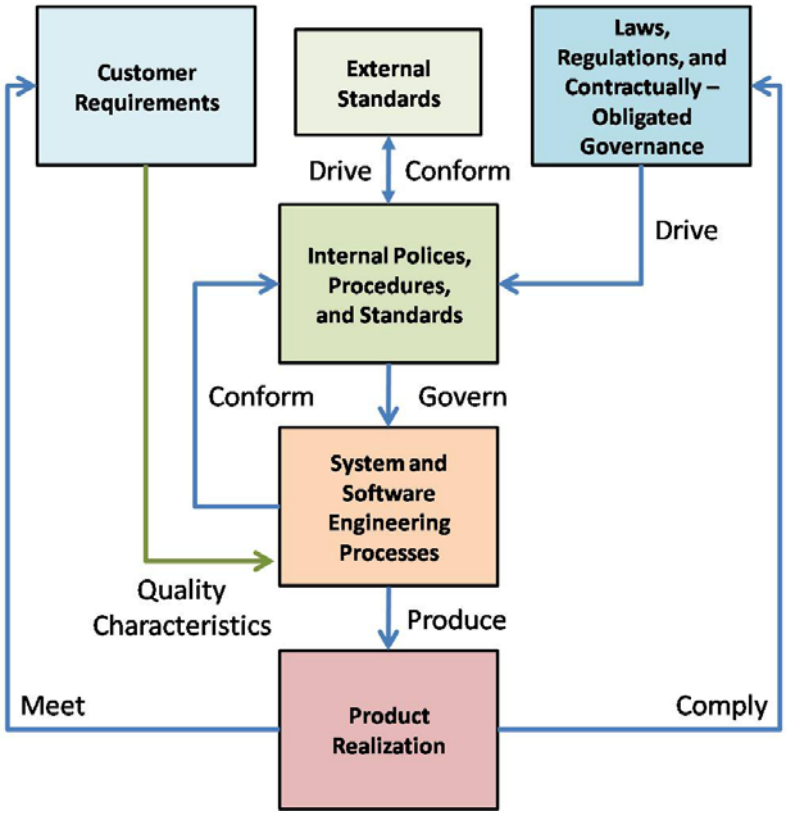
Compliance vs. Conformance

- There is a difference between compliance and conformance
  - Compliance refers to mandatory adherence to laws, rules, and regulations
  - Conformance refers to voluntary adherence to standards and best practices.
- Compliance requirements and conformance objectives are addressed as part of an organization's business strategy through the development and promulgation of an internal governance structure consisting of:
  - Policies
  - Procedures
  - Standards
  - Practices
- These are aligned with external compliance and conformance drivers



Governance in the Engineering Life Cycle

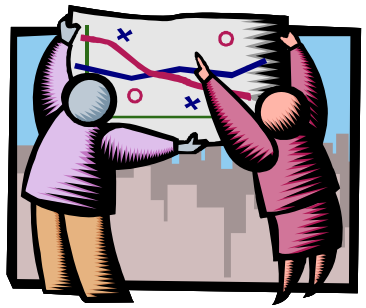
- Customer requirements for the system, defining the system's quality requirements, set the expectations for the system. It is against these quality requirements that engineering trades will be made.
- Applicable laws, regulations, and other contractually-obligated governance set the constraints bounding the engineering this trade space.
- External standards drive Internal policies, procedures, and standards
- Internal policies, procedures, and standards institutionalize external governance requirements (as well as external standards and business best practices) and drive the engineering processes for producing systems and software
- Engineering processes produce the product by trading off internal governance requirements along with customer quality requirements, to facilitate optimization among quality characteristics and compliance with external governance requirements.



Engineering for Assurance

Using Process Benchmarking and Standards to Engineer for Secure Systems

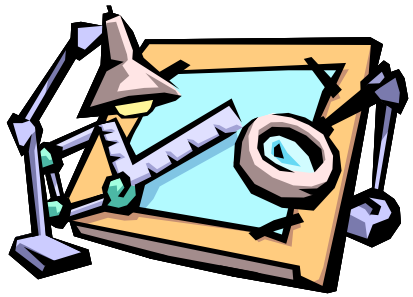
1. Understand Your Legal, Regulatory, and Business Requirements for Assurance



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

3. Look to Standards for Assurance Process Detail

4. Build, or Refine, and Execute Your Assurance Processes



5. Measure Your Results – Assess Risk and Modify Your Processes as Necessary

CMMI ® V1.3 OPF SP 1.1 Includes Examples Of Standards For Addressing Cyber Challenges

Subpractices

1. Identify policies, standards, and business objectives that are applicable to the organization's processes.

Examples of standards include the following:

- ISO/IEC 12207:2008 Systems and Software Engineering – Software Life Cycle Processes [ISO 2008a]
- ISO/IEC 15288:2008 Systems and Software Engineering – System Life Cycle Processes [ISO 2008b]
- ISO/IEC 27001:2005 Information technology – Security techniques – Information Security Management Systems – Requirements [ISO/IEC 2005]
- ISO/IEC 14764:2006 Software Engineering – Software Life Cycle Processes – Maintenance [ISO 2006b]
- ISO/IEC 20000 Information Technology – Service Management [ISO 2005b]
- Assurance Focus for CMMI [DHS 2009]
- NDIA Engineering for System Assurance Guidebook [NDIA 2008]
- Resiliency Management Model [SEI 2010c]

CMMI ® V1.3 OPF SP 1.1 Includes Examples Of Standards For Addressing Cyber Challenges

Subpractices

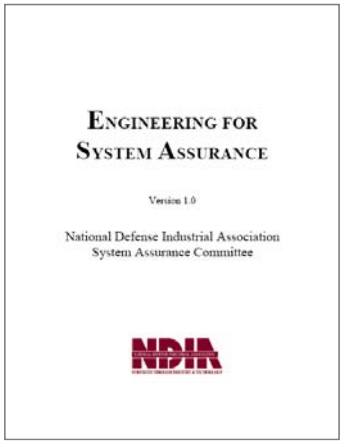
1. Identify policies, standards, and business objectives that are applicable to the organization's processes.

Examples of standards include the following:

- ISO/IEC 12207:2008 Systems and Software Engineering – Software Life Cycle Processes [ISO 2008a]
- ISO/IEC 15288:2008 Systems and Software Engineering – System Life Cycle Processes [ISO 2008b]
- ISO/IEC 27001:2005 Information technology – Security techniques – Information Security Management Systems – Requirements [ISO/IEC 2005]
- ISO/IEC 14764:2006 Software Engineering – Software Life Cycle Processes – Maintenance [ISO 2006b]
- ISO/IEC 20000 Information Technology – Service Management [ISO 2005b]
- Assurance Focus for CMMI [DHS 2009]
- NDIA Engineering for System Assurance Guidebook [NDIA 2008]
- Resiliency Management Model [SEI 2010c]

DoD-Related Guidance For Systems Assurance

- National Defense Industrial Association Guidebook on Engineering for System Assurance (http://www.acq.osd.mil/sse/docs/SA-Guidebook-v1-Oct2008.pdf)
  - 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/IEEE 15288, System Life Cycle Processes
    - DoD Specific Guidance, mapped to DoD Acquisition Life Cycle
      - 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)
  - Adopted as NATO AEP-67, Engineering for System Assurance in NATO Programmes, February 2010



NDIA System Assurance Guidebook – Mapped To ISO/IEC/IEEE 15288, System Life Cycle Processes

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

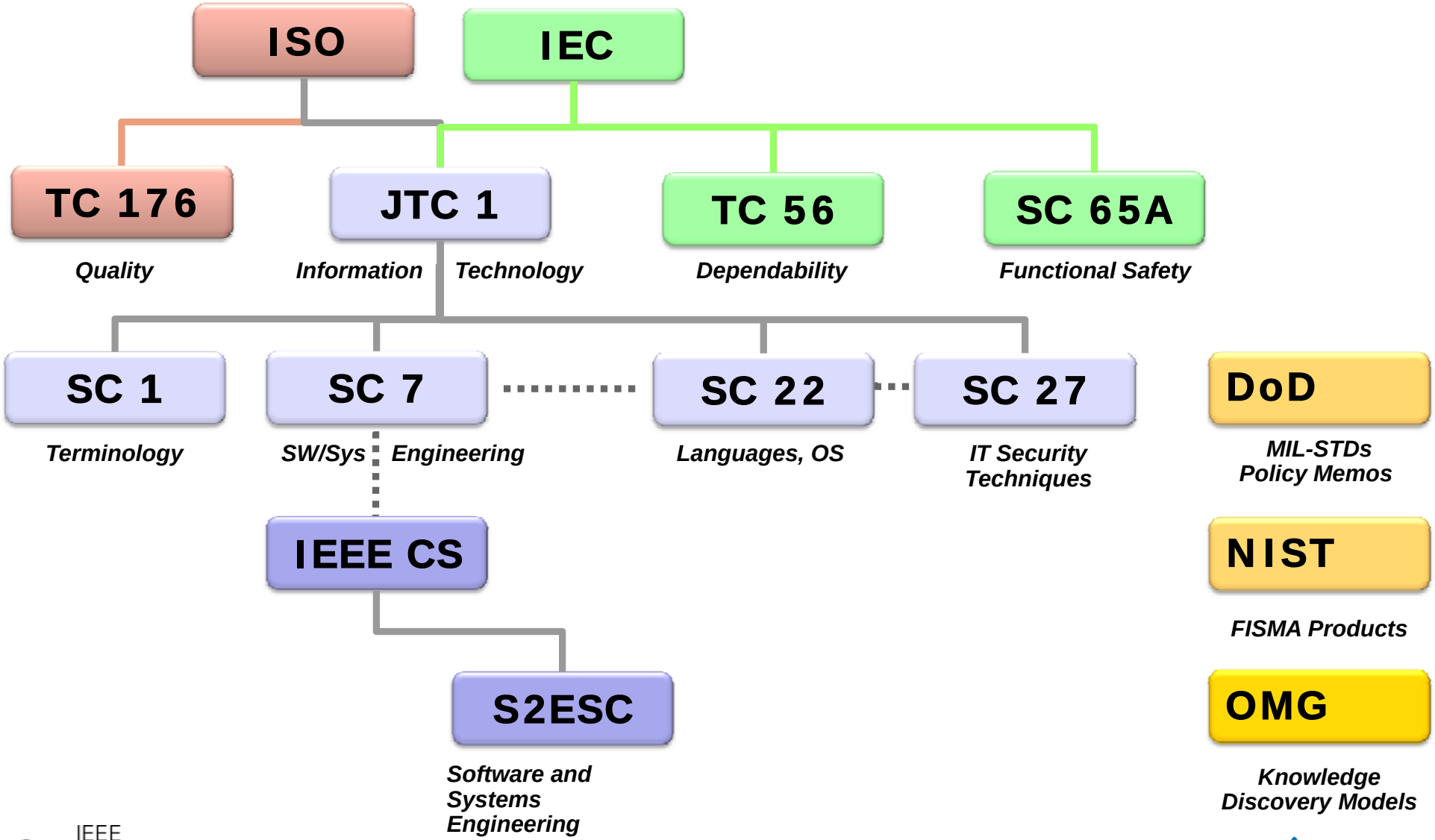
- Technical Processes
  - Stakeholder Requirements Definition
  - Requirements Analysis
  - Architectural Design
  - Implementation
  - Integration
  - Verification
  - Transition
  - Validation
  - Operation
  - Maintenance
  - Disposal

- **Assurance Case Process**

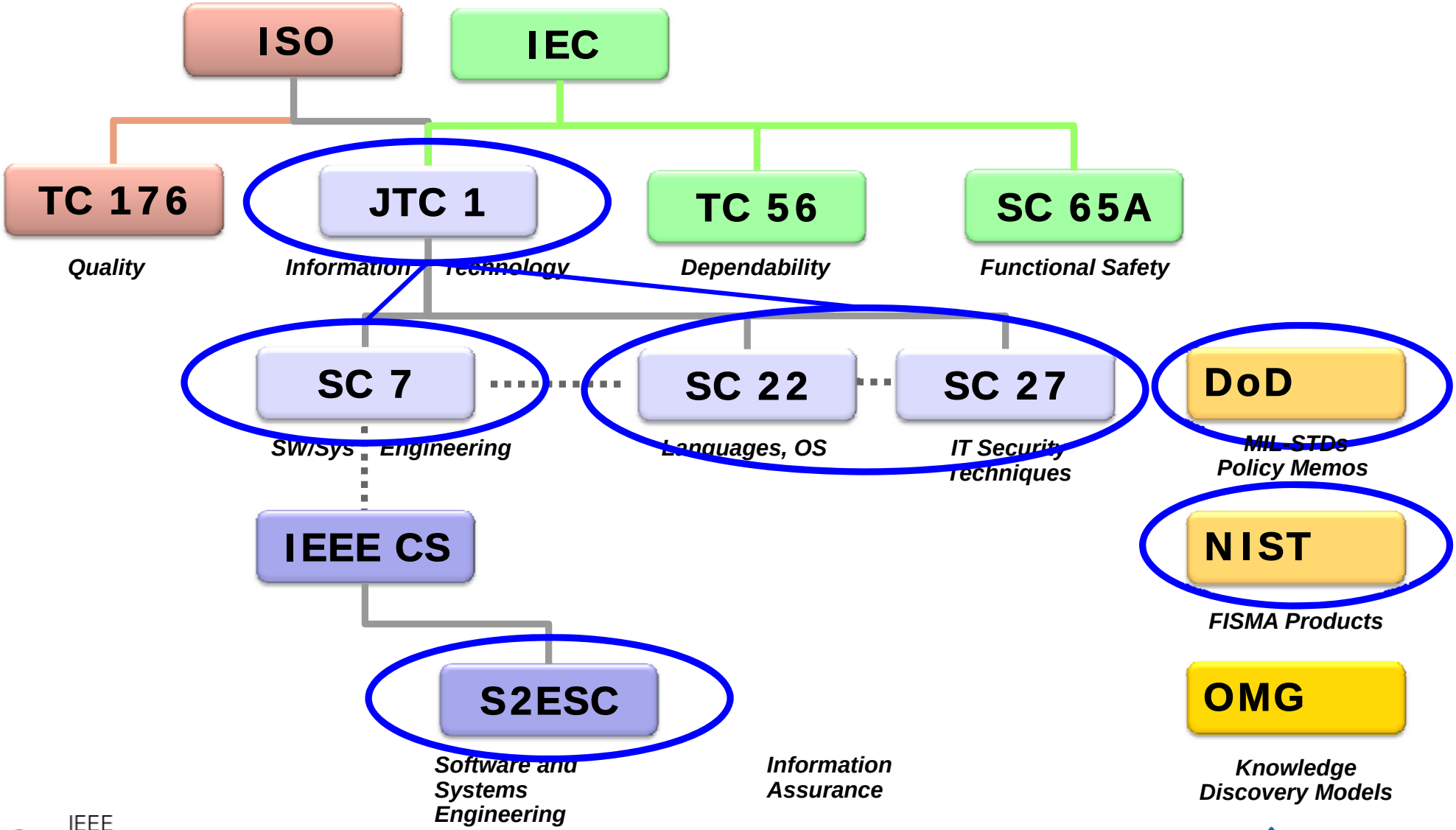
- Enterprise Processes
  - Acquisition
  - Enterprise Environment Management
  - Investment Management
  - System Life Cycle Process Management
  - Resource Management [including human resource training]
  - Quality Management

Standards for Assurance

Standards Organizations Supporting Assurance



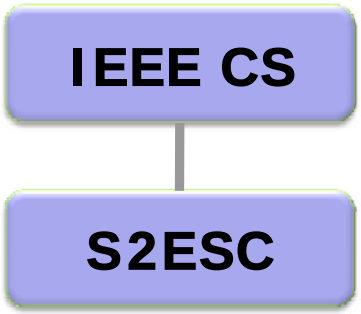
Standards Organizations Supporting Assurance



ISO / IEC JTC1 Standards for Assurance

SC 7	ISO / IEC / IEEE 15026 System and Software Assurance
SC 22	ISO / IEC TR 24772 Programming Language Vulnerabilities
SC 27	ISO / IEC 15408 Common Criteria for IT Security Evaluation
	ISO / IEC 21827 System Security Engineering Capability Maturity Model (SSE CMM)
	ISO / IEC 27000 series Information Security Management Systems (ISMS)
	ISO / IEC WD 27036-3 Supply Chain Risk Management

IEEE Standards for Systems and Software Assurance



ISO / IEC / IEEE 15026
System and Software Assurance

IEEE 730
Software Quality Assurance

IEEE 828
Software Configuration Management

IEEE 1008
IEEE Standard for Software Unit Testing

IEEE Std 1012
System and Software Verification and Validation

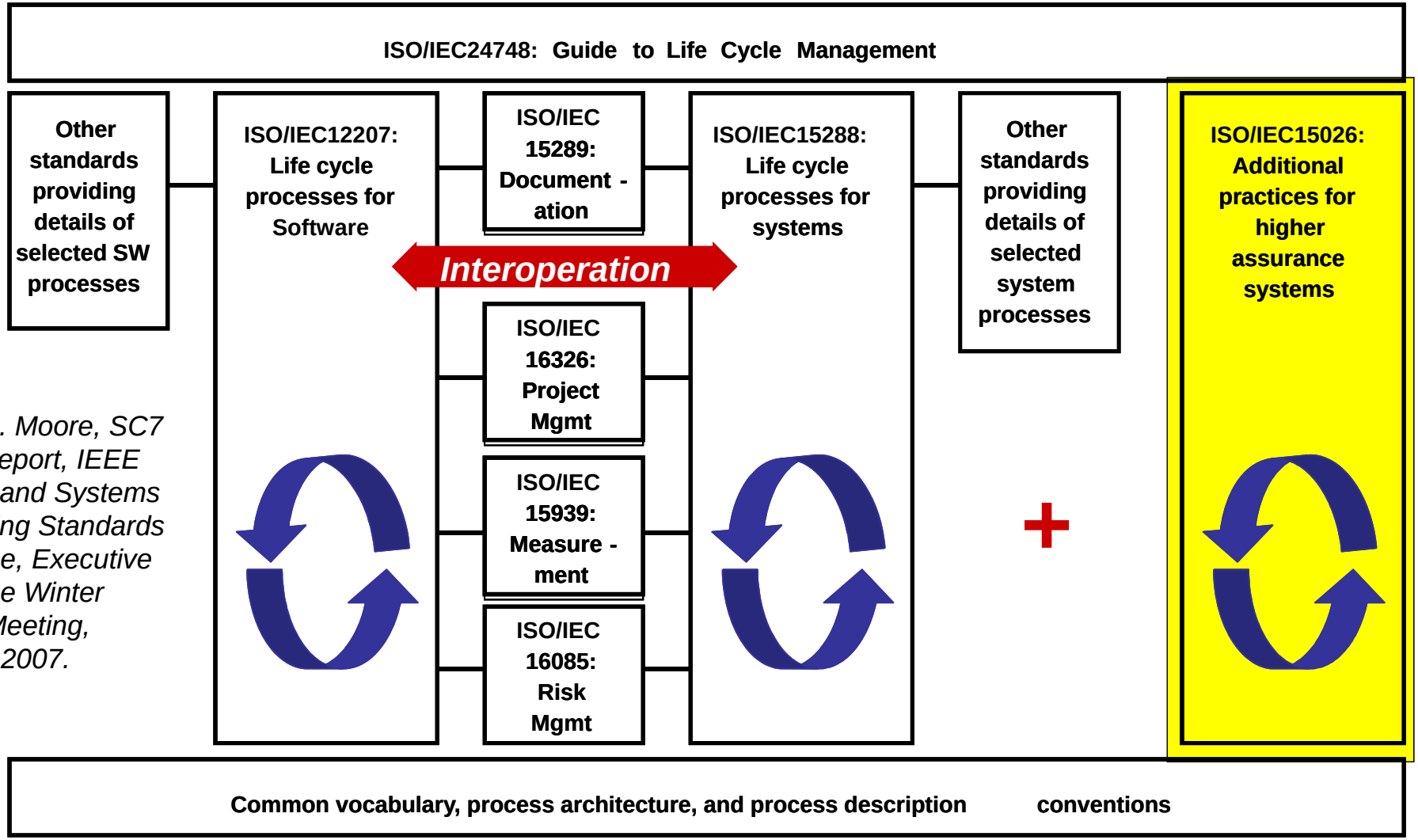
IEEE Std 1016
Software Design Descriptions

ISO / IEC / IEEE 29148
Requirements Engineering

Over 40 standards in the S3ESC Collection
http://www.computer.org/portal/web/s2esc

Assurance in the ISO/IEC JTC1/SC7/IEEE System and Software Life Cycles

SC 7
S2ESC



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

ISO/IEC/IEEE 15026, System and Software Assurance

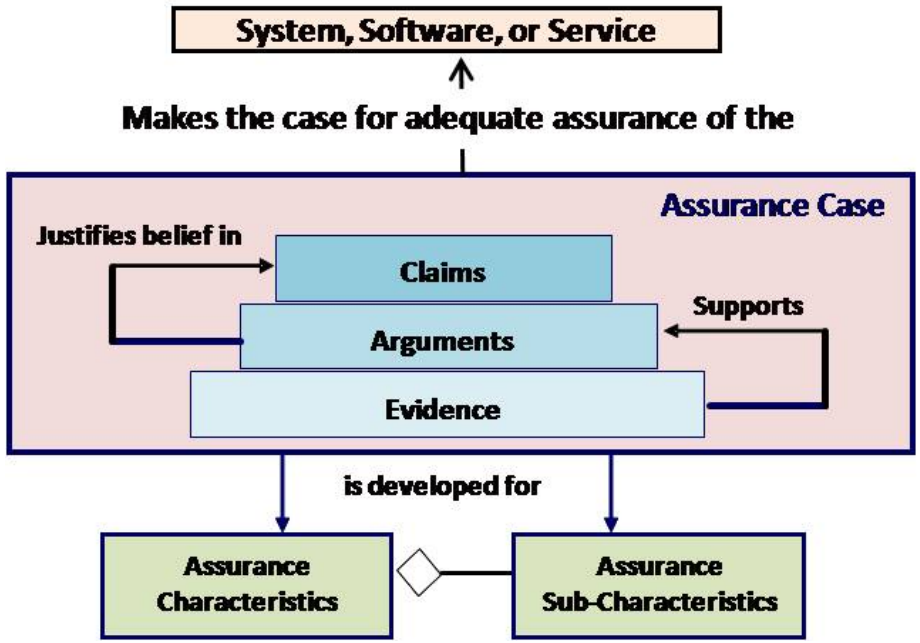
SC 7
S2ESC

- 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
  - 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 requirements and guidance regarding how claims of assurance are treated in life cycle processes.

The ISO/IEC/IEEE 15026 Assurance Case

SC 7
S2ESC

- Set of structured assurance claims, supported by evidence and reasoning, that demonstrates how assurance needs have been satisfied.
  - Shows compliance with assurance objectives



- **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

IEEE computer society

CSC

IEEE

ISO/IEC TR 24772, Programming Language Vulnerabilities

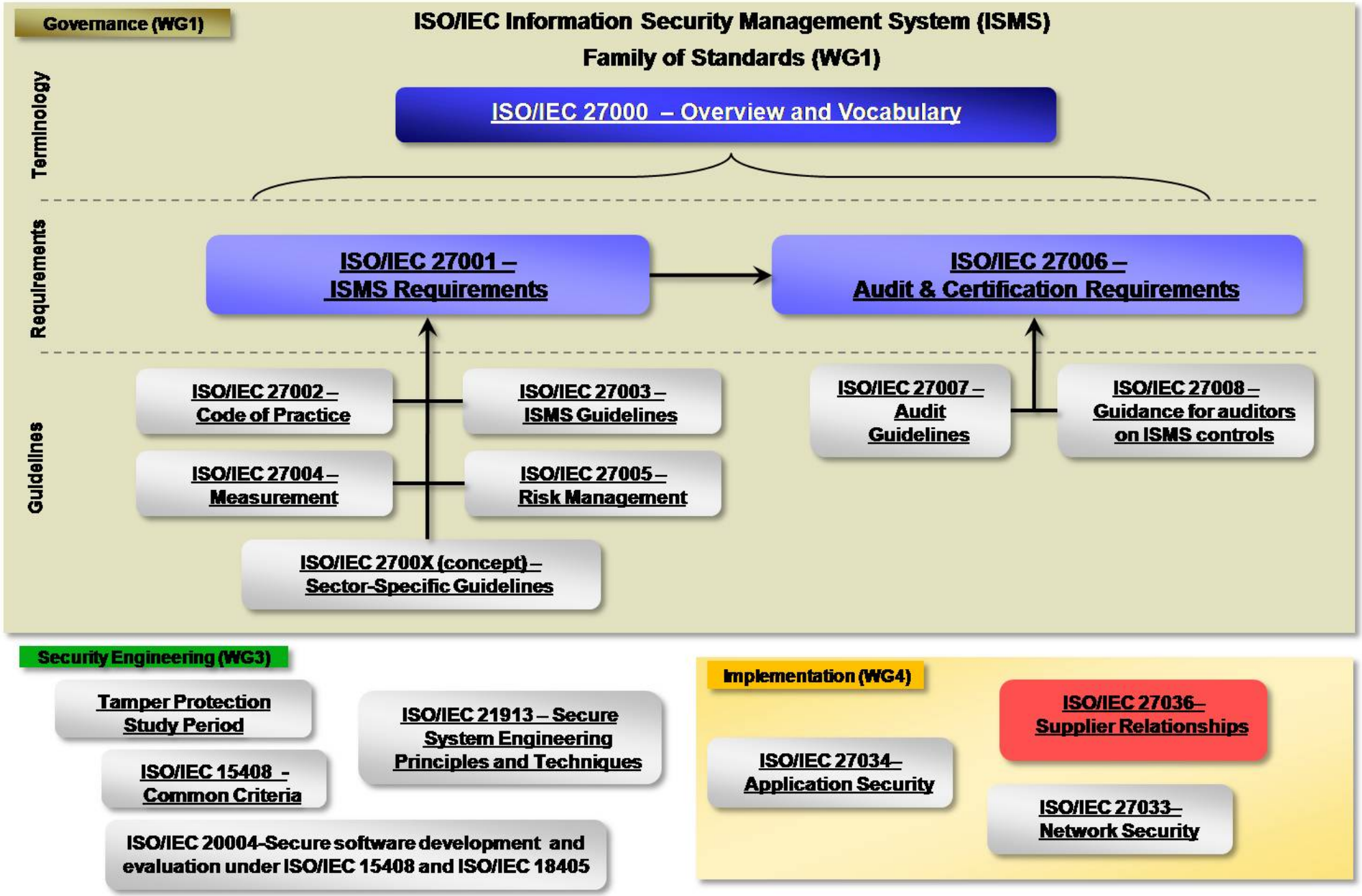
SC 22

- A catalog of 60+ issues that arise in coding when using any language and how those issues may lead to security and safety vulnerabilities
- Cross-referenced to CWE (Common Weakness Enumeration database)
- Each discussion includes
  - Description of the mechanism of failure
  - Recommendations for programmers: How to avoid or mitigate the problem
  - Recommendations for standardizers: How to improve programming language specifications
- Second edition will add annexes specific to particular programming languages

ISO/IEC 27000 Series – Information Security Management Systems

SC 27

- Specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization's overall business risks
- Specifies requirements for the implementation of security controls customized to the needs of individual organizations
- Designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties

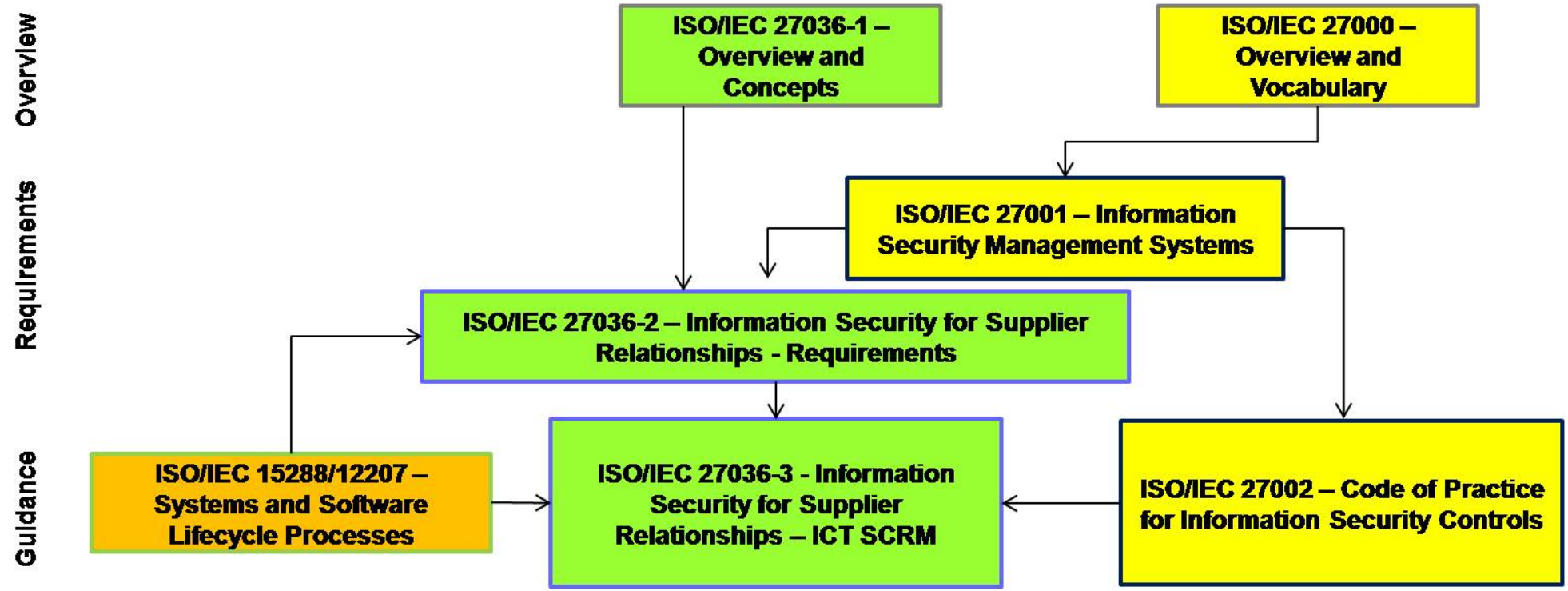

Governance (WG1)
ISO/IEC Information Security Management System (ISMS)
Family of Standards (WG1)
Terminology
ISO/IEC 27000 – Overview and Vocabulary
Requirements
ISO/IEC 27001 – ISMS Requirements
ISO/IEC 27006 – Audit & Certification Requirements
Guidelines
ISO/IEC 27002 – Code of Practice
ISO/IEC 27003 – ISMS Guidelines
ISO/IEC 27004 – Measurement
ISO/IEC 27005 – Risk Management
ISO/IEC 27007 – Audit Guidelines
ISO/IEC 27008 – Guidance for auditors on ISMS controls
ISO/IEC 2700X (concept) – Sector-Specific Guidelines
Security Engineering (WG3)
Tamper Protection Study Period
ISO/IEC 21913 – Secure System Engineering Principles and Techniques
ISO/IEC 15408 - Common Criteria
ISO/IEC 20004-Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405
Implementation (WG4)
ISO/IEC 27036– Supplier Relationships
ISO/IEC 27034– Application Security
ISO/IEC 27033– Network Security

ISO/IEC ISO/IEC 27036 – Information Security for Supplier Relationships

SC 27

- Addresses information security in relationships between acquirers and suppliers and applies to all types of organizations
- Specifies the information security requirements and guidance associated with managing a supplier relationship
  - Identifying and categorizing suppliers; agreeing, monitoring, validating, and changing supplier arrangements; and exiting).
- Covers all types of supplier relationships, including outsourcing, product and service acquisition, and cloud computing including ICT
- Multipart standard
  - Part 1 – Overview and Concepts
  - Part 2 – Common Requirements
  - Part 3 – Guidelines for ICT Supply Chain
  - Part 4 – Guidelines for Outsourcing (currently not being worked)
  - Part 5 – Cloud Computing (scope is being created by Cisco)
  - Part 6 – placeholder for TTF pending further inputs from OTPF
- Relies on collaborative relationships
  - Information security for supplier relationships – Information Security Forum (ISF)
  - Lifecycle processes – SC7 – Software and System Engineering
  - Anti-counterfeiting tools – TC246 – Project committee: Anti-counterfeiting tools
  - Fraud prevention – TC247 – Fraud countermeasures and controls
  - Supply chain – TC8 – Ships and marine technology
  - Resiliency – TC223 – Societal Security

ISO/IEC 27036 Dependencies and Influences



Processes and Techniques

- ISO/IEC 15026 – Software Assurance
- ISO/IEC 27034 – Application Security
- Security Engineering and Design techniques
- NASPO and other Anti -Counterfeiting techniques
- Microsoft Secure Development Lifecycle (SDL)
- SAFECode
- OWASP
- BSIMM

- Common Criteria – ISO/IEC 15408
- OMG KDM BPMN, RIF, XMI, RDF
- OWASP Top 10
- SANS TOP 25
- Secure Content Automation Protocol (SCAP)
- Secure Coding Checklists
- Encryption
- Software Asset Tagging
- Trusted Platform Module (TPM)

ISO/IEC 27036 – Expected Timelines

Timeframe	Expected Outcomes
October 2011-May 2012	• Part 1 – **Committee Draft** • Part 2 unlikely to be ready for Committee Draft • Part 3 likely to be ready but needs to wait for Part 2 and ISO/IEC 27002 to stabilize for mapping and referencing purposes
May 2012-October 2012	• Part 1 **– Final Draft** • Part 2 **– Committee Draft** • Part 3 **– Committee Draft**
October 2012- May 2013	• Part 1 **ready for publication** • Parts 2 and 3 **– Final Draft**
May 2013-October 2013	• Part 1 **published/available** for purchase • Parts 2 and 3 **ready for publication** • **27036 Parts 1-3 available for use**
Other pieces that need to be in place	• Working with other countries to ensure ISO/IEC 27002, ISO controls catalog, provides appropriate "hooks" for 27036 being used in the context of ISO/IEC 27001 certification • Establishing architectural relationship between ISO/IEC 27036 and other standards for future use cases
Ongoing	• Continue collaboration and information sharing with contributing efforts and monitor emerging efforts for applicability

DoD Standards for System and Software Assurance

DoD

- DODD 8500.1, Information Assurance (IA)
- DODI 8500.2, Information Assurance (IA) Implementation
- DODI 8510.01, DOD IA Certification and Accreditation Process (DIACAP)
- DODD 8570.01 IA Training, Certification, and Workforce Management
- DISA Security Technical Implementation Guides (STIGS)

Federal Information Security Management Act (FISMA) Implementation

NIST

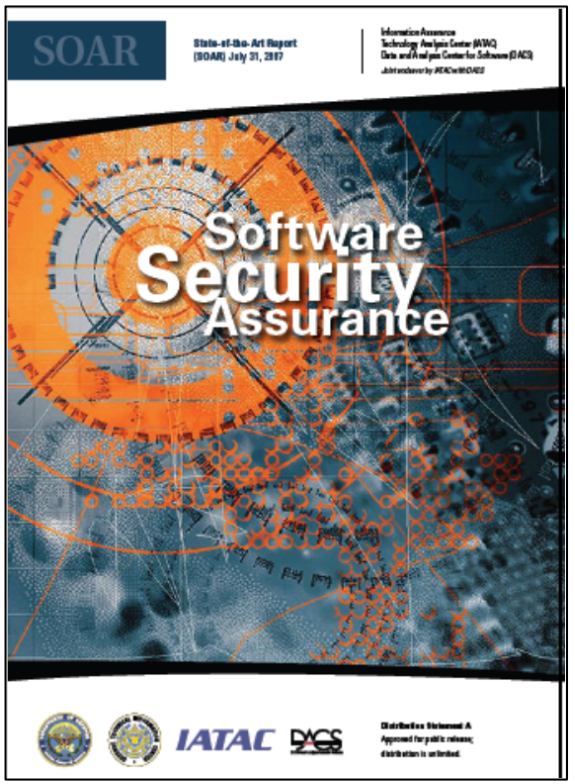
- **FIPS Publication 199**, Standards for Security Categorization of Federal Information and Information System
- **FIPS Publication 200**, Minimum Security Requirements for Federal Information and Federal Information Systems
- **NIST Special Publication 800-18 Revision 1**, Guide for Developing Security Plans for Federal Information Systems and Organizations
- **NIST Special Publication 800-30, Revision 1**, Risk Management Guide for Information Technology Systems
- **NIST Special Publication 800-37, Revision 1**, Guide for Applying the Risk Management Framework to Federal Information Systems
- **NIST Special Publication 800-39**, Enterprise-wide Risk Management
- **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

Source: http://csrc.nist.gov/groups/SMA/fisma/overview.html

Additional Guidance for 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, including trends in:
  - Techniques for the production of secure software
  - Technologies that exist or are emerging to address the software security challenge
  - Current activities and organizations in government, industry, and academia, in the U.S. and abroad, that are devoted to systematic improvement of software security
  - Research trends worldwide that might improve the state of the art for software security
- Free via http://iac.dtic.mil/iatac/download/security.pdf



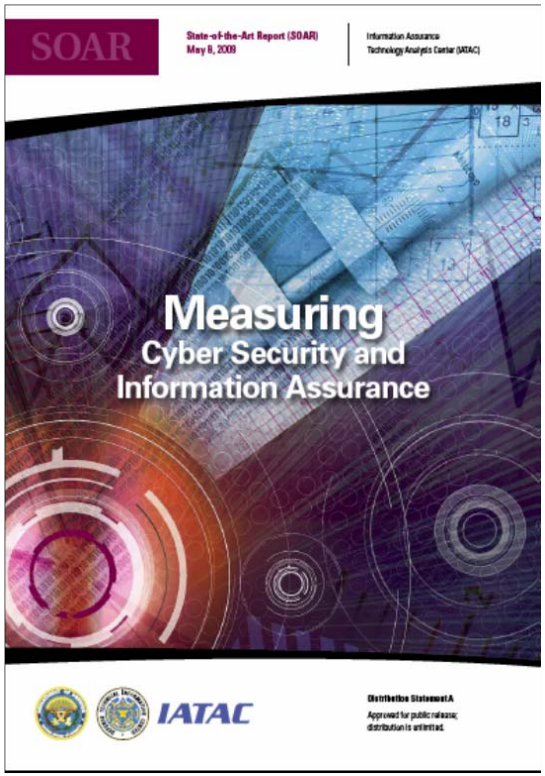
Enhancing the Development Life Cycle to Produce Secure Software

- Describes how to integrate security principles and practices in software development life cycle
- Addresses security requirements, secure design principles, secure coding, risk-based software security testing, and secure sustainment
- Provides guidance for selecting secure development methodologies, practices, and technologies

Free via
https://www.thedacs.com/techs/enhanced_life_cycles/

Measuring Cyber Security and Information Assurance

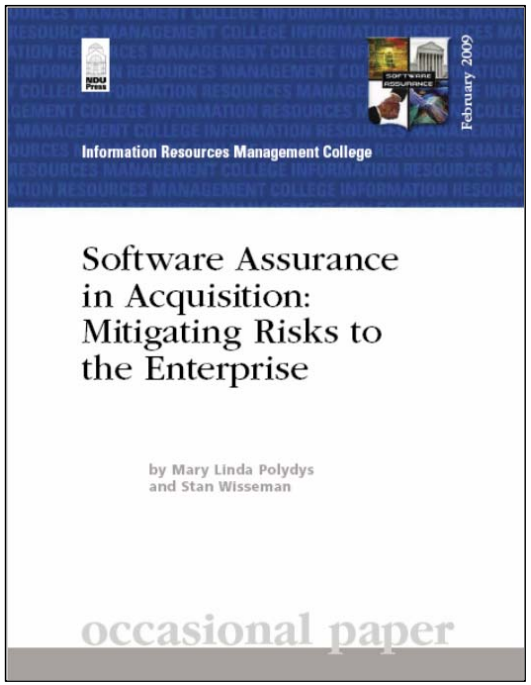
- Provides a broad picture of the current state of cyber security and information assurance (CS/IA), as well as, a comprehensive look at the progress made in the CS/IA measurement discipline over the last nine years since IATAC published its IA Metrics Critical Review and Technology Assessment (CR/TA) Report in 2000



Available free via
http://iac.dtic.mil/iatac/download/cybersecurity.pdf

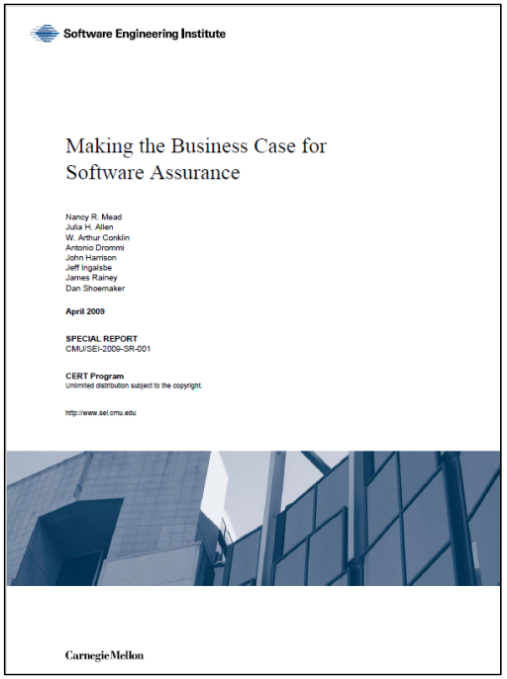
Software Assurance in Acquisition: Mitigating Risks to the Enterprise

- Provides information on how to incorporate Software Assurance considerations in key decisions
  - How to exercise due diligence throughout the acquisition process relative to potential risk exposures that could be introduced by the supply chain
  - Includes practices that enhance SwA in the purchasing process
    - Due diligence questionnaires designed to support risk mitigation efforts by eliciting information about the software supply chain (these are also provided in Word format so they can be customized)
    - Sample contract provisions
    - Sample language to include in statements of work
- Pre-publication version available free via https://buildsecurityin.us-cert.gov/swa/downloads/SwA_in_Acquisition_102208.pdf
- Final version published by National Defense University Press, Feb 2009



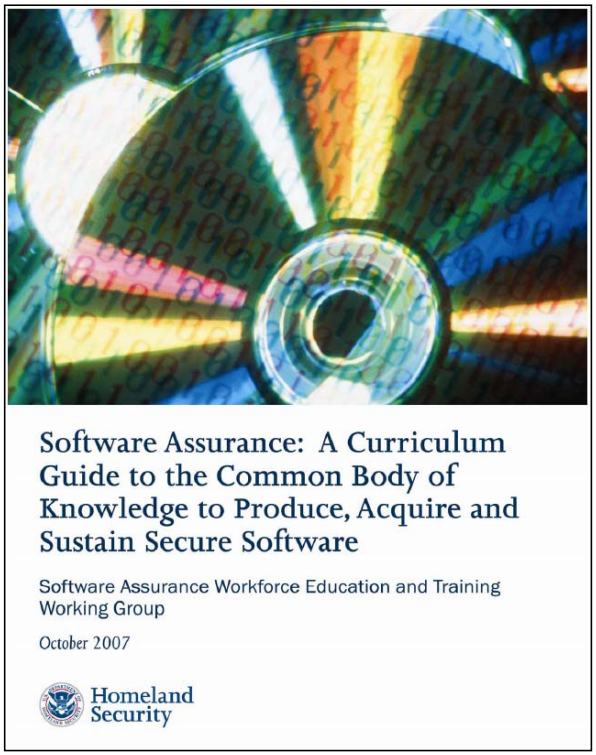
Making the Business Case for Software Assurance

- Provides background, context and examples for making the business case for software assurance:
  - Motivators
  - Cost/Benefit Models Overview
  - Measurement
  - Risk
  - Prioritization
  - Process Improvement & Secure Software
  - Globalization
  - Organizational Development
  - Case Studies and Examples
- Available free via http://www.sei.cmu.edu/library/abstracts/reports/09sr001.cfm

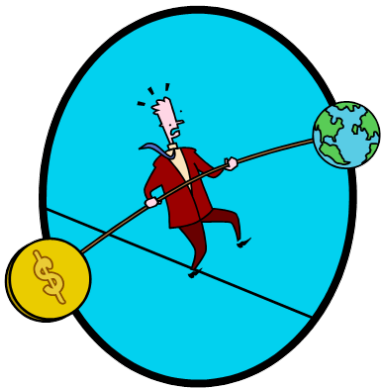


Software Assurance: A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software

- Provides a framework intended to identify workforce needs for competencies, leverage sound practices, and guide curriculum development for education and training relevant to software assurance
- Available via https://buildsecurityin.us-cert.gov/bsi/940-BSI/version/default/part/AttachmentData/data/CurriculumGuideToTheCBK.pdf

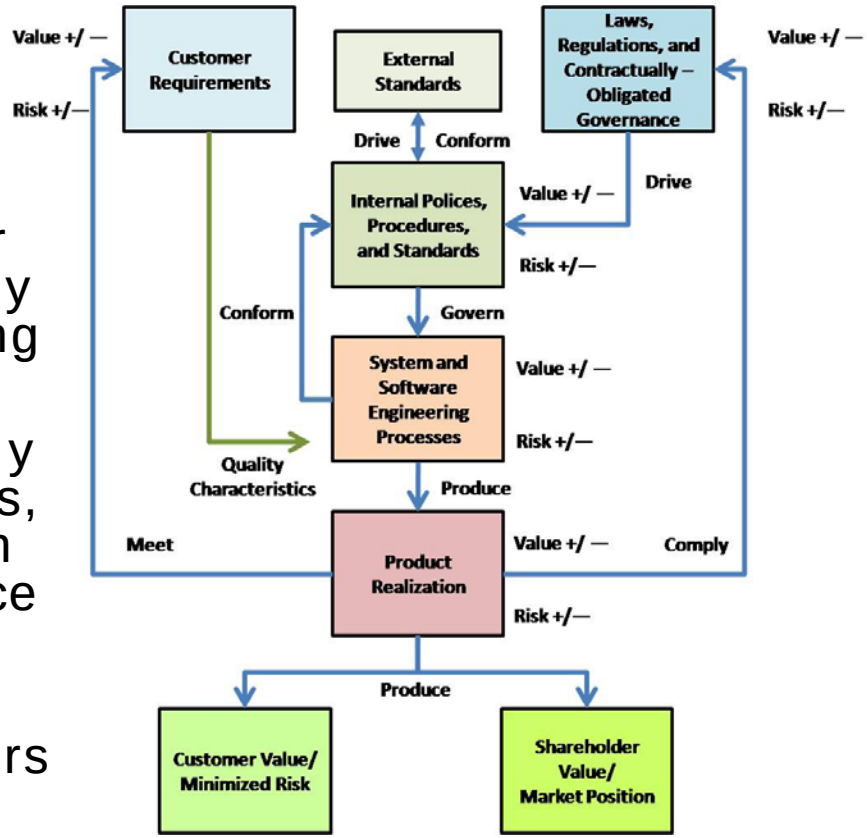


Rationalizing Governance, Engineering Practice, and Engineering Economics



Key Questions in Rationalizing Governance, Engineering Practice, and Engineering Economics

- How does compliance with a particular external governance requirement impact organizational risk and value delivery?
- Where multiple external compliance requirements exist, have I examined their overlaps and chosen a compliance strategy that optimizes compliance while minimizing risk and maximizing value?
- Have I added value and reduced risk to my engineering processes through the policies, procedures, and standards I've adopted in compliance with those external governance requirements?
- Does my product provide value in the market place while limiting risk to acquirers and users?



For More Information . . .

Paul R. Croll
Fellow
CSC
10721 Combs Drive
King George, VA 22485-5824

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