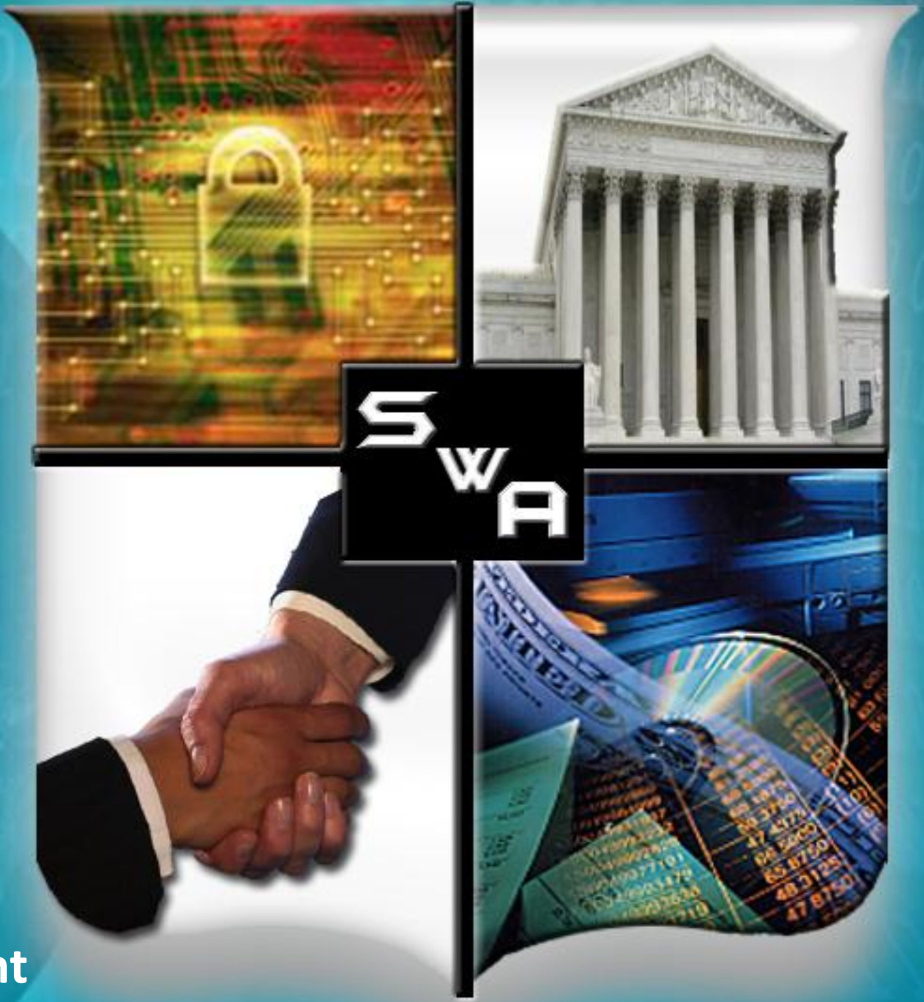
SOFTWARE ASSURANCE FORUM

Homeland Security

Commerce

National Defense

BUILDING SECURITY IN



Public/Private Collaboration Efforts for Software Supply Chain Risk Management

Next SwA Working Group Sessions 14-16 Dec 2010 at MITRE, McLean, VA

Layered
Assurance
Workshop

BUILDING SECURITY IN
SOFTWARE ASSURANCE

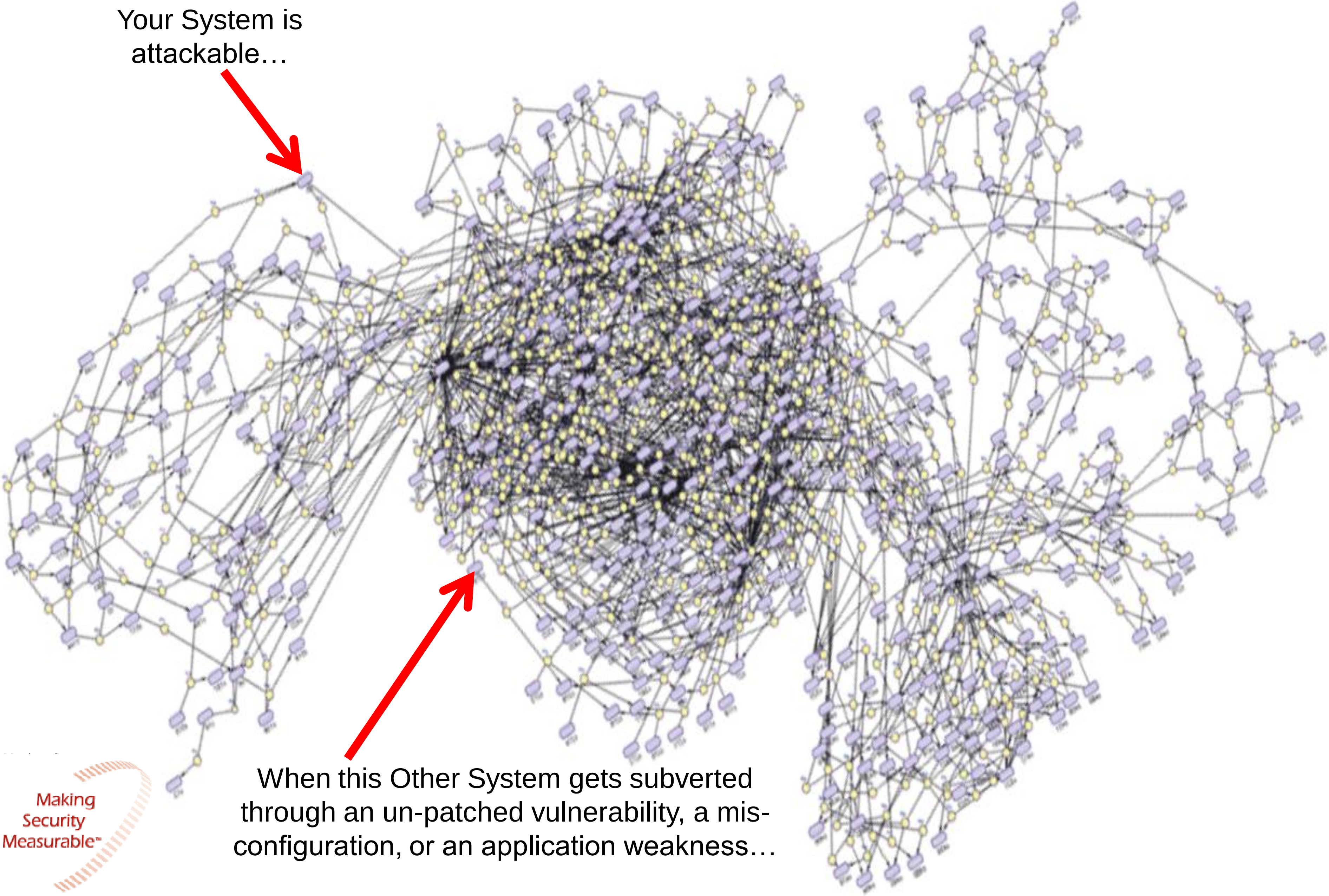
Software Assurance:
Enabling Software Resilience and Mitigating Supply Chain Risk

Dec 6, 2010

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

Homeland
Security

Today Everything's Connected



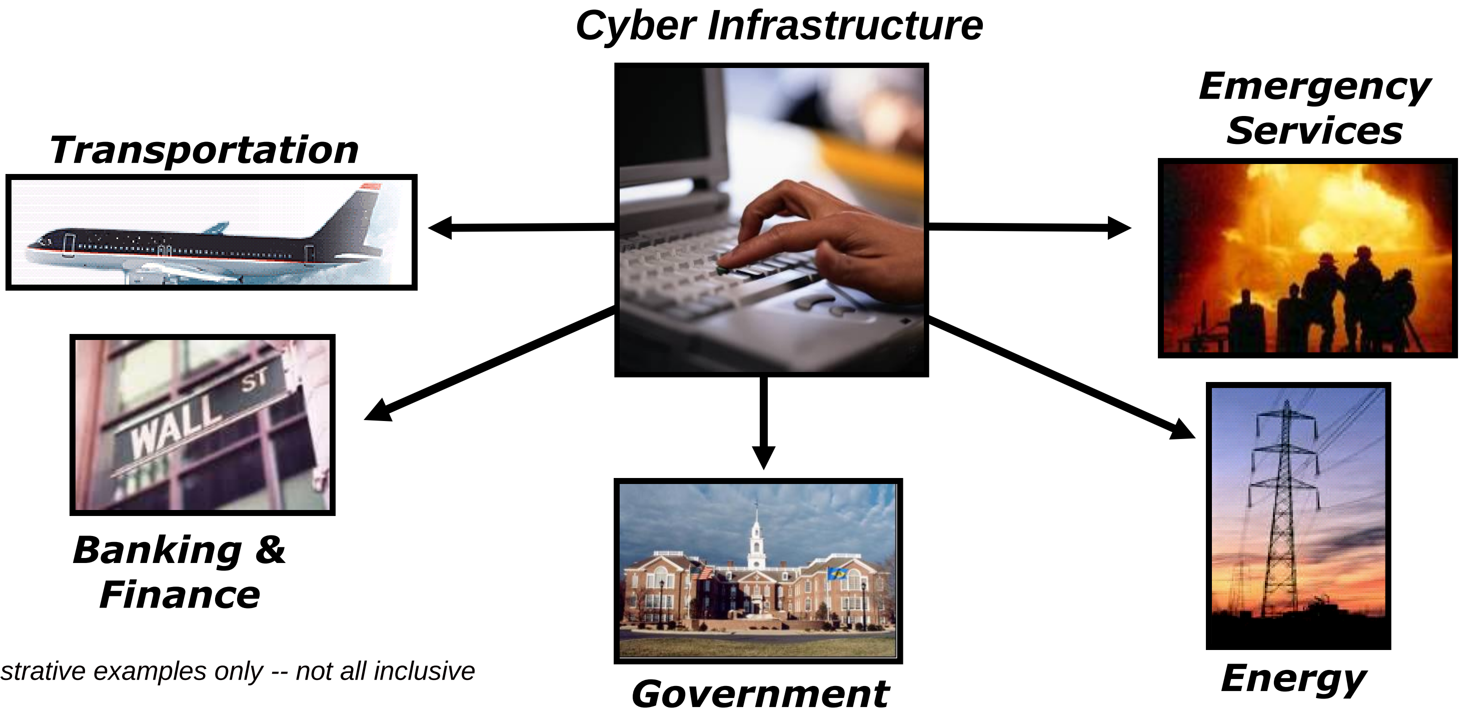
Your System is attackable…

When this Other System gets subverted through an un-patched vulnerability, a mis-configuration, or an application weakness…

Making Security Measurable™

Cyber Infrastructure:
Critical to National and Economic Security

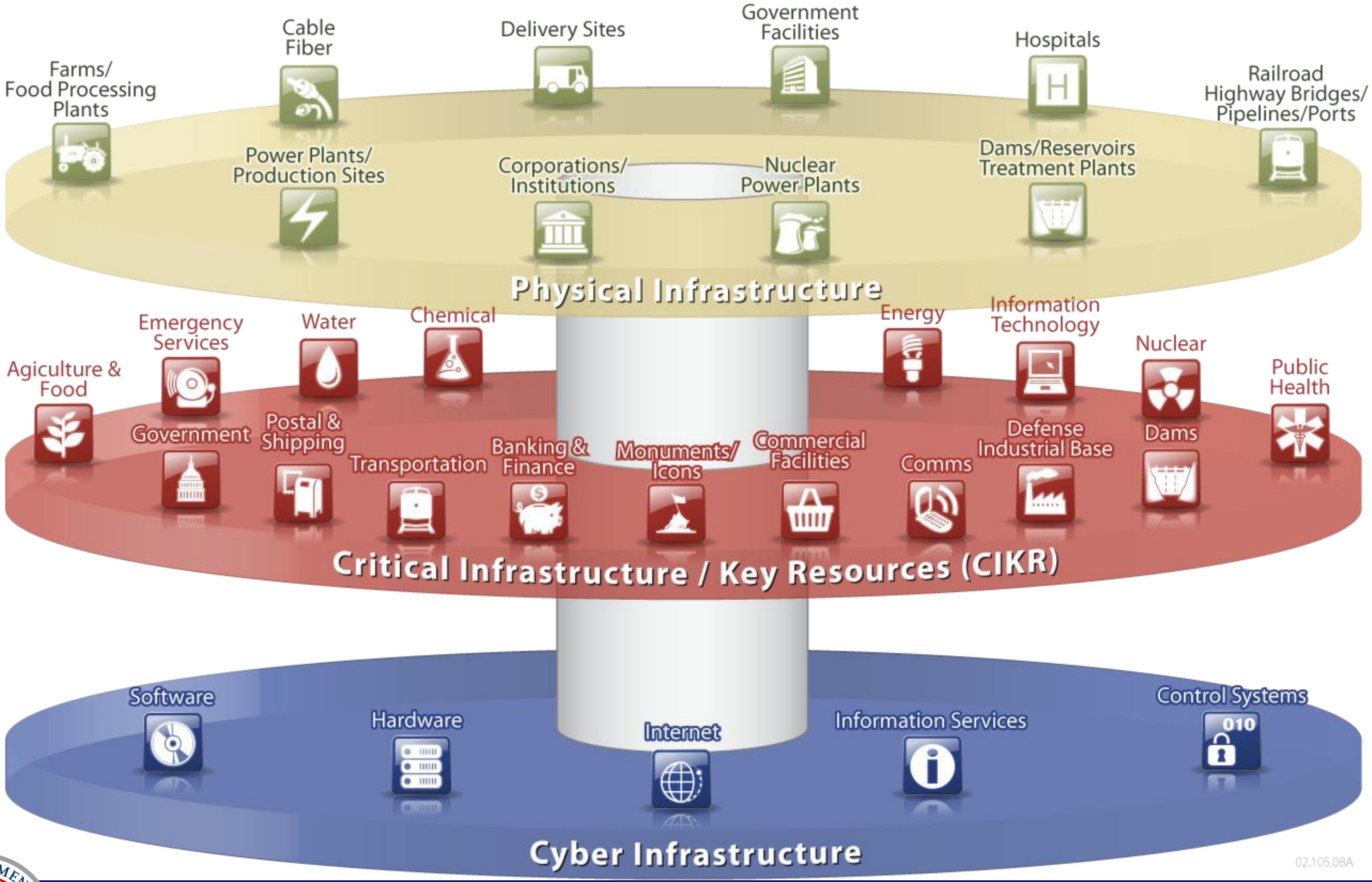
Cyber Infrastructure represents the convergence of information technology and communications systems, is inherent to nearly every aspect of modern life



Illustrative examples only -- not all inclusive

Interdependencies Between Physical & Cyber Infrastructures: Requires Convergence of Safety, Security and Dependability

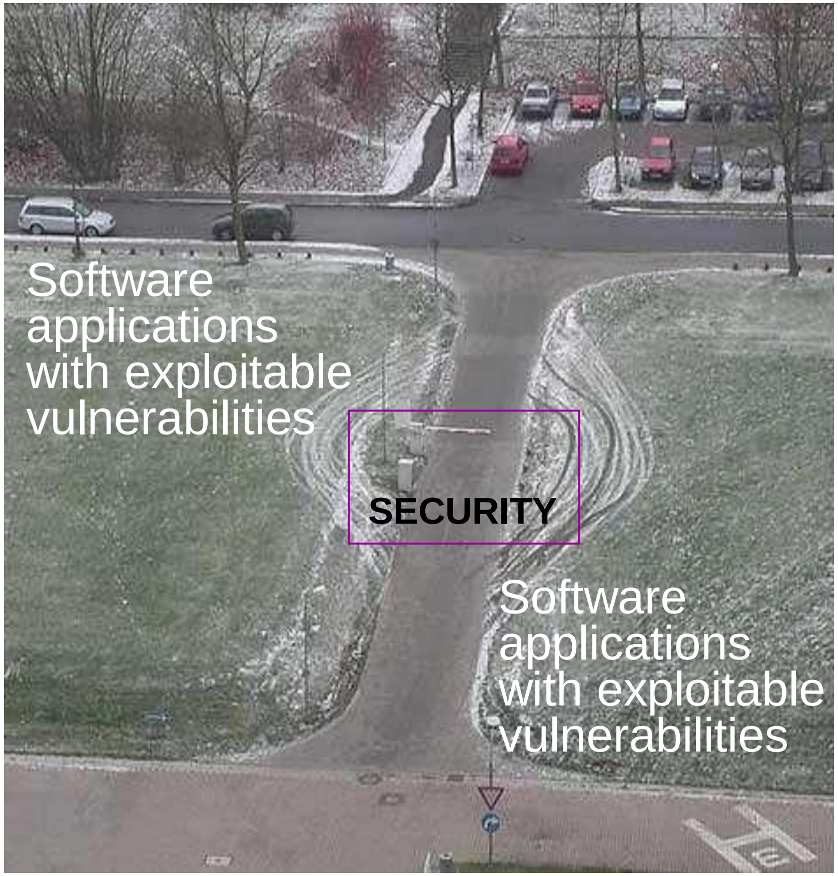
-- Need for secure software applications



Homeland Security

Security is a Requisite Quality Attribute: Vulnerable Software Enables Exploitation

- Rather than attempt to break or defeat network or system security, hackers are opting to target application software to circumvent security controls.
  - ❑ **75% of hacks occurred at application level**
    - – "90% of software attacks were aimed at application layer" (Gartner & Symantec, June 2006)
  - ❑ most exploitable software vulnerabilities are attributable to non-secure coding practices (and not identified in testing).
- Functional correctness must be exhibited even when software is subjected to abnormal and hostile conditions


Software applications with exploitable vulnerabilities
SECURITY
Software applications with exploitable vulnerabilities

In an era riddled with asymmetric cyber attacks, claims about system reliability, integrity & safety must include provisions for built-in security of the enabling software.

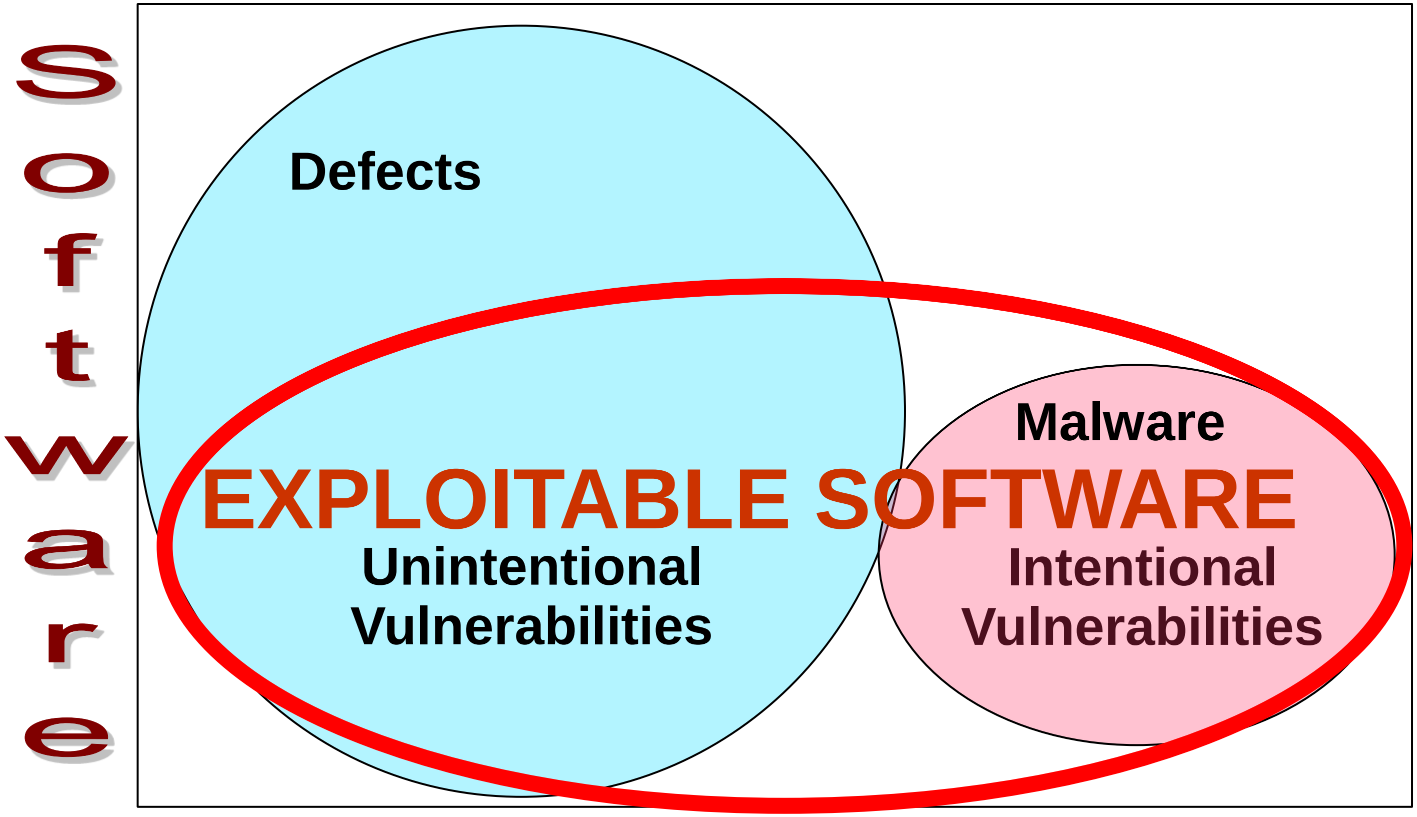
Critical Considerations

- Software is the core constituent of modern products and services – it enables functionality and business operations
- Dramatic increase in mission risk due to increasing:
  - Software dependence and system interdependence (weakest link syndrome)
  - Software Size & Complexity (obscures intent and precludes exhaustive test)
  - Outsourcing and use of un-vetted software supply chain (COTS & custom)
  - Attack sophistication (easing exploitation)
  - Reuse (unintended consequences increasing number of vulnerable targets)
  - Number of vulnerabilities & incidents with threats targeting software
  - Risk of Asymmetric Attack and Threats
- Increasing awareness and concern

Software and the processes for acquiring and developing software represent a material weakness

Software Assurance Addresses Exploitable Software:
Outcomes of non-secure practices and/or malicious intent

Exploitation potential of vulnerability is independent of "intent"



'High quality' can reduce security flaws attributable to defects; yet traditional S/W quality assurance does not address intentional malicious behavior in software

*Intentional vulnerabilities: spyware & malicious logic deliberately imbedded (might not be considered defects)

Homeland Security

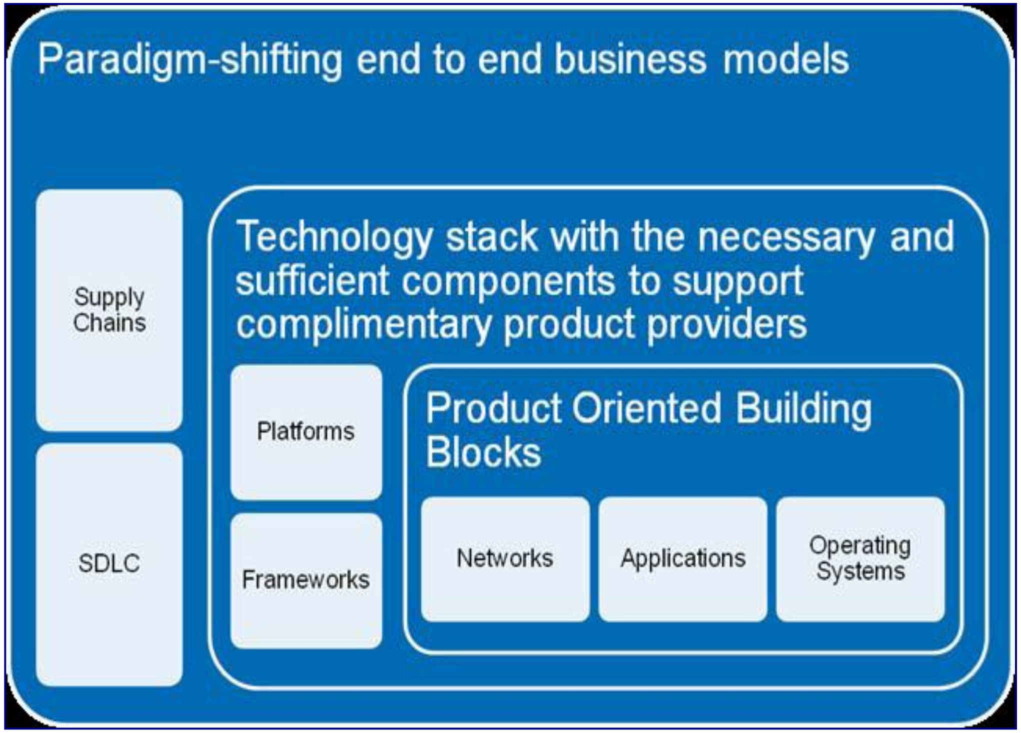
Note: Chart is not to scale – notional representation -- for discussions

IT/software security risk landscape is a convergence between “defense in depth” and “defense in breadth”

Enterprise Risk Management and Governance are security motivators

Acquisition could be considered the beginning of the lifecycle; more than development

> “In the digital age, sovereignty is demarcated not by territorial frontiers but by supply chains.”
>
> – Dan Geer, CISO In-Q-Tel



Paradigm-shifting end to end business models

Supply Chains

SDLC

Technology stack with the necessary and sufficient components to support complimentary product providers

Platforms

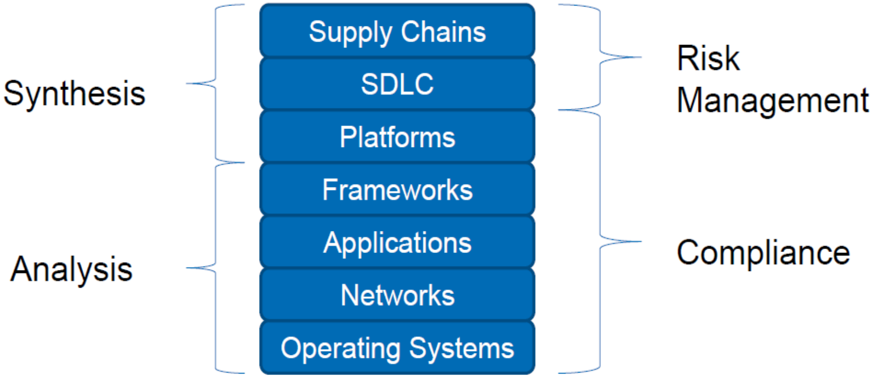
Frameworks

Product Oriented Building Blocks

Networks

Applications

Operating Systems



Synthesis

Analysis

Supply Chains

SDLC

Platforms

Frameworks

Applications

Networks

Operating Systems

Risk Management

Compliance

Software Assurance provides a focus for:

-- Secure Software Components,

-- Security in the Software Life Cycle,

-- Software Security in Services, and

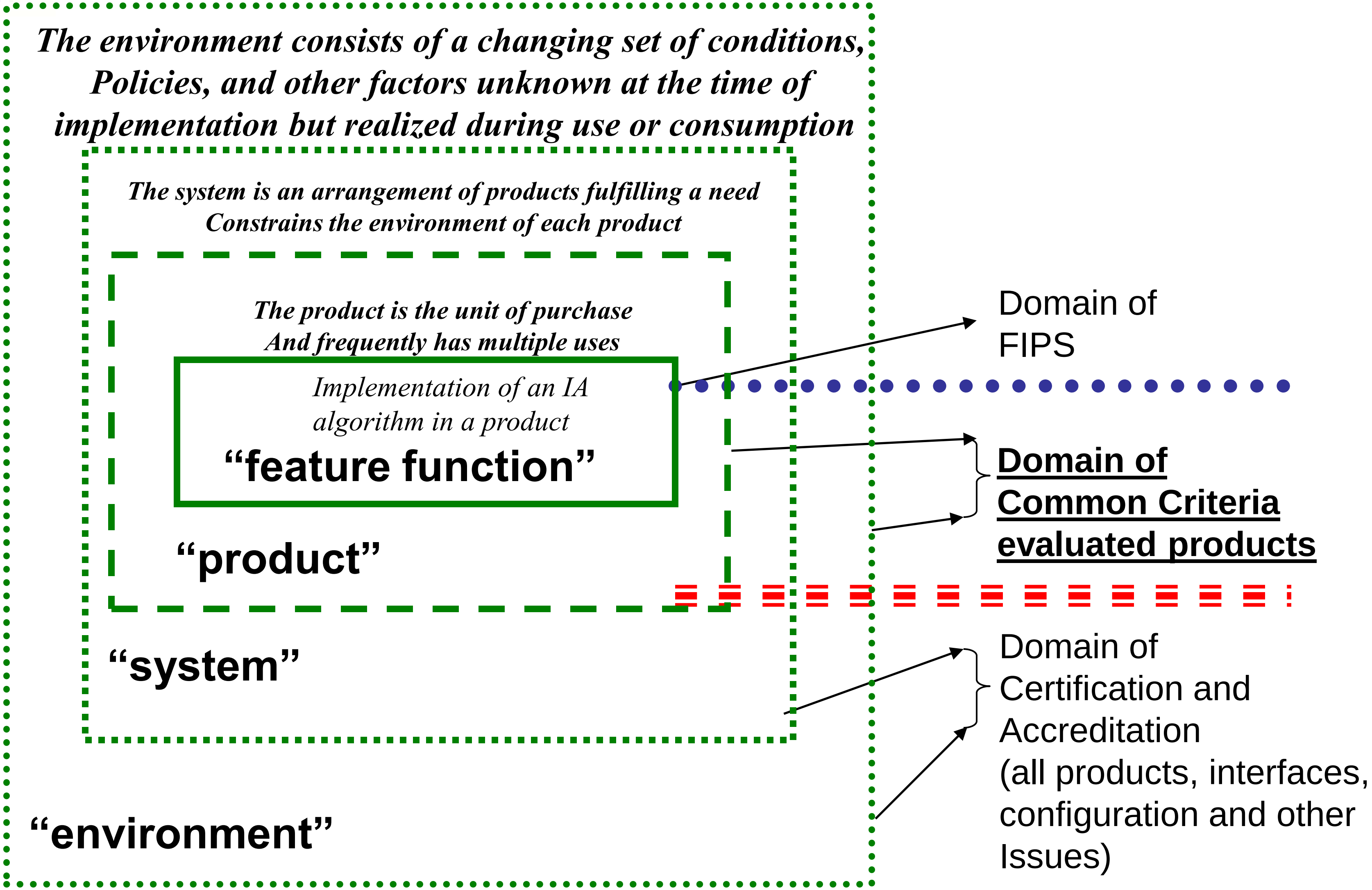
-- Software Supply Chain Risk Management

Security-Enhanced Capabilities:
Mitigating Risks to the Enterprise

- With today’s global software supply chain, Software 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.
- 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 (including procurement, SwEng, QA, & testing).
  - IT/Software Assurance processes/practices span development/acquisition.
  - Derived (non-explicit) security requirements should be elicited/considered.
- More comprehensive diagnostic capabilities and standards 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)

Context for Enterprise IT Security and Layered Assurance



The environment consists of a changing set of conditions, Policies, and other factors unknown at the time of implementation but realized during use or consumption

The system is an arrangement of products fulfilling a need Constrains the environment of each product

The product is the unit of purchase And frequently has multiple uses

Implementation of an IA algorithm in a product

“feature function”

“product”

“system”

“environment”

Domain of FIPS

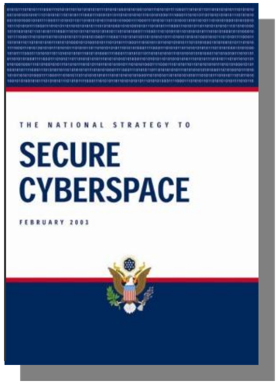
<u>Domain of Common Criteria evaluated products</u>

Domain of Certification and Accreditation (all products, interfaces, configuration and other Issues)

Assurance Challenges in Mitigating Software Supply Chain Risks

- Complexity hampers our ability to determine and predict code behavior; so any "assurance" claims for security/safety-critical applications are limited.
- Without adequate diagnostic capabilities and commonly recognized standards from which to benchmark process capabilities and assert claims about the assurance of products, systems and services, the "providence and pedigree of supply chain actors" become a more dominant consideration for security/safety-critical applications:
  - Enterprises and Consumers lack requisite transparency for more informed decision-making for mitigating risks;
  - Favoring domestic suppliers does not necessarily address 'assurance' in terms of capabilities to deliver secure/safe components, systems or software-reliant services.
- Several needs arise:
  - Need internationally recognized standards to support processes and provide transparency for more informed decision-making for mitigating enterprise risks.
  - Need 'Assurance' to be explicitly addressed in standards & capability benchmarking models for organizations involved with security/safety-critical applications.
  - Need more comprehensive diagnostic capabilities to provide sufficient evidence that "code behavior" can be well understood to not possess exploitable or malicious constructs.
  - Need rating schemes for software products and supplier capabilities

DHS Software Assurance Program Overview



- Program established in response to the National Strategy to Secure Cyberspace - Action/Recommendation 2-14:

  > *"DHS will facilitate a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software code development, including processes and procedures that diminish the possibilities of erroneous code, malicious code, or trap doors that could be introduced during development."*

- DHS Program goals promote the **security and resilience** of software across the development, acquisition, and operational life cycle

- DHS Software Assurance (SwA) program is scoped to address:
  - **Trustworthiness** - No exploitable vulnerabilities or malicious logic exist in the software, either intentionally or unintentionally inserted,
  - **Dependability (Correct and Predictable Execution)** - Justifiable confidence that software, when executed, functions as intended,
  - **Survivability** - If compromised, damage to the software will be minimized; it will recover quickly to an acceptable level of operating capacity; it's 'rugged';
  - **Conformance** – Planned, systematic set of multi-disciplinary activities that ensure processes/products conform to requirements, standards/procedures.

Homeland Security

See Wikipedia.org for "Software Assurance" - CNSS Instruction No. 4009, "National Information Assurance Glossary," Revised 2006, defines Software Assurance as: "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".

DHS NCSD Software Assurance (SwA) Program

Through public-private collaboration promotes security and resilience of software throughout the lifecycle; focused on reducing exploitable software weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient software products. Collaboratively advancing software-relevant rating schemes

- **Serves as a focal point for interagency public-private collaboration to enhance development and acquisition processes and capability benchmarking to address software security needs.**
  - Hosts interagency Software Assurance Forums, Working Groups and training to provide public-private collaboration in advancing software security and providing publicly available resources.
  - Provides collaboratively developed, peer-reviewed information resources on Software Assurance, via journals, guides & on-line resources suitable for use in education, training, and process improvement.
  - Provides input and criteria for leveraging international standards and maturity models used for process improvement and capability benchmarking of software suppliers and acquisition organizations.

- **Enables software security automation and measurement capabilities through use of common indexing and reporting capabilities for malware, exploitable software weaknesses, and common attacks which target software.**
  - Collaborates with the National Institute of Standards and Technology, international standards organizations, and tool vendors to create standards, metrics and certification mechanisms from which tools can be qualified for software security verification.
  - Manages programs for Malware Attribute Enumeration Classification (MAEC), Common Weakness Enumeration (CWE), and Common Attack Pattern Enumeration and Classification (CAPEC).
  - Manages programs for Common Vulnerabilities & Exposures (CVE) and Open Vulnerability & Assessment Language (OVAL) that provide information feeds for Security Content Automation Protocol (SCAP), vulnerability databases, and security/threat alerts from many organizations

Software Assurance “End State” Objectives…

- **Government, in collaboration with industry / academia, raised expectations for product assurance with requisite levels of integrity and security:**
  - Helped advance more comprehensive software assurance diagnostic capabilities to mitigate risks stemming from exploitable vulnerabilities and weaknesses;
  - Collaboratively advanced use of software security measurement & benchmarking schemes
  - Promoted use of methodologies and tools that enabled security to be part of normal business.
- **Acquisition managers & users factored risks posed by the software supply chain as part of the trade-space in risk mitigation efforts:**
  - Information on suppliers’ process capabilities (business practices) would be used to determine security risks posed by the suppliers’ products and services to the acquisition project and to the operations enabled by the software.
  - Information about evaluated products would be available, along with responsive provisions for discovering exploitable vulnerabilities, and products would be securely configured in use.
- **Suppliers delivered quality products with requisite integrity and made assurance claims about the IT/software safety, security and dependability:**
  - Relevant standards would be used from which to base business practices & make claims;
  - Qualified tools used in software lifecycle enabled developers/testers to mitigate security risks;
  - Standards and qualified tools would be used to certify software by independent third parties;
  - IT/software workforce had requisite knowledge/skills for developing secure, quality products.

…Enabling Software Supply Chain Transparency

Software Assurance Forum & Working Groups*

BUILDING SECURITY IN
SOFTWARE ASSURANCE

… 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

SwA Common Body of Knowledge (CBK) & Glossary
Organization of SwSys Security Principles/Guidelines
SwA Developers' Guide on Security-Enhancing SDLC

Software Security Assurance State of the Art Report

Systems Assurance Guide (via DoD and NDIA)

SwA-related standards – ISO/IEC JTC1 SC7/27/22, IEEE CS, OMG, TOG, & CMM-based Assurance

Practical Measurement Framework for SwA/InfoSec
Making the Business Case for Software Assurance

SwA Metrics & Tool Evaluation (with NIST)
SwA Ecosystem w/ DoD, NSA, NIST, OMG & TOG
NIST Special Pub 500 Series on SwA Tools

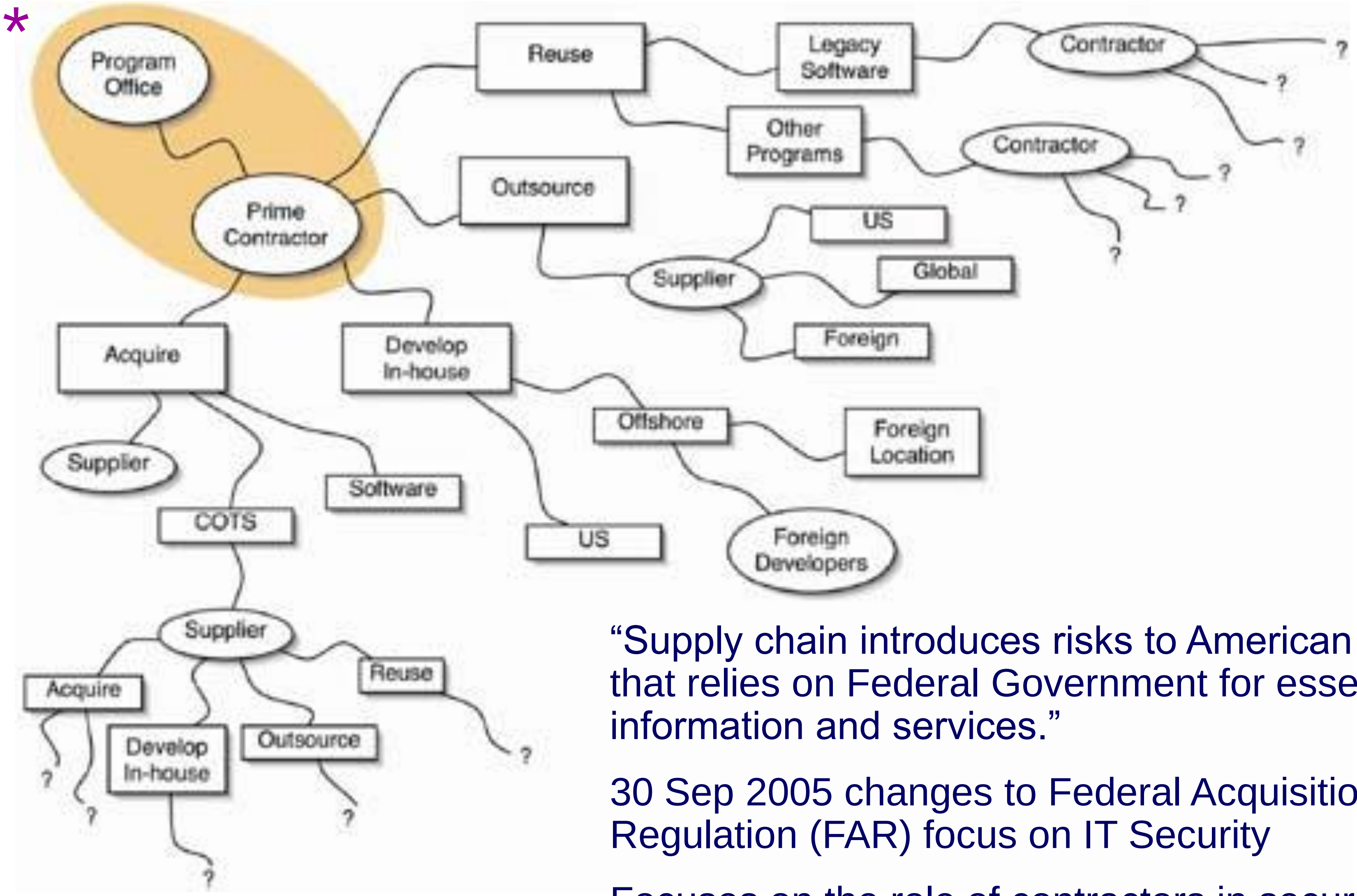
Common Weakness Enumeration (CWE) dictionary
Common Attack Pattern Enumeration (CAPEC)

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.

*



“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.

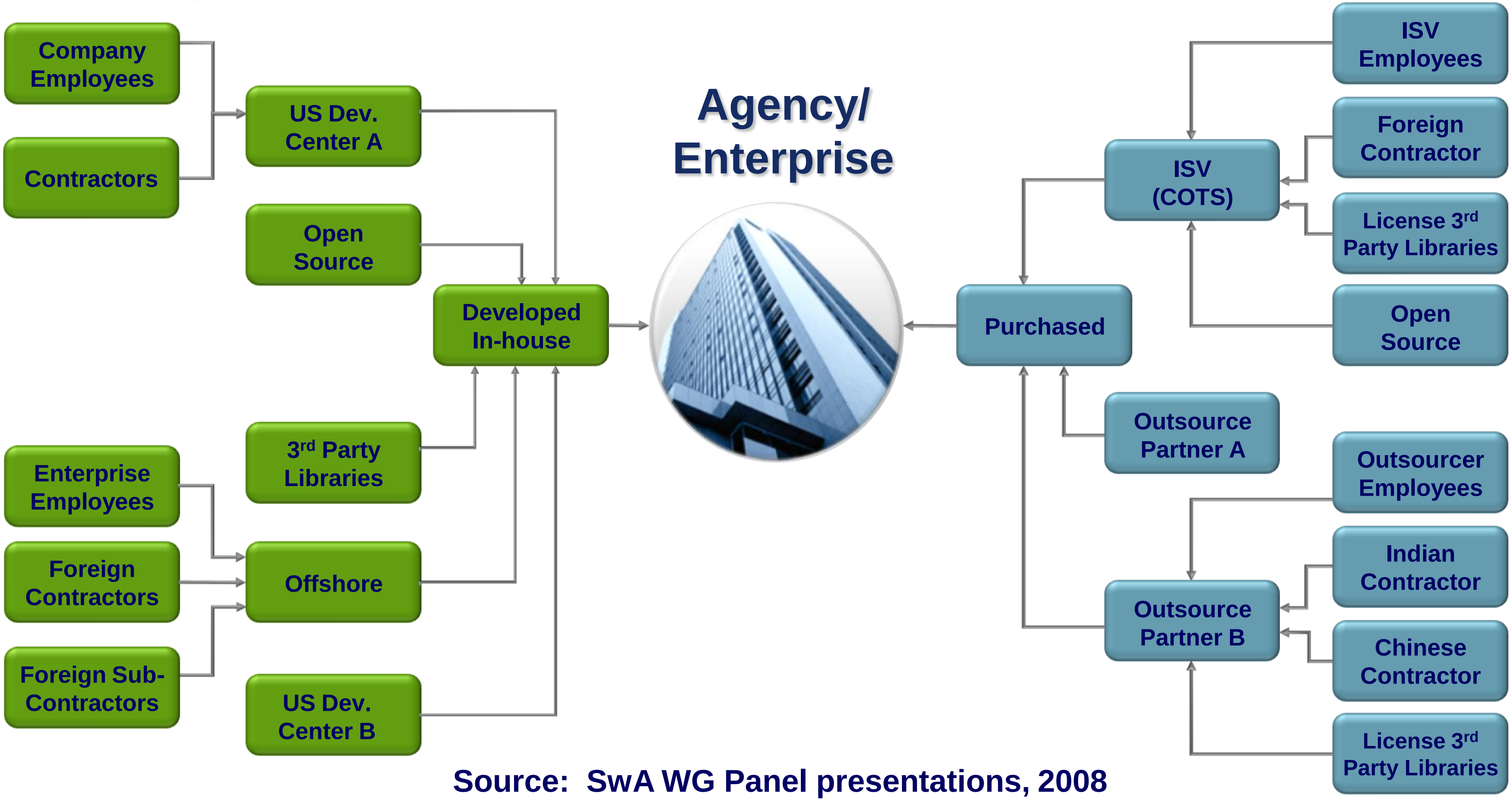
“Scope of Supplier Expansion and Foreign Involvement” graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article “Software Development Security: A Risk Management Perspective” synopsis of May 2004 GAO-04-678 report “Defense Acquisition: Knowledge of Software Suppliers Needed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

Enterprise Processes for deploying capabilities:
Increasingly Distributed and Complex

New Considerations for Quality & Security

Development Process

Procurement Process



Company Employees

Contractors

US Dev. Center A

Open Source

Developed In-house

3rd Party Libraries

Enterprise Employees

Foreign Contractors

Foreign Sub-Contractors

Offshore

US Dev. Center B

Agency/ Enterprise

Purchased

ISV Employees

Foreign Contractor

ISV (COTS)

License 3rd Party Libraries

Open Source

Outsource Partner A

Outsourcer Employees

Indian Contractor

Outsource Partner B

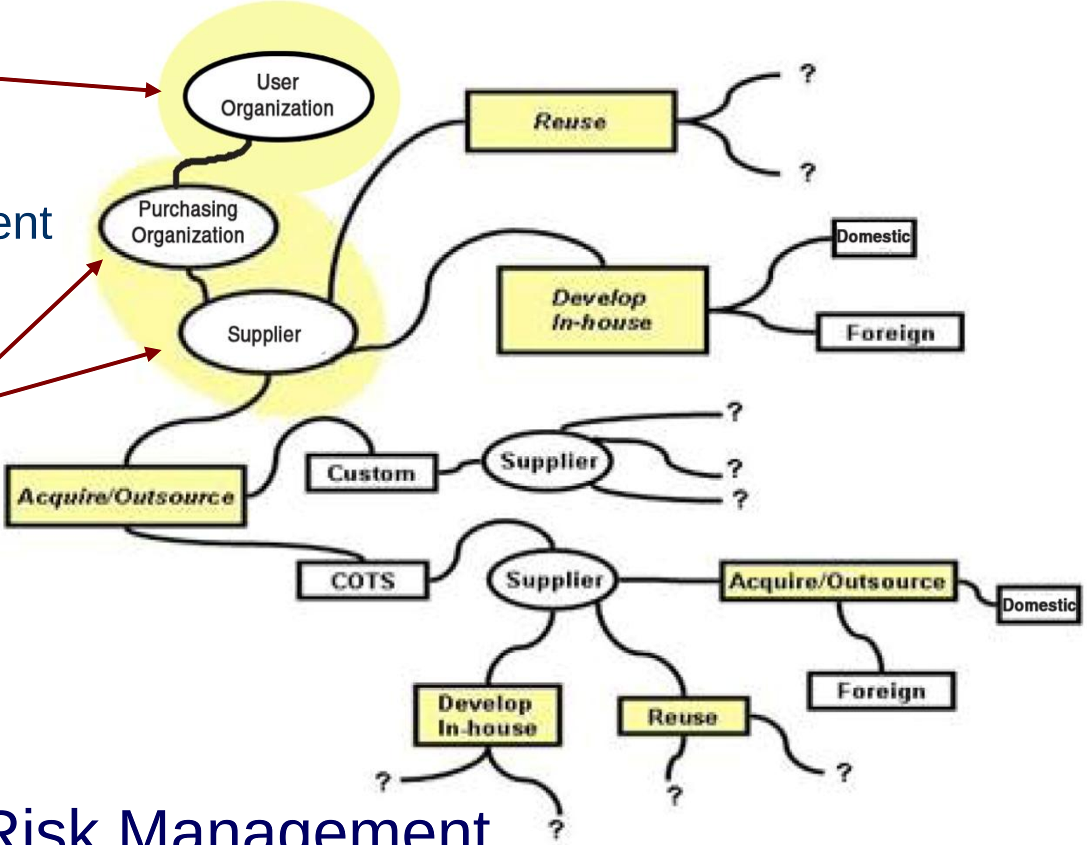
Chinese Contractor

License 3rd Party Libraries

Source: SwA WG Panel presentations, 2008

Risk Management (Enterprise <=> Project):
Shared Processes & Practices // Different Focuses

- Enterprise-Level:
  - Regulatory compliance
  - Changing threat environment
  - Business Case
- Program/Project-Level:
  - Cost
  - Schedule
  - Performance



Software Supply Chain Risk Management traverses enterprise and program/project interests

The New Issue is Virtual Security

- In addition to physical security, we now worry about cyber risks:
  - Theft of intellectual property
  - Fake or counterfeit products
  - Import/export of strong encryption
  - IT/software with deliberately embedded malicious functionality
    - Logic bombs and self-modifying code
    - Other "added features" like key loggers
    - Deliberately hidden back doors for unauthorized remote access
  - Exploitable IT/software from suppliers with poor security practices
    - Failure to use manufacturing processes/capabilities to design and build secure products (no malicious intent) in delivering exploitable products
    - Resuppliers (VARs, integrators, and service providers) often lack incentives and capabilities to adequately check content of sub-contracted and outsourced IT/software products

- IT/software security laws, policies, & standards are immature

Adopted in part from Marcus H. Sachs, Verizon, *"Supply Chain Risk Management: Can we Secure the IT Supply Chain in the Age of Globalization?" Software Assurance Forum, 15 Oct 2008*

Understanding the Threat and Controlling the Attack

One who knows the enemy and knows himself will not be endangered in a hundred engagements.

One who does not know the enemy but knows himself will sometimes be victorious; sometimes meet with defeat.

One who knows neither the enemy nor himself will invariably be defeated in every engagement.

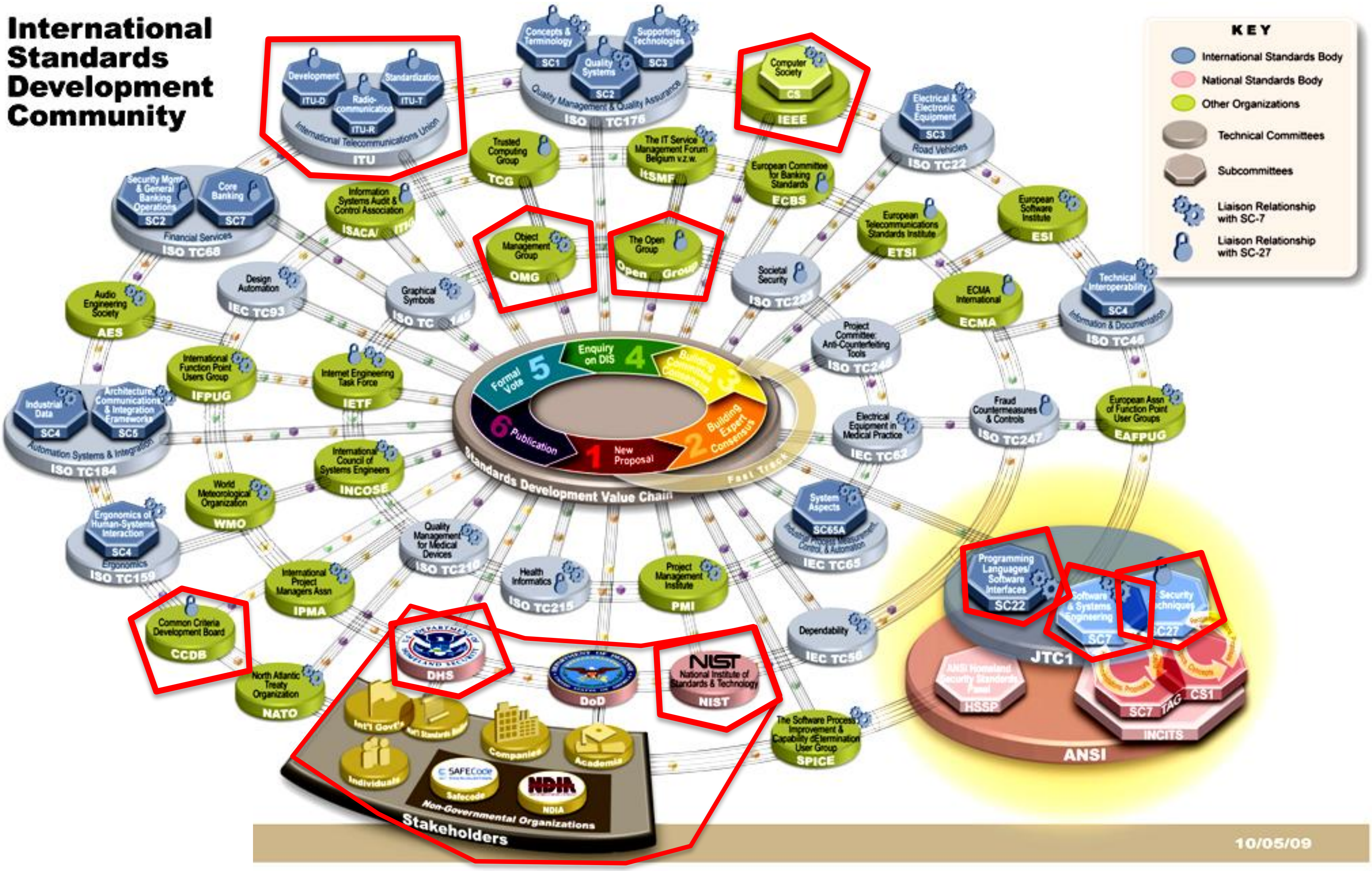
- **The Art of War, Sun Tzu**

An appropriate defense can only be established if one knows its weaknesses and how it will be attacked; thus controlling attack surface/vectors

- **Software Assurance Forum, Joe Jarzombek**

Homeland Security

We are engaged with many parts of the Community for Software Assurance-related standardization



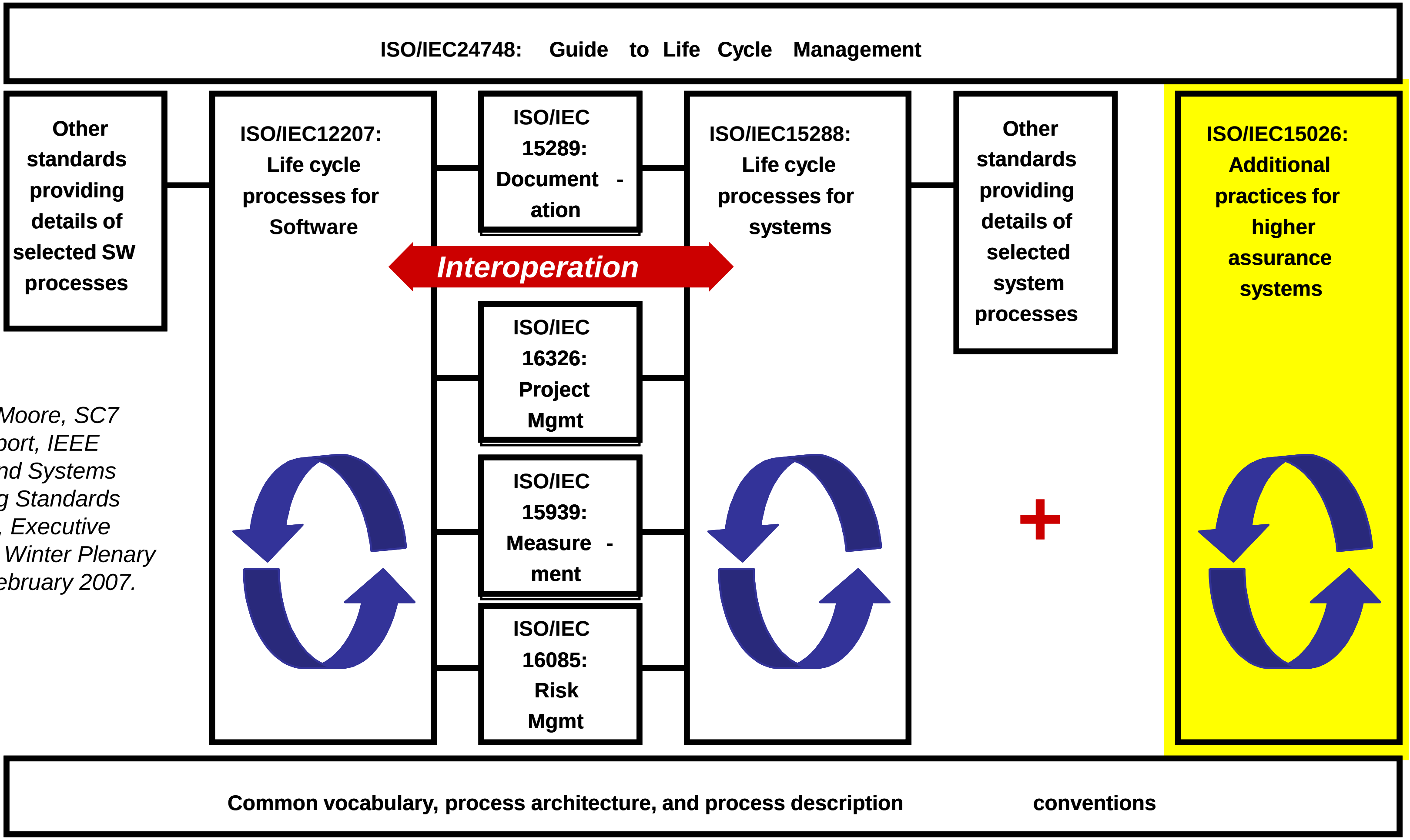
International Standards Development Community
KEY
International Standards Body
National Standards Body
Other Organizations
Technical Committees
Subcommittees
Liaison Relationship with SC-7
Liaison Relationship with SC-27
Development
ITU-D
Radio-communication
ITU-R
Standardization
ITU-T
International Telecommunications Union
ITU
Concepts & Terminology
SC1
Quality Systems
SC2
Supporting Technologies
SC3
Quality Management & Quality Assurance
ISO TC176
Computer Society
CS
IEEE
Electrical & Electronic Equipment
SC3
Road Vehicles
ISO TC22
Security Mgmt & General Banking Operations
SC2
Core Banking
SC7
Financial Services
ISO TC68
Trusted Computing Group
TCG
The IT Service Management Forum Belgium v.z.w.
itSMF
European Committee for Banking Standards
ECBS
Information Systems Audit & Control Association
ISACA/ITG
European Telecommunications Standards Institute
ETSI
European Software Institute
ESI
Object Management Group
OMG
The Open Group
Open Group
Societal Security
ISO TC223
Audio Engineering Society
AES
Design Automation
IEC TC93
Graphical Symbols
ISO TC 145
ECMA International
ECMA
Technical Interoperability
SC4
Information & Documentation
ISO TC46
Project Committee: Anti-Counterfeiting Tools
ISO TC246
International Function Point Users Group
IFPUG
Internet Engineering Task Force
IETF
Industrial Data
SC4
Architecture Communications & Integration Frameworks
SC5
Automation Systems & Integration
ISO TC184
Enquiry on DIS
4
Building Committee Consensus
3
Building Expert Consensus
2
New Proposal
1
Publication
6
Formal Vote
5
Fast Track
Standards Development Value Chain
Fraud Countermeasures & Controls
ISO TC247
Electrical Equipment in Medical Practice
IEC TC62
European Assn of Function Point User Groups
EAFPUG
International Council of Systems Engineers
INCOSE
World Meteorological Organization
WMO
System Aspects
SC65A
Industrial Process Measurement Control & Automation
IEC TC65
Ergonomics of Human-Systems Interaction
SC4
Ergonomics
ISO TC159
Quality Management for Medical Devices
ISO TC210
Health Informatics
ISO TC215
Project Management Institute
PMI
International Project Managers Assn
IPMA
Dependability
IEC TC56
Programming Languages/Software Interfaces
SC22
Software & Systems Engineering
SC7
Security Techniques
SC27
JTC1
Common Criteria Development Board
CCDB
DHS
DoD
NIST
National Institute of Standards & Technology
ANSI Homeland Security Standards Panel
HSSP
SC7 TAG
CS1
INCITS
ANSI
North Atlantic Treaty Organization
NATO
The Software Process Improvement & Capability dEtermination User Group
SPICE
Int'l Gov'ts
Nat'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
Non-Governmental Organizations
Stakeholders
10/05/09

ISO/IEC JTC1

- **SC22: ISO/IEC Technical Report (TR) 24772 Information technology -- Programming languages -- Guidance to avoiding vulnerabilities in programming languages through language selection and use.**
  - This technical report was reviewed and approved by the project editor, then published in early October.
  - As published, the document includes language-independent summaries of nearly 70 classes of vulnerabilities.
  - The working group is already drafting the 2nd Edition of the report which will add information specific to individual programming languages.

- **SC7: ISO/IEC 15026-2, Software Assurance Case has entered Final Draft International Standard (FDIS) ballot; the final ISO/IEC ballot completed in December 2010.**
  - Upon completion, it will be submitted for its final IEEE recirculation.
  - It is reasonable to anticipate publication of the standard, by both ISO/IEC and IEEE, in spring 2011.

ISO/IEC/IEEE 15026,
System and Software Assurance



ISO/IEC24748: Guide to Life Cycle Management

Other standards providing details of selected SW processes

ISO/IEC12207: Life cycle processes for Software

ISO/IEC 15289: Documentation

Interoperation

ISO/IEC 16326: Project Mgmt

ISO/IEC 15939: Measurement

ISO/IEC 16085: Risk Mgmt

ISO/IEC15288: Life cycle processes for systems

Other standards providing details of selected system processes

+

ISO/IEC15026: Additional practices for higher assurance systems

Common vocabulary, process architecture, and process description conventions

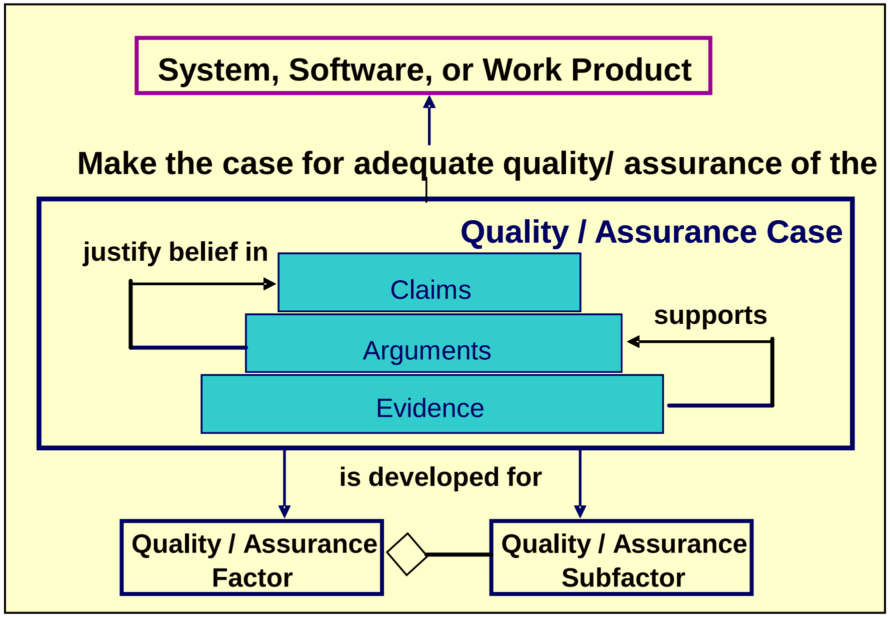
Source: J. Moore, SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Winter Plenary Meeting, February 2007.

"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 cycle

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

ISO/IEC/IEEE 15026 Assurance Case

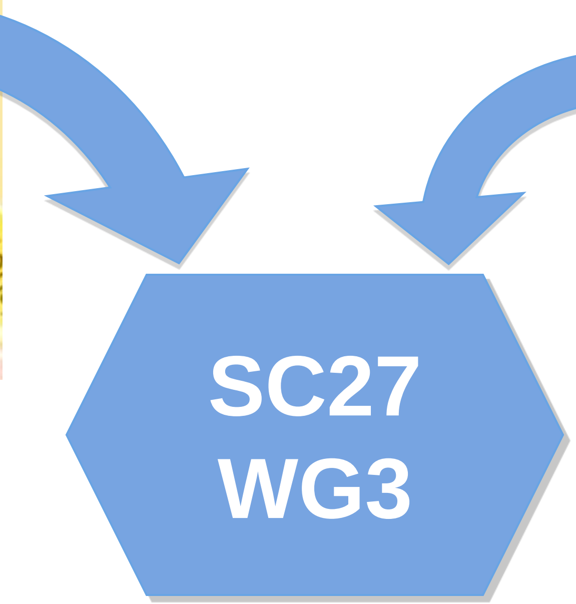
- **Set of structured assurance claims, supported by evidence and reasoning (arguments), that demonstrates how assurance needs have been satisfied.**
  - Shows compliance with assurance objectives
  - Provides an argument for the safety and security of the product or service.
  - Built, collected, and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

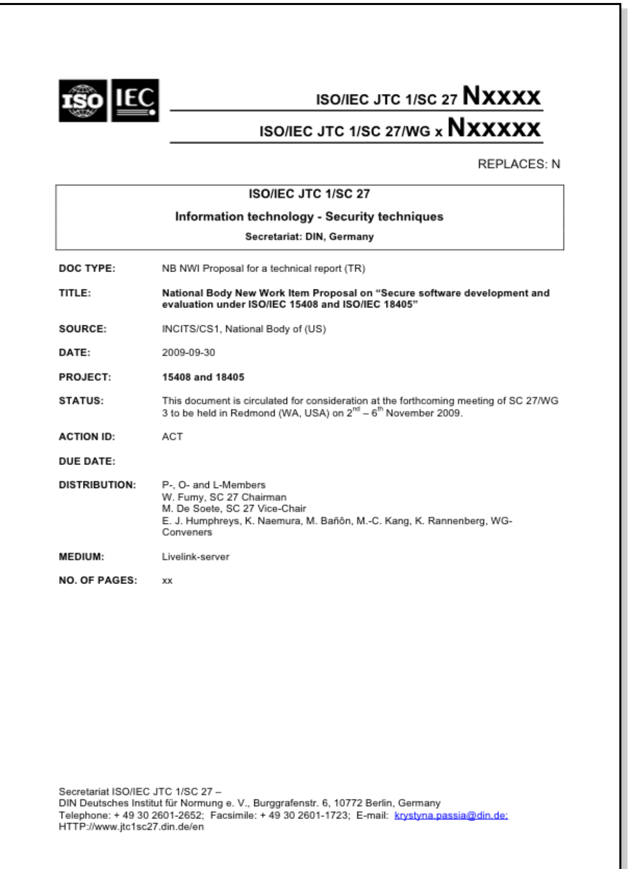

System, Software, or Work Product
Make the case for adequate quality/ assurance of the
Quality / Assurance Case
justify belief in
Claims
supports
Arguments
Evidence
is developed for
Quality / Assurance Factor
Quality / Assurance Subfactor

- **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





ISO/IEC JTC 1/SC 27 **Nxxxx**

ISO/IEC JTC 1/SC 27/WG x **Nxxxxx**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	NB NWI Proposal for a technical report (TR)
TITLE:	**National Body New Work Item Proposal on "Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405"**
SOURCE:	INCITS/CS1, National Body of (US)
DATE:	2009-09-30
PROJECT:	**15408 and 18405**
STATUS:	This document is circulated for consideration at the forthcoming meeting of SC 27/WG 3 to be held in Redmond (WA, USA) on 2nd – 6th November 2009.
ACTION ID:	ACT
DUE DATE:	
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. J. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	xx

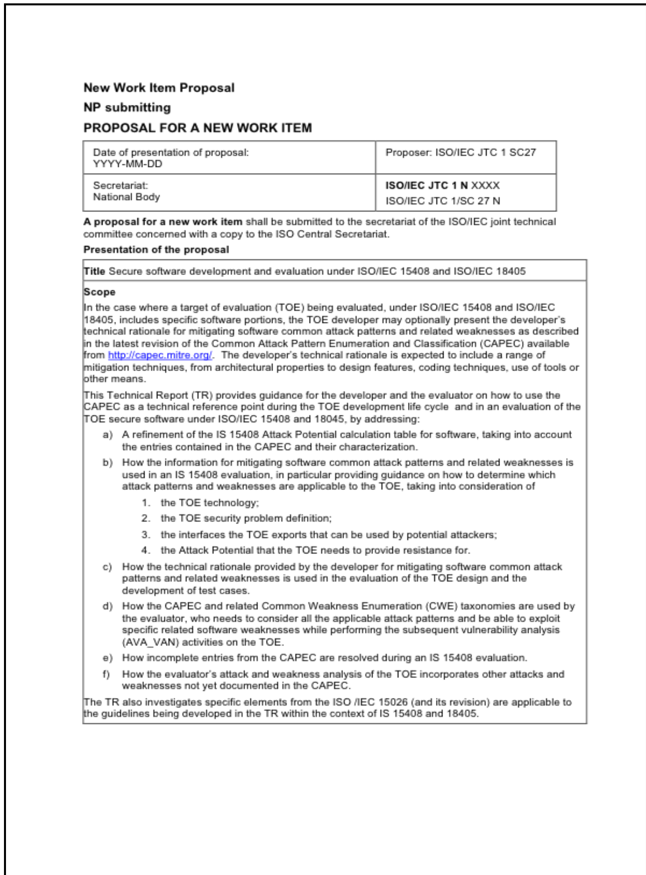
Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

Common Criteria v4 CCDB

- TOE to leverage CAPEC & CWE
- Also investigating how to leverage ISO/IEC 15026

NIAP Evaluation Scheme

- Above plus
- Also investigating how to leverage Security Content Automation Protocol (SCAP)



New Work Item Proposal

NP submitting

PROPOSAL FOR A NEW WORK ITEM

Date of presentation of proposal: YYYY-MM-DD	Proposer: ISO/IEC JTC 1 SC27
Secretariat: National Body	**ISO/IEC JTC 1 N** XXXX ISO/IEC JTC 1/SC 27 N

A proposal for a new work item shall be submitted to the secretariat of the ISO/IEC joint technical committee concerned with a copy to the ISO Central Secretariat.

Presentation of the proposal

Title Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405

Scope

In the case where a target of evaluation (TOE) being evaluated, under ISO/IEC 15408 and ISO/IEC 18405, includes specific software portions, the TOE developer may optionally present the developer's technical rationale for mitigating software common attack patterns and related weaknesses as described in the latest revision of the Common Attack Pattern Enumeration and Classification (CAPEC) available from http://capec.mitre.org/. The developer's technical rationale is expected to include a range of mitigation techniques, from architectural properties to design features, coding techniques, use of tools or other means.

This Technical Report (TR) provides guidance for the developer and the evaluator on how to use the CAPEC as a technical reference point during the TOE development life cycle and in an evaluation of the TOE secure software under ISO/IEC 15408 and 18045, by addressing:

a) A refinement of the IS 15408 Attack Potential calculation table for software, taking into account the entries contained in the CAPEC and their characterization.

b) How the information for mitigating software common attack patterns and related weaknesses is used in an IS 15408 evaluation, in particular providing guidance on how to determine which attack patterns and weaknesses are applicable to the TOE, taking into consideration of

   1. the TOE technology;
   2. the TOE security problem definition;
   3. the interfaces the TOE exports that can be used by potential attackers;
   4. the Attack Potential that the TOE needs to provide resistance for.

c) How the technical rationale provided by the developer for mitigating software common attack patterns and related weaknesses is used in the evaluation of the TOE design and the development of test cases.

d) How the CAPEC and related Common Weakness Enumeration (CWE) taxonomies are used by the evaluator, who needs to consider all the applicable attack patterns and be able to exploit specific related software weaknesses while performing the subsequent vulnerability analysis (AVA_VAN) activities on the TOE.

e) How incomplete entries from the CAPEC are resolved during an IS 15408 evaluation.

f) How the evaluator's attack and weakness analysis of the TOE incorporates other attacks and weaknesses not yet documented in the CAPEC.

The TR also investigates specific elements from the ISO /IEC 15026 (and its revision) are applicable to the guidelines being developed in the TR within the context of IS 15408 and 18405.

Need for Rating Schemes

- Rating of Suppliers providing software products and services
  - Standards-based or model-based frameworks to support process improvement and enable benchmarking of organizational capabilities
  - Credential programs for professionals involved in software lifecycle activities and decisions
- Rating of Software products:
  - Supported by automation
  - Standards-based
  - Rules for aggregation and scaling
  - Verifiable by independent third parties
  - Labeling to support various needs (eg., security, dependability, etc)
  - Meaningful and economical for consumers and suppliers

Collaborate with OWASP “Security Facts” labeling efforts

Homeland Security

SwA Collaboration for Content & Peer Review

Build Security In

Setting a higher standard for software assurance

Sponsored by DHS National Cyber Security Division

BSI https://buildsecurityin.us-cert.gov focuses on making Software Security a normal part of Software Engineering

Software Assurance

Community Resources and Information Clearinghouse

Sponsored by DHS National Cyber Security Division

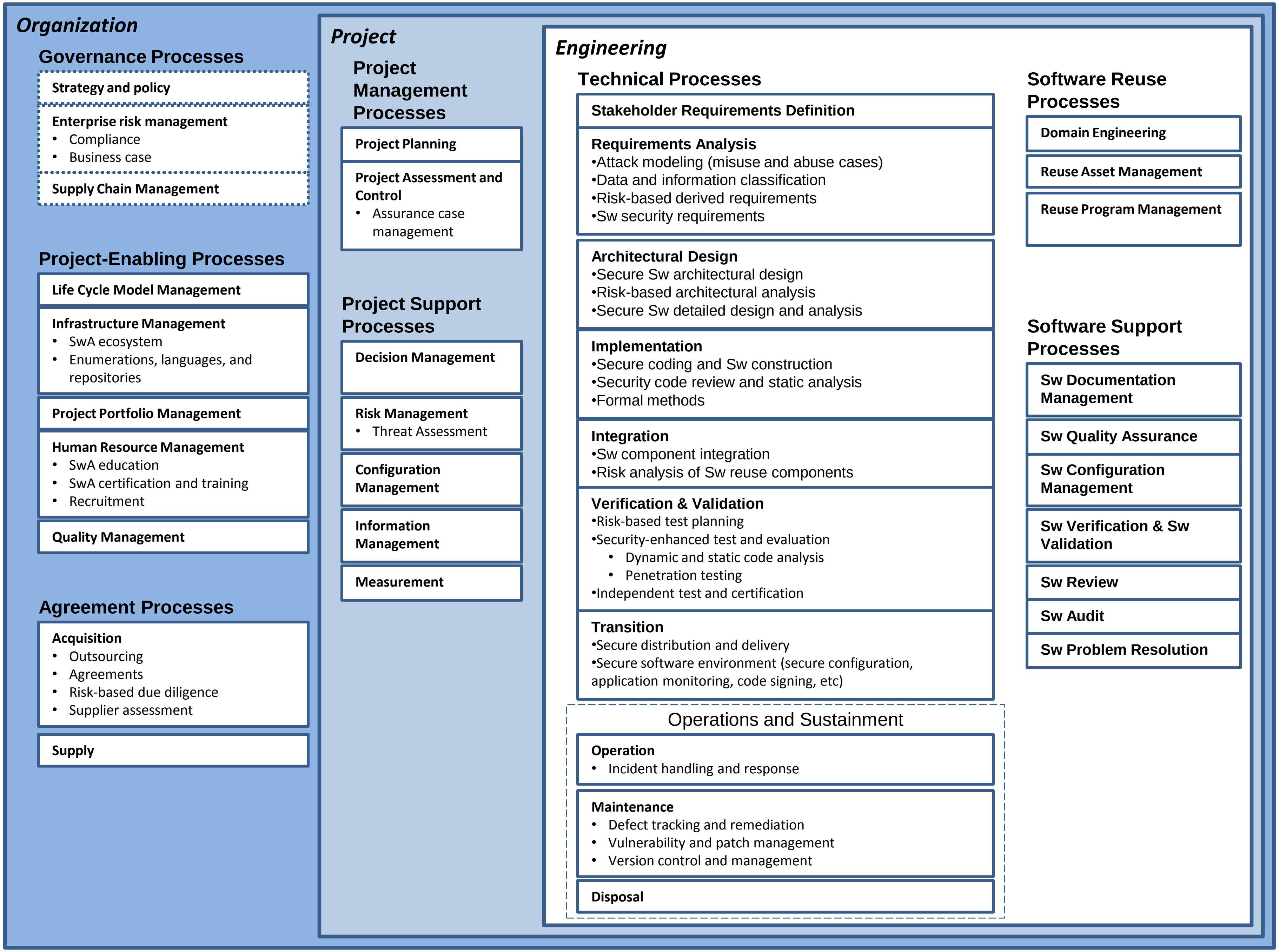
SwA Community Resources and Information Clearinghouse (CRIC)

https://buildsecurityin.us-cert.gov/swa/ focuses on all contributing disciplines, practices and methodologies that advance risk mitigation efforts to enable greater resilience of software/cyber assets.

The SwA CRIC provides a primary resource for SwA Working Groups.

Where applicable, SwA CRIC & BSI provide relevant links to each other.

Life-Cycle Standards View Categories (ISO/IEC 15288 and 12207)



Organization

Governance Processes

Strategy and policy

Enterprise risk management
- Compliance
- Business case

Supply Chain Management

Project-Enabling Processes

Life Cycle Model Management

Infrastructure Management
- SwA ecosystem
- Enumerations, languages, and repositories

Project Portfolio Management

Human Resource Management
- SwA education
- SwA certification and training
- Recruitment

Quality Management

Agreement Processes

Acquisition
- Outsourcing
- Agreements
- Risk-based due diligence
- Supplier assessment

Supply

Project

Project Management Processes

Project Planning

Project Assessment and Control
- Assurance case management

Project Support Processes

Decision Management

Risk Management
- Threat Assessment

Configuration Management

Information Management

Measurement

Engineering

Technical Processes

Stakeholder Requirements Definition

Requirements Analysis
•Attack modeling (misuse and abuse cases)
•Data and information classification
•Risk-based derived requirements
•Sw security requirements

Architectural Design
•Secure Sw architectural design
•Risk-based architectural analysis
•Secure Sw detailed design and analysis

Implementation
•Secure coding and Sw construction
•Security code review and static analysis
•Formal methods

Integration
•Sw component integration
•Risk analysis of Sw reuse components

Verification & Validation
•Risk-based test planning
•Security-enhanced test and evaluation
- Dynamic and static code analysis
- Penetration testing

•Independent test and certification

Transition
•Secure distribution and delivery
•Secure software environment (secure configuration, application monitoring, code signing, etc)

Operations and Sustainment

Operation
- Incident handling and response

Maintenance
- Defect tracking and remediation
- Vulnerability and patch management
- Version control and management

Disposal

Software Reuse Processes

Domain Engineering

Reuse Asset Management

Reuse Program Management

Software Support Processes

Sw Documentation Management

Sw Quality Assurance

Sw Configuration Management

Sw Verification & Sw Validation

Sw Review

Sw Audit

Sw Problem Resolution

Software Assurance (SwA) Pocket Guide Series

SwA in Acquisition & Outsourcing

- Software Assurance in Acquisition and Contract Language
- Software Supply Chain Risk Management and Due-Diligence

SwA in Development

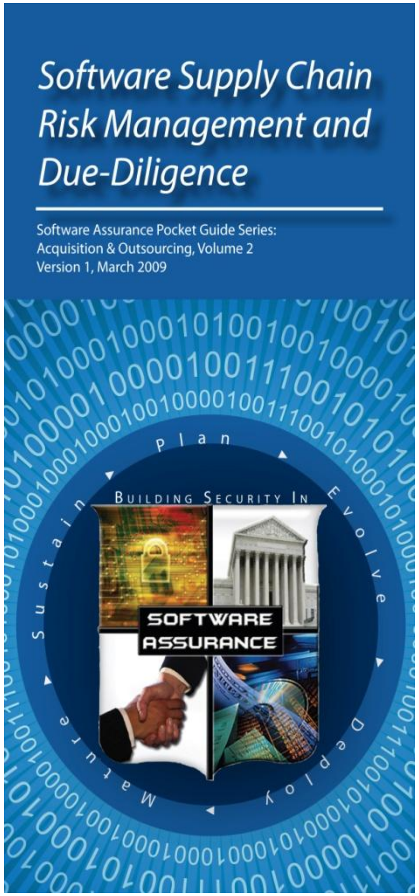
- Integrating Security into the Software Development Life Cycle
- Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
- Risk-based Software Security Testing
- Requirements and Analysis for Secure Software
- Architecture and Design Considerations for Secure Software
- Secure Coding and Software Construction
- Security Considerations for Technologies, Methodologies & Languages

SwA Life Cycle Support

- SwA in Education, Training and Certification
- Secure Software Distribution, Deployment, and Operations
- Code Transparency & Software Labels
- ☆ Assurance Case Management
- Secure Software Environment and Assurance EcoSystem

SwA Measurement and Information Needs

- Making Software Security Measurable
- Practical Measurement Framework for SwA and InfoSec
- SwA Business Case and Return on Investment



Software Supply Chain Risk Management and Due-Diligence

Software Assurance Pocket Guide Series:
Acquisition & Outsourcing, Volume 2
Version 1, March 2009

SwA Pocket Guides and SwA-related documents are collaboratively developed with peer review; they are subject to update and are freely available for download via the DHS Software Assurance Community Resources and Information Clearinghouse at https://buildsecurityin.us-cert.gov/swa (see SwA Resources)

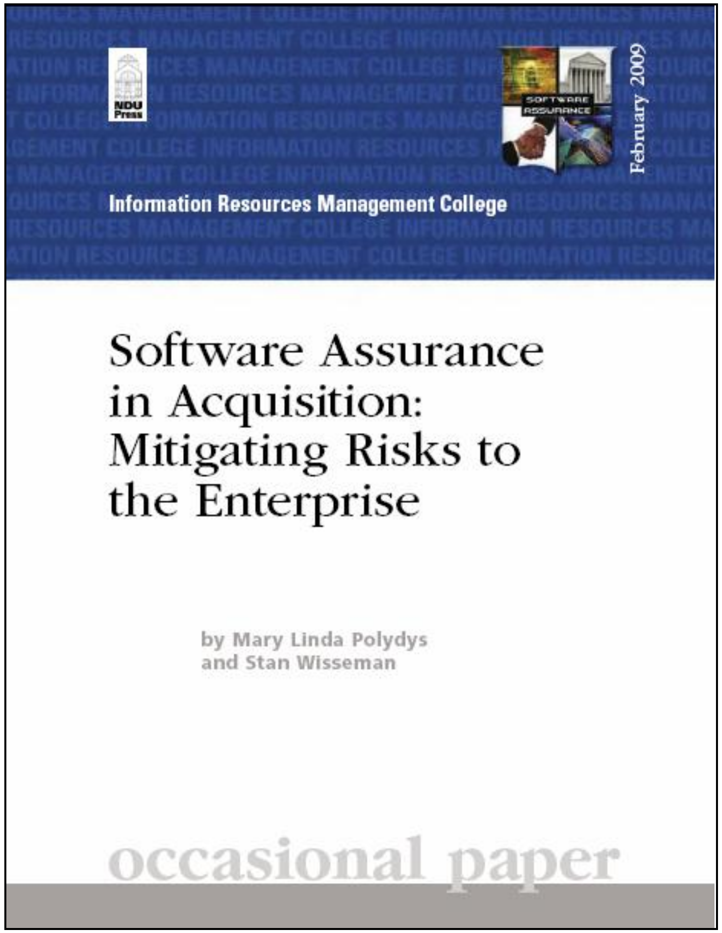
SwA Acquisition & Outsourcing Handbook

"Software Assurance in Acquisition:

Mitigating Risks to the Enterprise"

Version 1.0, Oct 2008, available for community use

published by National Defense University Press, Feb 2009



NDU Press

February 2009

SOFTWARE ASSURANCE

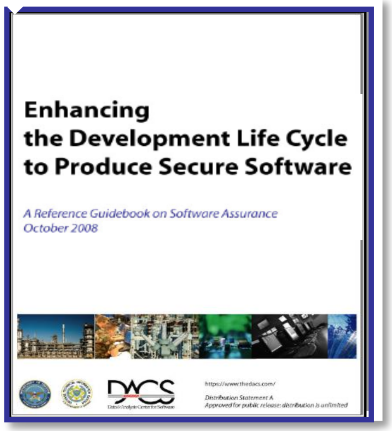
Information Resources Management College

Software Assurance in Acquisition: Mitigating Risks to the Enterprise

by Mary Linda Polydys and Stan Wisseman

occasional paper

Many SwA Resources Focus On Development



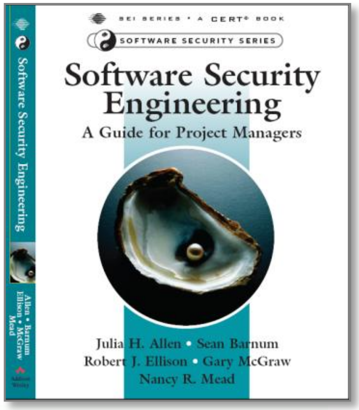
Enhancing
the Development Life Cycle
to Produce Secure Software

*A Reference Guidebook on Software Assurance
October 2008*

DACS
Data & Analysis Center for Software

https://www.thedacs.com/

*Distribution Statement A
Approved for public release: distribution is unlimited*

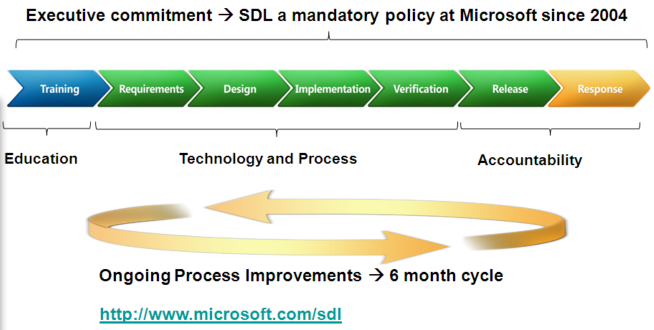


SEI SERIES • A CERT® BOOK

SOFTWARE SECURITY SERIES

Software Security Engineering
A Guide for Project Managers

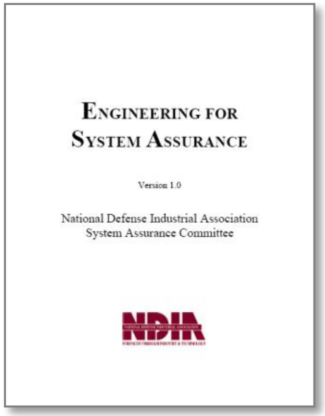
Julia H. Allen • Sean Barnum
Robert J. Ellison • Gary McGraw
Nancy R. Mead



Executive commitment → SDL a mandatory policy at Microsoft since 2004

Ongoing Process Improvements → 6 month cycle

http://www.microsoft.com/sdl

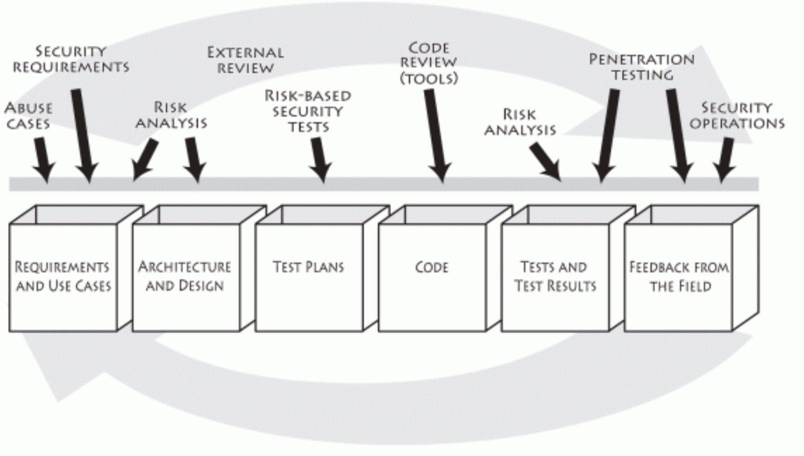


Engineering for
System Assurance

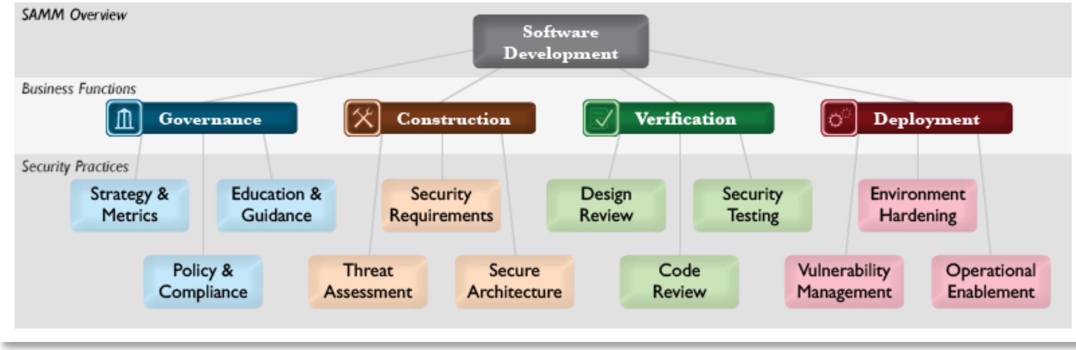
Version 1.0

National Defense Industrial Association
System Assurance Committee

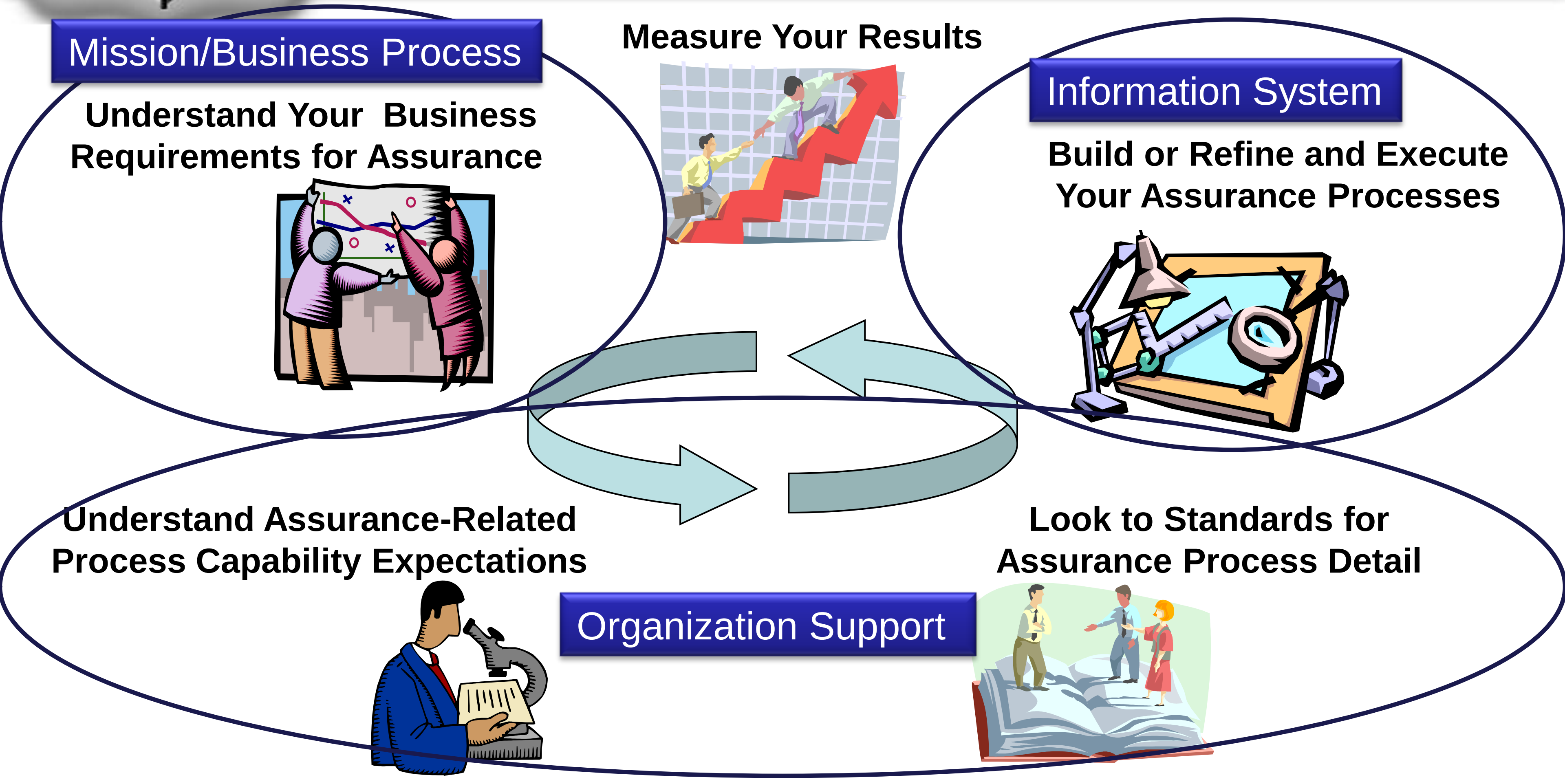
NDIA



Assurance for CMMI ®



Process Improvement Lifecycle - A Process for Achieving Assurance



Mission/Business Process

Understand Your Business Requirements for Assurance

Measure Your Results

Information System

Build or Refine and Execute Your Assurance Processes

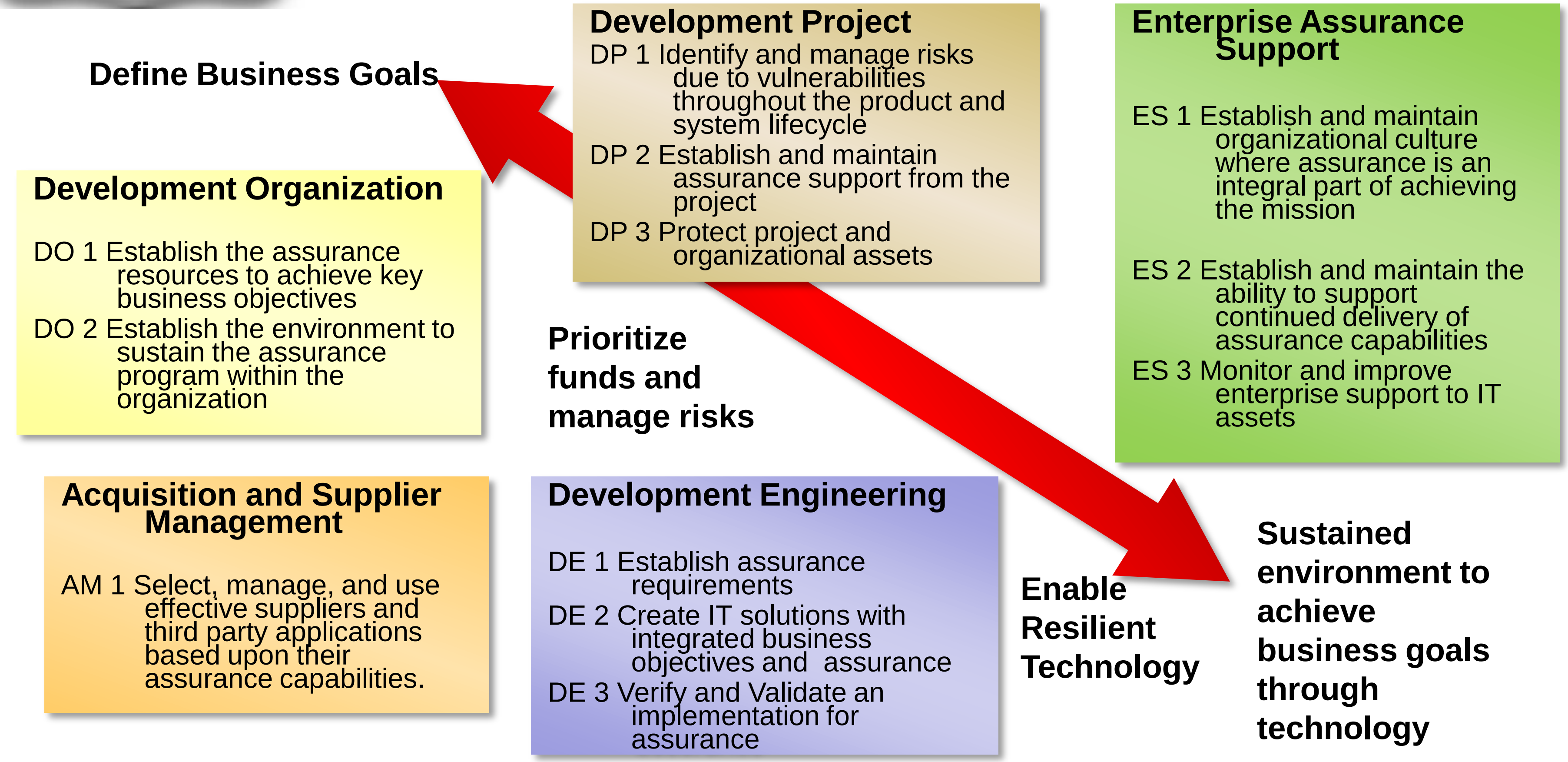
Understand Assurance-Related Process Capability Expectations

Look to Standards for Assurance Process Detail

Organization Support

Adapted from: Paul Croll, Computer Sciences Corporation, August 2007

The Assurance PRM Is A Holistic Framework



Define Business Goals

Development Project

DP 1 Identify and manage risks due to vulnerabilities throughout the product and system lifecycle

DP 2 Establish and maintain assurance support from the project

DP 3 Protect project and organizational assets

Enterprise Assurance Support

ES 1 Establish and maintain organizational culture where assurance is an integral part of achieving the mission

ES 2 Establish and maintain the ability to support continued delivery of assurance capabilities

ES 3 Monitor and improve enterprise support to IT assets

Development Organization

DO 1 Establish the assurance resources to achieve key business objectives

DO 2 Establish the environment to sustain the assurance program within the organization

Prioritize funds and manage risks

Acquisition and Supplier Management

AM 1 Select, manage, and use effective suppliers and third party applications based upon their assurance capabilities.

Development Engineering

DE 1 Establish assurance requirements

DE 2 Create IT solutions with integrated business objectives and assurance

DE 3 Verify and Validate an implementation for assurance

Enable Resilient Technology

Sustained environment to achieve business goals through technology

Created to facilitate Communication Across An Organization’s Multi-Disciplinary Stakeholders

Courtesy of Michele Moss, BAH, SwA Processes & Practices

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

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

The DHS SwA Processes and Practices Working Group has synthesized the contributions of leading government and industry experts into a set of high-level goals and supporting practices (an evolution of the SwA community's Assurance Process Reference Model)

The goals and practices are mapped to specific industry resources providing additional detail and real world implementation and supporting practices

- Assurance Focus for CMMI
- Building Security In Maturity Model
- Open Software Assurance Maturity Model
- CERT® Resilience Management Model
- CMMI for Acquisition
- CMMI for Development
- CMMI for Services
- SwA Community's Assurance Process Reference Model –Initial Mappings
- SwA Community's Assurance Process Reference Model - Self Assessment
- SwA Community's Assurance Process Reference Model – Mapping to Assurance Models

Other valuable resources that are in the process of being mapped include

- NIST IR 7622: DRAFT Piloting Supply Chain Risk Management Practices for Federal Information Systems
- NDIA System Assurance Guidebook
- Microsoft Security Development Lifecycle
- SAFECode

Process Reference Model for Assurance – Goals and Practices September 2010

In the following table, all references to “assurance” are intended to include system and software assurance, information assurance, and cyber security in support of the business/mission functions supported by systems and software.

Goal	Practice List
Development – Engineering	
DE 1 Establish assurance requirements	Understand the operating environment and define the operating constraints for mission and information assurance within the environments of system development.
	Develop customer mission and information assurance requirements
	Define product and product component assurance requirements
	Identify operational concepts and associated scenarios for intended and unintended use and associated assurance considerations
	Identify appropriate controls for integrity and availability of the system to in support of organizational objectives
	Analyze assurance requirements
	Balance assurance needs against cost benefits
	Obtain Agreement of risk for assurance level

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

It can be used by acquirers, suppliers and integrators as a to tool to discuss areas of strength and weakness

- What assurance goals are being met?
- What practices are being implemented?
- Who are the suppliers and how are they managing risk?

SwA Community Assurance Process Reference Model – Self Assessment

In the following table, all references to “assurance” are intended to include system and software assurance, and cyber security in support of the business/mission functions supported by systems and software.

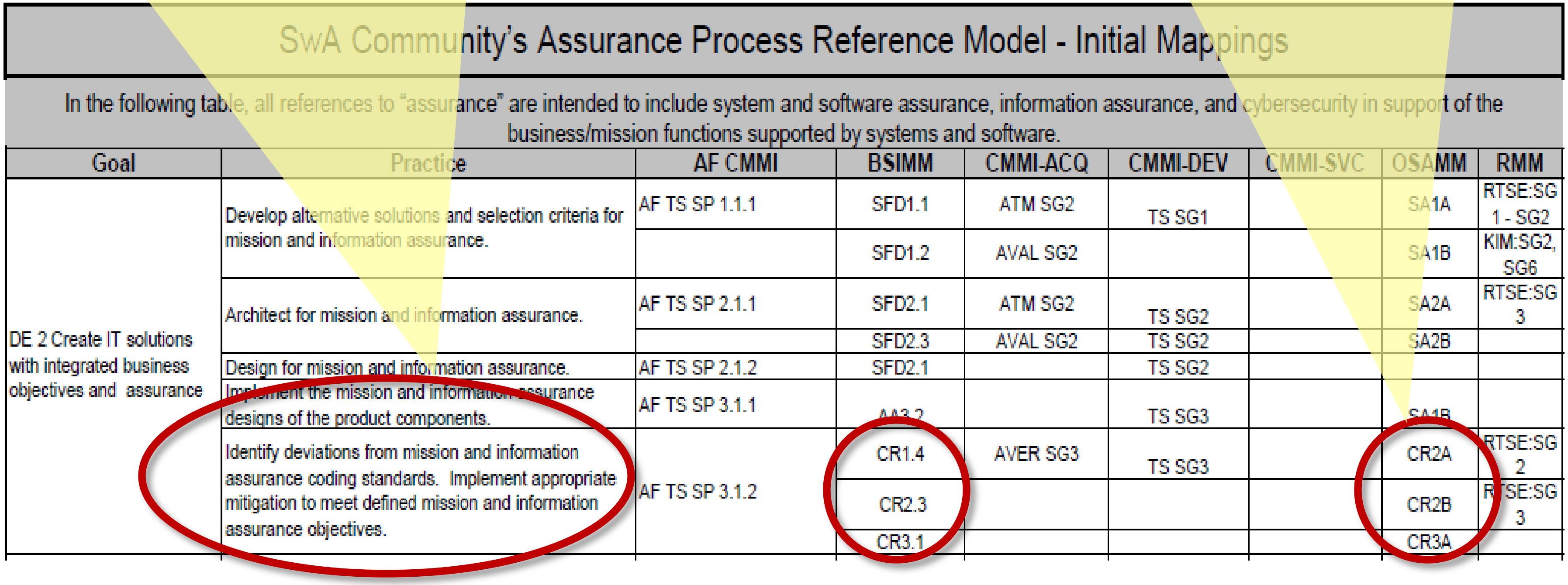
Goal	Practice	Practice Implementation Level	Notes
	Development – Engineering		
DE 1 Establish assurance requirements	Understand the operating environment and define the operating constraints for mission and information assurance within the environments of system development.		
	Develop customer mission and information assurance requirements		
	Define product and product component assurance requirements		
	Identify operational concepts and associated scenarios for intended and unintended use and associated assurance considerations		
	Identify appropriate controls for integrity and availability of the system to in support of organizational objectives		
	Analyze assurance requirements		
	Balance assurance needs against cost benefits		
	Obtain Agreement of risk for assurance level		

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

It can be used as a navigation tool to guide SwA implementation efforts

You have been asked to ensure that the OWASP Top Ten (an assurance coding Standard) are not in the Code

You can look at the OSAMM for guidance on how to do it



SwA Community's Assurance Process Reference Model - Initial Mappings

In the following table, all references to "assurance" are intended to include system and software assurance, information assurance, and cybersecurity in support of the business/mission functions supported by systems and software.

Goal	Practice	AF CMMI	BSIMM	CMMI-ACQ	CMMI-DEV	CMMI-SVC	OSAMM	RMM
DE 2 Create IT solutions with integrated business objectives and assurance	Develop alternative solutions and selection criteria for mission and information assurance.	AF TS SP 1.1.1	SFD1.1	ATM SG2	TS SG1		SA1A	RTSE:SG 1 - SG2
			SFD1.2	AVAL SG2			SA1B	KIM:SG2, SG6
	Architect for mission and information assurance.	AF TS SP 2.1.1	SFD2.1	ATM SG2	TS SG2		SA2A	RTSE:SG 3
			SFD2.3	AVAL SG2	TS SG2		SA2B	
	Design for mission and information assurance.	AF TS SP 2.1.2	SFD2.1		TS SG2			
	Implement the mission and information assurance designs of the product components.	AF TS SP 3.1.1	AA3.2		TS SG3		SA1B	
	Identify deviations from mission and information assurance coding standards. Implement appropriate mitigation to meet defined mission and information assurance objectives.	AF TS SP 3.1.2	CR1.4	AVER SG3	TS SG3		CR2A	RTSE:SG 2
			CR2.3				CR2B	RTSE:SG 3
			CR3.1				CR3A	

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

It can be used to begin the translation of SwA to other across disciplines

SwA Community Assurance Process Reference Model – Mapping to Foundational Practices

In the following table, all references to "assurance" are intended to include system and software assurance, and cyber security in support of the business/mission functions supported by systems and software.

Goal	Practice	CMMI-ACQ	CMMI-DEV	CMMI-SVC
Development – Engineering				
DE 1 Establish assurance requirements	Understand the operating environment and define the operating constraints for mission and information assurance within the environments of system development.	PP SG1	IPPD SG1	
	Develop customer mission and information assurance requirements	ARD SG1, SG3	RD SG1	
		REQM SG1		
	Define product and product component assurance requirements	CM SG1	RD SG2	
	Identify operational concepts and associated scenarios for intended and unintended use and associated assurance considerations	RSKM SG1 – SG2	RD SG3	
	Identify appropriate controls for integrity and availability of the system to in support of organizational objectives	RSKM SG1	RSKM SG1	
	Analyze assurance requirements	ARD SG3	RD SG3	
	Balance assurance needs against cost benefits	ARD SG3	RD SG3	
	Obtain Agreement of risk for assurance level	RSKM SG2	RSKM SG2	

Efforts are underway to map to

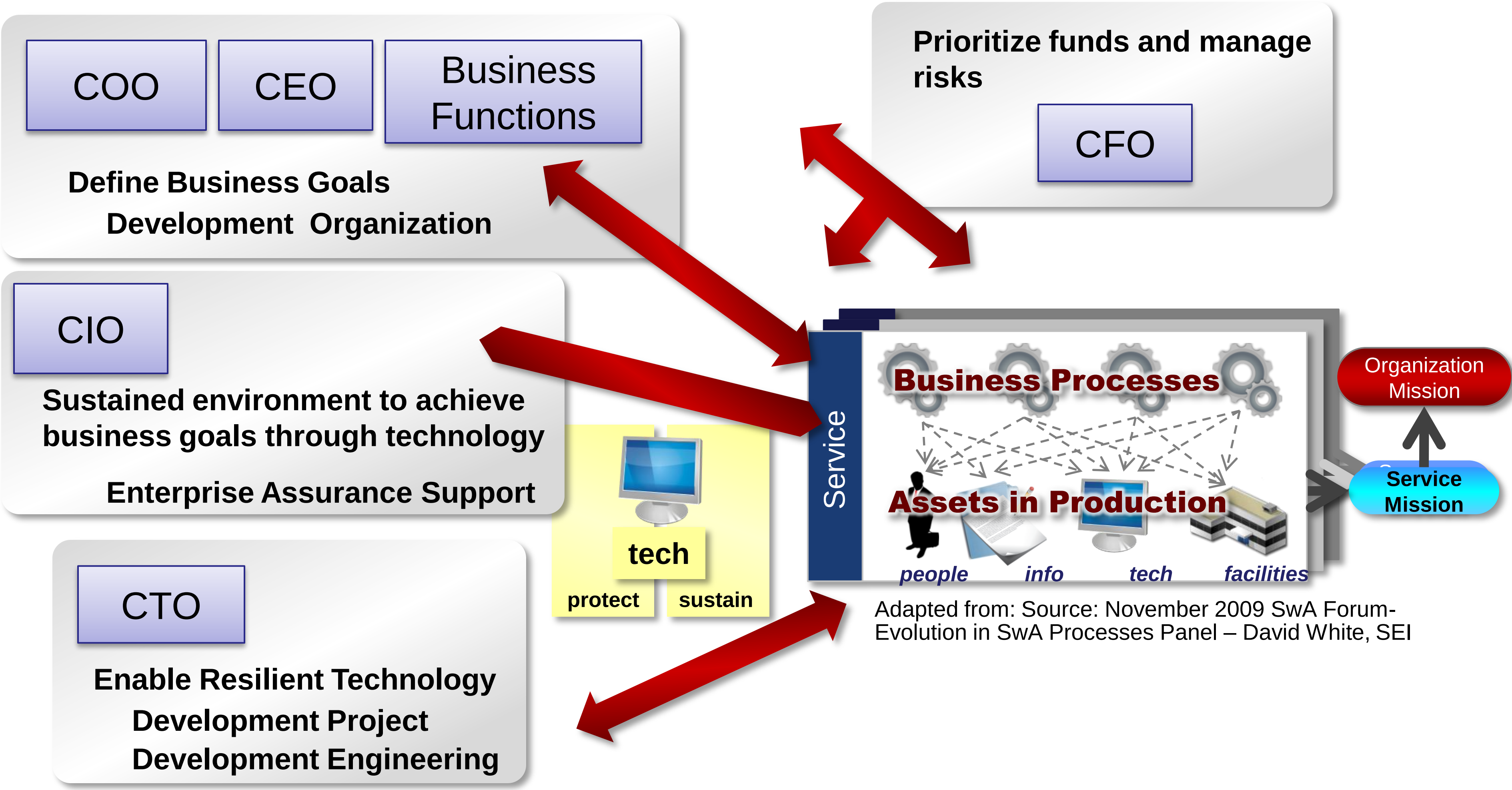
- ***ISO/IEEE 15288***
- ***ISO/IEEE 12207***

Common SwA References Recommendations for Training

Assurance PRM	SAFEcode	MS SDL	Open SAMM	BSIMM
•Establish and maintain the strategic assurance training needs of the organization •Ensure resources have the training needed to do their job	1. Foundational (everyone) 2. Advanced (secure coding and testing practices) 3. Specialized (role-based)	1. Basic Concepts 2. Common Baseline 3. Custom Training	1. Technical Security Awareness training 2. Role specific guidance 3. Comprehensive security training and certifications	1. Create the software security satellite 2. Make customized, role-based training available on demand 3. Provide recognition for skills and career path progression

Source: SwA Benchmarking and Implementation, Moss, SSTC 2010

It can be used to begin the translation of SwA Activities across organizational leadership



COO | CEO | Business Functions

Define Business Goals

Development Organization

Prioritize funds and manage risks

CFO

CIO

Sustained environment to achieve business goals through technology

Enterprise Assurance Support

CTO

Enable Resilient Technology

Development Project

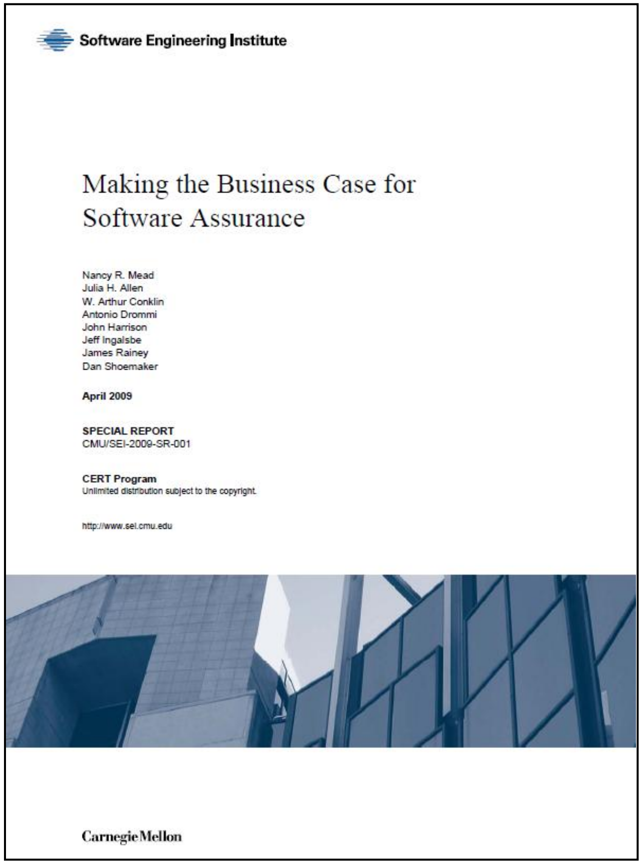
Development Engineering

Adapted from: Source: November 2009 SwA Forum- Evolution in SwA Processes Panel – David White, SEI

Business Case for Software Assurance

April 2009 SwA Report provides background, context and examples:

- Motivators
- Cost/Benefit Models Overview
- Measurement
- Risk
- Prioritization
- Process Improvement & Secure Software
- Globalization
- Organizational Development
- Case Studies and Examples



Software Engineering Institute

Making the Business Case for
Software Assurance

Nancy R. Mead
Julia H. Allen
W. Arthur Conklin
Antonio Drommi
John Harrison
Jeff Ingalsbe
James Rainey
Dan Shoemaker

April 2009

SPECIAL REPORT
CMU/SEI-2009-SR-001

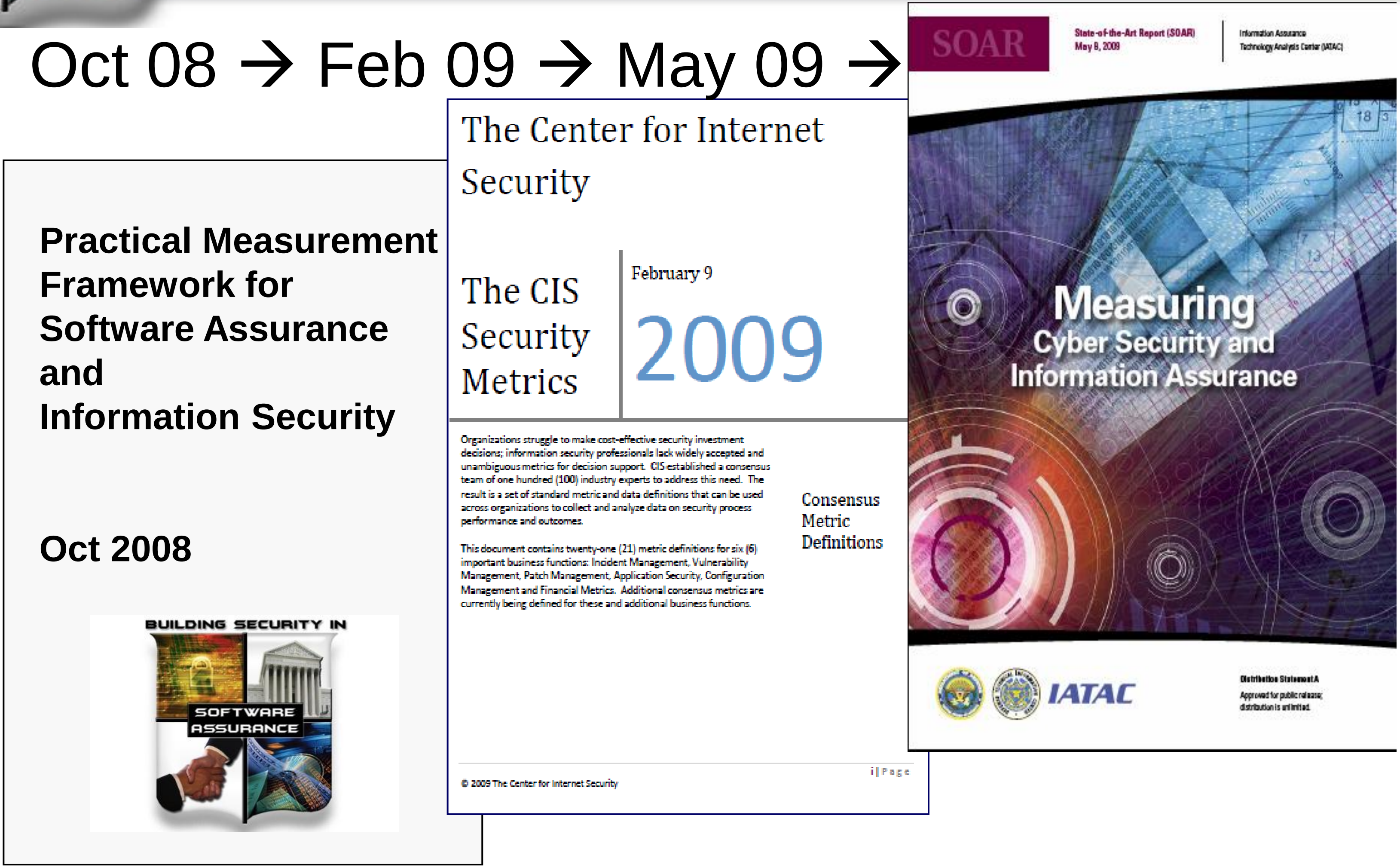
CERT Program
Unlimited distribution subject to the copyright.

http://www.sei.cmu.edu

CarnegieMellon

Security Measurement Resources

Oct 08 → Feb 09 → May 09 →



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)

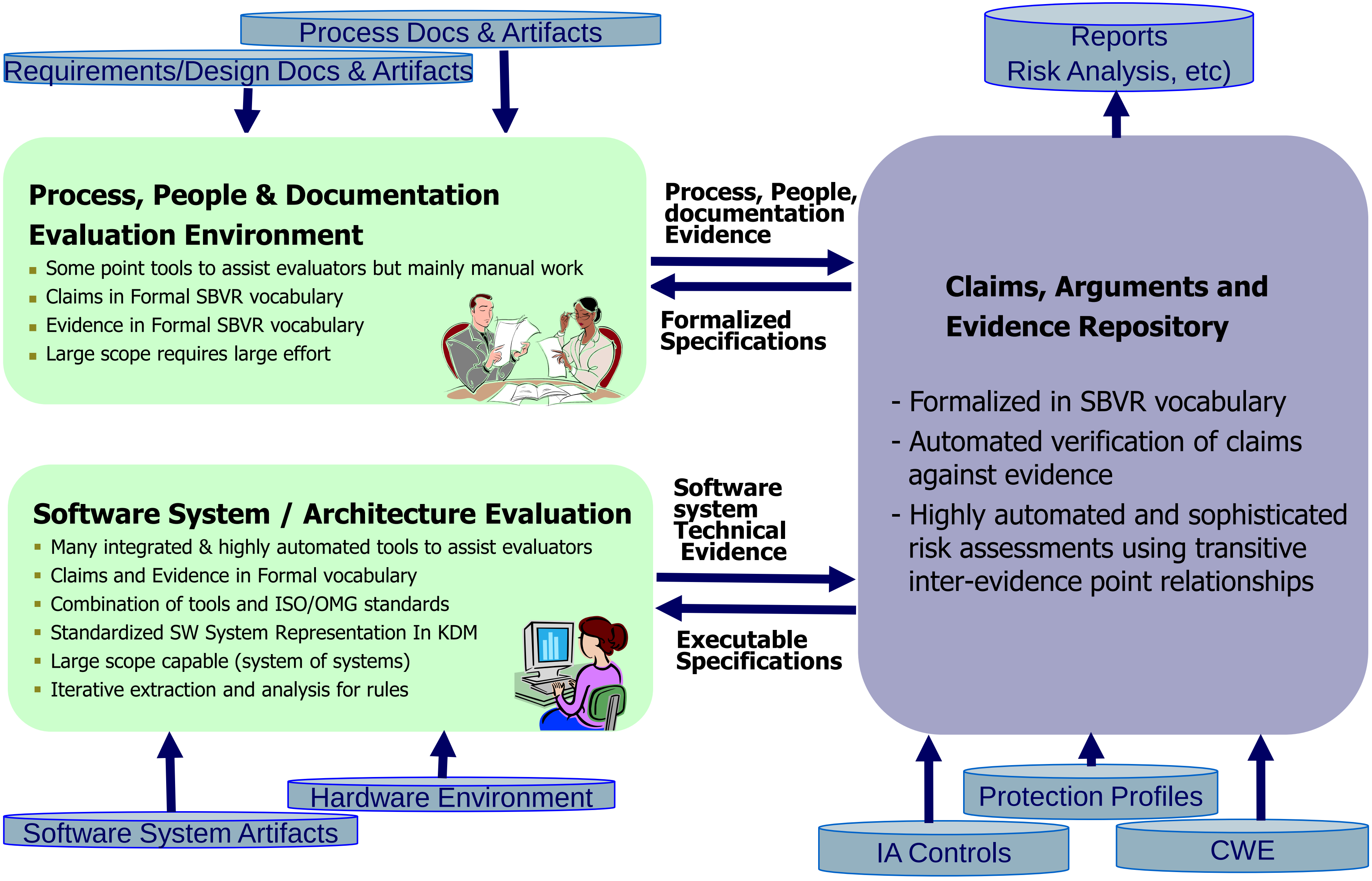
Measuring Cyber Security and Information Assurance

IATAC

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

Software Assurance Ecosystem: The Formal Framework

The value of formalization extends beyond software systems to include related software system process, people and documentation



Process Docs & Artifacts
Requirements/Design Docs & Artifacts
Reports
Risk Analysis, etc)
Process, People, documentation Evidence
Formalized Specifications
Software system Technical Evidence
Executable Specifications
Hardware Environment
Software System Artifacts
IA Controls
Protection Profiles
CWE

Process, People & Documentation Evaluation Environment

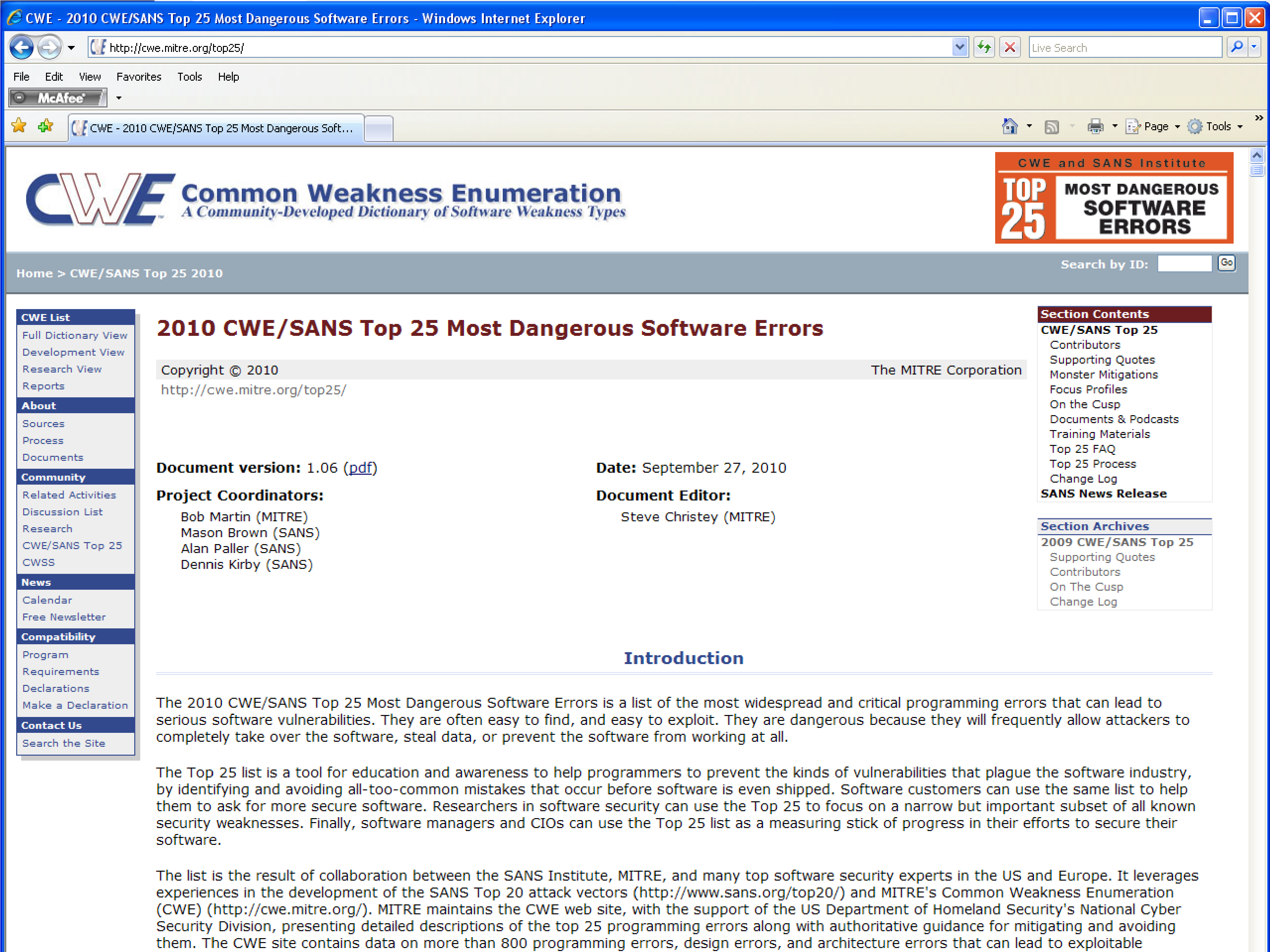
- Some point tools to assist evaluators but mainly manual work
- Claims in Formal SBVR vocabulary
- Evidence in Formal SBVR vocabulary
- Large scope requires large effort

Software System / Architecture Evaluation

- Many integrated & highly automated tools to assist evaluators
- Claims and Evidence in Formal vocabulary
- Combination of tools and ISO/OMG standards
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

Claims, Arguments and Evidence Repository

- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships



2010 CWE/SANS Top 25 Most Dangerous Software Errors

Copyright © 2010 The MITRE Corporation

http://cwe.mitre.org/top25/

Document version: 1.06 (pdf)

Date: September 27, 2010

Project Coordinators:

Bob Martin (MITRE)
Mason Brown (SANS)
Alan Paller (SANS)
Dennis Kirby (SANS)

Document Editor:

Steve Christey (MITRE)

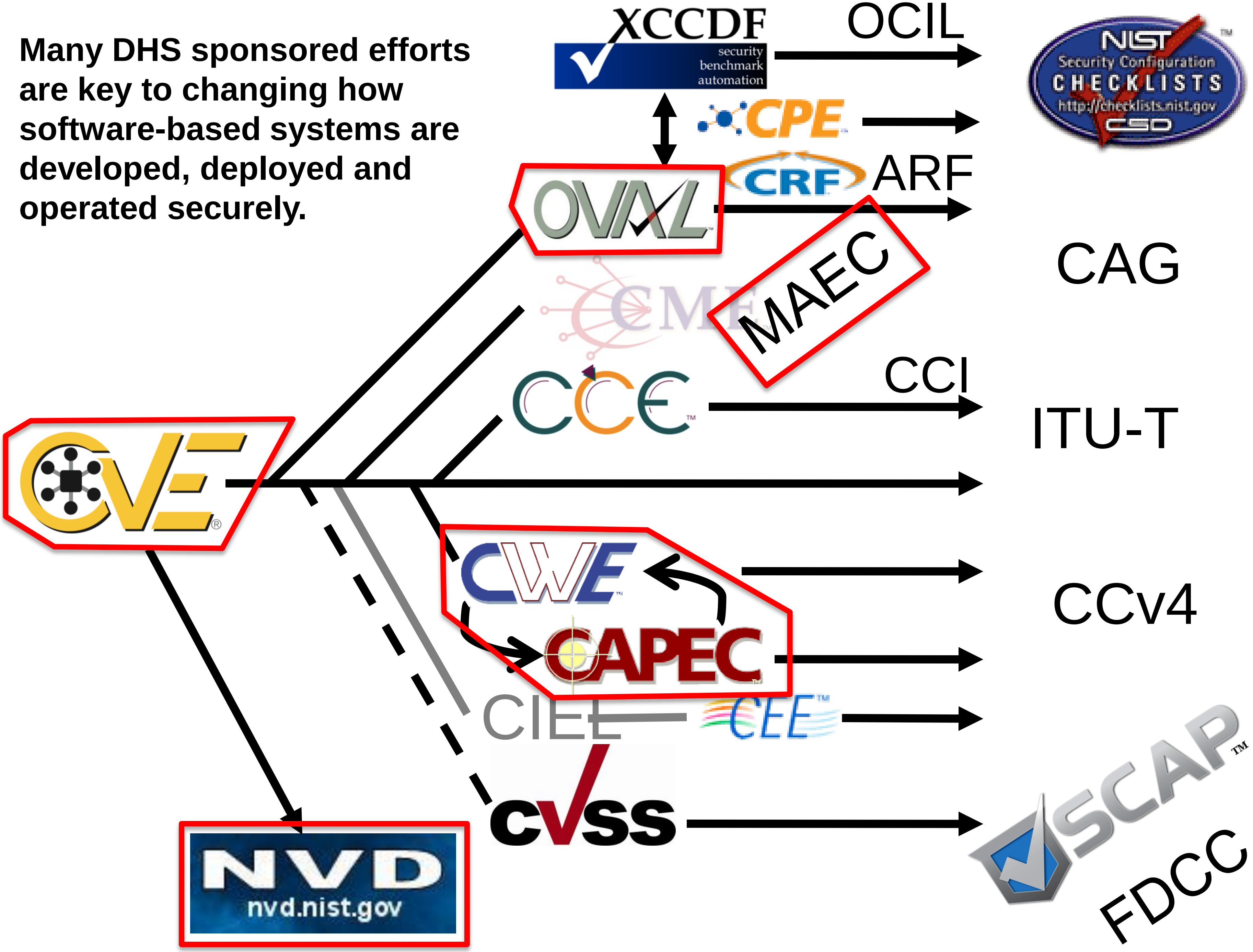
Introduction

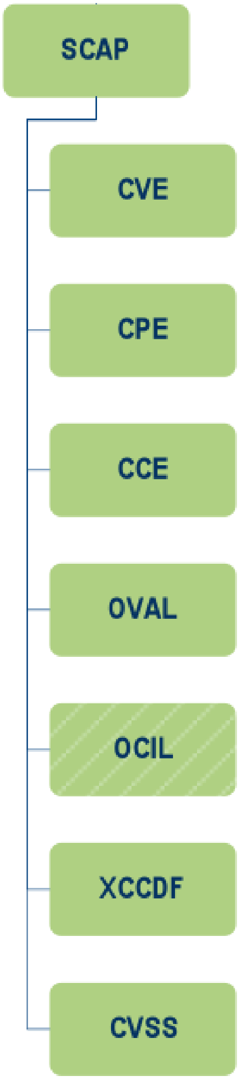
The 2010 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical programming errors that can lead to serious software vulnerabilities. They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

The Top 25 list is a tool for education and awareness to help programmers to prevent the kinds of vulnerabilities that plague the software industry, by identifying and avoiding all-too-common mistakes that occur before software is even shipped. Software customers can use the same list to help them to ask for more secure software. Researchers in software security can use the Top 25 to focus on a narrow but important subset of all known security weaknesses. Finally, software managers and CIOs can use the Top 25 list as a measuring stick of progress in their efforts to secure their software.

The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts in the US and Europe. It leverages experiences in the development of the SANS Top 20 attack vectors (http://www.sans.org/top20/) and MITRE's Common Weakness Enumeration (CWE) (http://cwe.mitre.org/). MITRE maintains the CWE web site, with the support of the US Department of Homeland Security's National Cyber Security Division, presenting detailed descriptions of the top 25 programming errors along with authoritative guidance for mitigating and avoiding them. The CWE site contains data on more than 800 programming errors, design errors, and architecture errors that can lead to exploitable

Many DHS sponsored efforts are key to changing how software-based systems are developed, deployed and operated securely.


XCCDF
security benchmark automation
OCIL
NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD
CPE
CRF
ARF
OVAL
MAEC
CAG
CME
CCI
CCE
ITU-T
CVE
CWE
CAPEC
CCv4
CIEL
CEE
CVSS
SCAP
FDCC
NVD
nvd.nist.gov


SCAP

CVE

CPE

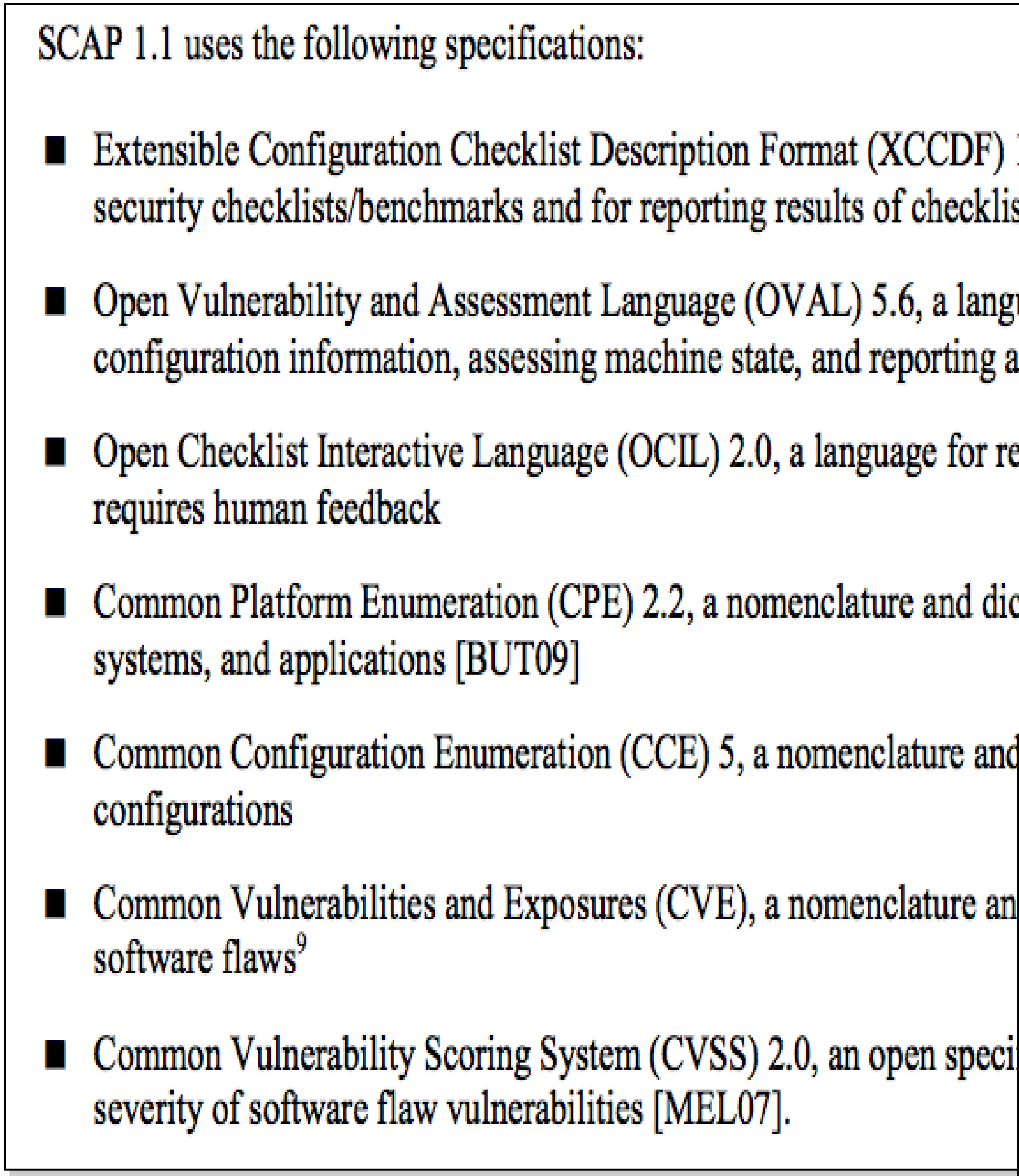
CCE

OVAL

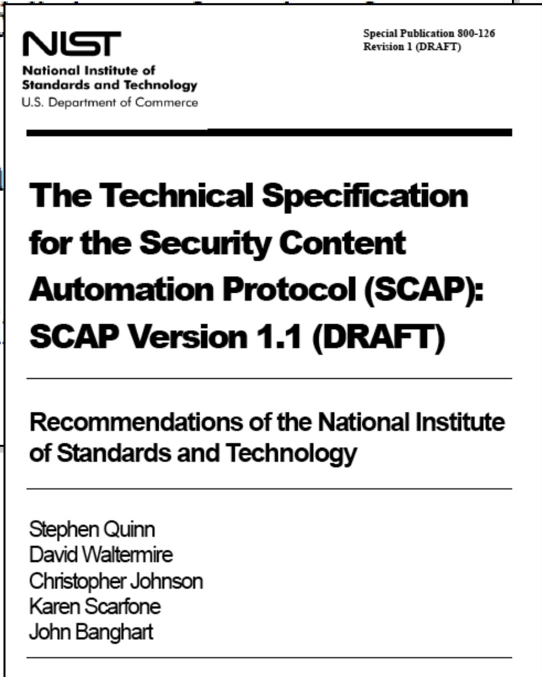
OCIL

XCCDF

CVSS


SCAP 1.1 uses the following specifications:

- Extensible Configuration Checklist Description Format (XCCDF) 1.1.4, a language for authoring security checklists/benchmarks and for reporting results of checklist evaluation [QUI08]
- Open Vulnerability and Assessment Language (OVAL) 5.6, a language for representing system configuration information, assessing machine state, and reporting assessment results
- Open Checklist Interactive Language (OCIL) 2.0, a language for representing security checks that requires human feedback
- Common Platform Enumeration (CPE) 2.2, a nomenclature and dictionary of hardware, operating systems, and applications [BUT09]
- Common Configuration Enumeration (CCE) 5, a nomenclature and
configurations
- Common Vulnerabilities and Exposures (CVE), a nomenclature an
software flaws[9]
- Common Vulnerability Scoring System (CVSS) 2.0, an open speci
severity of software flaw vulnerabilities [MEL07].

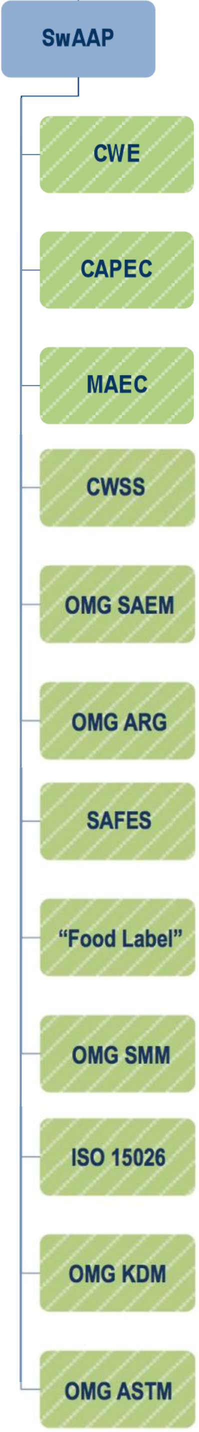

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-126
Revision 1 (DRAFT)

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1 (DRAFT)

Recommendations of the National Institute of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart



SwAAP

CWE

CAPEC

MAEC

CWSS

OMG SAEM

OMG ARG

SAFES

"Food Label"

OMG SMM

ISO 15026

OMG KDM

OMG ASTM

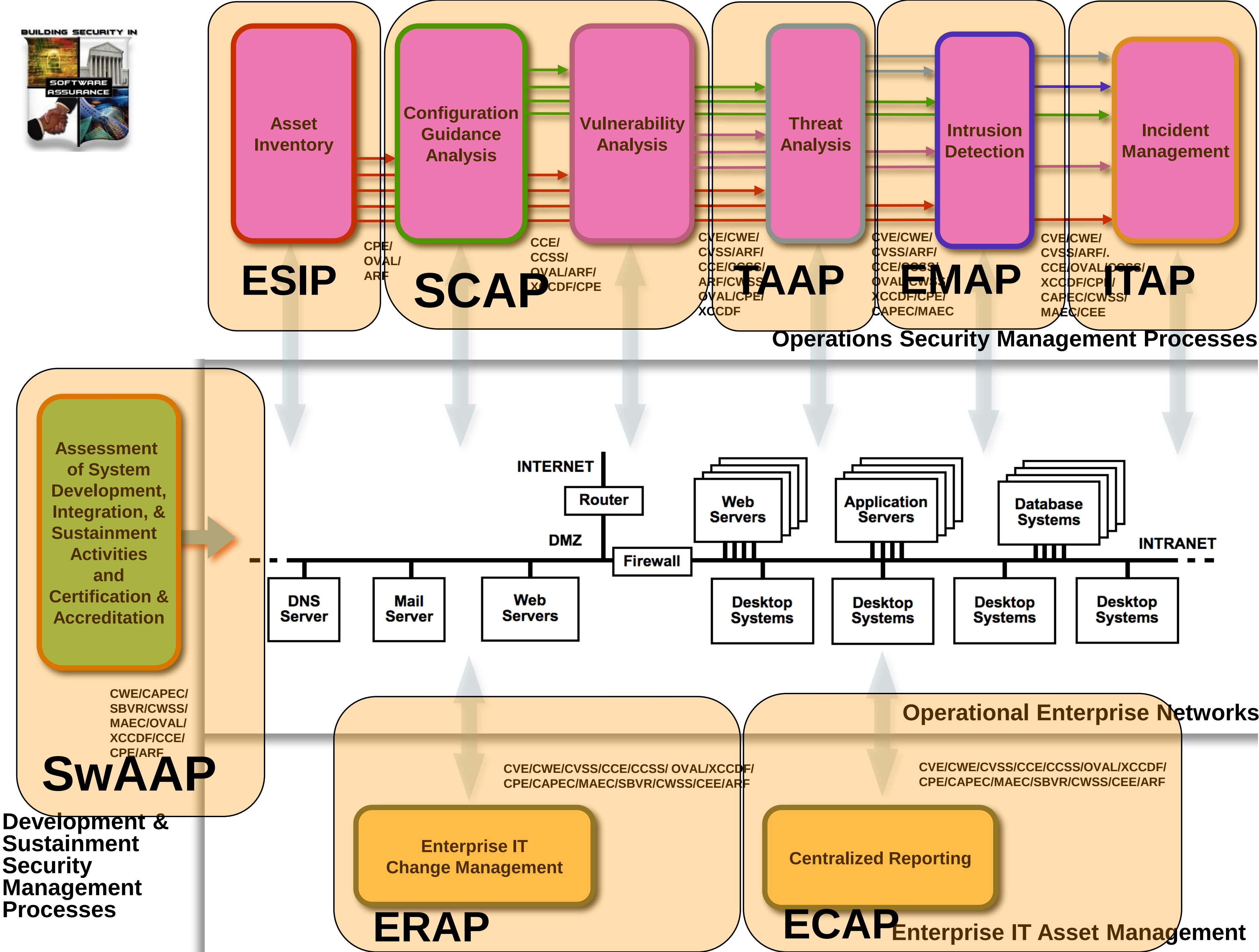
Software Assurance Automation Protocol (SwAAP)

- For measuring & enumerating software weaknesses and the assurance cases.

Common Weakness Enumeration (CWE),
Common Attack Pattern Enumeration & Classification (CAPEC),
Malware Attribute Enumeration & Characterization (MAEC),
Common Weakness Scoring System (CWSS),
Software Assurance Findings Expression Schema (SAFES),
NIST SAMATE's "Software Transparency Label",
ISO/IEC 15026 "Assurance Case" (ISO 15026),
OMG Software Assurance Evidence Metamodel (OMG SAEM),
OMG Argumentation Metamodel (OMG ARG),
OMG Structured Metrics Metamodel (OMG SMM),
OMG Knowledge Discovery Metamodel (OMG KDM),
OMG Abstract Syntax Tree Metamodel (OMG ASTM)

- plus SCAP to capture "accredited" system CPEs and CCE settings?
- OVAL checks for capturing "finger print" of software applications to address supply-chain risk measurement?

BUILDING SECURITY IN
SOFTWARE ASSURANCE



Asset Inventory

ESIP

CPE/
OVAL/
ARF

Configuration Guidance Analysis

Vulnerability Analysis

SCAP

CCE/
CCSS/
OVAL/ARF/
XCCDF/CPE

Threat Analysis

TAAP

CVE/CWE/
CVSS/ARF/
CCE/CCSS/
ARF/CWSS/
OVAL/CPE/
XCCDF

Intrusion Detection

EMAP

CVE/CWE/
CVSS/ARF/
CCE/CCSS/
OVAL/CWSS/
XCCDF/CPE/
CAPEC/MAEC

Incident Management

ITAP

CVE/CWE/
CVSS/ARF/.
CCE/OVAL/CCSS/
XCCDF/CPE/
CAPEC/CWSS/
MAEC/CEE

Operations Security Management Processes

Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/ARF

SwAAP

Development & Sustainment Security Management Processes

INTERNET

Router

DMZ

Firewall

INTRANET

DNS Server

Mail Server

Web Servers

Web Servers

Application Servers

Database Systems

Desktop Systems

Desktop Systems

Desktop Systems

Desktop Systems

Operational Enterprise Networks

CVE/CWE/CVSS/CCE/CCSS/ OVAL/XCCDF/
CPE/CAPEC/MAEC/SBVR/CWSS/CEE/ARF

Enterprise IT Change Management

ERAP

CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/SBVR/CWSS/CEE/ARF

Centralized Reporting

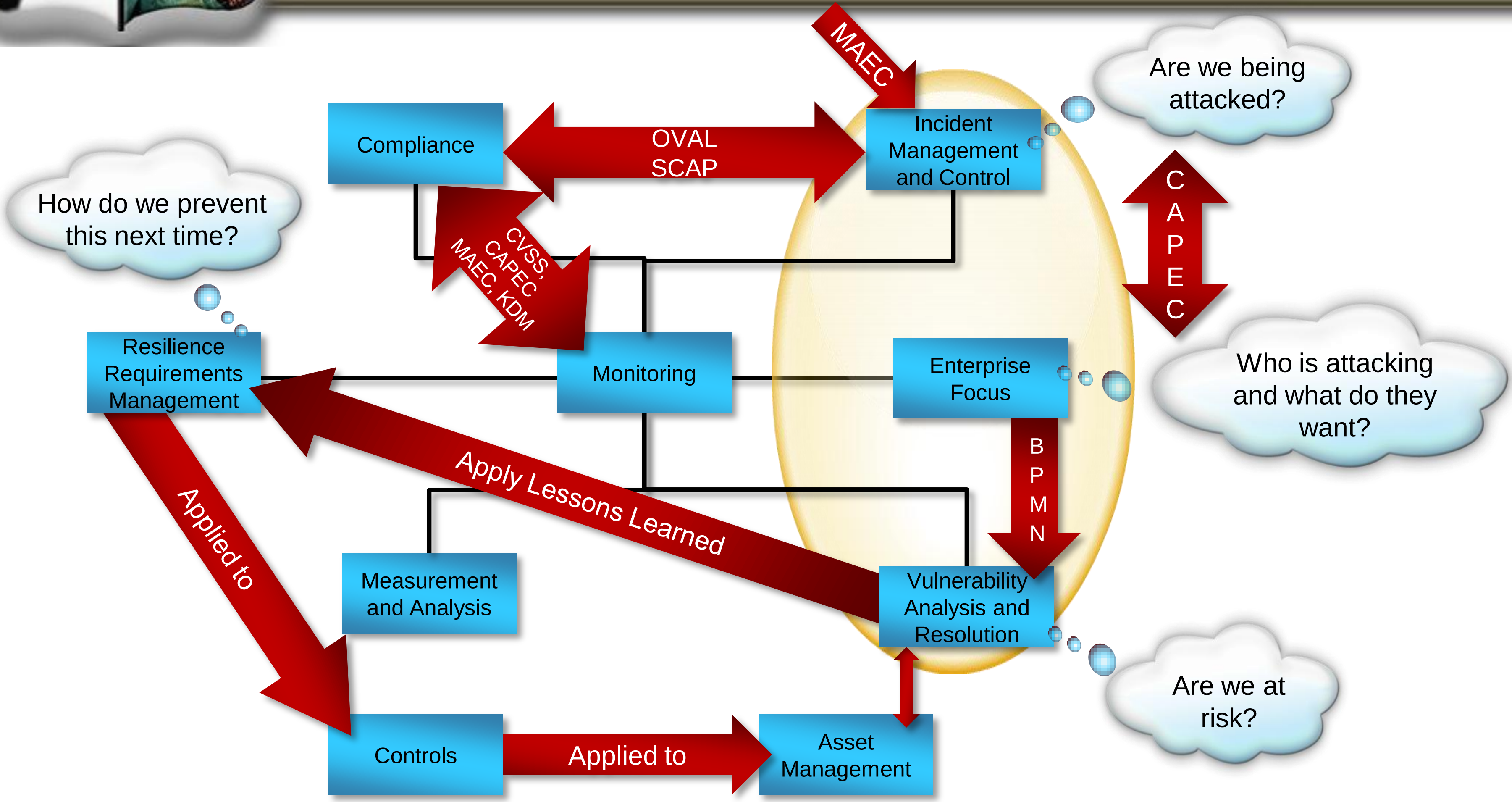
ECAP

Enterprise IT Asset Management

SOFTWARE ASSURANCE FORUM

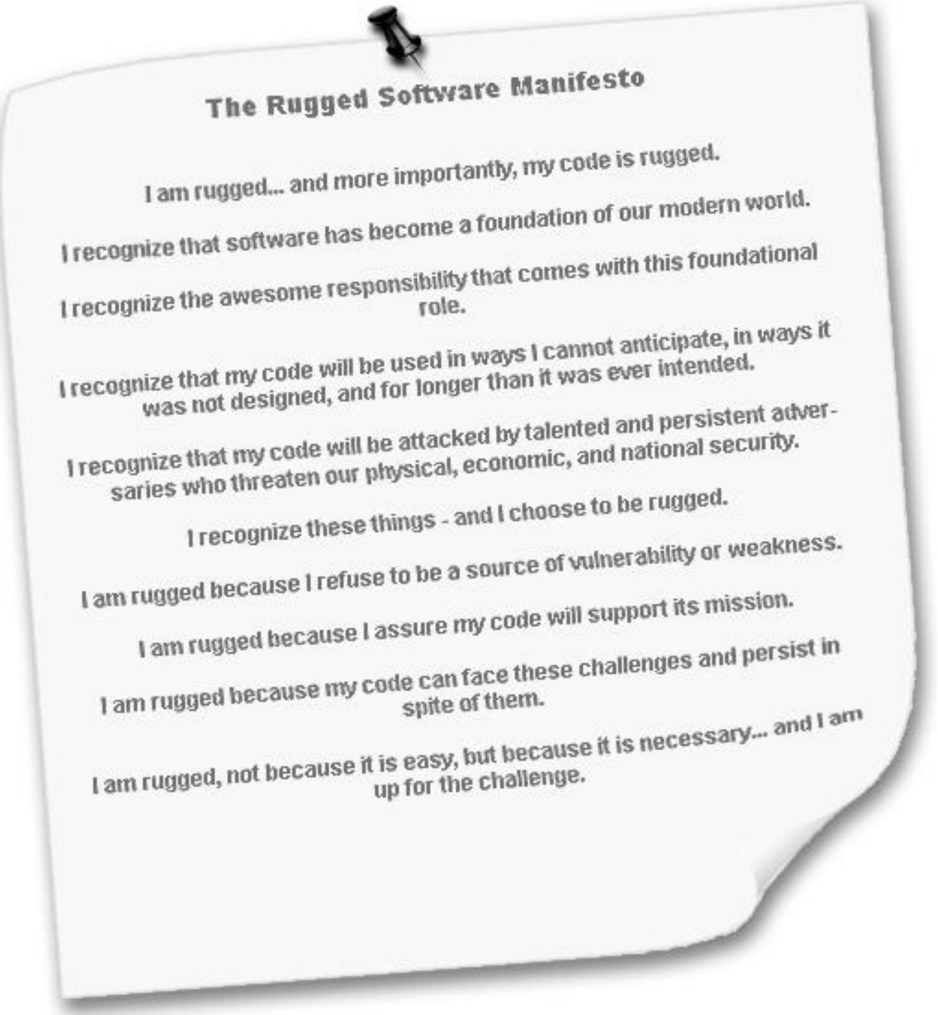
BUILDING SECURITY IN

SwA and Operational Resilience



Adapted from September 2010 SwA Forum, CERT RMM for Assurance , Lisa Young, SEI

Courtesy of Michele Moss



The Rugged Software Manifesto

I am rugged... and more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary... and I am up for the challenge.

The Rugged Software MANIFESTO

Focus on Resilience and Survivability - If compromised, damage to the software will be minimized, and it will recover quickly to an acceptable level of operating capacity; it is ‘rugged’

ruggedsoftware.org

I am rugged - and more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be rugged.

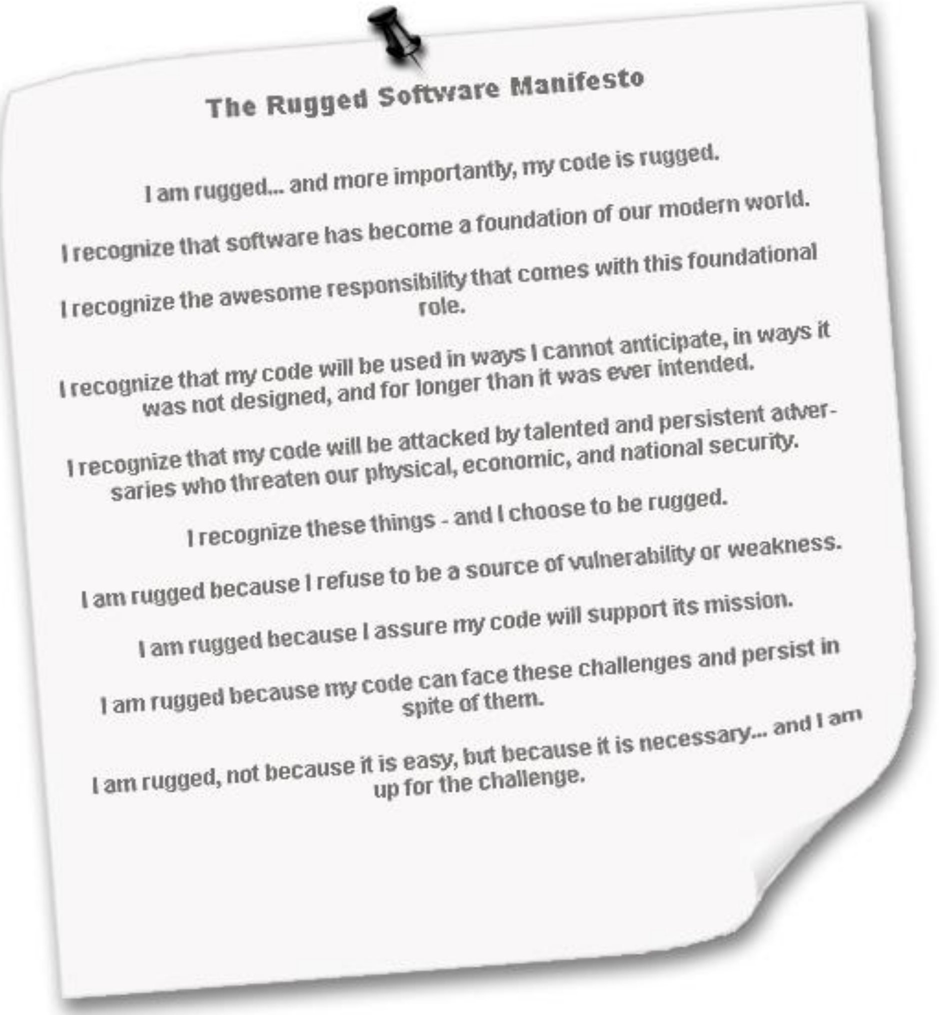
I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary… and I am up for the challenge.

Rugged?



The Rugged Software Manifesto

I am rugged... and more importantly, my code is rugged.

I recognize that software has become a foundation of our modern world.

I recognize the awesome responsibility that comes with this foundational role.

I recognize that my code will be used in ways I cannot anticipate, in ways it was not designed, and for longer than it was ever intended.

I recognize that my code will be attacked by talented and persistent adversaries who threaten our physical, economic, and national security.

I recognize these things - and I choose to be rugged.

I am rugged because I refuse to be a source of vulnerability or weakness.

I am rugged because I assure my code will support its mission.

I am rugged because my code can face these challenges and persist in spite of them.

I am rugged, not because it is easy, but because it is necessary... and I am up for the challenge.

ruggedsoftware.org

IT/Software Supply Chain Management is a National Security & Economic Issue

- Adversaries can gain “intimate access” to target systems, especially in a global supply chain that offers limited transparency
- Advances in science and technology will always outpace the ability of government and industry to react with new policies and standards
  - National security policies must conform with international laws and agreements while preserving a nation’s rights and freedoms, and protecting a nation’s self interests and economic goals
  - Forward-looking policies can adapt to the new world of global supply chains
  - International standards must mature to better address supply chain risk management, IT security, systems & software assurance
  - Assurance Rating Schemes for software products and organizations are needed
- IT/software suppliers and buyers can take more deliberate actions to security-enhance their processes and practices to mitigate risks
  - Government & Industry have significant leadership roles in solving this
  - Individuals can influence the way their organizations adopt security practices

Globalization will not be reversed; this is how we conduct business – To remain relevant, standards and capability benchmarking measures must address “assurance” mechanisms needed to manage IT/Software Supply Chain risks.

Next SwA Working Groups 14-16 Dec 2010 at MITRE, McLean, VA

BUILDING SECURITY IN
SOFTWARE ASSURANCE

SOFTWARE ASSURANCE FORUM

“Building Security In”

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

Joe Jarzombek, PMP, CSSLP
Director for Software Assurance
National Cyber Security Division
Department of Homeland Security
Joe.Jarzombek@dhs.gov
(703) 235-5126
LinkedIn SwA Mega-Community

Homeland Security

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Homeland Security

Commerce

National Defense

Next SwA Working Group Sessions 14-16 Dec 2010 at MITRE, McLean, VA