Software Assurance:

Measurably Enhancing the Resilience of Software-Reliant Systems

BUILDING SECURITY IN

SOFTWARE ASSURANCE

July 13, 2011

Homeland Security

Joe Jarzombek, PMP, CSSLP
Director for Software Assurance
National Cyber Security Division

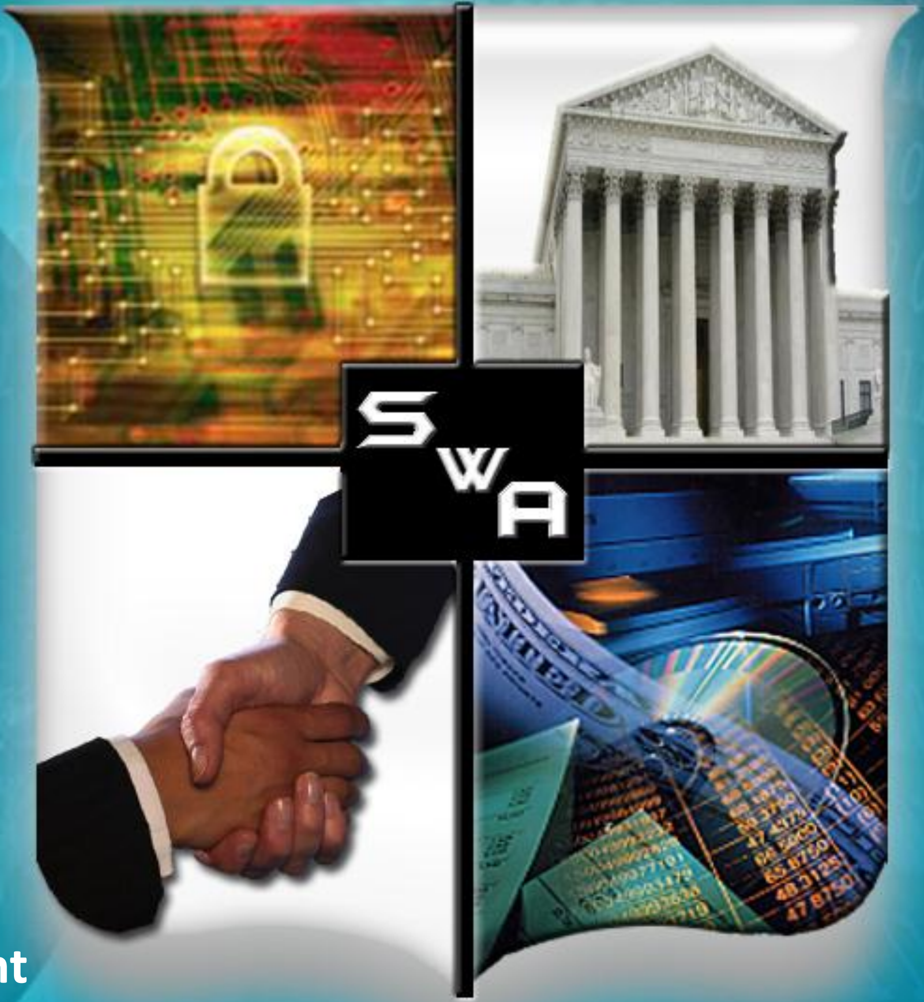
SOFTWARE ASSURANCE FORUM

Homeland Security

Commerce

National Defense

BUILDING SECURITY IN



Public/Private Collaboration Efforts for Software Supply Chain Risk Management

Next SwA Forum meets 12-16 Sep 2011 at SEI, Arlington, VA

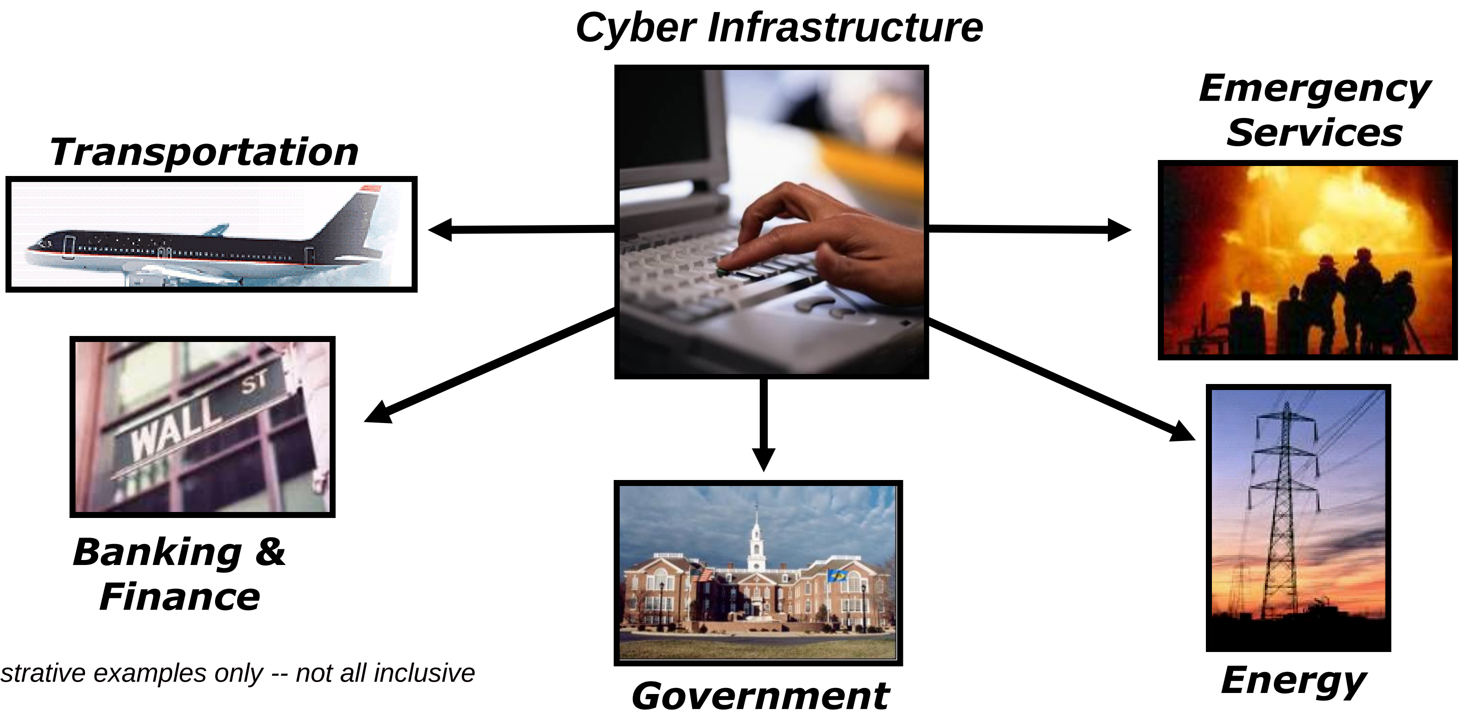
Interdependencies Between Physical & Cyber Infrastructures Requires Convergence of Safety, Security and Dependability

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

High Reliability and Human Safety Critical Software

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



Cyber Infrastructure

Transportation

Emergency Services

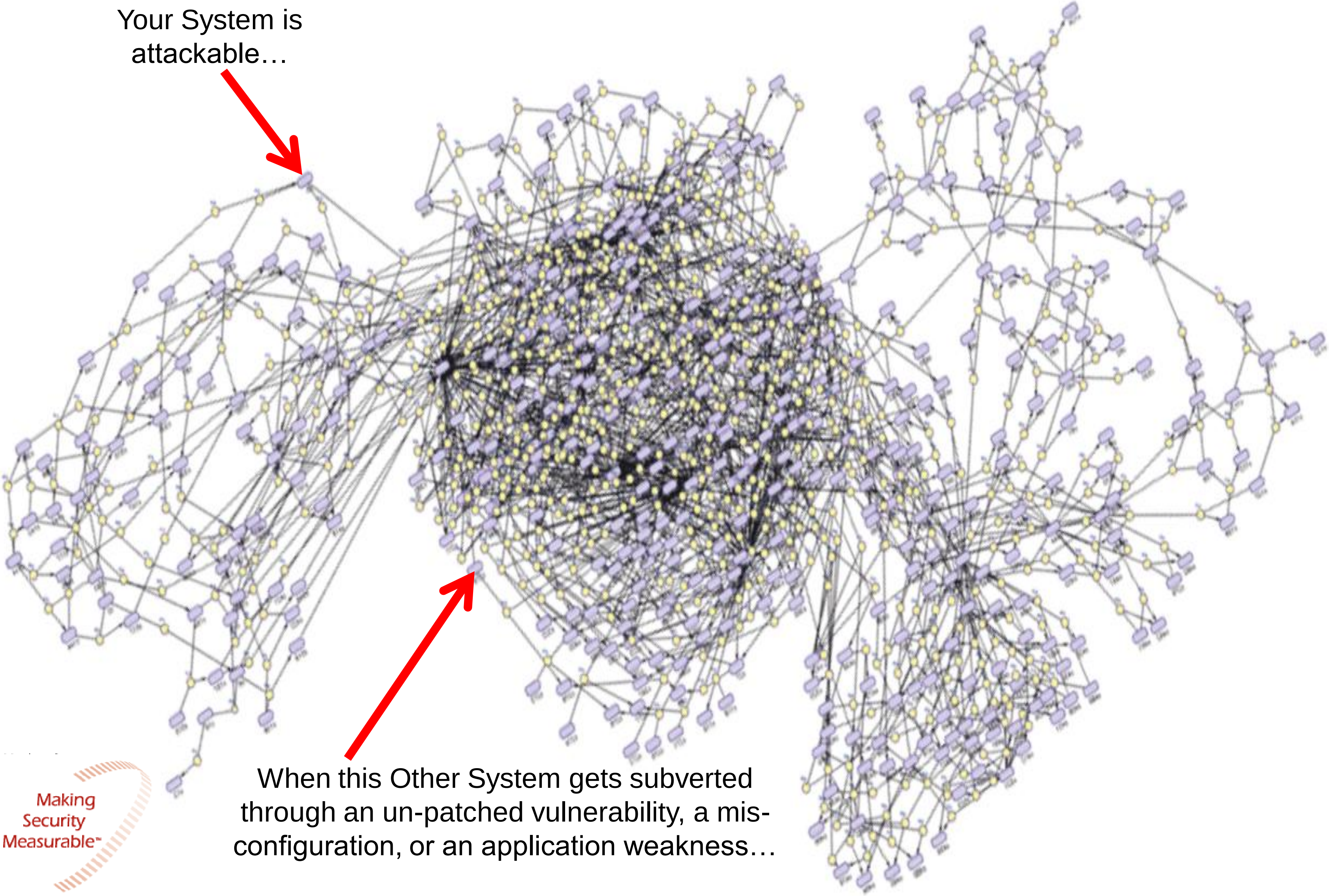
Banking & Finance

Government

Energy

Illustrative examples only -- not all inclusive

Today Everything's Connected



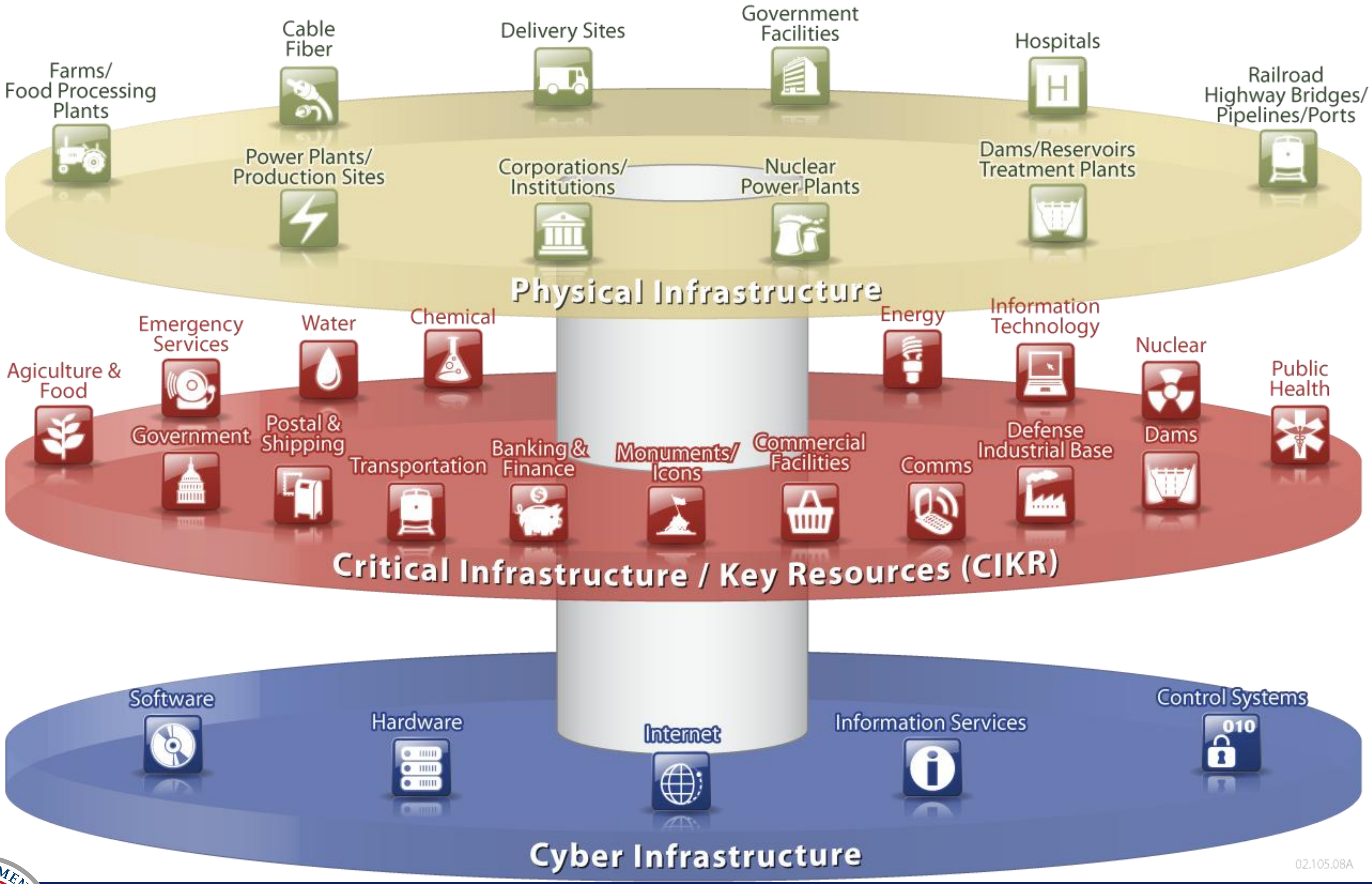
Your System is attackable…

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

Making Security Measurable™

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

-- Need for secure software applications



Software Security Assurance: Not just a good idea

- Many people responsible for protecting most critical infrastructure facilities have felt comfortable about security of their systems.
  - Facilities rely on industrial control systems (ICS) -- custom-built suites of systems that control essential mechanical functions of power grids, processing plants, etc -- usually not connected to the Internet, also known as "air-gapped."
  - Many industry owners, operators and regulators believed that this security model provided an infallible, invulnerable barrier to malicious cyber attacks from criminals and advanced persistent threat (APT) adversaries.

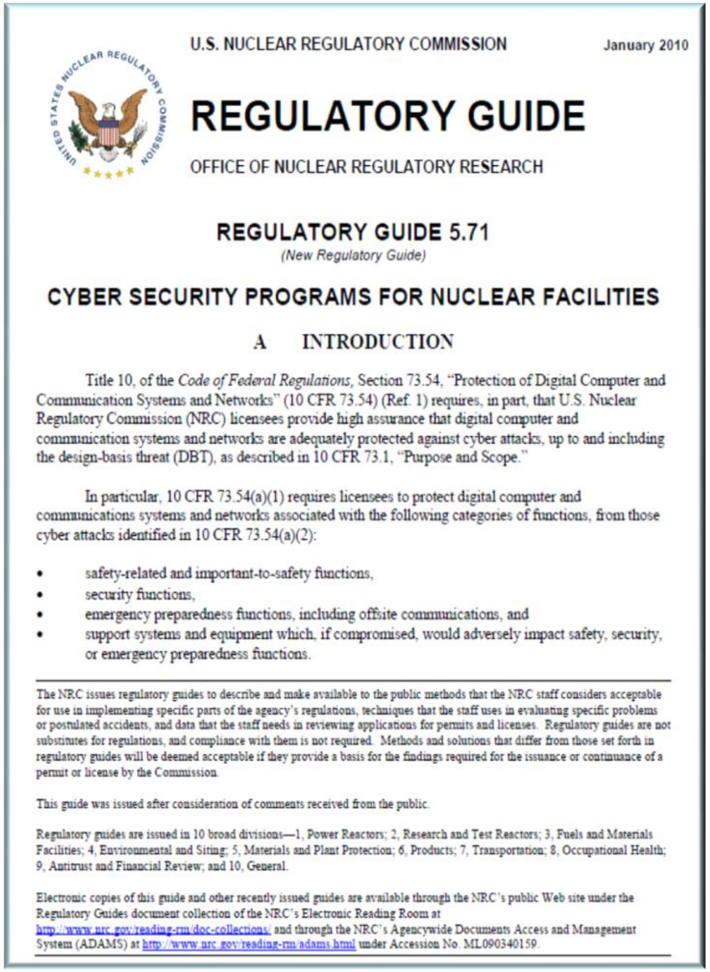
- National Defense Authorization Act (NDAA) -- which included a focus on software security (in Section 932, Strategy on Computer Software Assurance) -- serves as first cybersecurity law of 2011 and requires the U.S. Dept of Defense to develop a strategy for ensuring the security of software applications.

- Software Security Assurance, a set of practices for ensuring proactive application security, is key to making applications compliant with this new law.

"How Stuxnet Demonstrates That Software Assurance Equals Mission Assurance:
The rules of the game have changed," by Rob Roy, Federal CTO of Fortify, an HP Company

NRC Regulatory Guidance on Cyber Security

- NRC Regulatory Guide 5.71, “Cyber Security Programs for Nuclear Facilities,” Section C.12 in Appendix C, “System and Service Acquisition”
  - Directly relates to current NRC guidance on cyber security in the supply chain and SDLC of an ICS regulated by the agency.
  - Section C.12.2 “Supply Chain Protection” control drill down to the vendor level with requirements accountability for the RG 5.71 control baseline (Appendices B&C).
  - Section C.12.3 “Trustworthiness” requires developers employ software quality and validation methods to minimize flawed or malformed software; requires all tools to undergo commercial certification process
  - Section C.12.5 “Developer Security Testing”



U.S. NUCLEAR REGULATORY COMMISSION January 2010

REGULATORY GUIDE

OFFICE OF NUCLEAR REGULATORY RESEARCH

REGULATORY GUIDE 5.71

(New Regulatory Guide)

CYBER SECURITY PROGRAMS FOR NUCLEAR FACILITIES

A INTRODUCTION

Title 10, of the *Code of Federal Regulations,* Section 73.54, “Protection of Digital Computer and Communication Systems and Networks” (10 CFR 73.54) (Ref. 1) requires, in part, that U.S. Nuclear Regulatory Commission (NRC) licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat (DBT), as described in 10 CFR 73.1, “Purpose and Scope.”

In particular, 10 CFR 73.54(a)(1) requires licensees to protect digital computer and communications systems and networks associated with the following categories of functions, from those cyber attacks identified in 10 CFR 73.54(a)(2):

- safety-related and important-to-safety functions,
- security functions,
- emergency preparedness functions, including offsite communications, and
- support systems and equipment which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

The NRC issues regulatory guides to describe and make available to the public methods that the NRC staff considers acceptable for use in implementing specific parts of the agency’s regulations, techniques that the staff uses in evaluating specific problems or postulated accidents, and data that the staff needs in reviewing applications for permits and licenses. Regulatory guides are not substitutes for regulations, and compliance with them is not required. Methods and solutions that differ from those set forth in regulatory guides will be deemed acceptable if they provide a basis for the findings required for the issuance or continuance of a permit or license by the Commission.

This guide was issued after consideration of comments received from the public.

Regulatory guides are issued in 10 broad divisions—1, Power Reactors; 2, Research and Test Reactors; 3, Fuels and Materials Facilities; 4, Environmental and Siting; 5, Materials and Plant Protection; 6, Products; 7, Transportation; 8, Occupational Health; 9, Antitrust and Financial Review; and 10, General.

Electronic copies of this guide and other recently issued guides are available through the NRC’s public Web site under the Regulatory Guides document collection of the NRC’s Electronic Reading Room at http://www.nrc.gov/reading-rm/doc-collections/ and through the NRC’s Agencywide Documents Access and Management System (ADAMS) at http://www.nrc.gov/reading-rm/adams.html under Accession No. ML090340159.

See NRC Regulatory Guidance on Cyber Security http://pbadupws.nrc.gov/docs/ML0903/ML090340159.pdf

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.

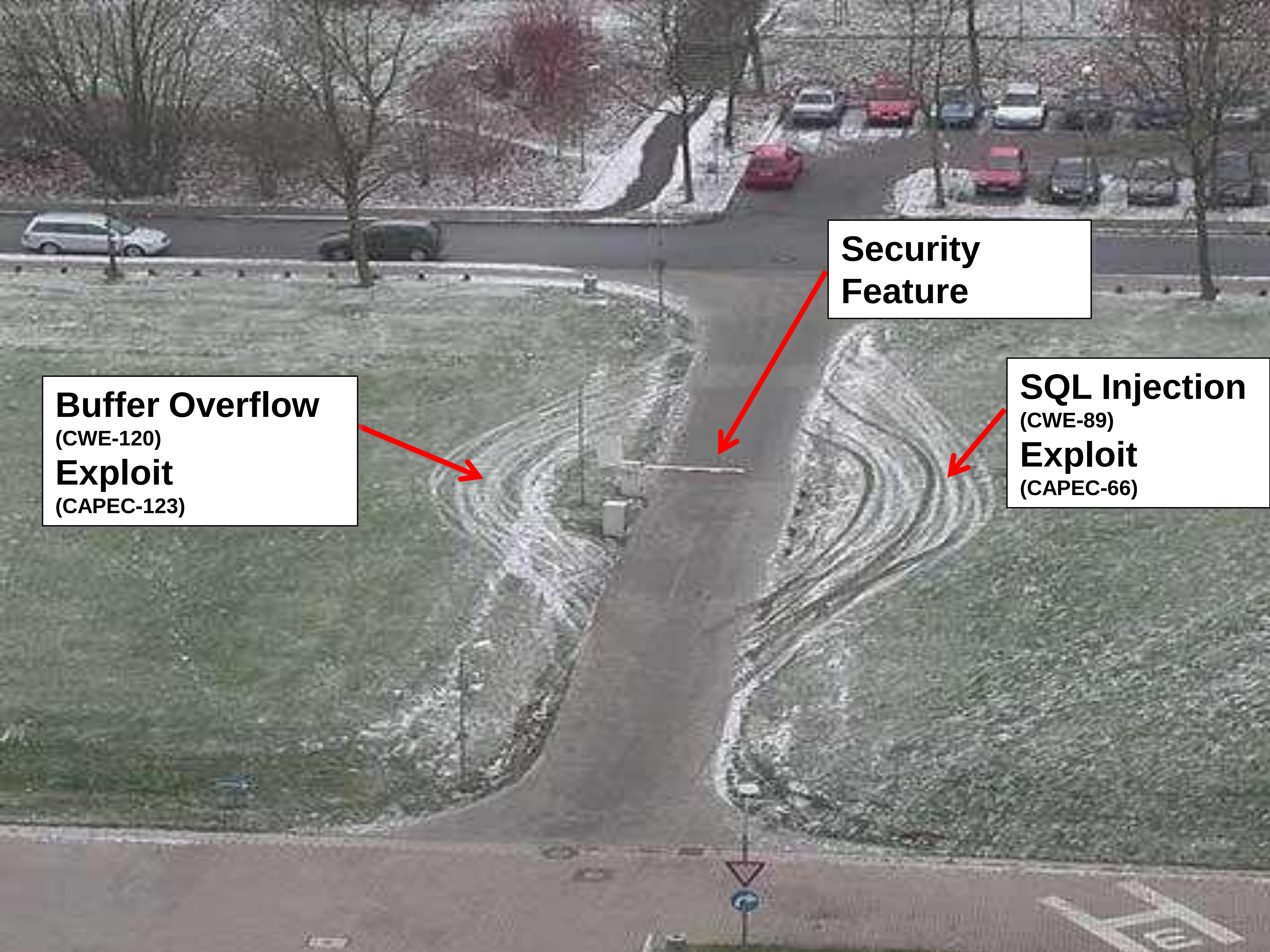
One who knows neither the enemy nor himself will invariably be defeated in every engagement.

- **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



Security Feature

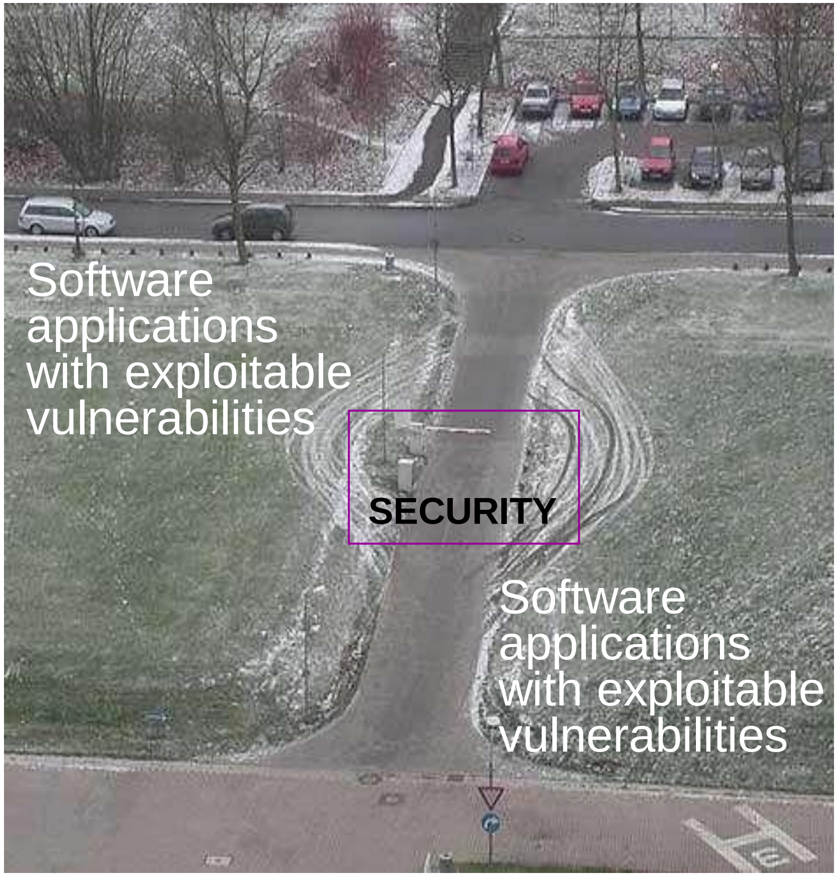
Buffer Overflow
(CWE-120)
Exploit
(CAPEC-123)

SQL Injection
(CWE-89)
Exploit
(CAPEC-66)

If the weaknesses in software were as easy to spot and their impact as obvious as…

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

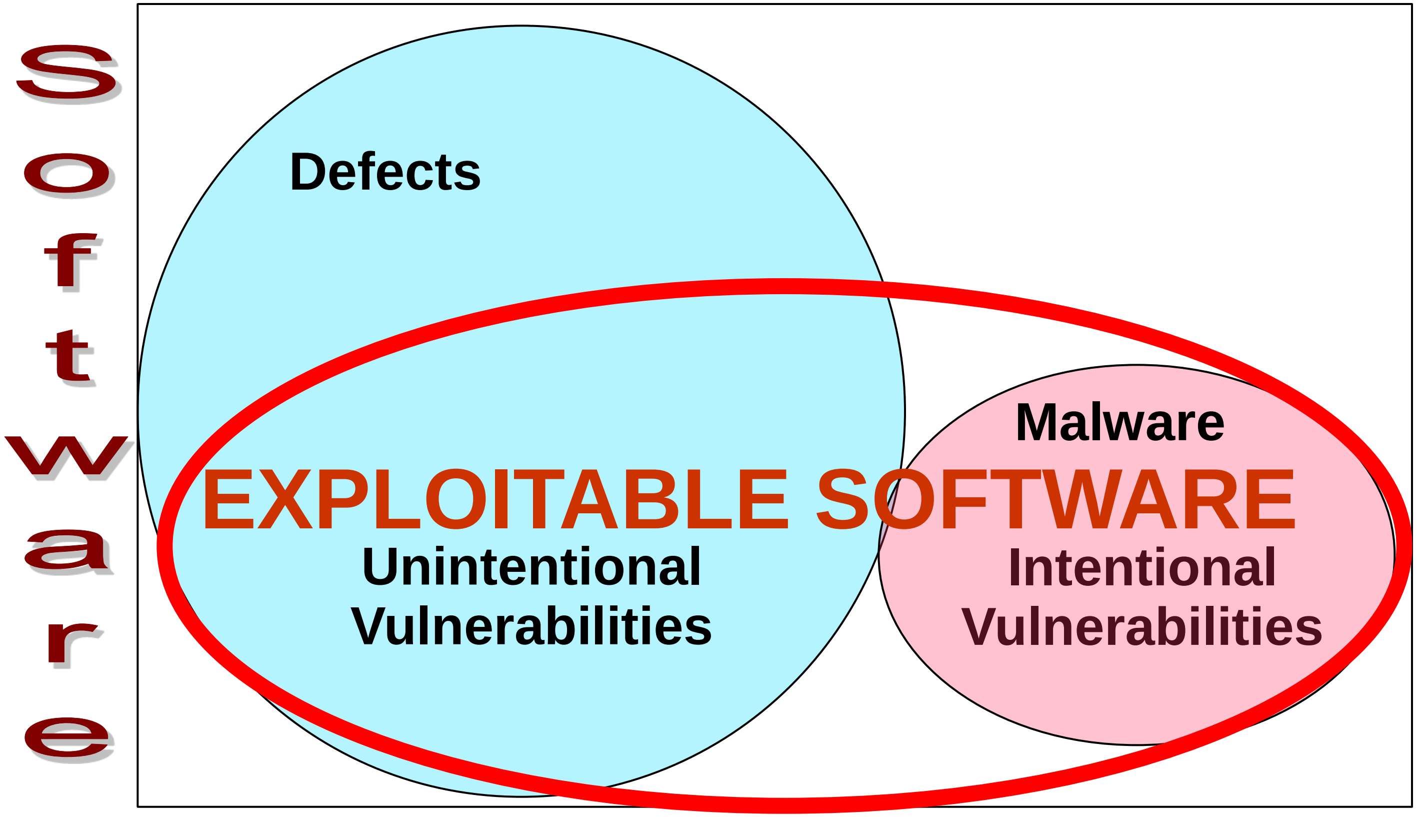
- Dramatic increase in mission risk due to increasing:
  - Software dependence and system interdependence (weakest link syndrome)
  - Software Size & Complexity (obscures intent and precludes exhaustive test)
  - Outsourcing and use of un-vetted software supply chain (COTS & custom)
  - Attack sophistication (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

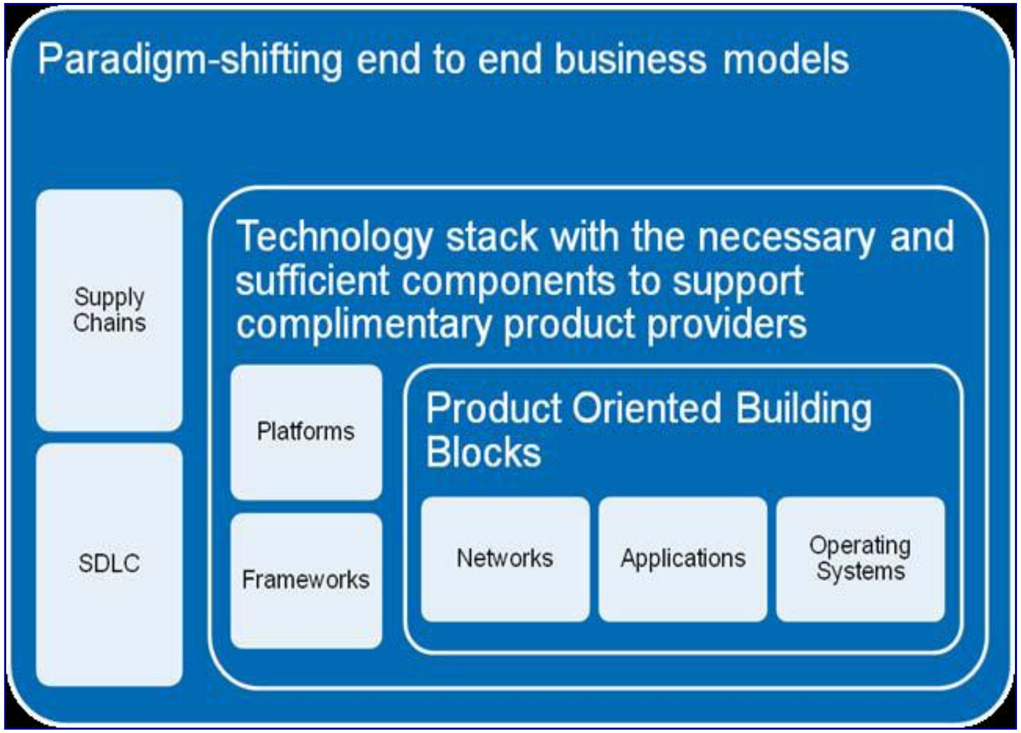
Note: Chart is not to scale – notional representation -- for discussions

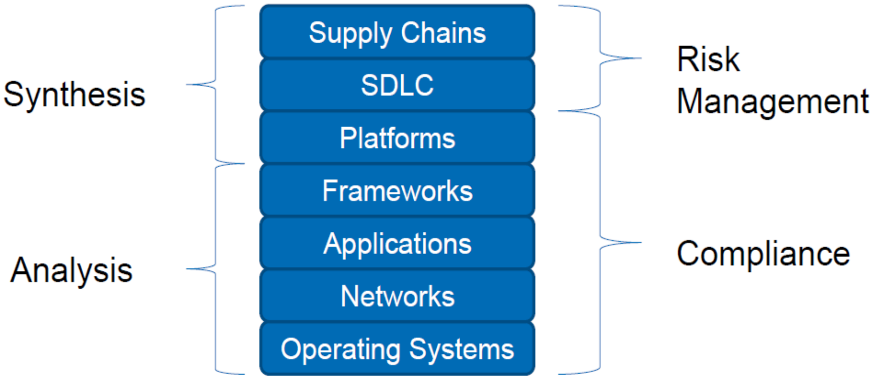
IT/software security risk landscape is a convergence between "defense in depth" and "defense in breadth"

Enterprise Risk Management and Governance are security motivators

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

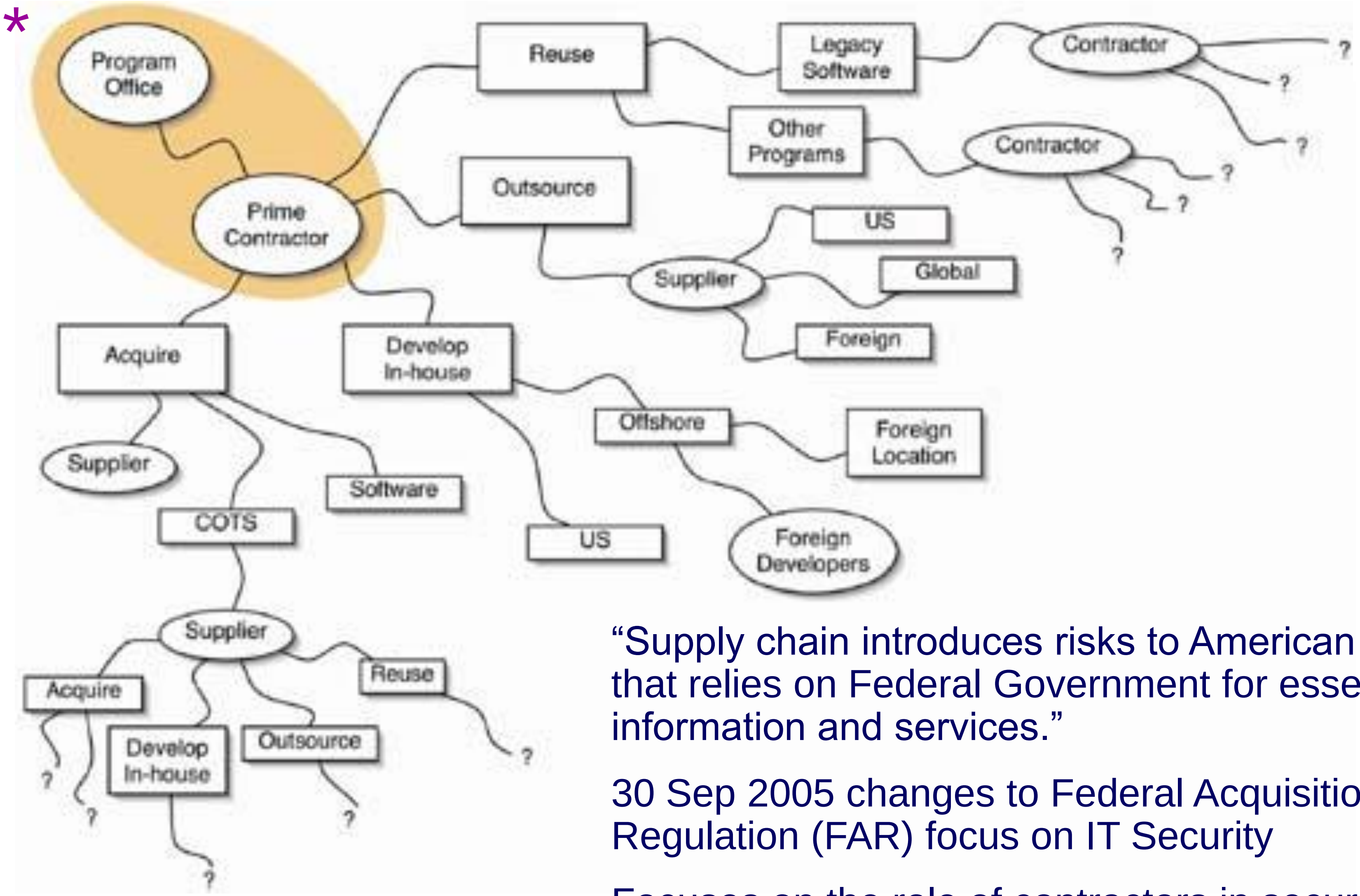
> "In the digital age, sovereignty is demarcated not by territorial frontiers but by supply chains."
>
> – Dan Geer, CISO In-Q-Tel


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



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

*



“Supply chain introduces risks to American society that relies on Federal Government for essential information and services.”

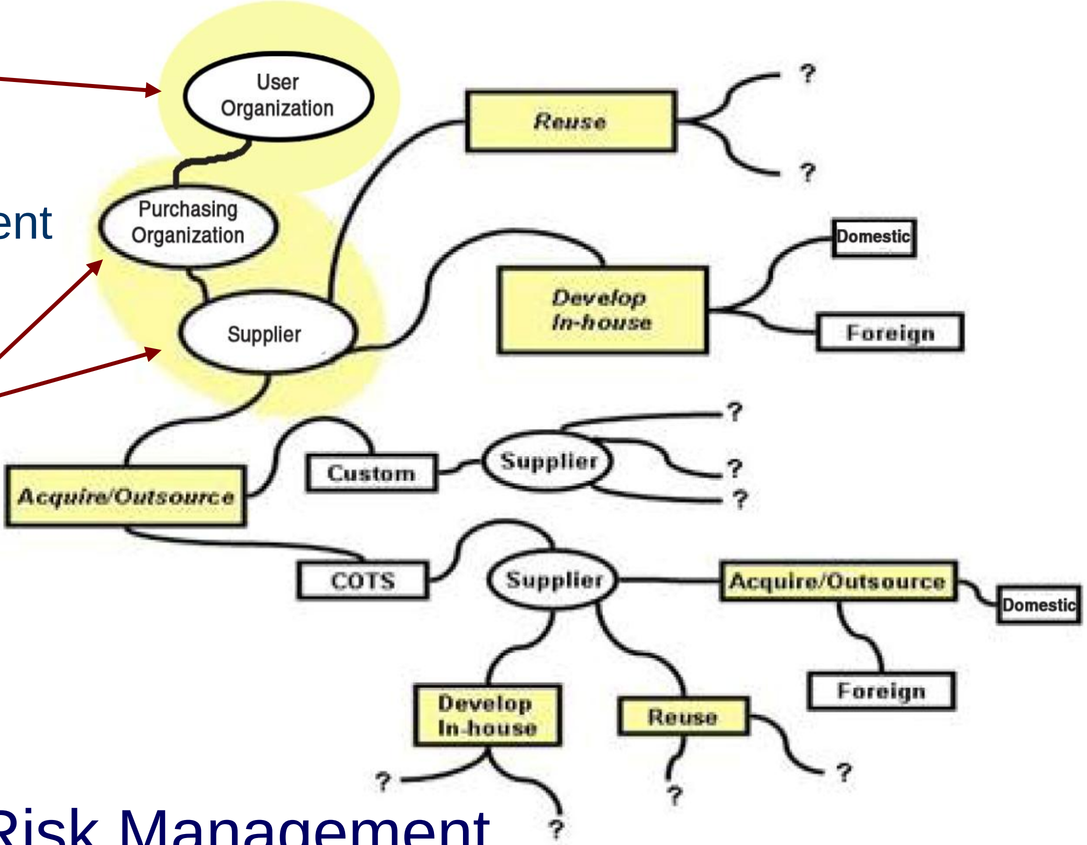
30 Sep 2005 changes to Federal Acquisition Regulation (FAR) focus on IT Security

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”

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

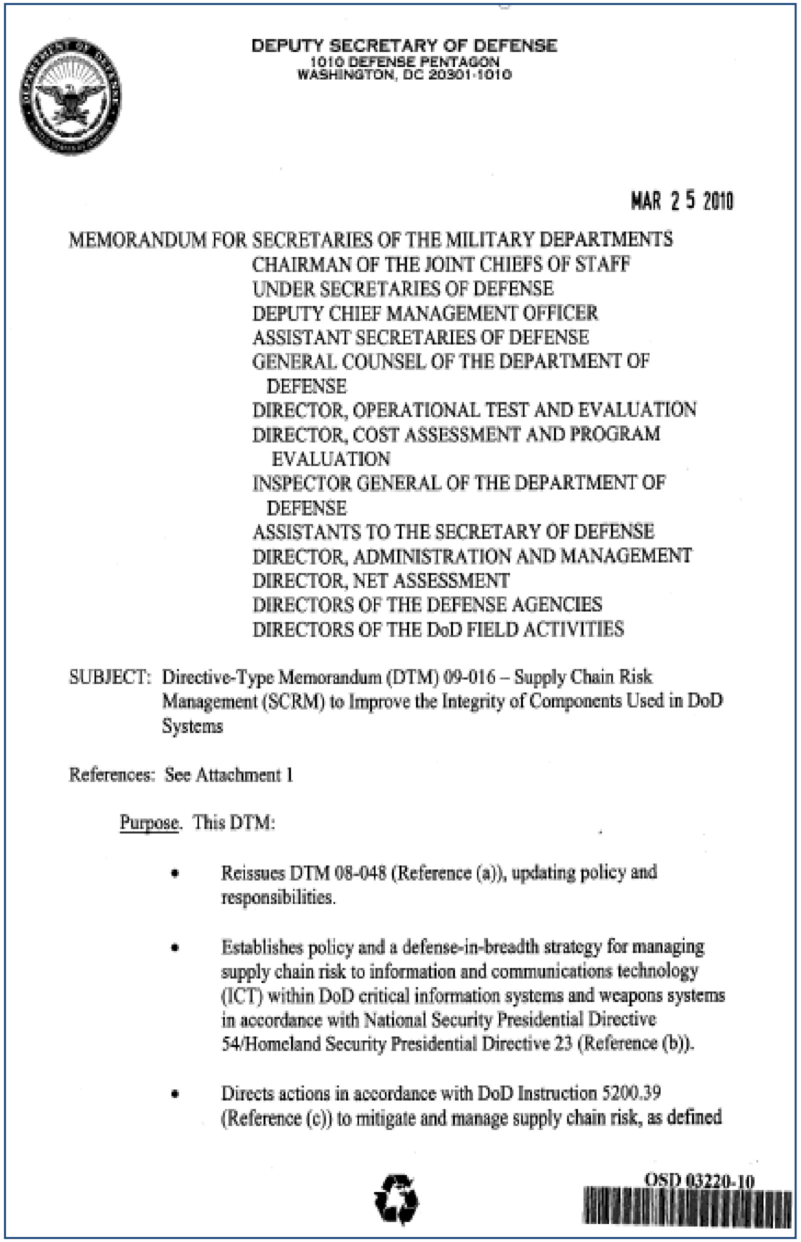
25 Mar 2010 DoD Directive-Type Memorandum (DTM) 09-016 – Supply Chain Risk Management to Improve the Integrity of Components Used in DoD Systems

Policy. It is DoD policy that:

- Supply chain risk shall be addressed early and across the entire system lifecycle through a defense-in-breadth approach to managing the risks to the integrity of ICT within covered systems.

SCRM. The management of supply chain risk whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., packaging, handling, storage, and transport).

supply chain risk. The risk that adversaries will insert malicious code into or otherwise subvert the design, manufacturing, production, distribution, installation, or maintenance of ICT components that may be used in DoD systems to gain unauthorized access to data, to alter data, to disrupt operations, or to interrupt communications.



DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 25 2010

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 09-016 – Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems

References: See Attachment 1

Purpose. This DTM:

- Reissues DTM 08-048 (Reference (a)), updating policy and responsibilities.
- Establishes policy and a defense-in-breadth strategy for managing supply chain risk to information and communications technology (ICT) within DoD critical information systems and weapons systems in accordance with National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Reference (b)).
- Directs actions in accordance with DoD Instruction 5200.39 (Reference (c)) to mitigate and manage supply chain risk, as defined

OSD 03220-10

Recommendations Addressing Globalization of Software

Defense Science Board Task Force September 2007 Report on "Mission Impact of Foreign Influence on DoD Software"

Findings relate to:

-The Industry Situation

-Dependence on Software-

-Software Vulnerabilities

-Threat of the Nation-State Adversary

-Awareness of Software Assurance Threat and Risk

-Status of Software Assurance

-Ongoing Efforts in Software Assurance

-Supplier Trustworthiness Considerations

-Finding Malicious Code

-Government Access to Source Code

Recommendations relate to:

-Procurement of COTS and Off-Shore Software

-Increase US Insight into Capabilities and Intentions

-Offensive Strategies can complicate Defensive Strategies

-System Engineering and Architecture for Assurance

-Improve the Quality of Software

-Improve Tools and Technology for Assurance

-More Knowledgeable Acquisition of Software

-Research and Development in Software Assurance

Eliminate excess functionality in mission-critical components

Improve effectiveness of Common Criteria

Improve usefulness of assurance metrics

Promote use of automated tools in development

Increase transparency and knowledge of suppliers' processes

Components should be supplied by suppliers of commensurate trustworthiness

Custom code for critical systems should be developed by cleared US citizens

Provide incentives to industry to produce higher quality code; improve assuredness of COTS SW

Use risk-based acquisition

Research programs to advance vulnerability detection and mitigation

Advance the issue of software assurance and globalization on national agenda as part of effort to reduce national cyber risk

Supply System Attacks

- Why send malicious code over the Internet if you can pre-infect computer parts or consumer devices?
- Some recent examples:
  - Fall 2007: hard drives from China arrived on store shelves pre-infected with a virus
  - Christmas 2007: hundreds of digital photo frames, USB memory sticks, GPS devices, and other plug-n-play devices were found to be infected with malware
  - January 2008: FBI announces a multi-year investigation into counterfeit Cisco routers
- **Exploitation potential of non-secure IT/software is often independent of "intent"**

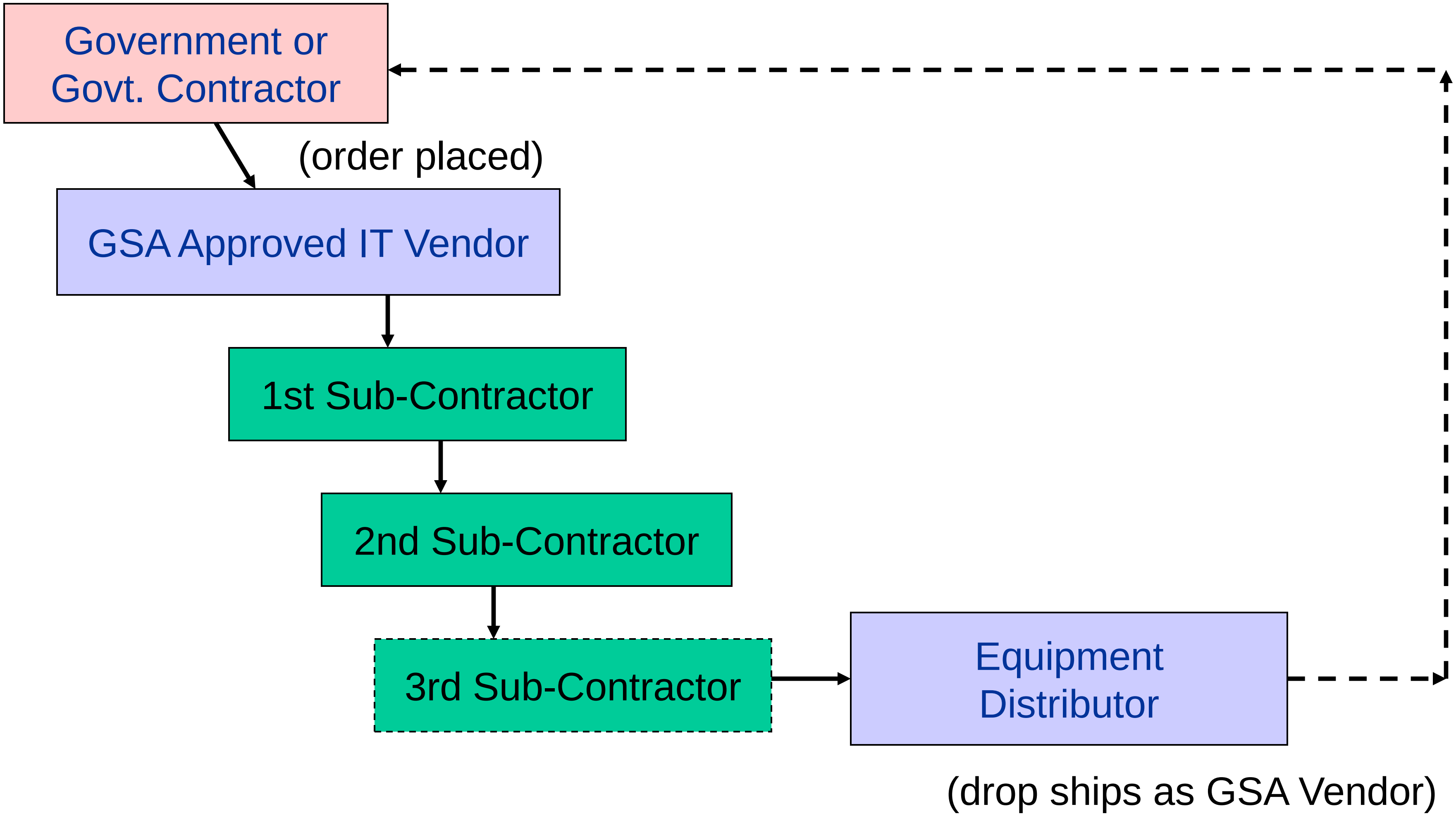
Adopted in part from Marcus H. Sachs, Verizon, *"Supply Chain Risk Management: Can we Secure the IT Supply Chain in the Age of Globalization?" Software Assurance Forum, 15 Oct 2008*

Major pipelines for IT/Software Supply Chain

1. From country where manufactured
   - to a certified domestic distributor to domestic end-user, or
   - through a certified distributor in a second country to domestic end-user
2. From country of origin
   - to online auction site (such as eBay or similar) to end-user
   - to distributor or retailer with unknown credentials to end-user
3. In most cases, IT/software is manufactured/produced by a non-vetted or uncertified supplier (especially for software) to domestic end-user
4. Transparency of supply chain complicated through re-supply of integrators, VARs, and service providers

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*

US Government Contracting Process



Supply Chain Risk Management (SCRM) processes, tools and techniques:

- Numerous SCRM processes, tools and techniques facilitate the implementation of SCRM USG-wide. Departments and Agencies shall adopt and tailor these recommended SCRM processes, tools, and techniques, and apply them to the procurement and operation of mission critical elements within NSS, to include those which:
  - Control the quality, configuration, and security of software, hardware, and systems throughout their lifecycles, including commercial elements or sub-elements.
  - Detect the occurrence, reduce the likelihood of occurrence, and mitigate the consequences of products containing counterfeit elements or malicious functions.
  - Develop requirements or capabilities to detect the occurrence of vulnerabilities within custom and commodity hardware and software through enhanced test and evaluation.

SCRM processes, tools and techniques:

- Enhance security through the implementation of system security engineering (e.g. criticality analysis and defensive engineering practices) throughout the system life cycle.
- Optimize acquisition and contracting to define requirements and source selection criteria that reduce supply chain risk, give preference to vendors that minimize supply chain risk in verifiable ways, and evaluate security equally with other desirable factors, such as low cost, rapid deployment, or new features.
- Implement acquisition processes to document and monitor risk mitigation methods and requirements and provide for the update of documentation throughout the system lifecycle.

Best Practices, Tools and Techniques References

General SCRM References

The following documents provide systems security engineering guidance and detailed risk management best practice for use in commercial or government systems.

Draft NISTIR 7622, *Piloting Supply Chain Risk Management for Federal Information Systems*, June 2010.

National Defense Industrial Association (NDIA) System Assurance Committee. 2008. *Engineering for System Assurance*.

SCRM References from the Department of Defense

The following documents describe SCRM best practice for NSS, provide guidance on the successful implementation of SCRM pilots that incorporate all-source threat information, summarize the DoD pilot experience, and identify trusted suppliers of integrate circuits as accredited by the Defense Microelectronic Agency.

Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11: Supply Chain Risk Management Pilot Program. February 25, 2010.

Concept of Operations for the DoD Comprehensive National Cybersecurity Initiative 11: Supply Chain Risk Management Pilot Program. August 25, 2009.

Draft Comprehensive National Cybersecurity Initiative (CNCI) DoD Supply Chain Risk Management (SCRM) Pilot Program Report, November 30, 2010

List of Trusted Integrated Circuits (IC) Suppliers available at http://www.dmea.osd.mil

SCRM References from the Department of Homeland Security

The following documents and the assessment tool provide guidance for civilian Departments and agencies guidance for the successful implementation of a SCRM pilot. Used with the NISTIR 7622, which identifies key practices, the following documents enable the development and operation of systems to manage supply chain risks.

- Concept of Operations for the Civilian Agency Pilot Program (CAPP)
- Template for a SCRM Pilot Plan of Action and Milestones
- SCRM Capability Assessment Tool

Best Practices, Tools and Techniques References

Software Assurance Community documents from Software.Assurance@dhs.gov

Software Assurance in Acquisition and Contract Language (https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html#acquisition)

Software Supply Chain Risk Management and Due Diligence (https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html#acquisition)

Polydys, Mary L. and Wisseman, Stan., Software Assurance in Acquisition: Mitigating Risks to the Enterprise, A Reference Guide for Security-Enhanced Software Acquisition and Outsourcing, Information Resources Management College Occasional Paper, National Defense University Press, Washington, D.C. February 2009. (http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA495389)

Polydys, Mary L. and Wisseman, Stan. (2007, May). "Software Assurance: Five Essential Considerations for Acquisition Officials." CrossTalk—The Journal of Defense Software Engineering, Vol. 20, No. 5. (https://buildsecurityin.us-cert.gov/swa/downloads/PolydysWisseman.pdf)

Robert J. Ellison, John B. Goodenough, Charles B. Weinstock, Carol Woody Evaluating and Mitigating Software Supply Chain Security Risks, May 2010 (https://buildsecurityin.us-cert.gov/swa/downloads/MitigatingSWsupplyChainRisks10tn016.pdf)

Goertzel, Karen, Theodore Winograd, et al. for Department of Homeland Security and Department of Defense Data and Analysis Center for Software. Enhancing the Development Life Cycle to Produce Secure Software: A Reference Guidebook on Software Assurance, October 2008. (https://www.thedacs.com/techs/enhanced_life_cycles/)

Bob Ellison, CERT, Software Engineering Institute and Carol Woody, CERT, Software Engineering Institute, “ Considering Software Supply Chain Risks,” CrossTalk—The Journal of Defense Software Engineering,, September/October 2010 (https://buildsecurityin.us-cert.gov/bsi/1207-BSI/version/1/part/4/data/1009EllisonWoody.pdf?branch=main&language=default)

Bob Ellison, CERT, Software Engineering Institute and Carol Woody, CERT, Software Engineering Institute, Supply-Chain Risk Management: Incorporating Security into Software Development, March 2010 (https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/acquisition/1140-BSI.html)

Best Practices, Tools and Techniques References

Industry Standards for SCRM

EIA-4899 - Standard for Preparing an Electronic Component Management Plan

IDEA-STD-1010 – Diminishing Manufacturing Sources and Material Shortages (DMSMS) Guidebook

SAE-AS9120 – Quality Management Systems for Aerospace Product Distributors

SAE-AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation and Disposition

Federal IT Security References

The following documents provide a foundation of federal information technology security practices or provide detailed guidance specific to managing risks inherent in the information technology product or services supply chain.

CNSS Instruction No. 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009

NIST Special Publication 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009 (includes updates as of 05-01-2010).

NIST Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: *A Security Life Cycle Approach*, February 2010.

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
    - Re-suppliers (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

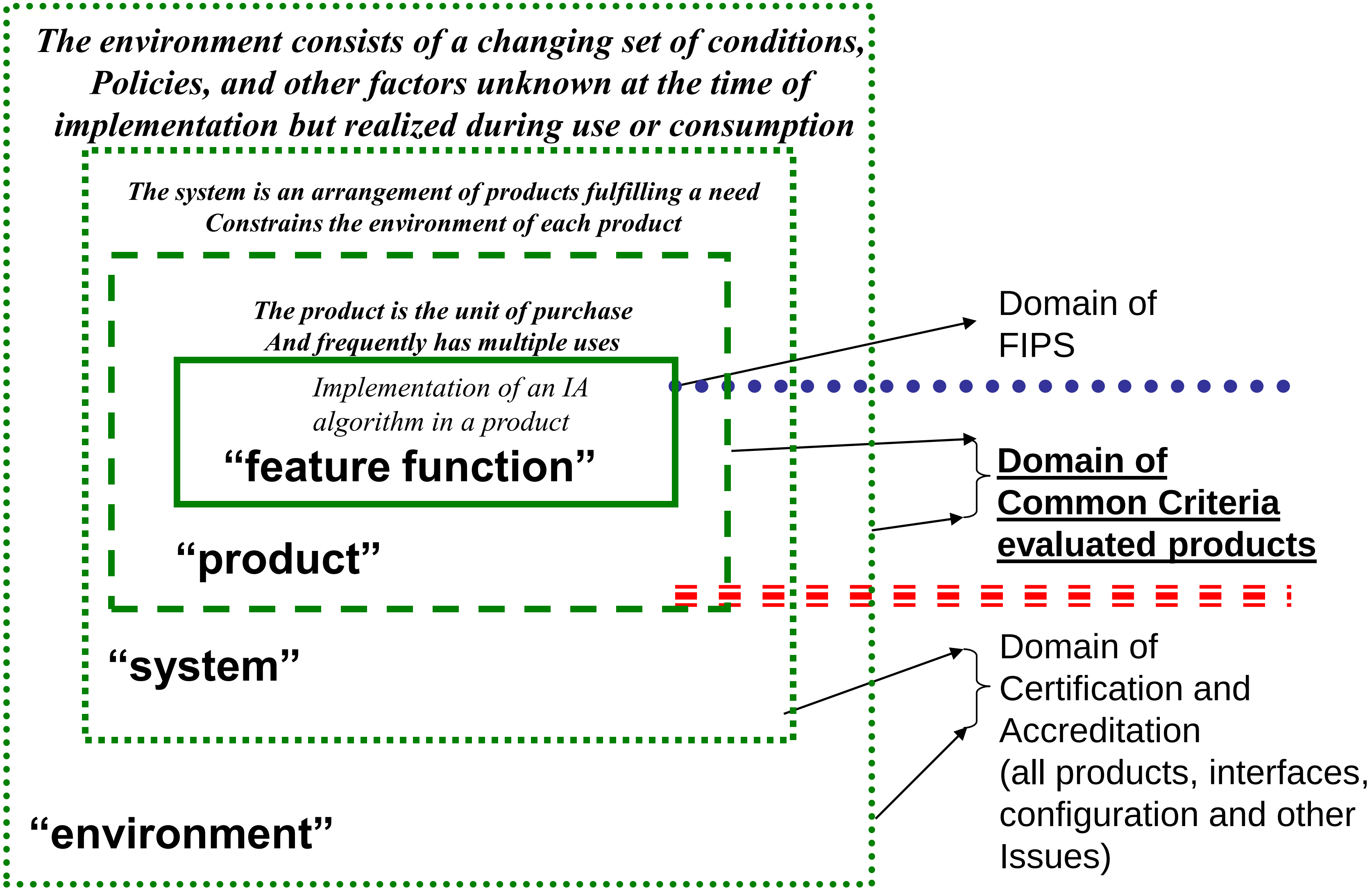
Homeland Security

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*

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 “provenance 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

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

Domain of Common Criteria evaluated products

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

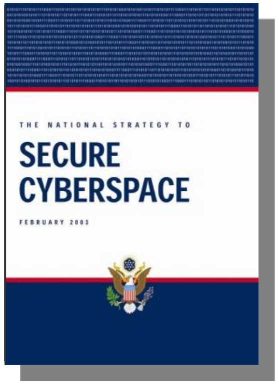
Software-Reliant Systems at Risk

- Until recently, the absence of a common measure for software weaknesses and attack patterns has limited ability to assess and remediate exploitable software flaws.
- Organizations can achieve consistent measures for prioritizing risk mitigation efforts and focus on the security and resilience of software:
  - Leverage the use of common dictionaries of exploitable weaknesses, malware attribute, & attack patterns;
  - Enable interoperability among tools & automation of risk mitigation;
  - Enable better informed decision-making for the development and acquisition of more resilient software products and services;
  - Enable more focused training of developers to avoid software faults.

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.”*



THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

- 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), Common Attack Patterns (CAPEC), and Cyber Observables (CybOX).
  - 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 Forum & Working Groups*

… encourage the production, evaluation and acquisition of more secure and resilient software through targeting:

People	Processes	Technology	Acquisition
Developers and users education & training	Sound practices, standards, & practical guidelines for secure software development	Security test criteria, measurement, diagnostic tools, common languages & enumerations, SwA Research & Development	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

SwA Curriculum Project: Masters and Undergraduate

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)
Common Attack Pattern Enumeration (CAPEC)
Malware Attribute Enumeration and Characterization

SwA in Acquisition: Mitigating Risks to Enterprise
Software Project Management for SwA SOAR

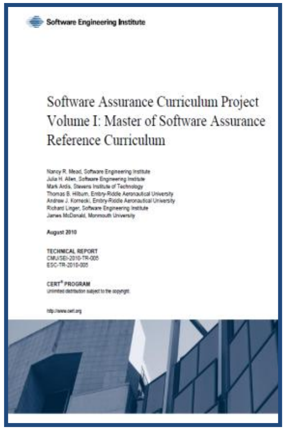
Homeland Security

* 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.

Software Assurance Curriculum Project

- **Vol I: Master of Software Assurance Reference Curriculum**

  In Dec 2010 the IEEE Computer Society and the ACM recognized the Master of Software Assurance (MSwA) Reference Curriculum as a certified master's degree program in SwA —the first curriculum to focus on assuring the functionality, dependability, and security of software and systems.



Software Engineering Institute

Software Assurance Curriculum Project
Volume I: Master of Software Assurance
Reference Curriculum

Nancy R. Mead, Software Engineering Institute
Julia H. Allen, Software Engineering Institute
Mark Ardis, Stevens Institute of Technology
Thomas B. Hilburn, Embry-Riddle Aeronautical University
Andrew J. Kornecki, Embry-Riddle Aeronautical University
Richard Linger, Software Engineering Institute
James McDonald, Monmouth University

August 2010

TECHNICAL REPORT
CMU/SEI-2010-TR-005
ESC-TR-2010-005

CERT® PROGRAM
Unlimited distribution subject to the copyright.

http://www.cert.org

- **Vol II: SwA Undergraduate Course Outlines**

  see www.sei.cmu.edu/library/abstracts/reports/10tr019.cfm to download the PDF version of the report CMU/SEI-2010-TR-019

- **Vol III: Master of SwA Course Syllabi**
- **Vol IV: Community College Education**

•To facilitate implementation, the MSwA project team is offering assistance, free of charge, to educational institutions looking to launch an MSwA degree program.
• For more information on SwA Curriculum Project and MSwA, go to https://buildsecurityin.us-cert.gov/bsi/1165-BSI.html.

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

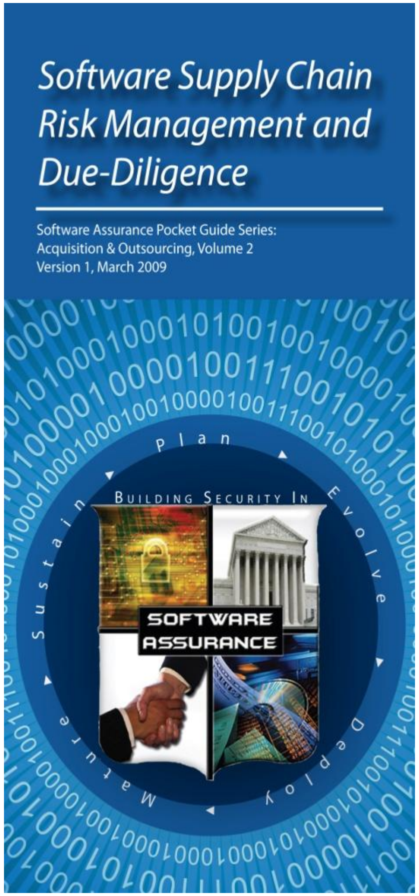
- Integrating Security into the Software Development Life Cycle
- Key Practices for Mitigating the Most Egregious Exploitable Software Weaknesses
- Risk-based Software Security Testing
- Requirements and Analysis for Secure Software
- Architecture and Design Considerations for Secure Software
- Secure 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 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

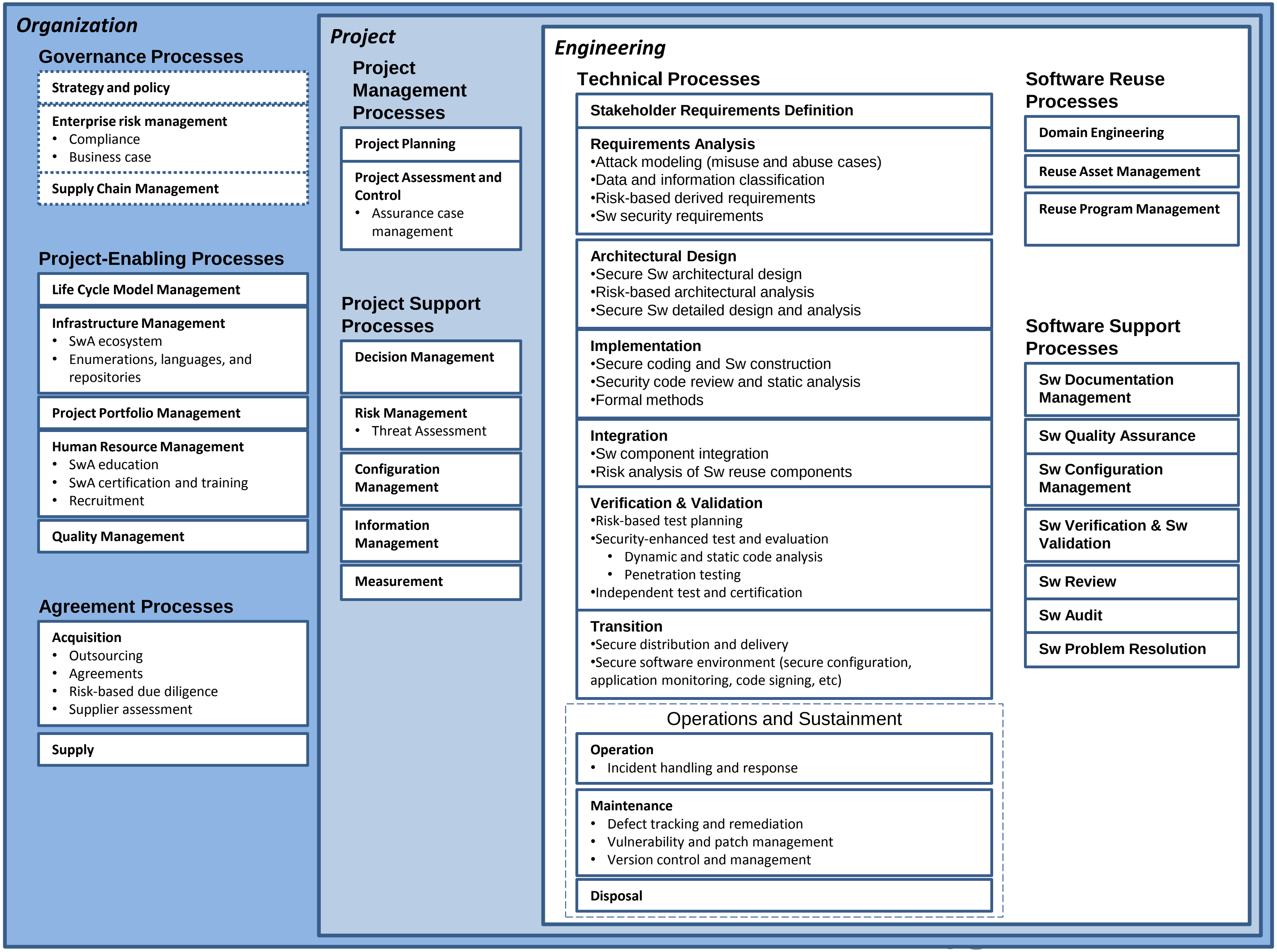
SwA Community Resources and Information Clearinghouse (CRIC)

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

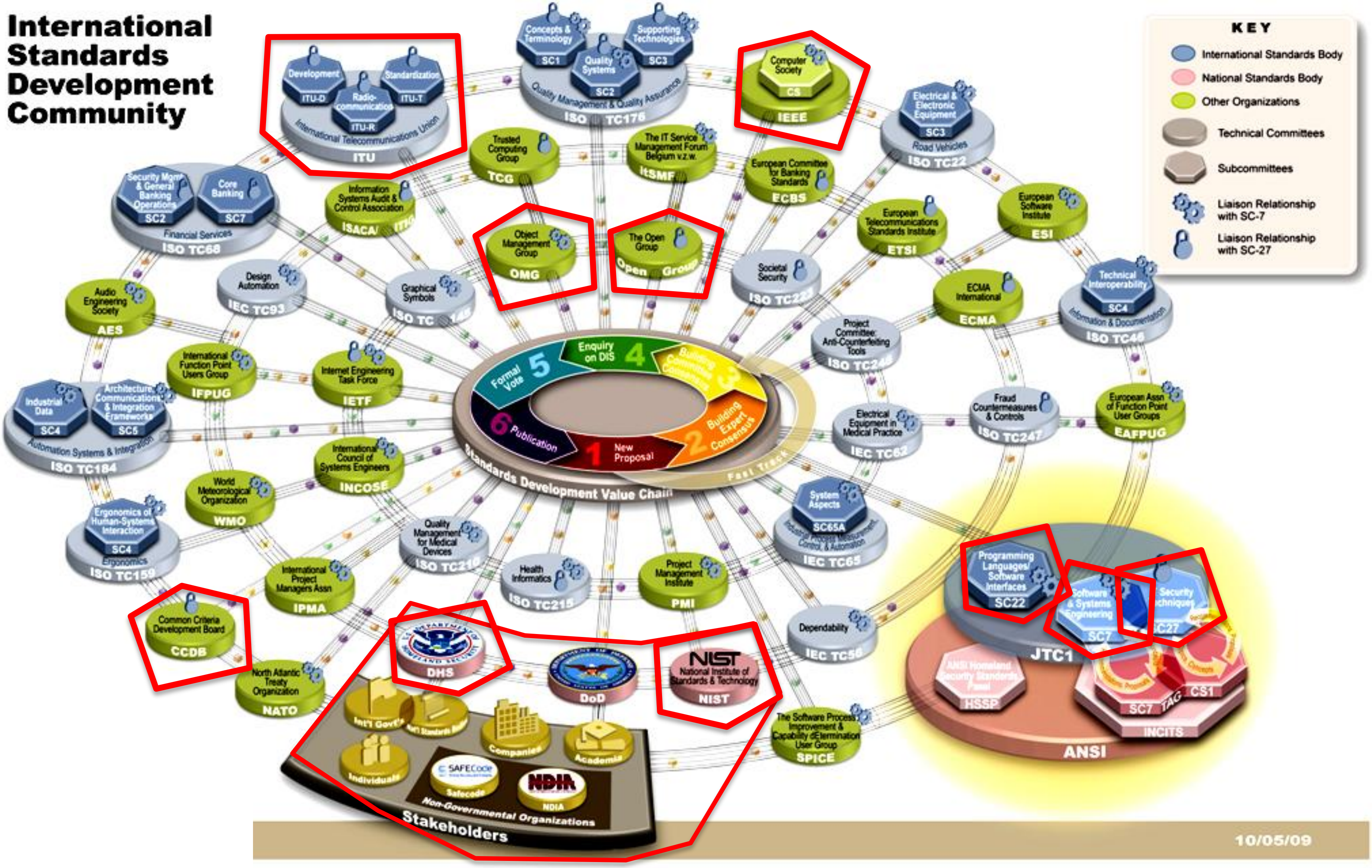
Sw Verification & Sw Validation

Sw Review

Sw Audit

Sw Problem Resolution

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

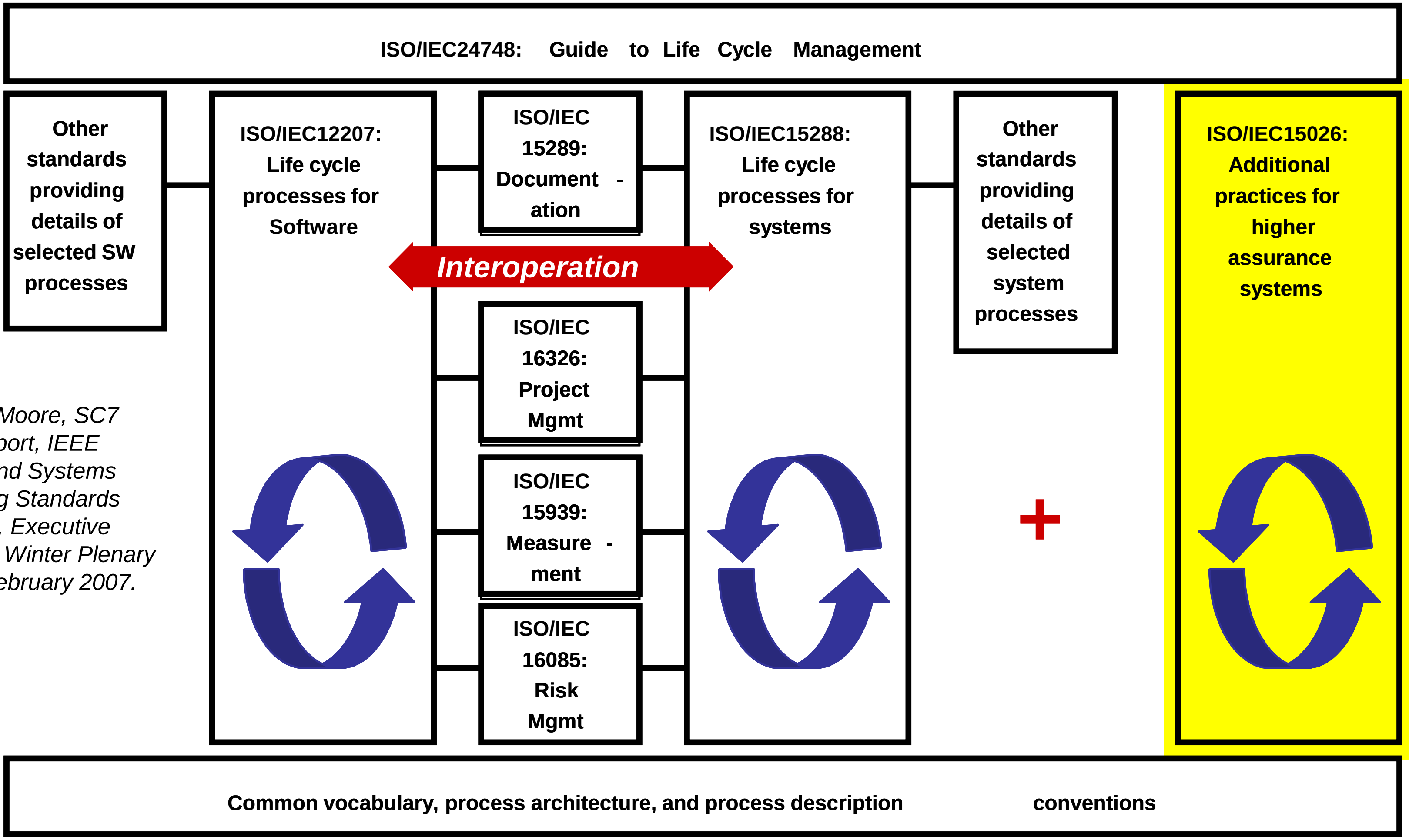

International Standards Development Community
KEY
International Standards Body
National Standards Body
Other Organizations
Technical Committees
Subcommittees
Liaison Relationship with SC-7
Liaison Relationship with SC-27
Development
ITU-D
Radio-communication
ITU-R
Standardization
ITU-T
International 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
ECMA International
ECMA
Technical Interoperability
SC4
Information & Documentation
ISO TC46
Audio Engineering Society
AES
Design Automation
IEC TC93
Graphical Symbols
ISO TC 145
Project Committee: Anti-Counterfeiting Tools
ISO TC248
International Function Point Users Group
IFPUG
Internet Engineering Task Force
IETF
Industrial Data
SC4
Architecture, Communications & Integration Frameworks
SC5
Automation Systems & Integration
ISO TC184
Formal Vote
5
Enquiry on DIS
4
Building Committee Consensus
3
Building Expert Consensus
2
New Proposal
1
Publication
6
Standards Development Value Chain
Fast Track
Electrical Equipment in Medical Practice
IEC TC62
Fraud Countermeasures & Controls
ISO TC247
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
Int'l Gov'ts
Int'l Standards Bodies
Companies
Academia
Individuals
SAFECode
Safecode
NDIA
Non-Governmental Organizations
Stakeholders
The Software Process Improvement & Capability dEtermination User Group
SPICE
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 October 2010.
  - 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, System and Software Assurance**
  - 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: Document - ation

Interoperation

ISO/IEC 16326: Project Mgmt

ISO/IEC 15939: Measure - ment

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

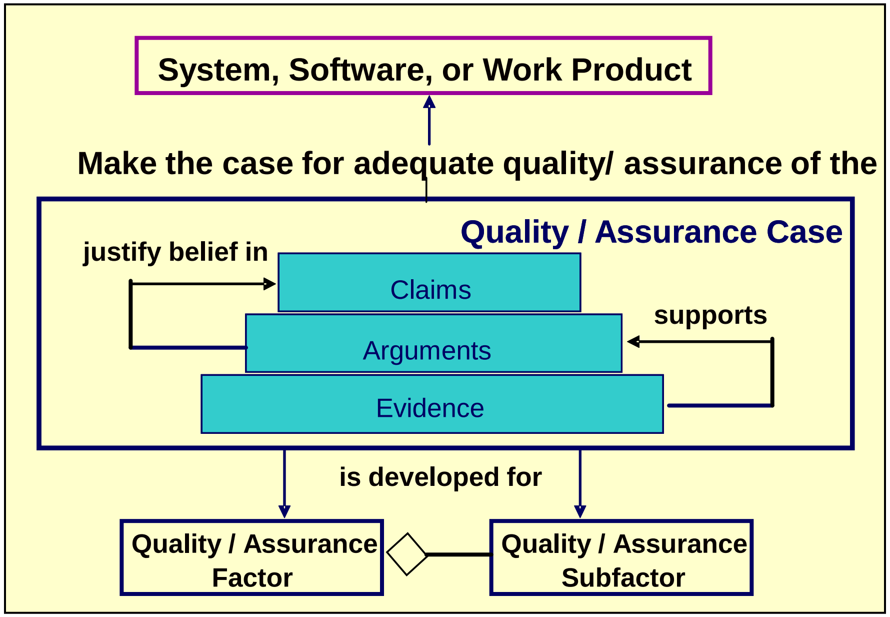
Source: J. Moore, SC7 Liaison Report, IEEE Software and Systems Engineering Standards Committee, Executive Committee Winter Plenary Meeting, February 2007.

“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

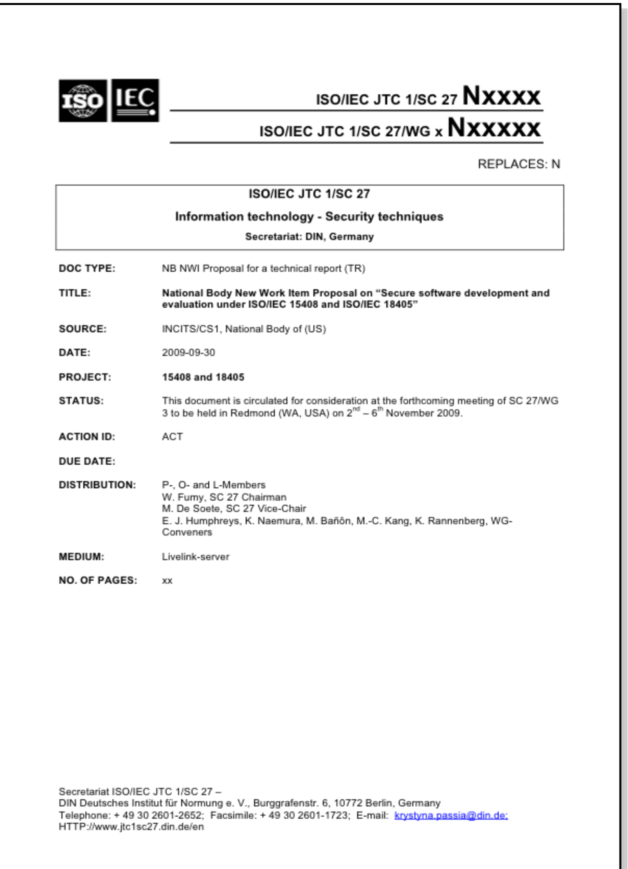
Quality / Assurance Subfactor

- **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

SC27 WG3



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. Bañôn, M.-C. Kang, K. Rannenberg, WG-Conveners
MEDIUM:	Livelink-server
NO. OF PAGES:	xx

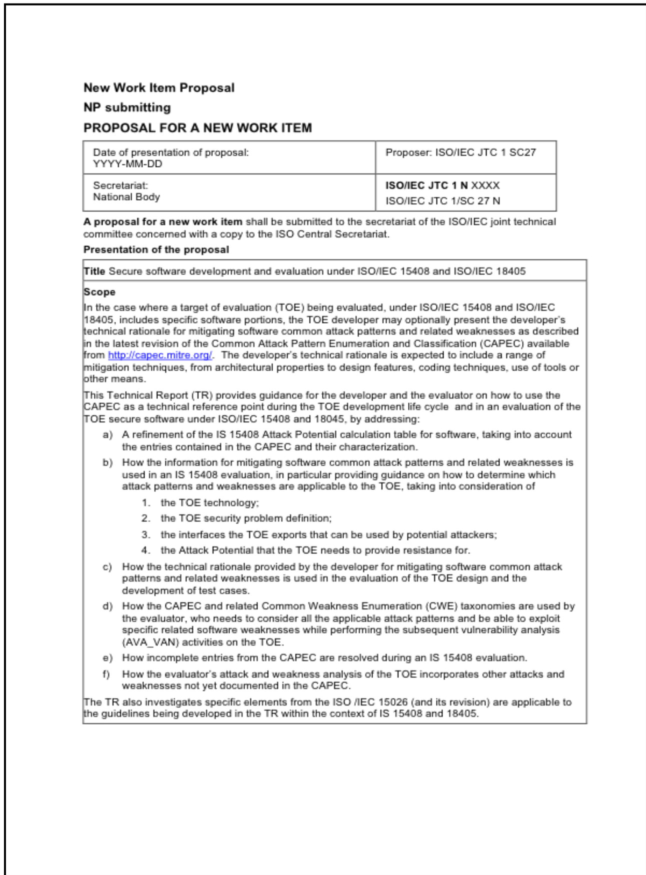
Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de;
HTTP://www.jtc1sc27.din.de/en

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.

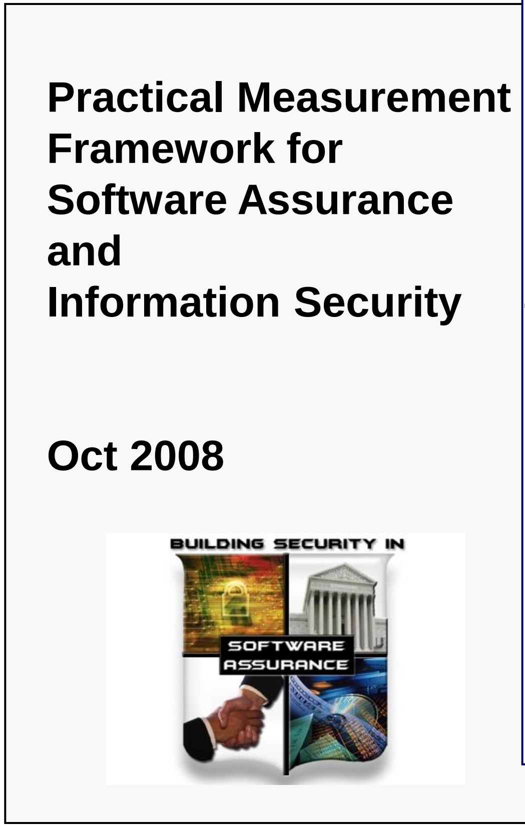
The TR also investigates specific elements from the ISO /IEC 15026 (and its revision) are applicable to the guidelines being developed in the TR within the context of IS 15408 and 18405.

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

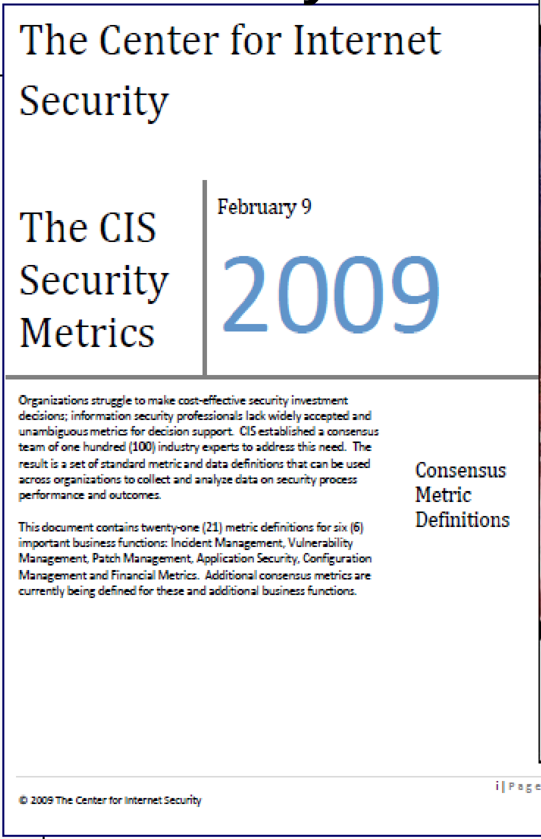
Security Measurement Resources

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

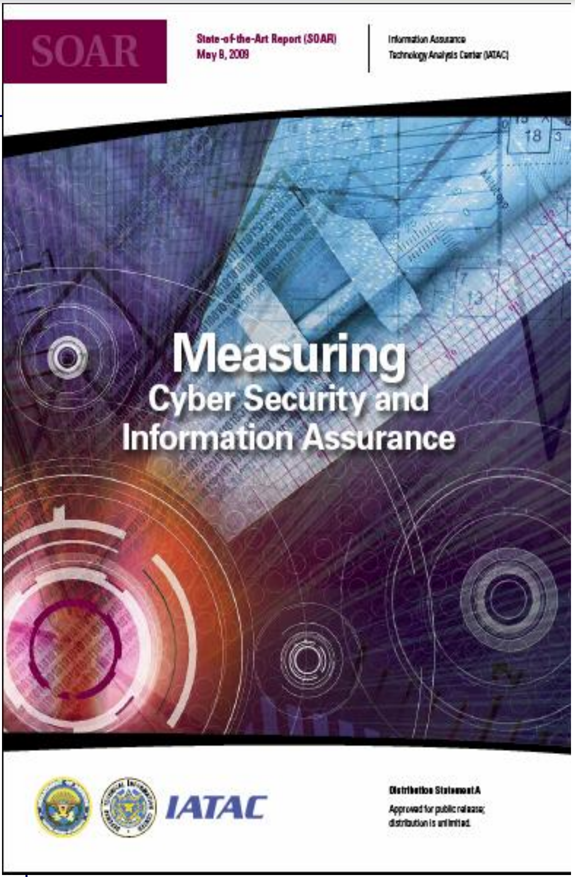
Organizations struggle to make cost-effective security investment decisions; information security professionals lack widely accepted and unambiguous metrics for decision support. CIS established a consensus team of one hundred (100) industry experts to address this need. The result is a set of standard 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)

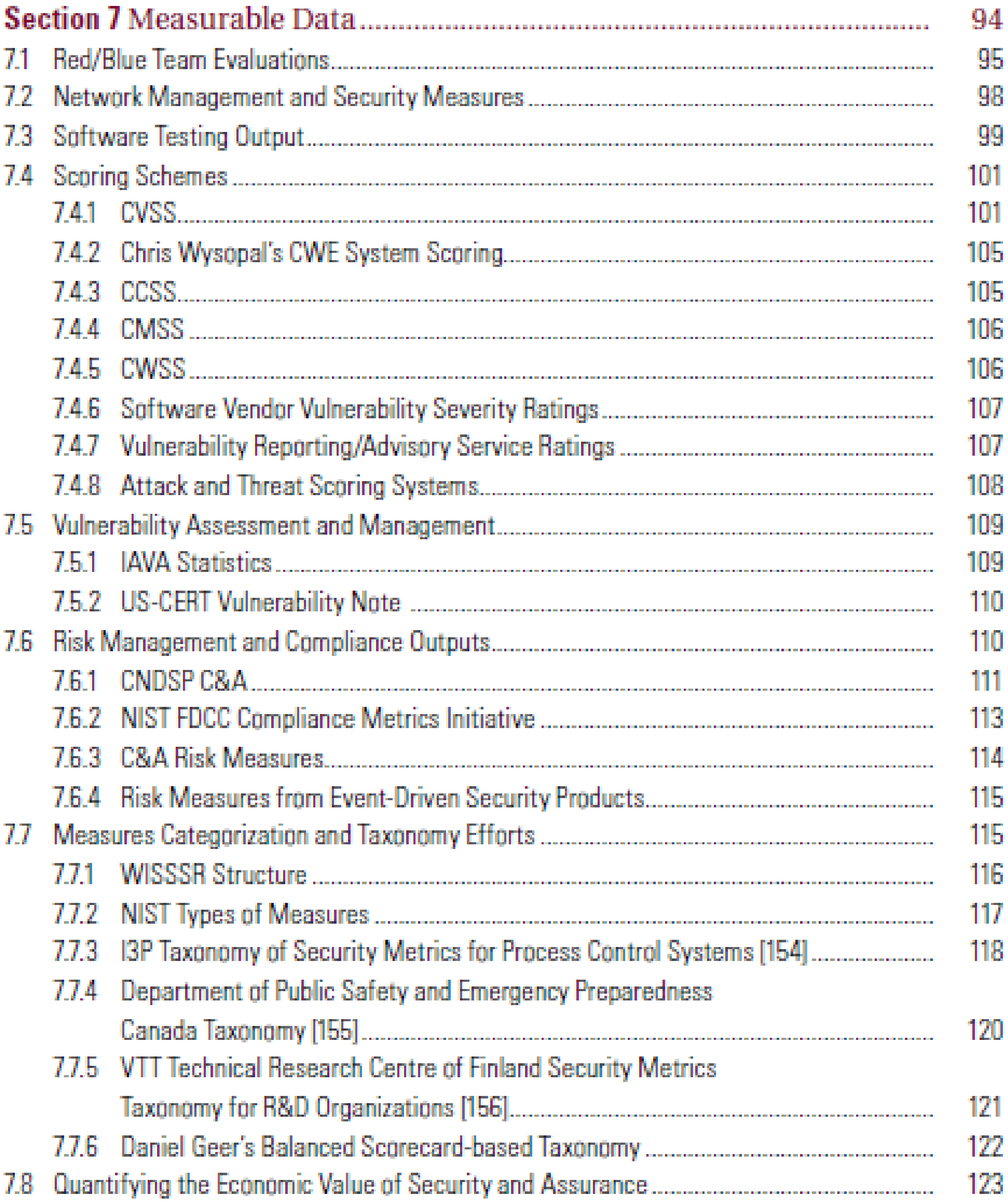
Measuring
Cyber Security and Information Assurance

IATAC

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

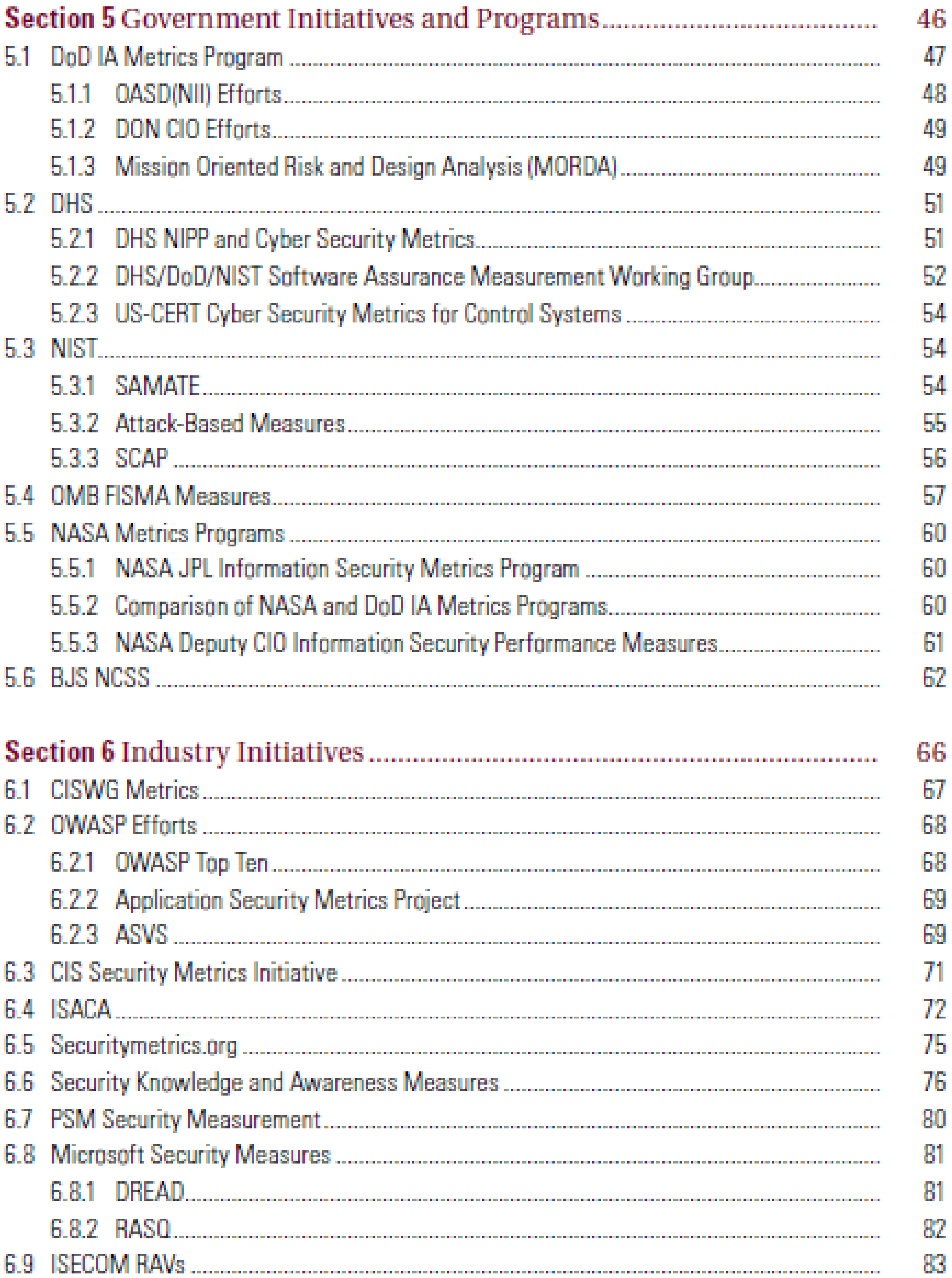
https://buildsecurityin.us-cert.gov/swa/measresrc.html

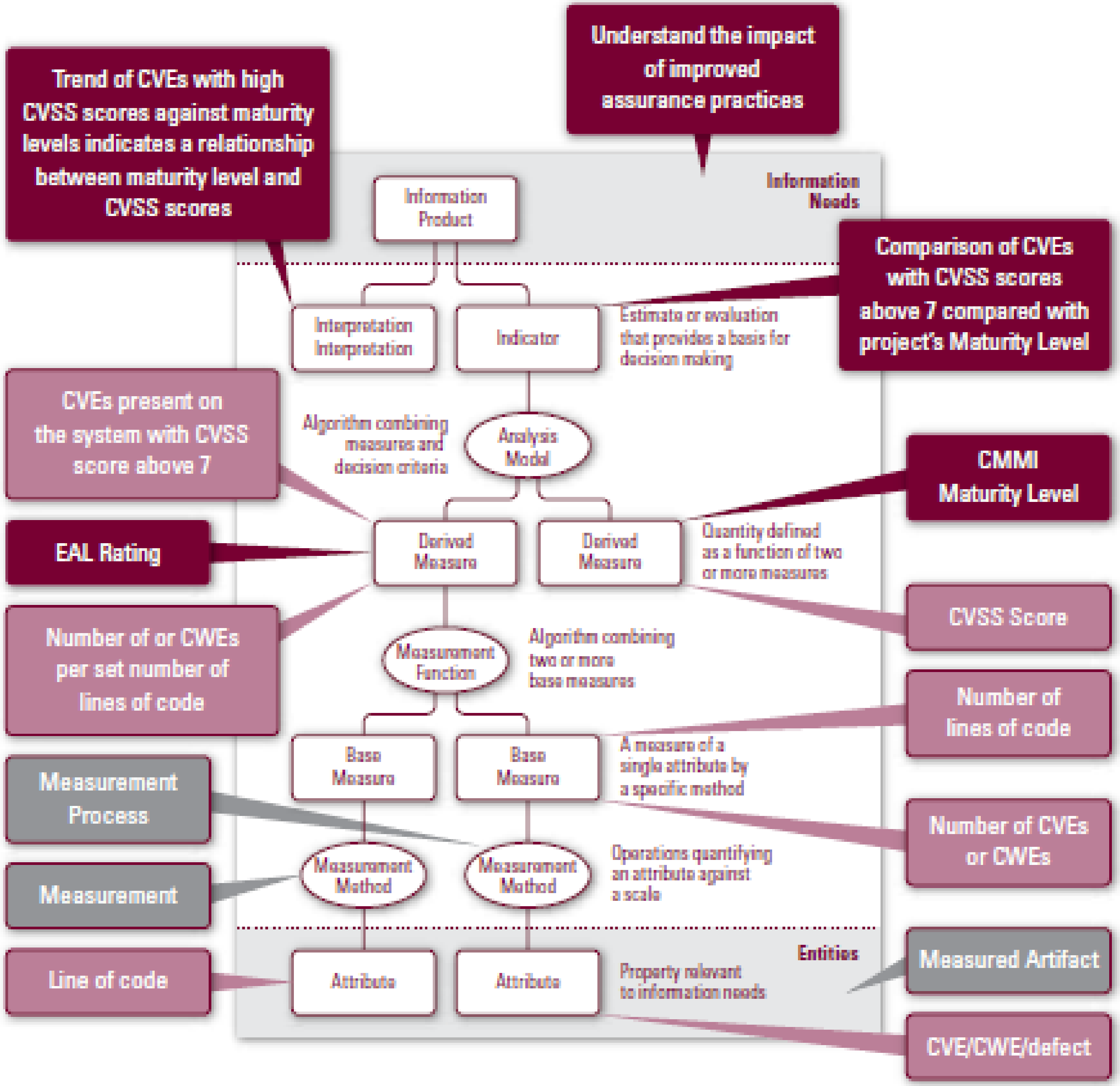
Extensive examples of measurable data relevant to cyber security and information assurance



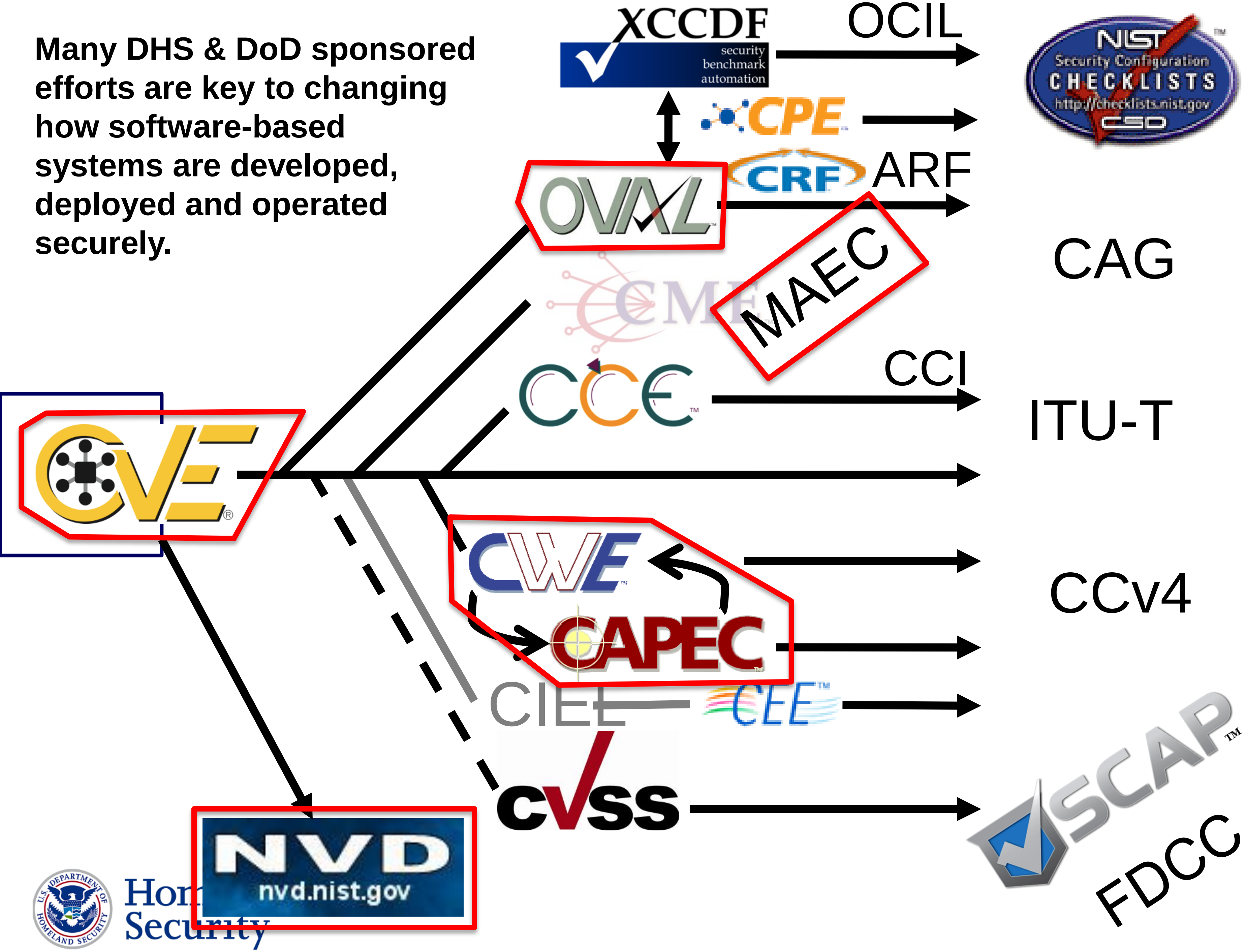
Homeland Security

Extensive examples of government and industry activities leveraging the use of measurable data relevant to cyber security and information assurance



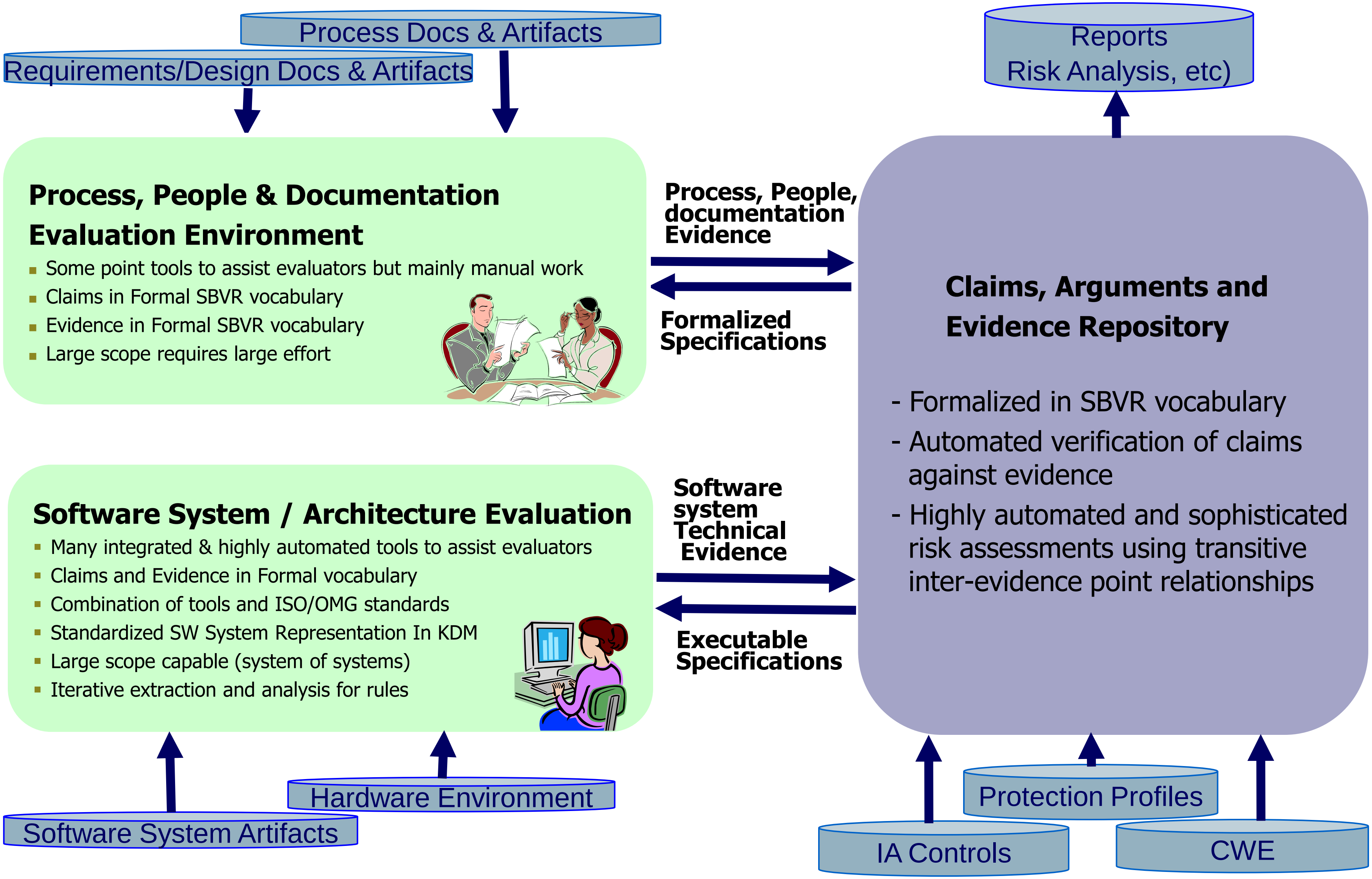

Understand the impact of improved assurance practices
Trend of CVEs with high CVSS scores against maturity levels indicates a relationship between maturity level and CVSS scores
Information Needs
Information Product
Comparison of CVEs with CVSS scores above 7 compared with project's Maturity Level
Interpretation Interpretation
Indicator
Estimate or evaluation that provides a basis for decision making
CVEs present on the system with CVSS score above 7
Algorithm combining measures and decision criteria
Analysis Model
CMMI Maturity Level
EAL Rating
Derived Measure
Derived Measure
Quantity defined as a function of two or more measures
CVSS Score
Number of or CWEs per set number of lines of code
Measurement Function
Algorithm combining two or more base measures
Number of lines of code
Base Measure
Base Measure
A measure of a single attribute by a specific method
Measurement Process
Number of CVEs or CWEs
Measurement
Measurement Method
Measurement Method
Operations quantifying an attribute against a scale
Entities
Measured Artifact
Line of code
Attribute
Attribute
Property relevant to information needs
CVE/CWE/defect

Many DHS & DoD 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
CME
CAG
CCE
CCI
ITU-T
CVE
CWE
CCv4
CAPEC
CIEL
CEE
CVSS
SCAP
FDCC
NVD
nvd.nist.gov
U.S. Department of Homeland Security
Homeland Security

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 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

Process, People, documentation Evidence

Formalized Specifications

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

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

Software system Technical Evidence

Executable Specifications

Hardware Environment

Software System Artifacts

Protection Profiles

IA Controls

CWE

Leverage Common Weakness Enumeration (CWE)

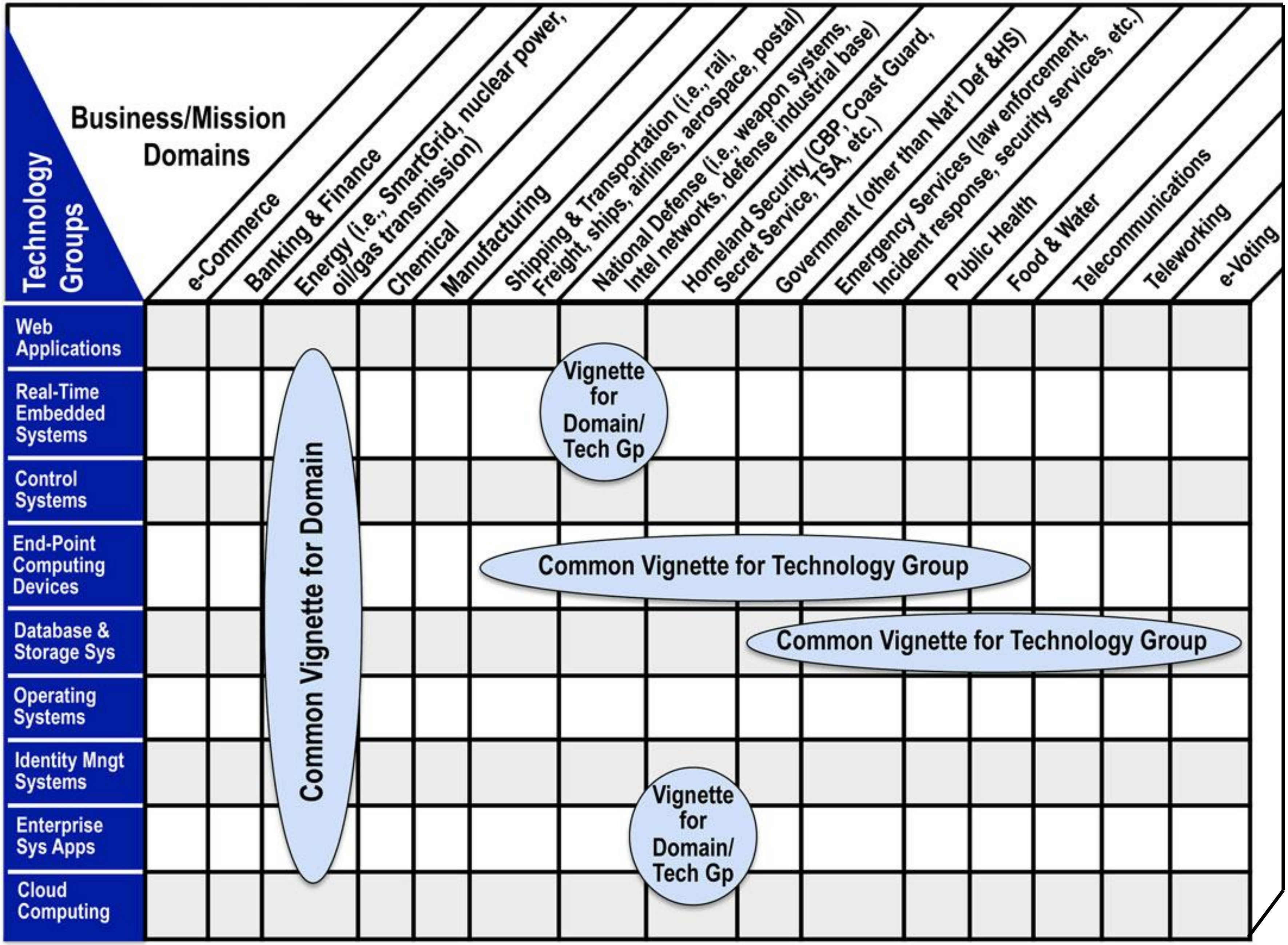
CWE is a formal list of software weakness types created to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code.
- Serve as a standard measuring stick for software security tools targeting these weaknesses.
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts.

Some Common Types of Software Weaknesses:

Buffer Overflows, Format Strings, Etc.
Structure and Validity Problems
Common Special Element Manipulations
Channel and Path Errors
Handler Errors
User Interface Errors
Pathname Traversal and Equivalence Errors
Authentication Errors
Resource Management Errors
Insufficient Verification of Data
Code Evaluation and Injection
Randomness and Predictability

Leveraging Vignettes in Cyber Security Standardization for Key ICT Applications in various Domains


Business/Mission Domains
Technology Groups
e-Commerce
Banking & Finance
Energy (i.e., SmartGrid, nuclear power, oil/gas transmission)
Chemical
Manufacturing
Shipping & Transportation (i.e., rail, Freight, ships, airlines, aerospace, postal)
National Defense (i.e., weapon systems, Intel networks, defense industrial base)
Homeland Security (CBP, Coast Guard, Secret Service, TSA, etc.)
Government (other than Nat'l Def &HS)
Emergency Services (law enforcement, Incident response, security services, etc.)
Public Health
Food & Water
Telecommunications
Teleworking
e-Voting
Web Applications
Real-Time Embedded Systems
Control Systems
End-Point Computing Devices
Database & Storage Sys
Operating Systems
Identity Mngt Systems
Enterprise Sys Apps
Cloud Computing
Common Vignette for Domain
Vignette for Domain/ Tech Gp
Common Vignette for Technology Group
Common Vignette for Technology Group
Vignette for Domain/ Tech Gp

Common Weakness Risk Assessment Framework uses Vignettes with Archetypes to identify top CWEs in respective Domain/Technology Groups

Common Weakness Risk Analysis Framework (CWRAF)

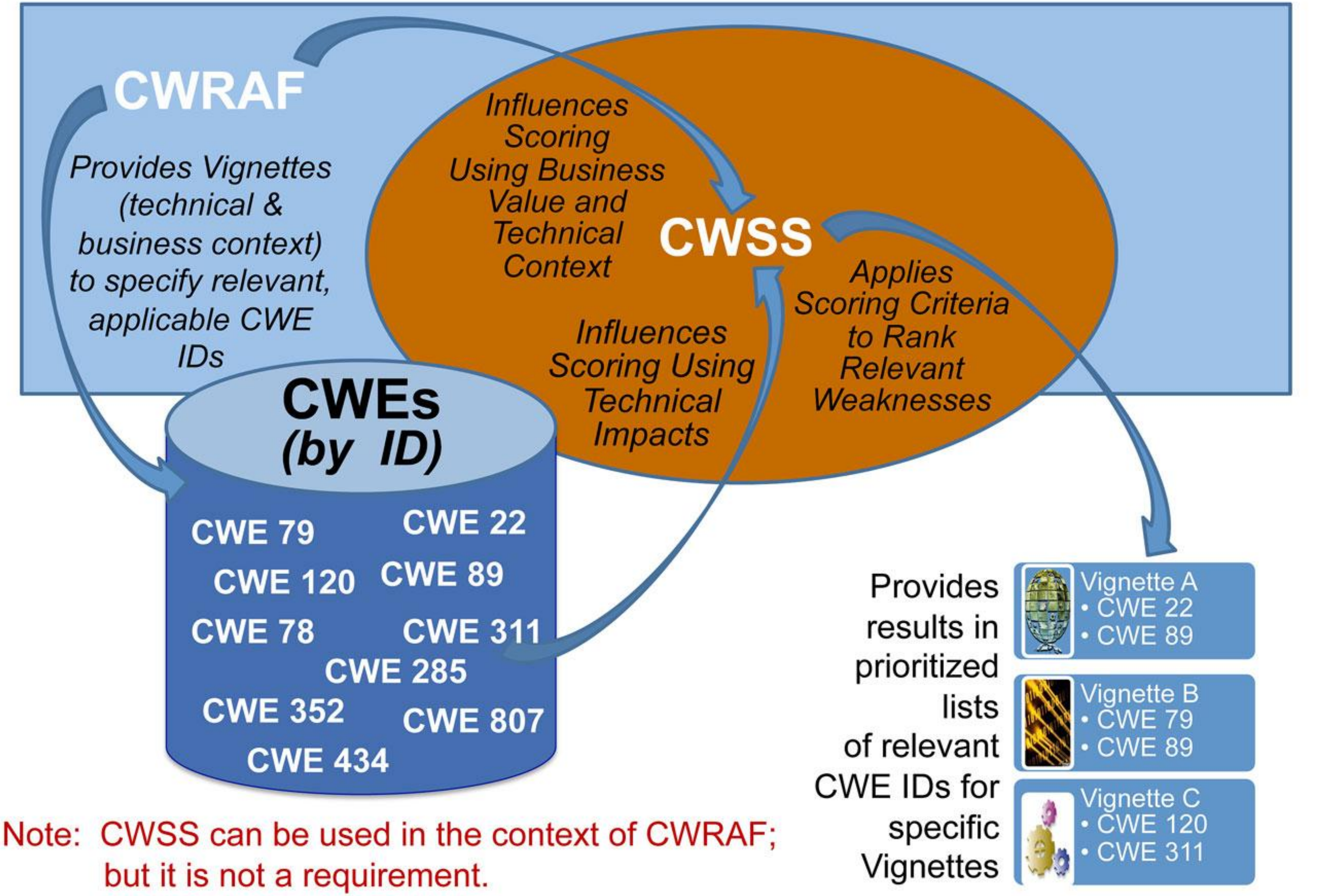
- CWRAF enables organizations to apply the Common Weakness Scoring System (CWSS)
  - using specialized, targeted scenarios ("vignettes")
  - that identify the business value context of deployed applications
  - to prioritize those software weaknesses (CWE) that are most relevant to their own businesses, missions, and deployed technologies.

- CWRAF:
  - includes a mechanism for measuring risk of weaknesses in a way that is closely linked with the risk to the business or mission;
  - supports the automatic selection and prioritization of relevant weaknesses, customized to the specific needs of the business or mission;
  - can be used by consumers to identify the most important weaknesses for their business domains, in order to inform their acquisition and protection activities as one part of the larger process of achieving software assurance; and
  - allows users to create custom Top-N lists to rank classes of weaknesses independent of any particular software package, to prioritize them relative to each other (e.g., "buffer overflows are higher priority than memory leaks"). This "Top-N list" approach is also used by the CWE/SANS Top 25, OWASP Top Ten, etc..

CWRAF - http://cwe.mitre.org/cwraf/index.html

CWRAF is a part of the CWE project, co-sponsored by the Software Assurance program in the National Cyber Security Division of the U.S. Department of Homeland Security. Community review/feedback of CWRAF & CWSS should be sent to cwss@mitre.org.

Relationships between CWRAF, CWSS, and CWE



CWRAF

Provides Vignettes (technical & business context) to specify relevant, applicable CWE IDs

Influences Scoring Using Business Value and Technical Context

CWSS

Influences Scoring Using Technical Impacts

Applies Scoring Criteria to Rank Relevant Weaknesses

CWEs (by ID)

CWE 79
CWE 22
CWE 120
CWE 89
CWE 78
CWE 311
CWE 285
CWE 352
CWE 807
CWE 434

Provides results in prioritized lists of relevant CWE IDs for specific Vignettes

Vignette A
- CWE 22
- CWE 89

Vignette B
- CWE 79
- CWE 89

Vignette C
- CWE 120
- CWE 311

Note: CWSS can be used in the context of CWRAF; but it is not a requirement.

CWRAF/CWSS Provides Risk Prioritization for CWE throughout Software Life Cycle

- Enables education and training to provide specific practices for eliminating on software fault patterns;
- Enables developers to mitigate top risks attributable to exploitable software;
- Enables testing organizations to use suite of test tools & methods (with CWE Coverage Claims Representation) that cover applicable concerns;
- Enables users and operation organizations to deploy and use software that is more resilient and secure;
- Enables procurement organizations to specify software security expectations through acquisition of software and services.

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

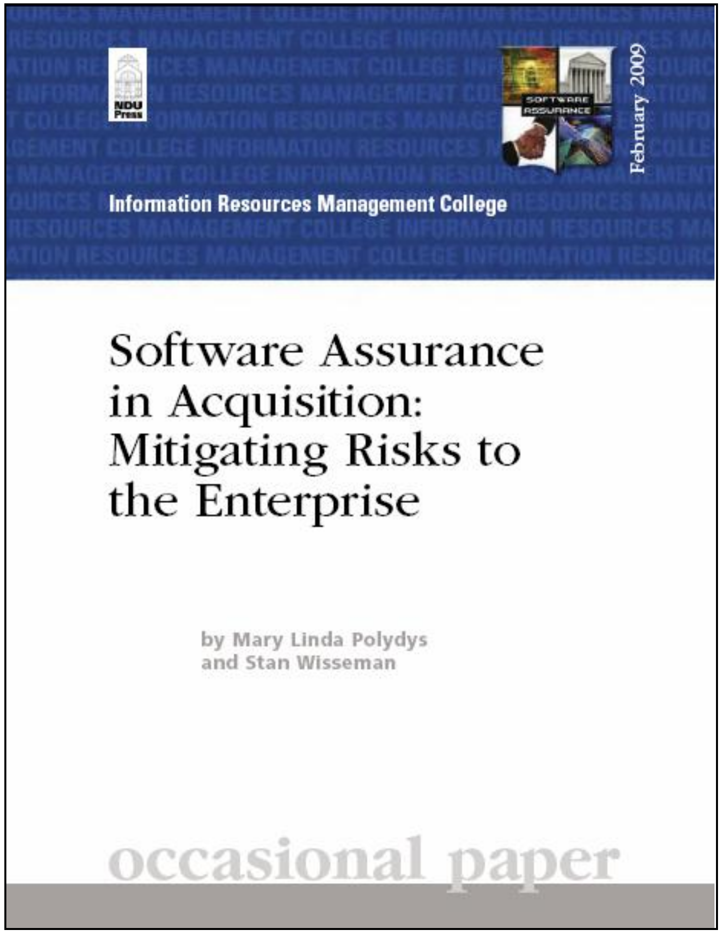
Collaborate with OWASP "Security Facts" labeling efforts

“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

SOFTWARE ASSURANCE

February 2009

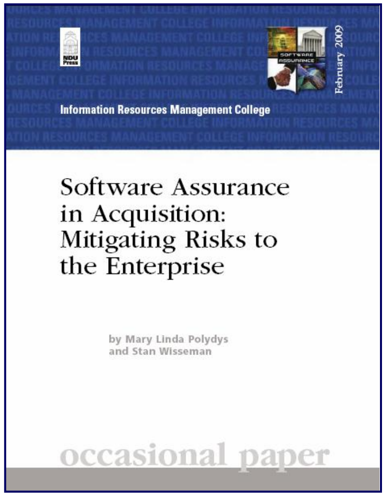
Information Resources Management College

Software Assurance in Acquisition: Mitigating Risks to the Enterprise

by Mary Linda Polydys
and Stan Wisseman

occasional paper

SwA Acquisition & Outsourcing Handbook



Information Resources Management College

February 2009

Software Assurance in Acquisition: Mitigating Risks to the Enterprise

by Mary Linda Polydys and Stan Wisseman

occasional paper

Software Supply Chain Risk Management and Due-Diligence -- Table 1 –SwA Concern Categories

SwA Concern Categories	Risks	Purpose for Questions
Software History and Licensing **Development Process Management** **Software Security Training and Awareness** **Planning and Requirements** **Architecture and Design** **Software Development** **Built-in Software Defenses** **Component Assembly** **Testing** **Software Manufacture and Packaging** **Installation** **Assurance Claims and Evidence** **Support** **Software Change Management** **Timeliness of Vulnerability Mitigation** **Individual Malicious Behavior** **Security "Track Record"** **Financial History and Status** **Organizational History** **Foreign Interests and Influences** **Service Confidentiality Policies** **Operating Environment for Services** **Security Services and Monitoring**		

Software Supply Chain Risk Management and Due-Diligence -- Table 1 –SwA Concern Categories

SwA Concern Categories	Risks	Purpose for Questions
Software History and Licensing	The software supplier’s development practice in using code of unknown origin may be unable to produce trustworthy software.	To address supply chain concerns and identify risks pertaining to history/pedigree of software during any and all phases of its life cycle that should have been considered by the supplier.
Development Process Management	If supplier project management does not perceive the value of SwA and enforce best practices, they will not be consistently implemented.	To determine whether project management enforces software assurance–related best practices.
Software Security Training and Awareness	Developers unaware of software assurance best practices are likely to implement software with security flaws (making it more susceptible to attack).	To determine whether training of developers in SwA best practices is a supplier policy and practice.
Planning and Requirements	If nonfunctional requirements (security, quality, safety) are not specified, developers will not implement them.	To determine whether the supplier’s requirements analysis process explicitly addresses SwA requirements.
Architecture and Design	The software may be designed without considering security or minimization of exploitable defects.	To determine how security is considered during the design phase.
Software Development	If developers lack qualified tools or if personnel are allowed to inappropriately access or change configuration items in the development environment, then delivered software might have unspecified features. The supplier might lack sufficient process capability to deliver secure products, systems or services.	To ascertain that the supplier has and enforces policies and SwA practices in the development of software that use secure software development environments to minimize risk exposures.
Built-in Software Defenses	The software may lack preventive measures to help it resist attack effectively and proactively.	To ensure that capabilities are designed to minimize the exposure of the software’s vulnerabilities to external threats and to keep the software in a secure state regardless of the input and parameters it receives from its users or environment.

Software Supply Chain Risk Management and Due-Diligence -- Table 1 –SwA Concern Categories

SwA Concern Categories	Risks	Purpose for Questions
Component Assembly	Insufficient analysis of software components used to assemble larger software packages may introduce vulnerabilities to the overall package.	To ensure that the software components are thoroughly vetted for their security properties, secure behaviors, and known types of weaknesses that can lead to exploitable vulnerabilities.
Testing	Software released with insufficient testing may contain an unacceptable number of exploitable defects.	To determine whether the appropriate set of analyses, reviews, and tests are performed on the software throughout the life cycle which evaluate security criteria.
Software Manufacture and Packaging	Vulnerabilities or malicious code could be introduced in the manufacturing or packaging process.	To determine how the software goes through the manufacturing process, how it is packaged, and how it remains secure.
Installation	The software may not install as advertised and the acquirer may not get the software to function as expected.	To ensure the supplier provides an acceptable level of support during the installation process.
Assurance Claims and Evidence	Supplier assurance claims (with supporting evidence) may be non-existent or insufficiently verified.	To determine how suppliers communicate their claims of assurance; ascertain what the claims have been measured against, and identify at what levels they will be verified.
Support	Supplier ceases to supply patches and new releases prior to the acquirer ending use of software. Vulnerabilities may go unmitigated.	To ensure understanding of supplier policy for security fixes and when products are no longer supported.
Software Change Management	Weak change control procedures can corrupt software and introduce new security vulnerabilities.	To determine whether software changes are adequately assessed and verified by supplier management.
Timeliness of Vulnerability Mitigation	Sometimes it can be extremely difficult to make a software supplier take notice and repair software to mitigate reported vulnerabilities.	To ensure security defects and configuration errors are fixed properly and in a timely fashion.

Software Supply Chain Risk Management and Due-Diligence -- *Table 1 –SwA Concern Categories*

SwA Concern Categories	Risks	Purpose for Questions
Individual Malicious Behavior	A developer purposely inserts malicious code, and supplier lacks procedures to mitigate risks from insider threats within the supply chain.	To determine whether the supplier has and enforces policies to minimize individual malicious behavior.
Security "Track Record"	A software supplier that is unresponsive to known software vulnerabilities may not mitigate/patch vulnerabilities in a timely manner.	To establish insight into whether the supplier places a high priority on security issues and will be responsive to vulnerabilities they will need to mitigate.
Financial History and Status	A software supplier that goes out of business will be unable to provide support or mitigate product defects and vulnerabilities.	To identify documented financial conditions or actions of the supplier that may impact its viability and stability, such as mergers, sell-offs, lawsuits, and financial losses.
Organizational History	There may be conflicting circumstances or competing interests within the organization that may lead to increased risk in the software development.	To understand the supplier's organizational background, roles, and relationships that might have an impact on supporting the software.
Foreign Interests and Influences	There may be controlling foreign interests (among organization officers or from countries) with malicious intent to the users' country or organization planning to use the software.	To help identify supplier companies that may have individuals with competing interests or malicious intent to a domestic buyer/user.
Service Confidentiality Policies	Without policies to enforce client data confidentiality/ privacy, acquirer's data could be at risk without service supplier liability.	To determine the service provider's confidentiality and privacy policies and ensure their enforcement.
Operating Environment for Services	Operating environment for the services may not be hardened or otherwise secure.	To understand the controls the supplier has established to operate the software securely.
Security Services and Monitoring	Insufficient security monitoring may allow attacks to impact services.	To ensure software and its operating environment are regularly reviewed for adherence to SwA requirements through periodic testing and evaluation.

Table 2- Questions for COTS (Proprietary & Open Source), GOTS, & Custom Software

	No	Question	COTS Propri-etary	COTS Open-Source	GOTS	Custom
→	1	Can the pedigree of the software be established? Briefly explain what is known of the people and processes that created the software.	✓	✓	✓	✓
→	2	Explain the change management procedure that identifies the type and extent of changes conducted on the software throughout its life cycle.	✓		✓	✓
→	3	What type of license(s) are available for the open source software? Is it compatible with other software components in use? Is indemnification provided, and will the supplier indemnify the purchasing organization from any issues in the license agreement? Explain.	✓	✓		✓
	4	Is there a clear chain of licensing from original author to latest modifier? Describe the chain of licensing.	✓			
	5	What assurances are provided that the licensed software does not infringe upon any copyright or patent? Explain.	✓		✓	✓
	6	Does the company have corporate policies and management controls in place to ensure that only corporate-approved (licensed and vetted) software components are used during the development process? Explain.	✓			✓
→	7	Are licensed software components still valid for the intended use?	✓		✓	
→	8	Is the software in question original source or a modified version?		✓		
	9	Has the software been reviewed to confirm that it does not infringe upon any copyright or patent?	✓	✓		✓
→	10	How long has the software source been available? Is there an active user community providing peer review and actively evolving the software?	✓	✓		

Table 2- Questions for COTS (Proprietary & Open Source), GOTS, and Custom Software

No.	Question	COTS Propri-etary	COTS Open-Source	GOTS	Custom
→ 11	Does the license/contract restrict the licensee from discovering flaws or disclosing details about software defects or weaknesses with others (e.g., is there a "gag rule" or limits on sharing information about discovered flaws)?	✓			✓
→ 12	Does the license/contract restrict communications or limit the licensee in any potential communication with third-party advisors about provisions for support (e.g., is there a "gag rule" or limits placed on the licensee that affect ability to discuss contractual terms or breaches) regarding the licensed or contracted product or service?	✓			✓
13	Does software have a positive reputation? Does software have a positive reputation relative to security? Are there reviews that recommend it?	✓	✓		
→ 14	Is the level of security where the software was developed the same as where the software will operate?			✓	✓
	Development Process Management				
15	What are the processes (e.g., ISO 9000, CMMI, etc.), methods, tools (e.g., IDEs, compilers), techniques, etc. used to produce and transform the software (brief summary response)?	✓		✓	✓
→ 16	What security measurement practices and data does the company use to assist product planning?	✓			✓
→ 17	Is software assurance considered in all phases of development? Explain.	✓		✓	✓
→ 18	How is software risk managed? Are anticipated threats identified, assessed, and prioritized?	✓		✓	✓

Table 1 –SwA Concern Categories -- (with interests relevant to security and privacy)		
SwA Concern Categories	**Risks**	**Purpose for Questions**
Service Confidentiality Policies	Without policies to enforce client data confidentiality/ privacy, acquirer's data could be at risk without service supplier liability.	To determine the service provider's confidentiality and privacy policies and ensure their enforcement.

Table 3 - Questions for Hosted Applications	
No.	Questions
Service Confidentiality Policies	
1	What are the customer confidentiality policies? How are they enforced?
2	What are the customer privacy policies? How are they enforced?
3	What are the policies and procedures used to protect sensitive information from unauthorized access? How are the policies enforced?
4	What are the set of controls to ensure separation of data and security information between different customers that are physically located in the same data center? On the same host server?
Operating Environment for Services	
5	Who configures and deploys the servers? Are the configuration procedures available for review, including documentation for all registry settings?
7	What are the data backup policies and procedures? How frequently are the backup procedures verified?
11	What are the agents or scripts executing on servers of hosted applications? Are there procedures for reviewing the security of these scripts or agents?
12	What are the procedures and policies used to approve, grant, monitor and revoke access to the servers? Are audit logs maintained?
13	What are the procedures and policies for handling and destroying sensitive data on electronic and printed media?
15	What are the procedures used to approve, grant, monitor, and revoke file permissions for production data and executable code?

More Due-Diligence Questions Relevant to Acquisition & Outsourcing

- Relevant to deliberate actions that are controllable and preventable by developers that have security implications
  - “Were any compiler warnings disabled for the software being delivered?”

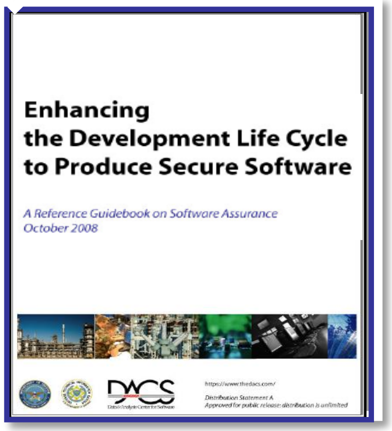
- Relevant to hosted applications and services
  - Cloud computing, “XXXX_as a Service,” SOA,

Seeking more examples from “security aware” community

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Many SwA Resources Focus On Development



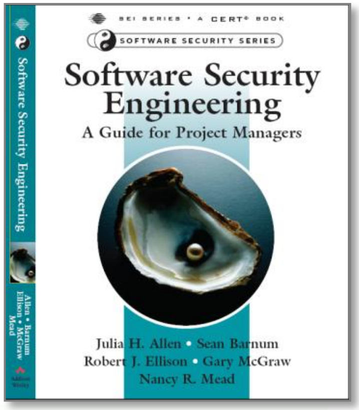
Enhancing the Development Life Cycle to Produce Secure Software

A Reference Guidebook on Software Assurance
October 2008

DACS

https://www.thedacs.com/

Distribution Statement A
Approved for public release: distribution is unlimited



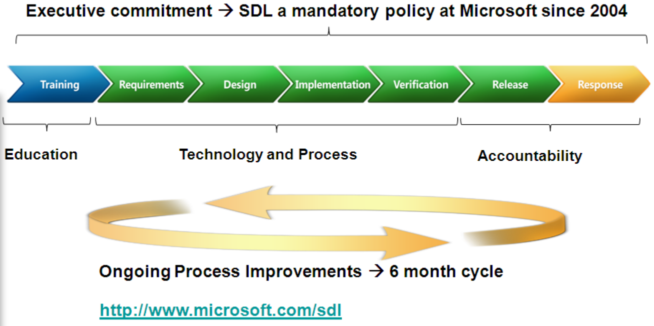
SEI SERIES • A CERT® BOOK

SOFTWARE SECURITY SERIES

Software Security Engineering

A Guide for Project Managers

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



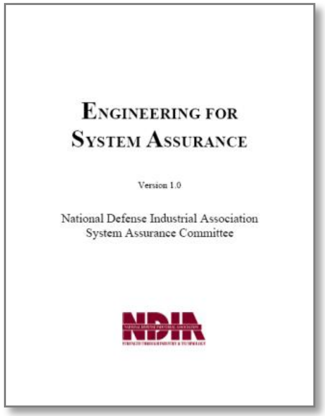
Executive commitment → SDL a mandatory policy at Microsoft since 2004

Training | Requirements | Design | Implementation | Verification | Release | Response

Education | Technology and Process | Accountability

Ongoing Process Improvements → 6 month cycle

http://www.microsoft.com/sdl

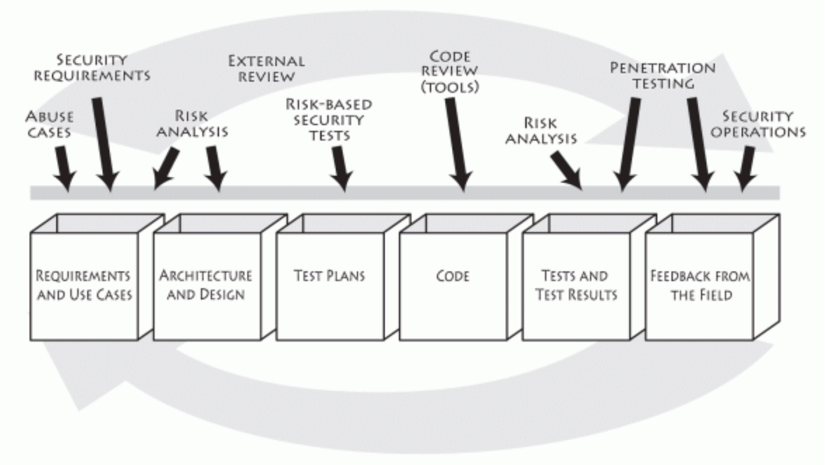


Engineering for System Assurance

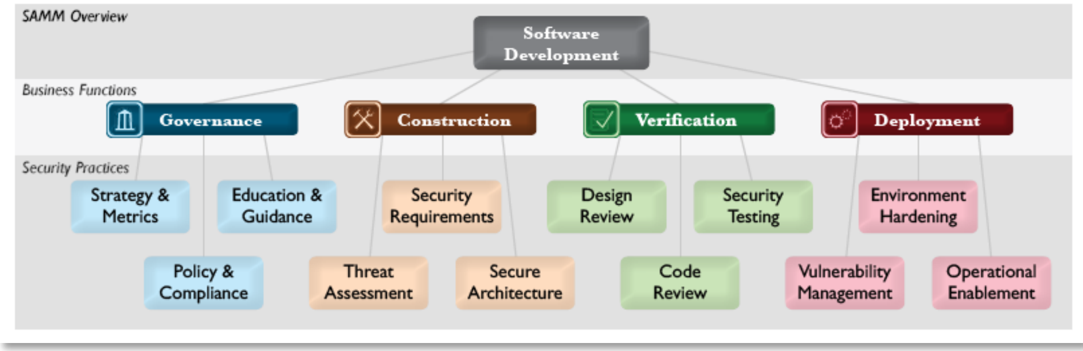
Version 1.0

National Defense Industrial Association
System Assurance Committee

NDIA



Assurance for CMMI ®



SAMM Overview

Software Development

Business Functions

Governance | Construction | Verification | Deployment

Security Practices

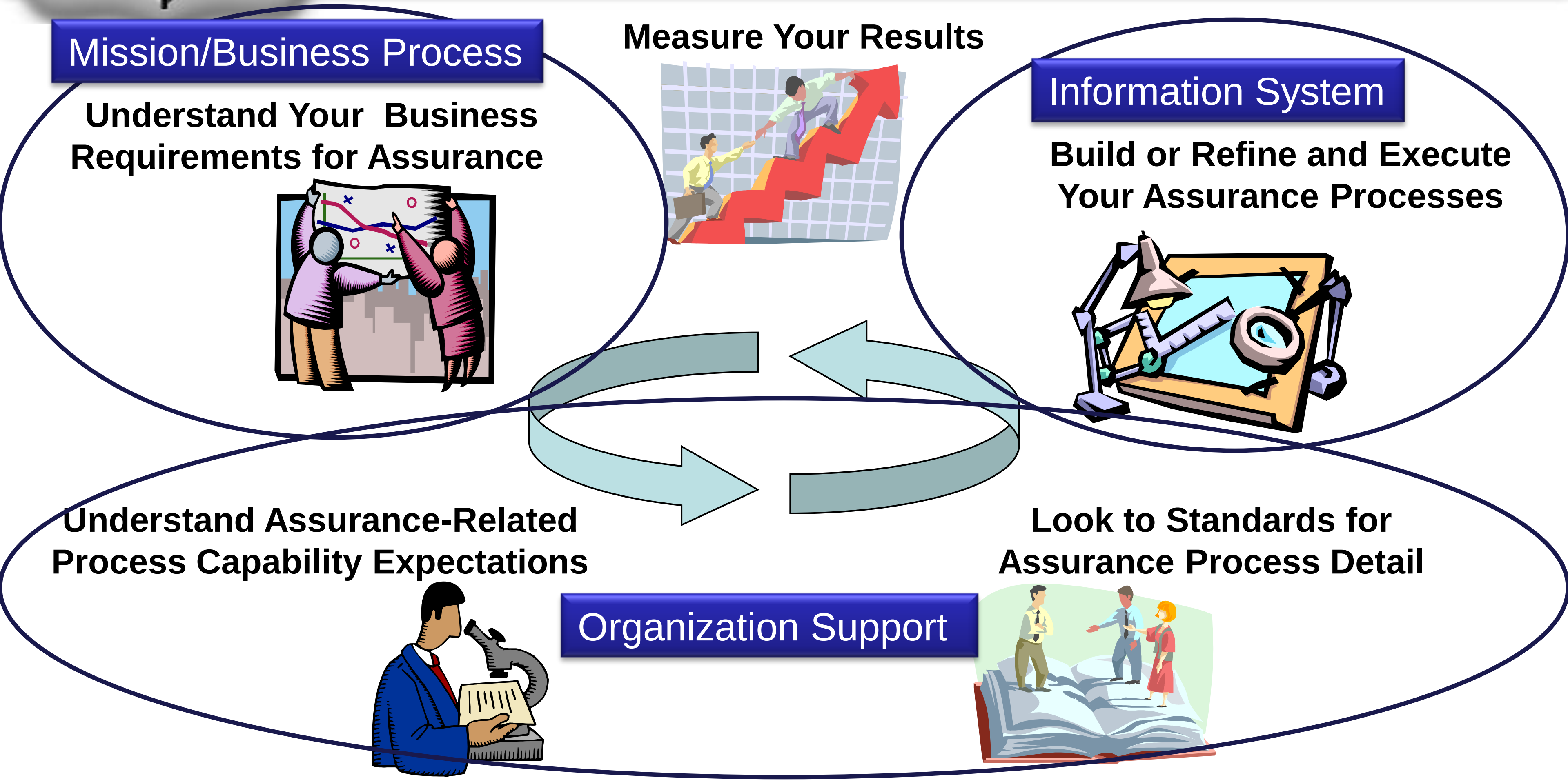
Strategy & Metrics; Education & Guidance; Policy & Compliance

Security Requirements; Threat Assessment; Secure Architecture

Design Review; Security Testing; Code Review

Environment Hardening; Vulnerability Management; Operational Enablement

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

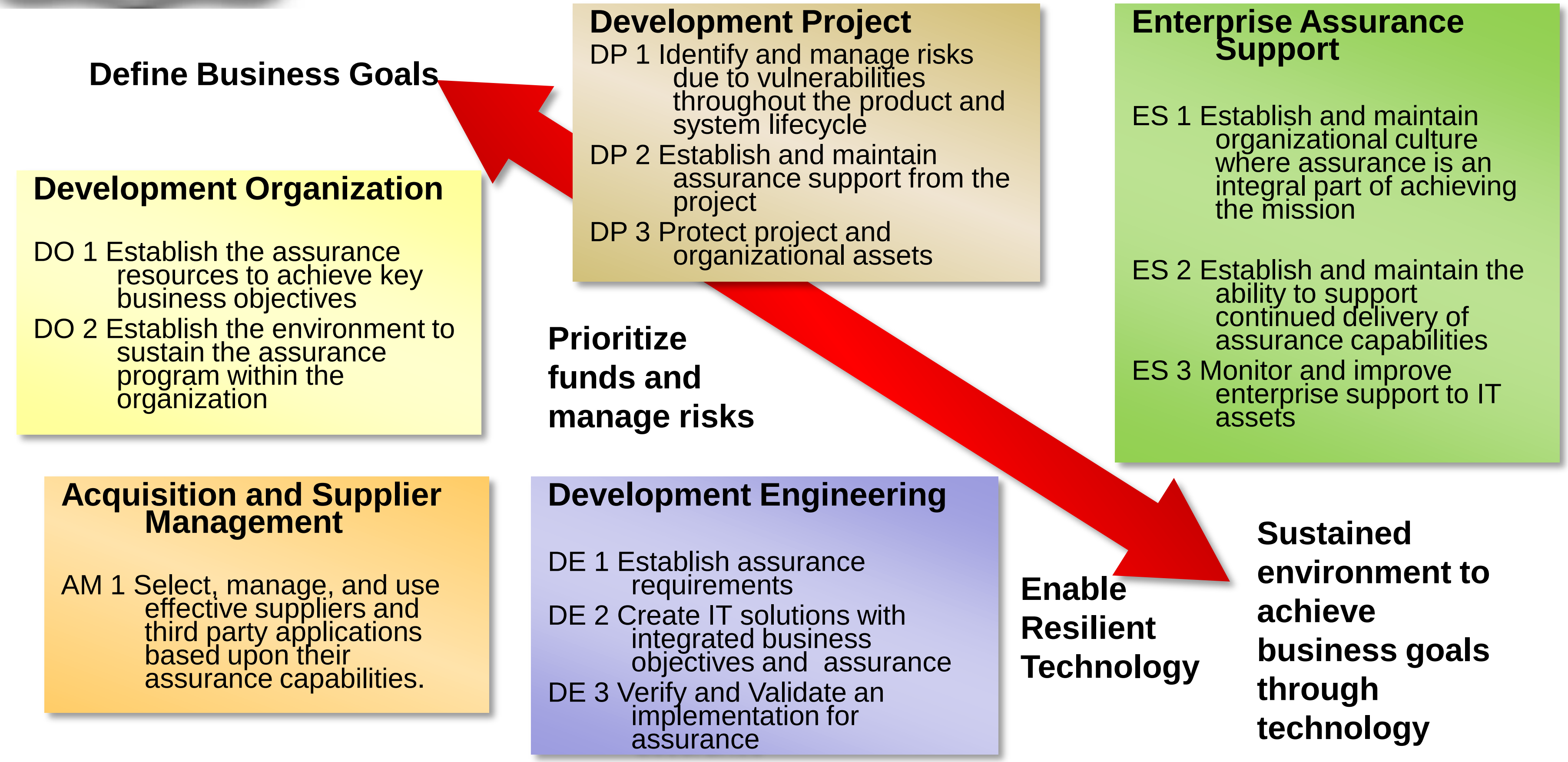
Organization Support

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

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

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

The Process Reference Model For Assurance

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.

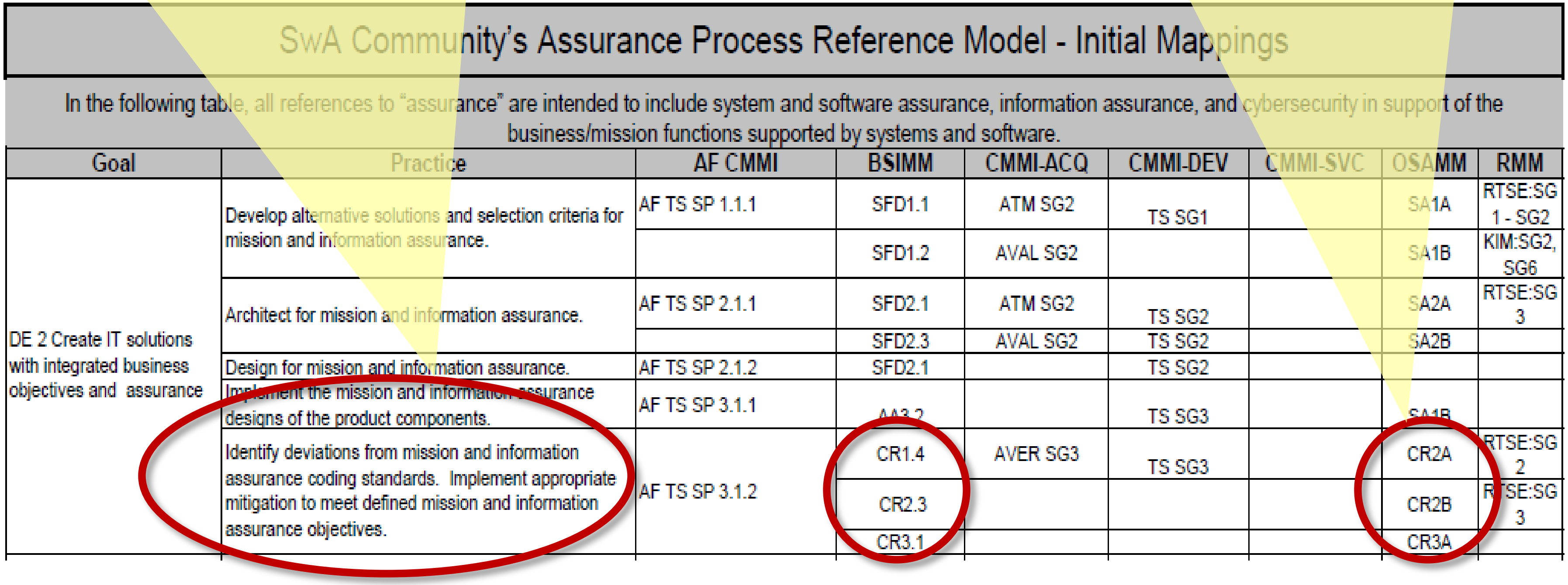
Goal	Practice	Practice Implementation Level	Notes
Development – Engineering			
DE 1 Establish assurance requirements	Understand the operating environment and define the operating constraints for mission and information assurance within the environments of system development.		
	Develop customer mission 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***

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

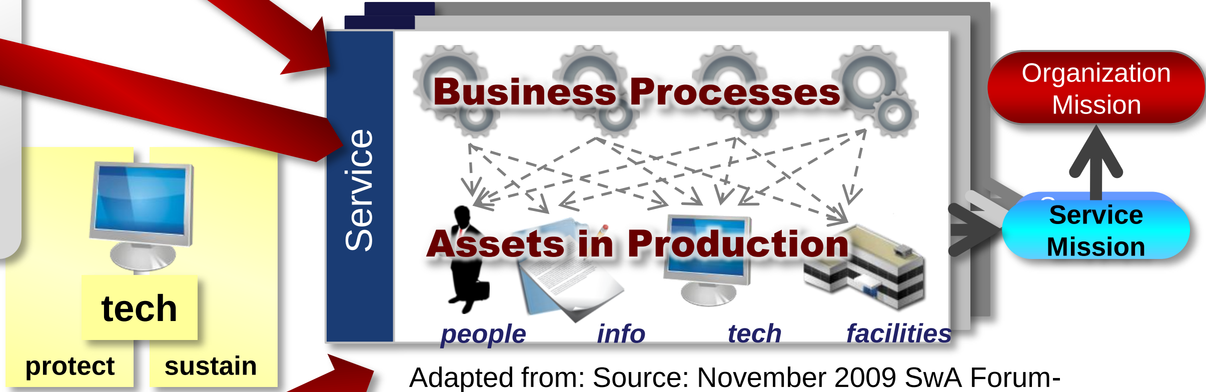
Enterprise Assurance Support

CTO

Enable Resilient Technology

Development Project

Development Engineering

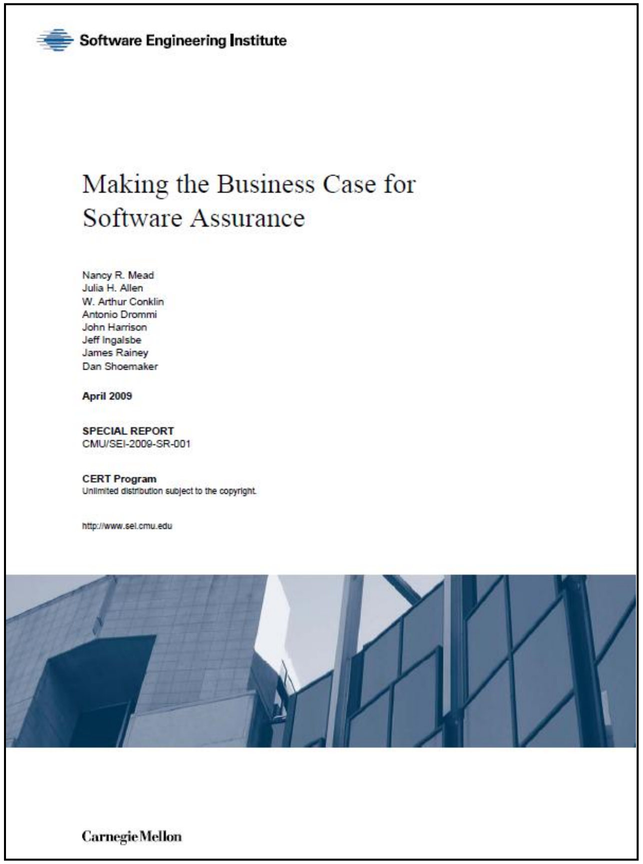


Adapted from: Source: November 2009 SwA Forum- Evolution in SwA Processes Panel – David White, SEI

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

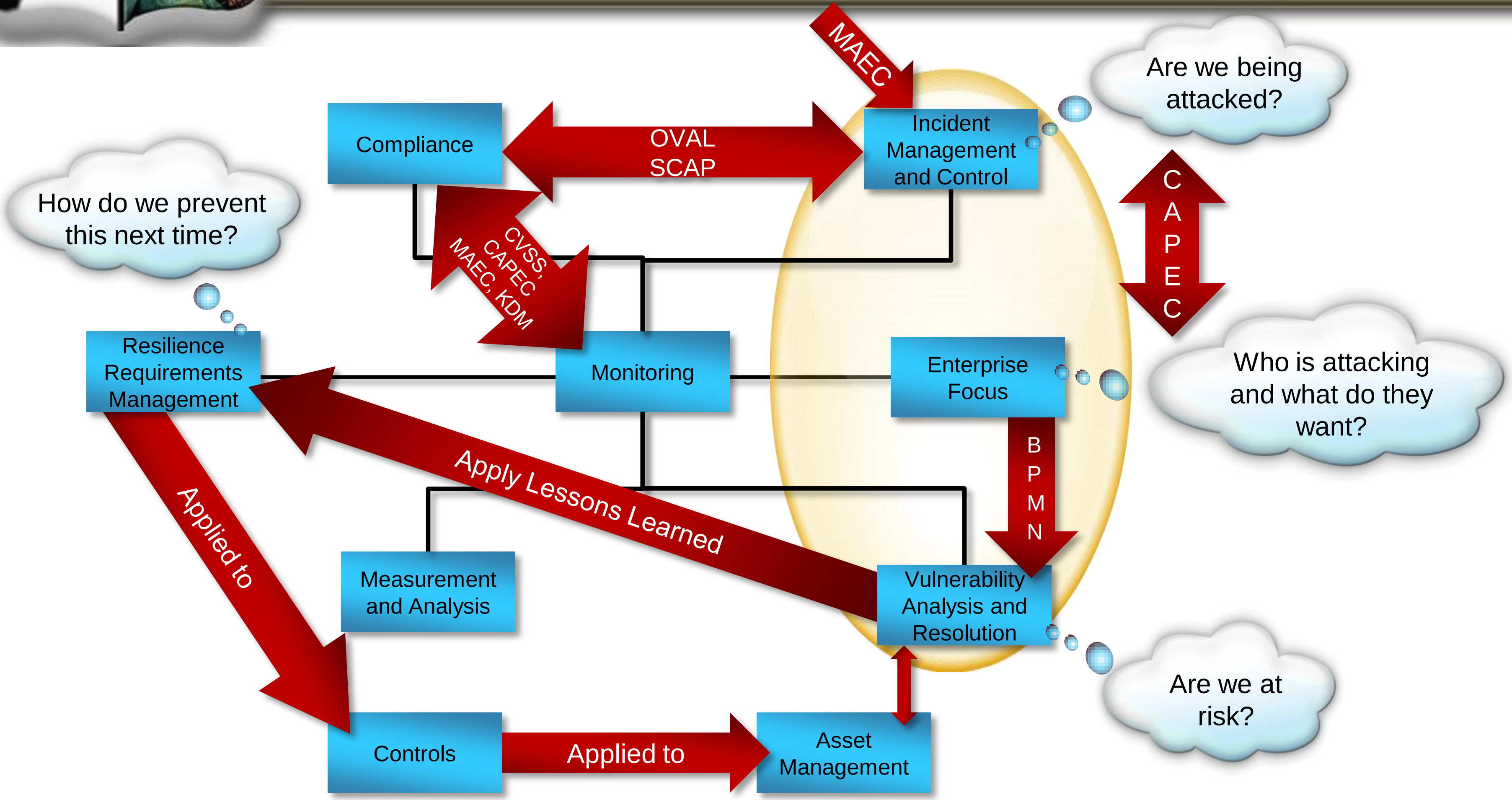
SPECIAL REPORT
CMU/SEI-2009-SR-001

CERT Program
Unlimited distribution subject to the copyright.

http://www.sei.cmu.edu

CarnegieMellon

SwA and Operational Resilience



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

Courtesy of Michele Moss

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 evolve to better address supply chain risk management, IT security, systems & software assurance, and measurement
  - 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 Forum 12-16 Sep 2011 at SEI, Arlington, VA

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

SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

Homeland Security

Commerce

National Defense

Next SwA Forum 12-16 Sep 2011 at SEI, Arlington, VA

Working for Homeland Security

The DHS Office of Cybersecurity and Communications (CS&C) serves as the national focal point for securing cyber space and the nation's cyber assets.

CS&C is actively seeking top notch talent in several areas including:

- Software assurance
- Information technology
- Telecommunications
- Program management
- Public affairs

To learn more about CS&C and potential career opportunities, please visit USAJOBS at www.usajobs.gov .