Reducing Risks in the Software Acquisition Life Cycle

Stan Wisseman
October 2008

Agenda

- Buyers vs. Sellers

- Need for enhancing acquisition process with SwA considerations

- DHS SwA Initiative
  - Overview
  - Acquisition Working Group

- Acquisition Phases
  - Planning
  - Contracting
  - Implementation and Acceptance
  - Follow-on

- DHS SwA Working Group Portal

We all need to be aware of our needs and potential risks when we make a purchase

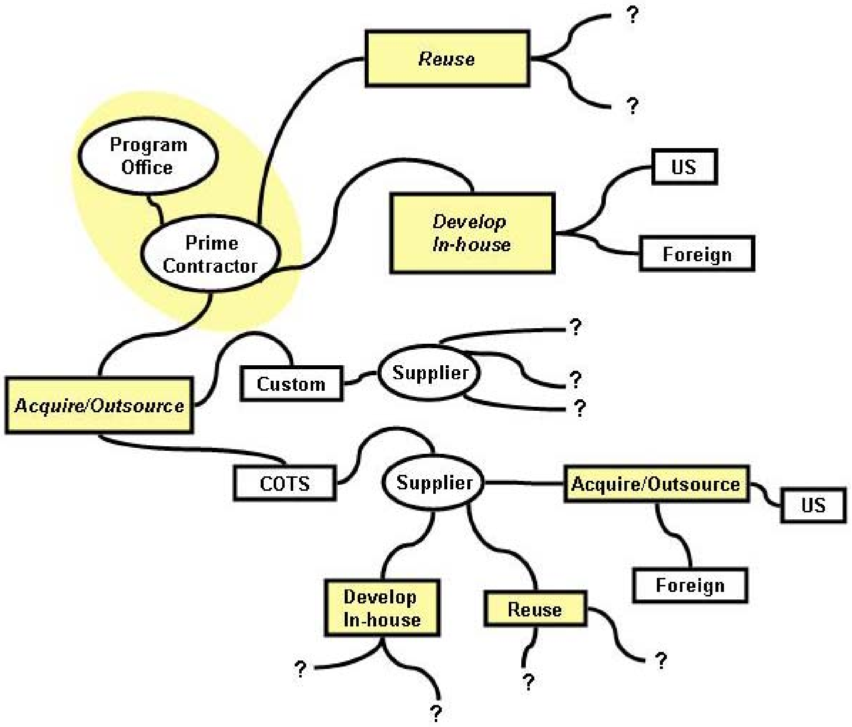
- When you purchase a car, you do the research, find a dealer and purchase the car, drive the car, pay off your loan and start again. With the acquisition process, you do your planning, you offer the contract, then implement the product or service, finally you go through the follow-on phase.

- With a car, you don't want to wait until after an accident to have safety features. Similarly, you don't want to wait until there is a security breech to worry about security features. Making sure you get the security features you want and assurances you need could save time and money in the long run.

You want to end up with a car that you want to drive – not a lemon

There are two sides to software acquisition

- There are buyers and sellers…
  - **Buyers** issue RFPs to acquire software and systems. Their point of reference is the acquisition lifecycle. These are typically government agencies and prime contractors. Their point of reference is the acquisition lifecycle.
  - **Sellers** are vendors, software developers, and integrators who develop software and build systems for sale to the government based on a contract. Their point of reference is the software development lifecycle.



Modified Walker, E. (2005, July). Software Development Security: A Risk Management Perspective. In *The DoD Software Tech News—Secure Software Engineering.* Vol*(8)*No*(2)*.

Acquisition is the first step to security. If security is not integrated during acquisition, unplanned costs could jeopardize the project

Quality without Security: 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.
  - ❑ most exploitable software vulnerabilities related to insecure coding practices.
  - ❑ **75% of hacks occurred at application level**
  - – 90% of software attacks were aimed at application layer (Gartner & Symantec, June 2006).
- Functional Correctness must be exhibited even when software is subjected to abnormal and hostile conditions; therefore,
  - ❑ in an era riddled with asymmetric cyber attacks, claims about system reliability, integrity and safety must also include provisions for built-in security of the enabling software.

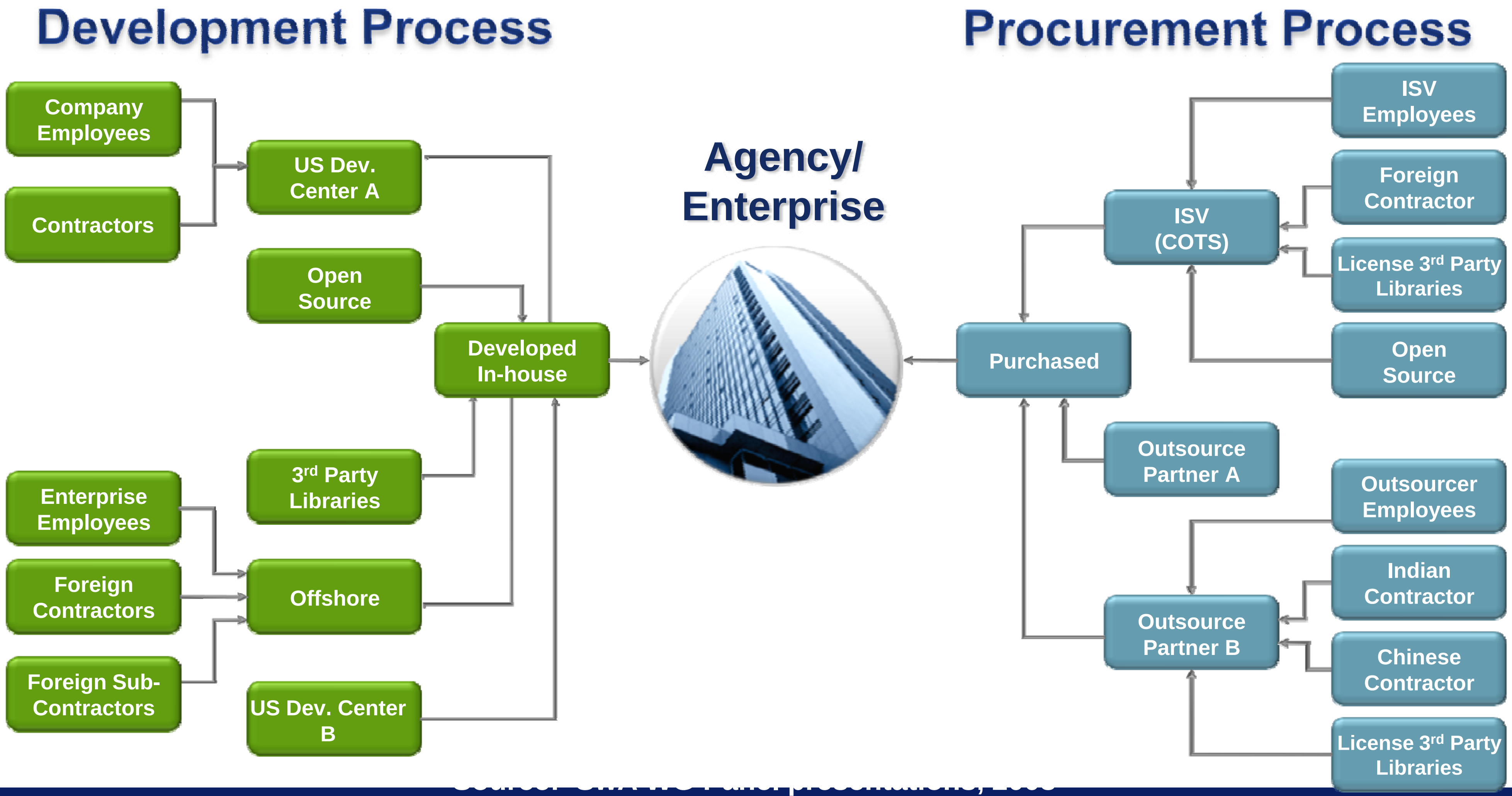
Software applications with exploitable vulnerabilities
SECURITY
Software applications with exploitable vulnerabilities

Adversaries have capabilities to subvert the IT/software supply chain

- Software & IT lifecycle processes offer opportunities to insert malicious code and to poorly design and build software which enables future exploitation.
- Government and businesses rely on COTS products and commercial developers using foreign and non-vetted domestic suppliers to meet majority of IT requirements.
- Off-shoring magnifies risks and creates new threats to security, business property and processes, and individuals' privacy – requires more comprehensive domestic strategies to mitigate those risks.
- Government lacks information on suppliers' process capabilities (business practices); cannot adequately determine security risks posed by the suppliers' products and services to the acquisition project and to the operations enabled by the software.

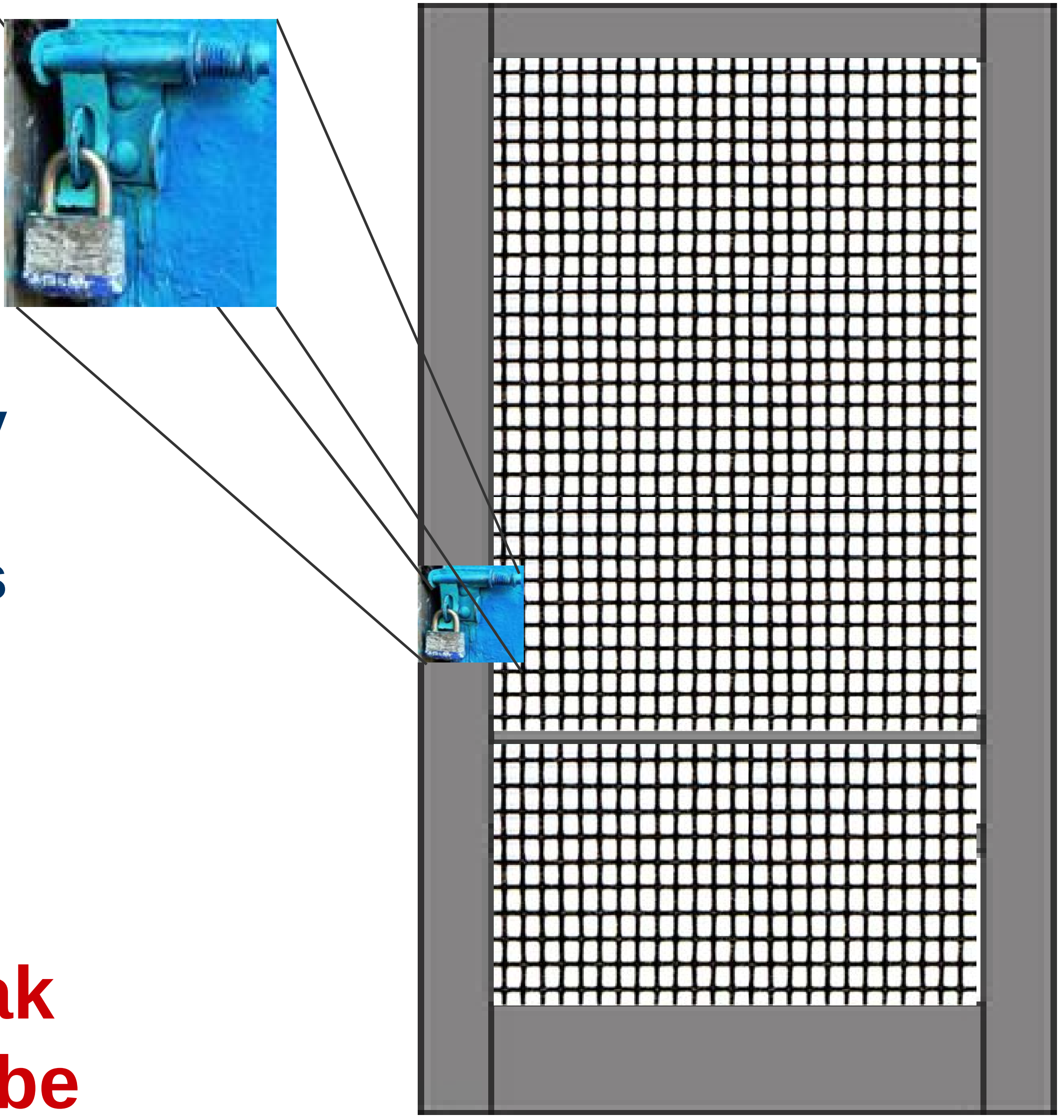
Illustration John Cuneo

Enterprise Processes: Increasingly Distributed and Complex: New Considerations for Quality & Security



Source: SwA WG Panel presentations, 200[illegible]

Need for more resilient products



Security Controls are necessary;
yet not sufficient, especially when considering the weaknesses in the products to which those controls and protection mechanisms are applied.

There is no need to break locks when access can be gained via other means.

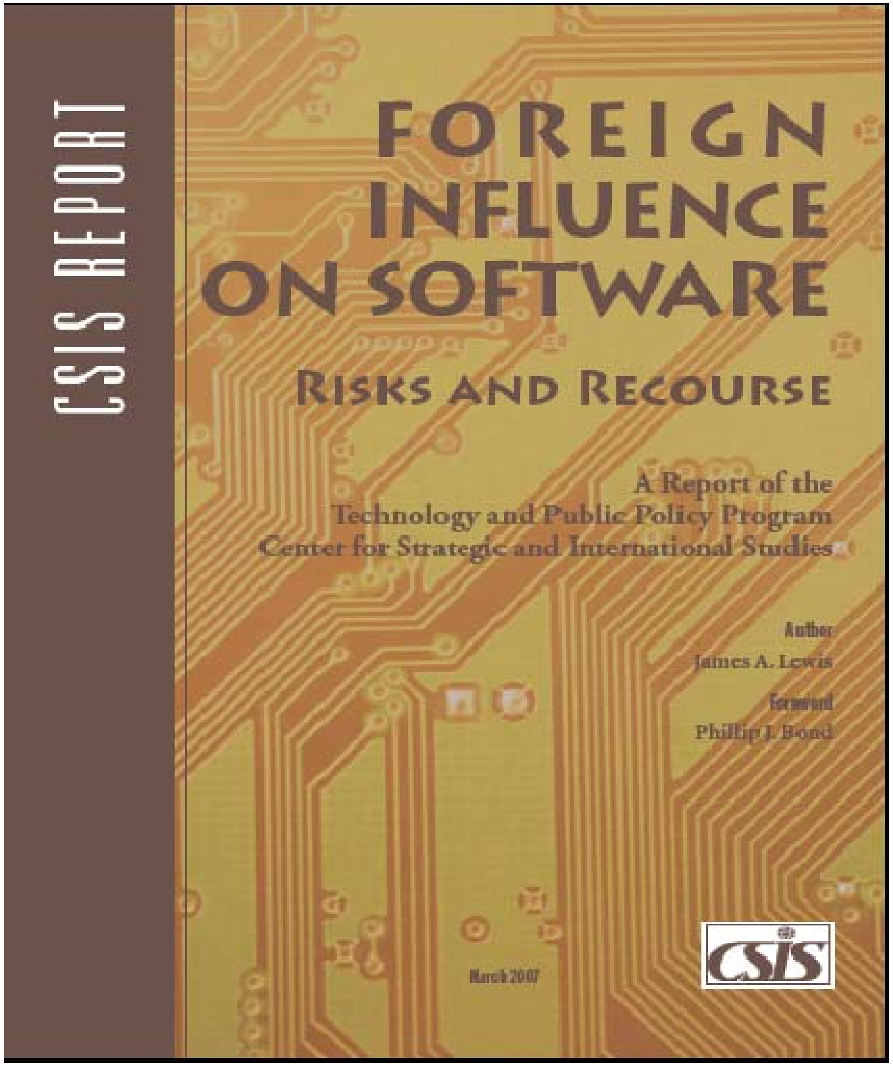
While more guidance is available, growing concern about inadequacies of suppliers' capabilities to deliver secure software

- Unknown development practices
  - How was the software built? What methodologies, practices, tools were used?
- Lack of visibility (the "black box" problem) (*OTS, legacy)
  - Questionable validity of security assumptions able to be made based solely on external observation of executing software
- Unknown review and testing regime
  - Only safe assumption: security was not considered during reviews, tests
- Security in sustainment
  - How committed is the supplier/development team long term to maintenance and patching?
  - Does the supplier/development team support bug and vulnerability reporting and tracking, with timely response?

Stack overflow at line: 1

Recommendations Addressing Globalization of Software
Center for Strategic and International Studies Report on Risks and Recourse

1. Assess risk (and share assessment)
2. Focus on assurance, not location
3. Avoid one-size-fits-all solutions
4. Refocus and reform existing certification processes
5. Identify commercial best practices and tools and expand their use
6. Create governance structure(s) for assurance
7. Accelerate info assurance efforts
8. Promote leadership in IT innovation



CSIS REPORT

FOREIGN INFLUENCE ON SOFTWARE

RISKS AND RECOURSE

A Report of the
Technology and Public Policy Program
Center for Strategic and International Studies

Author
James A. Lewis

Foreword
Phillip J. Bond

March 2007

CSIS

March 2007 Report

http://www.csis.org/media/csis/pubs/070323_lewisforeigninflubook.pdf

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

DHS Software Assurance (SwA) Forum and Working Groups * …

… encourage the production, evaluation and acquisition of better quality and more secure software through targeting

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

Products and Contributions

Build Security In - https://buildsecurityin.us-cert.gov and SwA community portal – http://.us-cert.gov/SwA

SwA Common Body of Knowledge (CBK) & Glossary SwA Developers' Guide on Security-Enhancing SDLC Systems Assurance Guide (via DoD and NDIA)

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

Software Security Assurance State of the Art Report

Practical Measurement Guidance for SwA/InfoSec

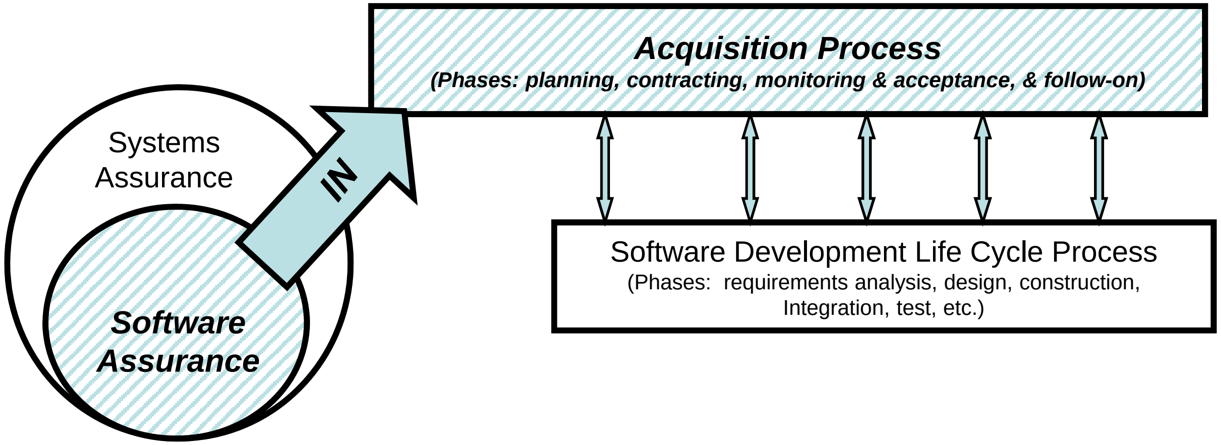
SwA Metrics & Tool Evaluation (with NIST) SwA Ecosystem w/ DoD, NSA, NIST, OMG & TOG NIST Special Pub 500 Series on SwA Tools

Common Weakness Enumeration (CWE) dictionary Common Attack Pattern Enumeration (CAPEC) Malware Identification & Enumeration (with ASC)

SwA in Acquisition: Mitigating Risks to the Enterprise

* 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.

Working Group produced document to help "build security in" and incorporate SwA considerations throughout the acquisition process


Acquisition Process
(Phases: planning, contracting, monitoring & acceptance, & follow-on)
Systems Assurance
IN
Software Assurance
Software Development Life Cycle Process
(Phases: requirements analysis, design, construction, Integration, test, etc.)

- Written from an acquisition process perspective versus the software development lifecycle process perspective
- For anyone, both government and private sector, involved in acquiring software products or services by contract, including work that is outsourced or sub-contracted
- NOT an exhaustive coverage of SwA considerations when acquiring software
- Co-chaired by Mary Polydys (NDU IRMC) and Stan Wisseman (Booz Allen)

Software Assurance in Acquisition: Mitigating Risks to the Enterprise

Version 1 will be published through the National Defense University Press (NDU) in Oct 2008

Executive Summary

1. Introduction

1.1 Background

1.2 Purpose and Scope

1.3 Audience—The Acquirer

1.4 Document Structure

2. Planning Phase

2.1 Needs Determination, Initial Risk Assessment, and Solution Alternatives

2.2 SwA Requirements

2.3 Acquisition Strategy and/or Plan

2.4 Evaluation Plan and Criteria

2.5 SwA Due Diligence Questionnaires

3. Contracting Phase

3.1 Request for Proposals
- 3.1.1 Work Statement
- 3.1.2 Terms and Conditions
- 3.1.3 Instructions to Suppliers
- 3.1.4 Certifications
- 3.1.5 Prequalification

3.2 Proposal Evaluation

3.3 Contract Negotiation and Contract Award

4. Implementation and Acceptance Phase

4.1 Contract Work Schedule

4.2 Change Control

4.3 Reviewing and Accepting Software Deliverables

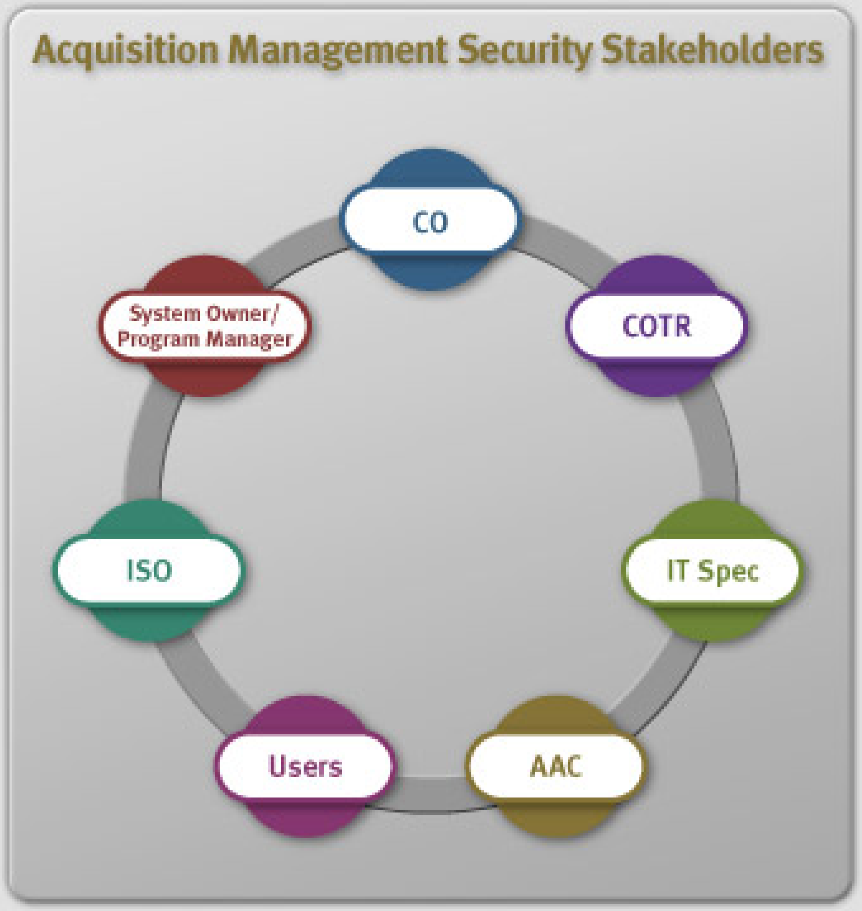
5. Follow-on Phase

5.1 Sustainment (or Post Release Support
- 5.1.1 Risk Management
- 5.1.2 Assurance Case Management—Transition to Ops
- 5.1.3 Other Change Management Considerations

5.2 Disposal or Decommissioning

Target audience are the industry and government acquisition officials involved in the acquisition/purchase of software by contract

- The generic term “acquisition official” is used to mean the members of the purchasing team.
- Guidance may also be used by suppliers (e.g., prime contractors, integrators, subcontractors, and vendors in the supply chain) to facilitate an understanding of what acquisition officials may request regarding SwA.

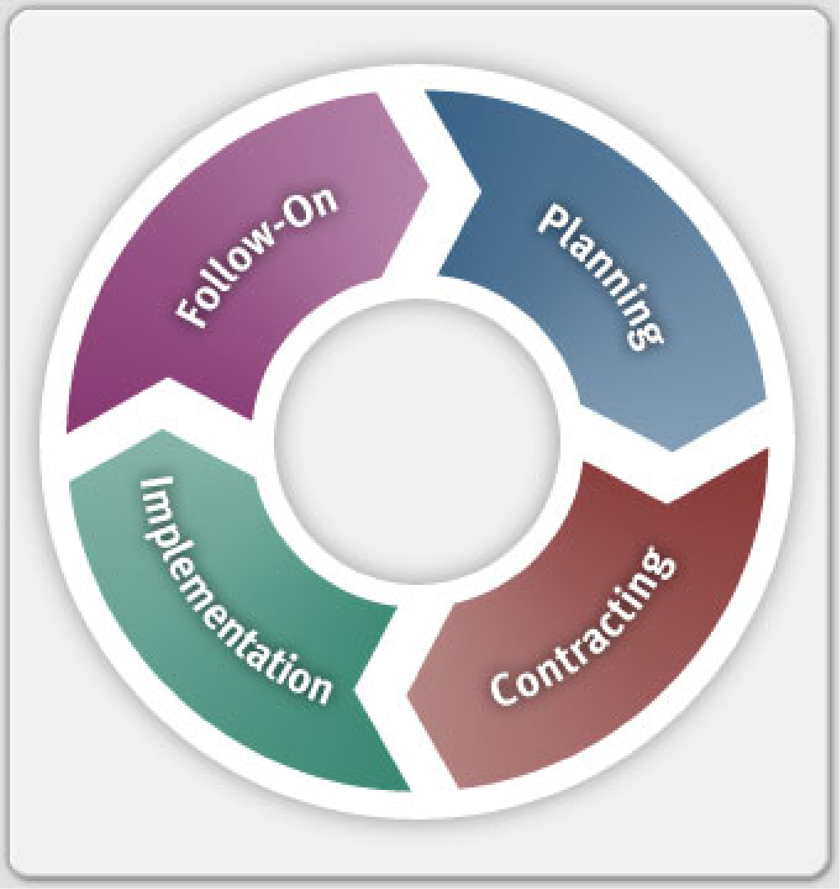

Acquisition Management Security Stakeholders
CO
COTR
IT Spec
AAC
Users
ISO
System Owner/ Program Manager

The objective is for acquirers to buy software that is more resistant to attack, has fewer vulnerabilities, and minimizes operational risks to the greatest extent possible

Acquisition officials should be able to:

- Understand the importance of integrating SwA practices within the software acquisition life cycle.
- Contractually capture SwA factors critical to the success of the acquisition and deployment of the application.
- Recognize risks that can be avoided or minimized.
- Implement security practices to be adopted by acquisition personnel.

Overview how to enhance Acquisition Life Cycle Phases with SwA Considerations

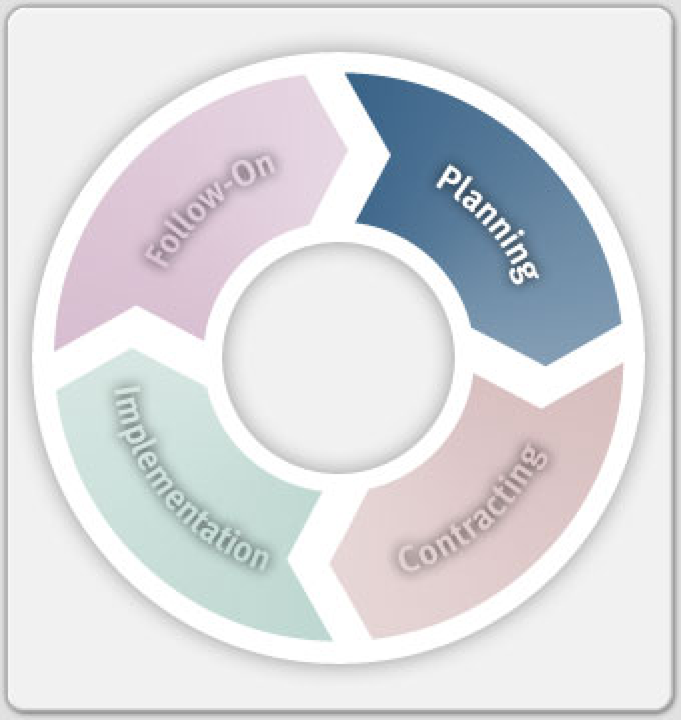


IEEE 1062 lifecycle is used in the acquisition guide, but phases are mapped to related acquisition lifecycles in other guides and standards

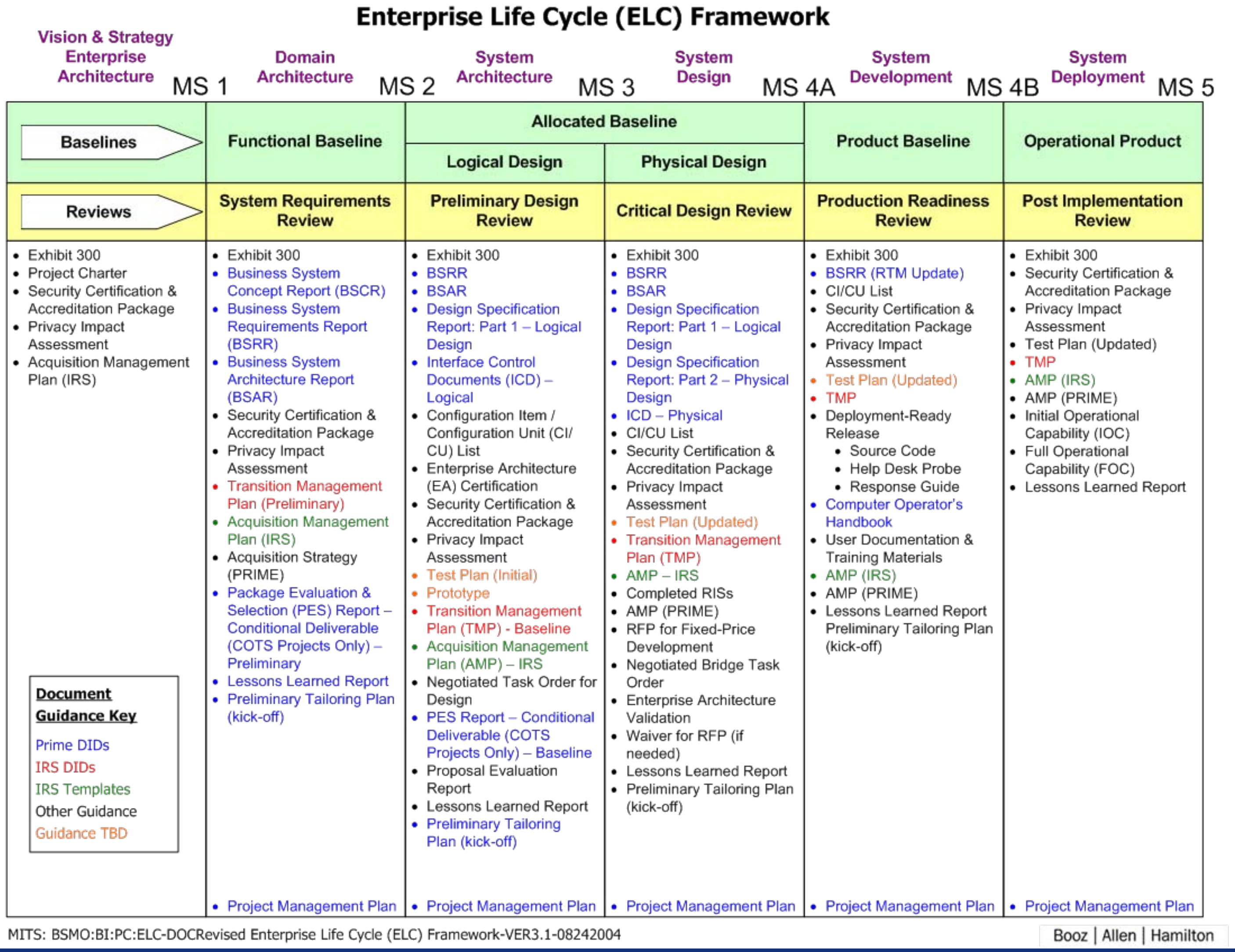
<table>
<tr><td>IEEE 1062</td><td colspan="2">Planning</td><td colspan="2">Contracting</td><td colspan="3">Implementation &amp; Acceptance</td><td colspan="2">Follow-on</td></tr>
<tr><td>NIST SP 800-64</td><td>Mission &amp; Business Planning</td><td>Acquisition Planning</td><td colspan="2">Acquisition</td><td colspan="2">Contract Performance</td><td colspan="2">Disposal &amp; Contract Closeout</td><td></td></tr>
<tr><td>DoDI 8000.2</td><td colspan="2">Pre-Systems Acquisition (Acquisition Strategy, e.g., concept &amp; technology development; contracting, and other strategies)</td><td colspan="5">Systems Acquisition
(Contracting for system development &amp; production/deployment)</td><td colspan="2">Sustainment (Operations &amp; Support)</td></tr>
<tr><td>ISO 12207 “Customer”</td><td colspan="2">Initiation</td><td>Request for Proposal</td><td>Contract Preparation &amp; Update</td><td>Supplier Monitoring</td><td colspan="2">Acceptance &amp; Completion</td><td colspan="2"></td></tr>
</table>

Acquisition planning

- Initial risk analysis
- Requirements analysis
- Alternative software approaches
- Acquisition Strategy and/or Plan
- Evaluation Plan and Criteria



Acquirers can help ensure they obtain the software and system security features and assurances they need to accomplish their missions – it starts with effective planning



Enterprise Life Cycle (ELC) Framework

Vision & Strategy Enterprise Architecture	Domain Architecture	System Architecture	System Design	System Development	System Deployment
MS 1	MS 2	MS 3	MS 4A	MS 4B	MS 5
Baselines	Functional Baseline	Allocated Baseline		Product Baseline	Operational Product
		Logical Design	Physical Design		
Reviews	System Requirements Review	Preliminary Design Review	Critical Design Review	Production Readiness Review	Post Implementation Review
• Exhibit 300 • Project Charter • Security Certification & Accreditation Package • Privacy Impact Assessment • Acquisition Management Plan (IRS)	• Exhibit 300 • Business System Concept Report (BSCR) • Business System Requirements Report (BSRR) • Business System Architecture Report (BSAR) • Security Certification & Accreditation Package • Privacy Impact Assessment • Transition Management Plan (Preliminary) • Acquisition Management Plan (IRS) • Acquisition Strategy (PRIME) • Package Evaluation & Selection (PES) Report – Conditional Deliverable (COTS Projects Only) – Preliminary • Lessons Learned Report • Preliminary Tailoring Plan (kick-off)	• Exhibit 300 • BSRR • BSAR • Design Specification Report: Part 1 – Logical Design • Interface Control Documents (ICD) – Logical • Configuration Item / Configuration Unit (CI/CU) List • Enterprise Architecture (EA) Certification • Security Certification & Accreditation Package • Privacy Impact Assessment • Test Plan (Initial) • Prototype • Transition Management Plan (TMP) - Baseline • Acquisition Management Plan (AMP) – IRS • Negotiated Task Order for Design • PES Report – Conditional Deliverable (COTS Projects Only) – Baseline • Proposal Evaluation Report • Lessons Learned Report • Preliminary Tailoring Plan (kick-off)	• Exhibit 300 • BSRR • BSAR • Design Specification Report: Part 1 – Logical Design • Design Specification Report: Part 2 – Physical Design • ICD – Physical • CI/CU List • Security Certification & Accreditation Package • Privacy Impact Assessment • Test Plan (Updated) • Transition Management Plan (TMP) • AMP – IRS • Completed RISs • AMP (PRIME) • RFP for Fixed-Price Development • Negotiated Bridge Task Order • Enterprise Architecture Validation • Waiver for RFP (if needed) • Lessons Learned Report • Preliminary Tailoring Plan (kick-off)	• Exhibit 300 • BSRR (RTM Update) • CI/CU List • Security Certification & Accreditation Package • Privacy Impact Assessment • Test Plan (Updated) • TMP • Deployment-Ready Release • Source Code • Help Desk Probe • Response Guide • Computer Operator's Handbook • User Documentation & Training Materials • AMP (IRS) • AMP (PRIME) • Lessons Learned Report Preliminary Tailoring Plan (kick-off)	• Exhibit 300 • Security Certification & Accreditation Package • Privacy Impact Assessment • Test Plan (Updated) • TMP • AMP (IRS) • AMP (PRIME) • Initial Operational Capability (IOC) • Full Operational Capability (FOC) • Lessons Learned Report
	• Project Management Plan	• Project Management Plan	• Project Management Plan	• Project Management Plan	• Project Management Plan

Document Guidance Key

Prime DIDs
IRS DIDs
IRS Templates
Other Guidance
Guidance TBD

MITS: BSMO:BI:PC:ELC-DOCRevised Enterprise Life Cycle (ELC) Framework-VER3.1-08242004

Booz | Allen | Hamilton

Performing an initial risk analysis helps determine the security category, baseline security controls, and assurance case required

- Acquisition officials should ask and have answered (by the application owner) the following questions*:
  - What is the value we need to protect?
  - To sustain this value, what software and information assets need to be protected? Why do they need to be protected? What happens if they're not protected?
  - What is the impact if the software behaves unpredictably? What is the *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability)?
  - What potential adverse conditions and consequences need to be prevented and managed? At what cost? How much disruption can we stand before we take action?
  - How is residual risk (the risk remaining after mitigation actions are taken) determined and effectively managed?
  - How will application security controls work together with its operating environment to control and mitigate risk?
  - How are the answers to these questions integrated into an effective, implementable, enforceable security strategy and plan?

**Allen 05; BSI Governance & Management article "How Much Security Is Enough?"*

When considering alternative approaches, acquisition officials and system/application owners should seek to reduce or manage the risks identified in the initial risk analysis

- Evaluate alternatives for treatment of risks (accept, mitigate, avoid, transfer, share with a third party (such as the supplier))
- Identify protection strategies that reduce risks to levels that are within acceptable tolerances.
- Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness.
- Identify approaches for managing residual risks that remain after protection strategies are adopted.

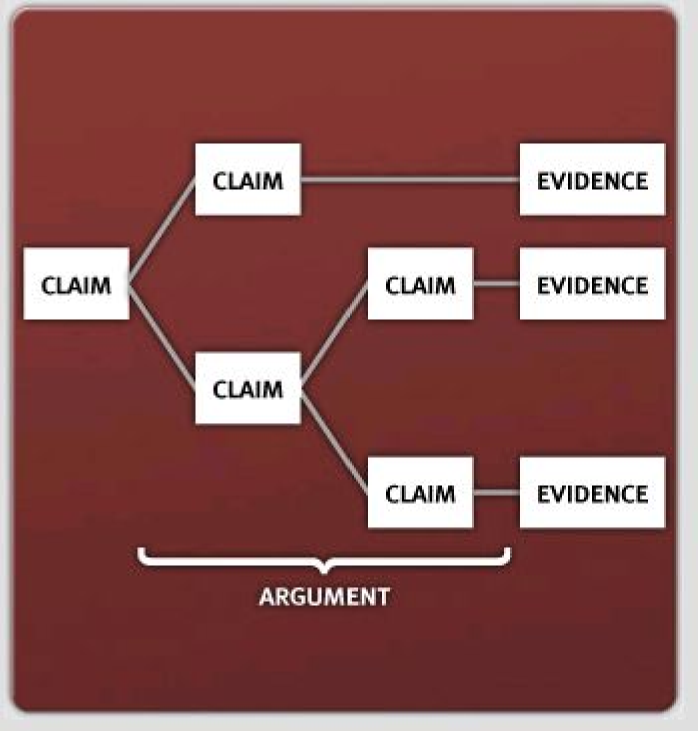
Alternative software approaches may include one or more software types or services – and each has their own risks

- Analyze risks of obtaining software from:
  - In-house custom development
  - Outsourced custom development
  - COTS
  - GOTS
  - Integration services
  - Open source software
  - Hosted services

- Software Due Diligence Questionnaires are a tool that provide a means for gathering information to evaluate quantitative, qualitative, and/or “go/no-go” Software Assurance criteria.

Including security in the initial requirements analysis is critical

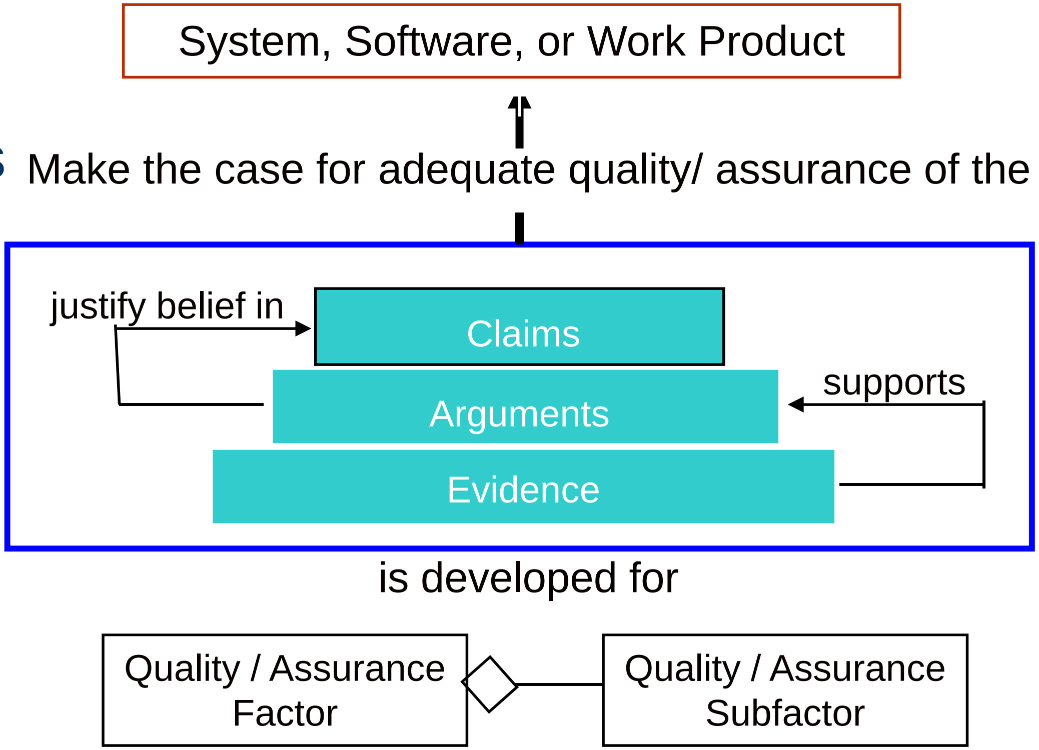
- Cannot assume security will be addressed by the developers by default.
- Based on security categories, determine minimum level of security controls.
- Augment with application-level functional and non-functional security requirements.
- Require an Assurance Case:
  - "a body of evidence organized into an argument demonstrating that some claim about a system holds, i.e., is assured. An assurance case is needed when it is important to who that a system exhibits some complex property such as safety, security, or reliability." Software Engineering Institute and DHS National Cyber Security Division



Suppliers should be able to describe an Assurance Case for their software and explain how claims can be validated

What constitutes sufficient Evidence to support Arguments that justify Claims?

How might “scaling” be structured to enable and encourage more suppliers and acquirers to make use of assurance cases?


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

Adopted from US TAG ISO/IEC 15026 proposal May 2007 and CMU SEI QUASAR tutorial by Donald Firesmith, March 2007

SwA considerations may impact contractual requirements

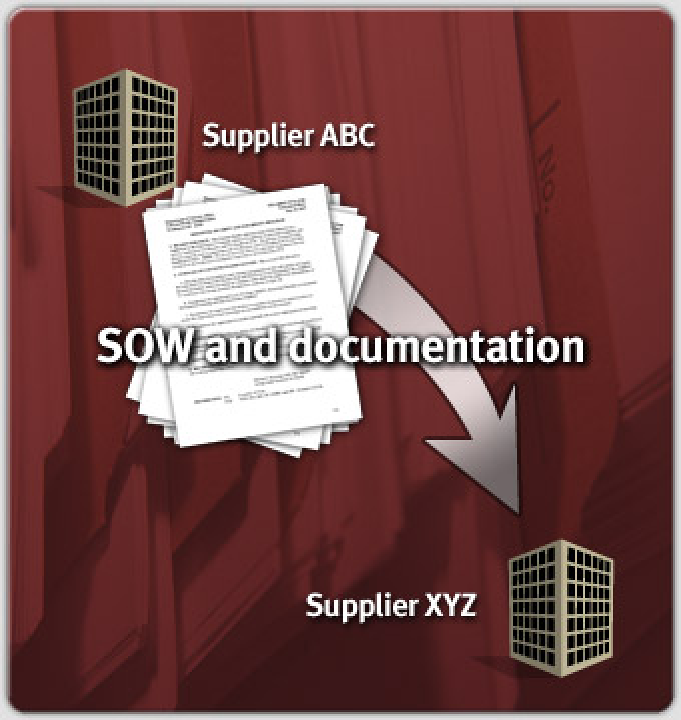
- SwA-related definitions to provide a common understanding.
- The arguments/evidence needed to prove the SwA requirements are met.
- SwA acceptance criteria (associated with the assurance case).
- Risk management that specifically addresses the mitigation of SwA risks.
- Software Architecture that includes SwA or other descriptions to provide a structure for the SwA case.
- Qualifications and required SwA training of software personnel and identification of key security personnel.
- Required information relative to foreign ownership, control, or influence and how this information relates to SwA risk management.
- Organization or agency specific requirements or mandates.

Acquisition strategies and plans provide a description of roles and responsibilities, a roadmap for completing milestones, and a discussion for including special considerations

- Examples of SwA considerations that acquisition decision makers should include in strategies and plans include:
  - *SwA Expertise* - personnel who possess significant SwA expertise should be part of the acquisition process
  - *Initial Security Category*
  - *SwA Requirements* - statements of critical, high-level SwA considerations.
  - *SwA Considerations in Contractor Selection* - high-level statements on how SwA will be considered in the selection of contractors.
  - *SwA Considerations in Contract Administration and Project Management* – statements on how the SwA requirements will be monitored during contract performance
  - *Plans for Independent Testing* – how independent testing of the software can be used to ensure its construction, safety, and functionality.

Integration services usually call for a prime contractor with (usually) multiple subcontractors – so plan accordingly

- Each subcontractor provides software products and/or services for part of the software-intensive system.
- The prime contractor is responsible for integrating the parts into a whole software-intensive system.
- SwA considerations should be captured in subcontractor contracts initiated by the prime.
- Subcontractor personnel experience should also be commensurate with the experience required for the scope and level of design effort to be performed.



When acquiring software, SwA criteria should be included in the solicitation and the evaluation plan must describe how to evaluate the products and services against the criteria

Categories	Priority	Product Score			Weighted Average			
		Product 1 Score (0-4)	Product 2 Score (0-4)	Product 3 Score (0-4)	Product 1	Product 2	Product 3	Average
					1.6	2.1	2.5	10.6
Software Pedigree	5				8.4	11.4	13.0	10.9
Development Process Management	3				9.0	9.0	9.0	9.0
Software Security Awareness and Training	3				9.0	9.0	9.0	9.0
Built-in Software Defenses	2				0.0	0.0	0.0	0.0
Assurance Claims and Evidence	3				0.0	0.0	0.0	0.0
Security Monitoring	3				0.0	0.0	0.0	0.0
Security Testing	4				0.0	0.0	0.0	0.0
Software Change Management	4				0.0	0.0	0.0	0.0

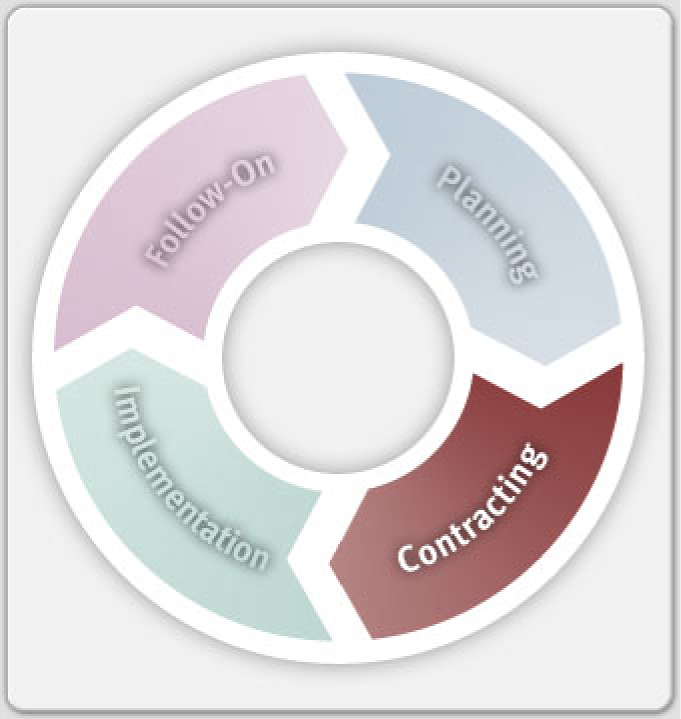
Due Diligence Questionnaires address different software types and SwA concerns and can be used to evaluate software/suppliers

Questions are organized into categories of SwA concerns

Assurance Claims and Evidence	
52	Does your company develop security measurement objectives for phases of the SDLC? Has your company identified specific statistical and/or qualitative analytical techniques for measuring attainment of security measures?
53	Has the software been measured/assessed for its resistance to identified relevant attack patterns? Are Common Vulnerabilities & Exposures (CVE®) or Common Weakness Enumeration (CWEs) used? How have the findings been mitigated?
54	Are static or dynamic software security analysis tools used to identify the weaknesses that can lead to exploitable vulnerabilities in the software? If yes, which tools are used? What classes of weaknesses are covered? When in the SDLC are these scans performed? Are SwA experts involved in the analysis of the scan results?
55	Does the software contain third-party developed components? If yes, are those components scanned by a static code analysis tool?
56	Has the software undergone any penetration testing? When? By whom? Are the test reports available under a nondisclosure agreement? How have the findings been mitigated?
57	Are there current publicly-known vulnerabilities in the software (e.g., an unrepaired CWE entry)?
58	How is the assurance of software produced by third-party developers assessed?

Contracting phase

- Work Statements
- Terms and Conditions
- Other contracting phase tools



Software risks can be addressed and mitigated in the work statement

- The following software assurance considerations can enhance work statements:
  - Definitions related to trustworthy software that provides a common understanding.
  - Description of the security category [see FIPS Pub 199 and DoDI 8500.2] that provides a common framework and understanding of security needs.
  - An Assurance Case that addresses the necessary security requirements (functions and properties) and the arguments and evidence needed to prove the requirements are met.
  - Software assurance risk management that includes a formal program for managing safety and security risks associated with the implementation of software.
  - Consideration for auditing the code for the desired security functionality and known types of weaknesses that can lead to exploitable vulnerabilities.
  - Software description that includes a Software Architecture and other descriptions as needed to provide a structure for the Assurance Case including software security-related aspects.
  - A security test plan that defines the approach for testing each of the SwA requirements
  - Configuration guidelines for all security configuration options.
  - Patch and upgrade processes that ensure security requirements continue to be met.

Some SwA considerations may be more appropriate as terms and conditions

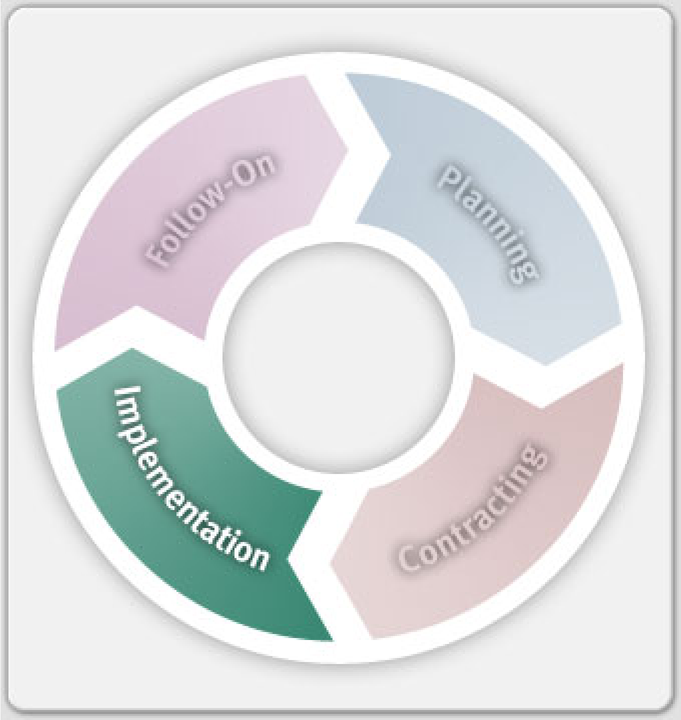
- Whether to include an item in the work statement or as a term or condition depends on the policies and structure of the acquisition organization and could include:
  - Legal responsibilities of supplier and acquirer relative to SwA.
  - Quality of software development processes.
  - SwA acceptance criteria.
  - Qualifications and training of software personnel and identification of key security personnel.
  - SwA training program.
  - Quantitative and qualitative measures that articulate expectations about the expected level of service and performance.
  - Required information relative to FOCI.
  - Required preset security features (this is particularly relevant to COTS).
  - Penalty clauses for failed SwA.

There are other tools available in the contracting phase in addition to the work statement and terms and conditions

- Instructions to suppliers
  - Clear instructions on what suppliers submit for evaluation, including instructions pertaining to onsite evaluation.
- Certifications
  - A way to provide assertions of software trustworthiness when information may be too costly to compile or too voluminous for proposal evaluation.
- Prequalification
  - A method to evaluate organizational capabilities or other technical management capabilities.
- Proposal evaluation
  - SwA SMEs should be used to evaluate each proposal.
- Contract negotiation and contract award
  - The give-and-take on SwA requirements, terms, and conditions should not compromise the ultimate assurance goals
  - All SwA agreements made during negotiation should be incorporated into the contract when it is awarded

Implementation phase

- Contract Work Schedule
- Change Control
- Reviewing and Accepting Software Deliverables



The Implementation and Acceptance Phase involves monitoring of the supplier’s work and accepting the final product

- Contract work schedule
  - Should include very specific scheduled work for delivering SwA deliverables and activities.
  - If a Work Breakdown Schedule (WBS) is used, should ensure that SwA deliverables are identified in the WBS

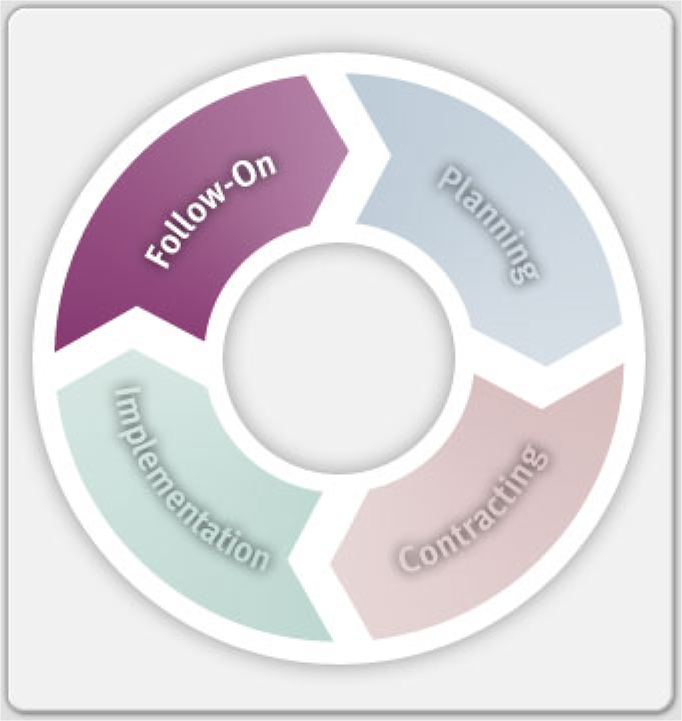
- Change Control
  - The change control procedures for a software-intensive system should ensure that SwA requirements are not compromised when changes are requested.
  - Each change control request should include a specific section that addresses the impact of the requested change on SwA requirements.

Software acceptance criteria should be explicit, measurable, and included in the Assurance Case or in the terms and conditions

- Risk management
  - Acquisition officials and contractors who are responsible for implementation should create a plan for managing risks associated with the security category
  - The plan should include an identification of SwA risks, plans for mitigating those risks, associated measures, and plans for continually assessing those risks
- Assurance case management
  - The Assurance Case must be managed as part of the risk management strategy for the acquisition
  - All elements of any project management methodology that an acquisition official uses are affected by development and management of an Assurance Case
- Independent software testing
  - Acquisition officials should consider independent software test
  - This testing organization can test either in a white or black box scenario depending on need

Follow-on phase

- Sustainment
- Risk Management
- Assurance Case Management
- Change management considerations
- Disposal



After release care should be taken to enforce SwA-related Work Statements and the Terms and Conditions

- The Follow-on Phase involves maintaining the software
  - Maintenance activities may place software at risk
  - Follow-on contract efforts should include the assurance/security requirements implemented and accepted in previous contracts flow
  - Continuous threat analyses and vulnerability assessments should feed into the assurance case necessary for the software
  - A trained and cleared SwA expert inside the organization should be involved

- Risk management continues
  - New risks inevitably emerge
  - The security category may be further refined
  - SwA risks and strategies for mitigating those risks are likely to change as well
  - Measures should be used to provide insights into the changes in the risk environment and into impacts of risk mitigation strategies

Assurance requirements for the Follow-on Phase may need to be defined in greater detail as the software transitions to O&M and the software risk exposure is clearer

- The continual assurance (and certification) of software-intensive systems presents some unique challenges:
  - Many software systems are not architecturally or detail designed for modifications and enhancements are made many years after procurement.
  - System and software engineering change control mechanisms can lack traceability, rigor, and documentation.
  - Adequate Assurance Case maintenance processes may not be in place before software/system transitions to operations.
  - Support personnel turnover causes loss of corporate knowledge about maintaining and ensuring integrity of legacy software.
  - Many software support agencies are not the original software manufacturer and do not employ the same methods, tools, and processes used in development.
  - During previous acquisition phases, the software transition planning is typically poorly executed and “assurance concerns” are “thrown over the fence” for follow-on maintenance.

Changes to the Assurance Case during the Follow-on Phase may be required due to a number of reasons

- Changes to the software system itself that may invalidate previous claims/evidence and assumptions, e.g., changes in operating system lock-down configurations

- Changes to the operational context or environment, e.g., previously isolated system becomes networked

- Changes to system threats, vulnerabilities, consequences, or new issues previously unknown.

- Modifications of measures to ensure they are appropriate for this phase of the acquisition process

Weak change control procedures can corrupt software and introduce new security vulnerabilities

- The schedules and frequency of new releases, updates, and security (and non-security) patches, and response times for technical support by software suppliers are beyond the control of the acquirer

- When any hardware or software component is changed, the extent of revalidation must be evaluated

- Patches and upgrades make direct changes to software and potentially the operating environment
  - Changes may degrade performance, introduce new vulnerabilities, or reintroduce old vulnerabilities.
  - To understand patch risks, the patch process must be examined in some detail during the initial acquisition and again when follow-on support contracts
  - Suppliers should provide updates in a secure fashion

Install New Software Setup

Welcome to the Installer Wizard for New Software.

The Installer Wizard will install New Software on your computer. To continue, click Next.

Disposal or decommissioning policies and procedures are often overlooked

- Acquisition officials/maintainers should ensure that policies and procedures are developed and followed to ensure the safe and secure disposal or decommissioning of software, along with ensuring data are destroyed or migrated safely and securely
- When a software-intensive system is retired or replaced, the data must be migrated by validated means to the new software-intensive system.

Launch http://www.us-cert.gov/SwA for Software Assurance Community of Practice (Dec 07)

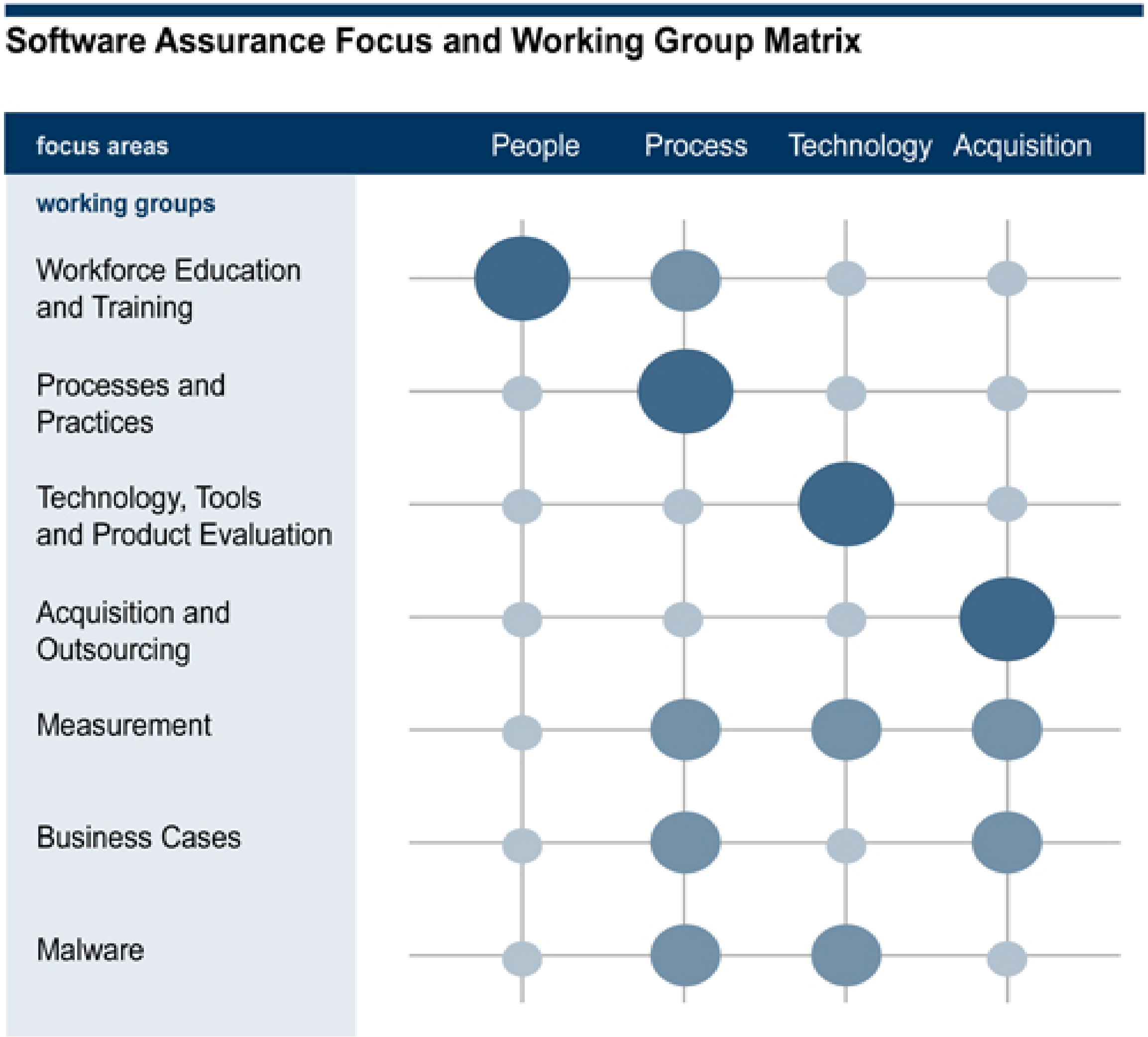
“Build Security In” will continue:

- As a related website (on same server)
- To serve as a detailed reference source for developers
- To be a part of the SwA Processes & Practices WG

SwA Working Groups

- Created to give focus to specific areas within the effort.
- More description provided for the specific efforts.
  - A comprehensive description would provide information to the user to determine what is the purpose of WGs and what they are like.
  - Also reference results of the working group activity here in this area as an example.
  - It will outline the different levels of participation: active & observer.

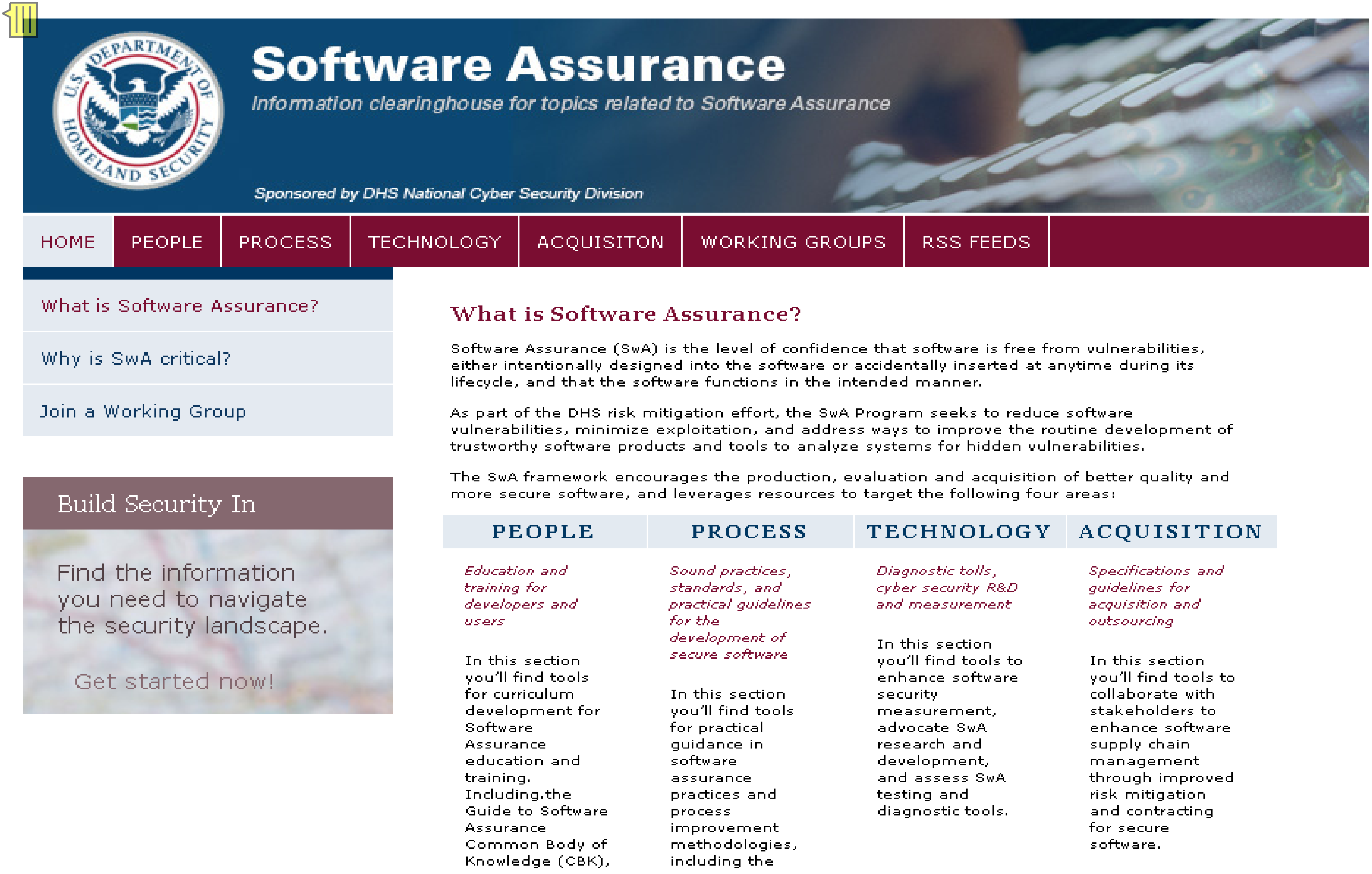
Matrix provides linkage among SwA WORKING GROUPS and SwA FOCUS AREAS



Software Assurance Focus and Working Group Matrix

focus areas working groups	People	Process	Technology	Acquisition
Workforce Education and Training	⬤	●	•	•
Processes and Practices	•	⬤	•	•
Technology, Tools and Product Evaluation	•	•	⬤	•
Acquisition and Outsourcing	•	•	•	⬤
Measurement	•	●	●	●
Business Cases	•	●	•	●
Malware	•	●	●	•

Serving broader stakeholder community


Software Assurance
Information clearinghouse for topics related to Software Assurance
Sponsored by DHS National Cyber Security Division
HOME
PEOPLE
PROCESS
TECHNOLOGY
ACQUISITON
WORKING GROUPS
RSS FEEDS
What is Software Assurance?
Why is SwA critical?
Join a Working Group
Build Security In
Find the information you need to navigate the security landscape.
Get started now!

What is Software Assurance?

Software Assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle, and that the software functions in the intended manner.

As part of the DHS risk mitigation effort, the SwA Program seeks to reduce software vulnerabilities, minimize exploitation, and address ways to improve the routine development of trustworthy software products and tools to analyze systems for hidden vulnerabilities.

The SwA framework encourages the production, evaluation and acquisition of better quality and more secure software, and leverages resources to target the following four areas:

PEOPLE	PROCESS	TECHNOLOGY	ACQUISITION
Education and training for developers and users	*Sound practices, standards, and practical guidelines for the development of secure software*	*Diagnostic tolls, cyber security R&D and measurement*	*Specifications and guidelines for acquisition and outsourcing*
In this section you'll find tools for curriculum development for Software Assurance education and training. Including.the Guide to Software Assurance Common Body of Knowledge (CBK),	In this section you'll find tools for practical guidance in software assurance practices and process improvement methodologies, including the	In this section you'll find tools to enhance software security measurement, advocate SwA research and development, and assess SwA testing and diagnostic tools.	In this section you'll find tools to collaborate with stakeholders to enhance software supply chain management through improved risk mitigation and contracting for secure software.

The SwA Acquisition guide is recommended in Sep 2007 Report of the DSB Task Force on “Mission Impact of Foreign Influence on DoD Software”* - Try it and provide feedback

- “…the mere fact of asking what vendors do to engineer security and quality into their lifecycle puts the vendor community on notice that it is important to DoD.”
  - The DoD/DHS software assurance forum has been working on a procurement guide focused on software assurance, which helps procurement officers glean (through a series of questions) what vendors have done (and not done) as part of their secure development process, how they handle vulnerabilities, and so on.”

- “Such a document, when reviewed by a larger audience and finalized, could be used as part of IT procurement cycles to help DoD better evaluate risk.”
  - “As long as this is sensible, the questions are phrased to allow expository answers, and the benefit derived is commensurate with the cost of vendors completing it, this is one way for DoD both to know what they are getting and to put vendors on notice that quality and security-worthiness has become a purchasing criteria for DoD.”
  - “There also needs to be some way for vendors to complete these questions so they are not repeating the same questionnaire for the same product (or subsequent releases of it) needlessly.”

* Under the Recommendations on Risk-Based Acquisition (starting on page 64)

Questions?

Stan Wisseman
Senior Associate

Booz | Allen | Hamilton

Tel (703) 902-4673
wisseman_stan@bah.com