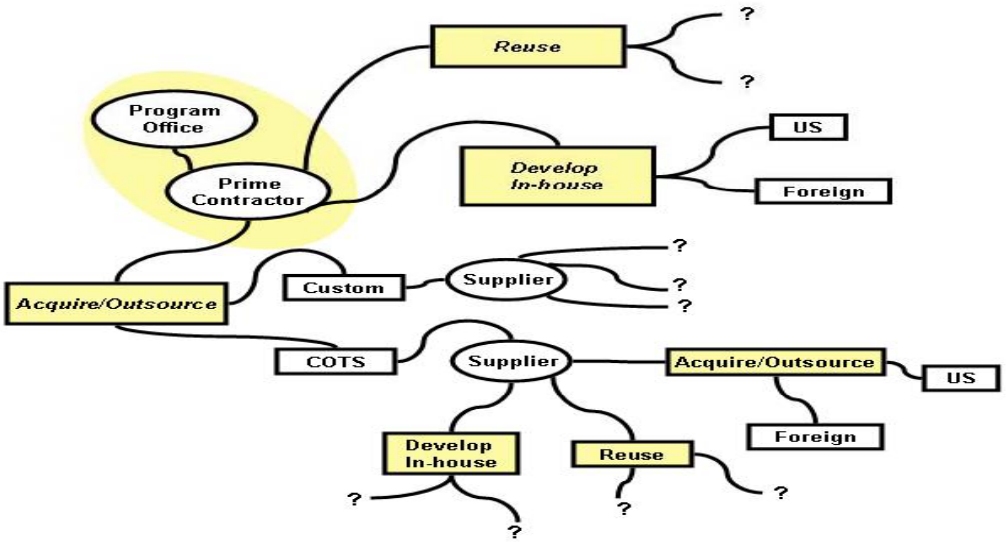
# Reducing Risks in the Software Acquisition Life Cycle



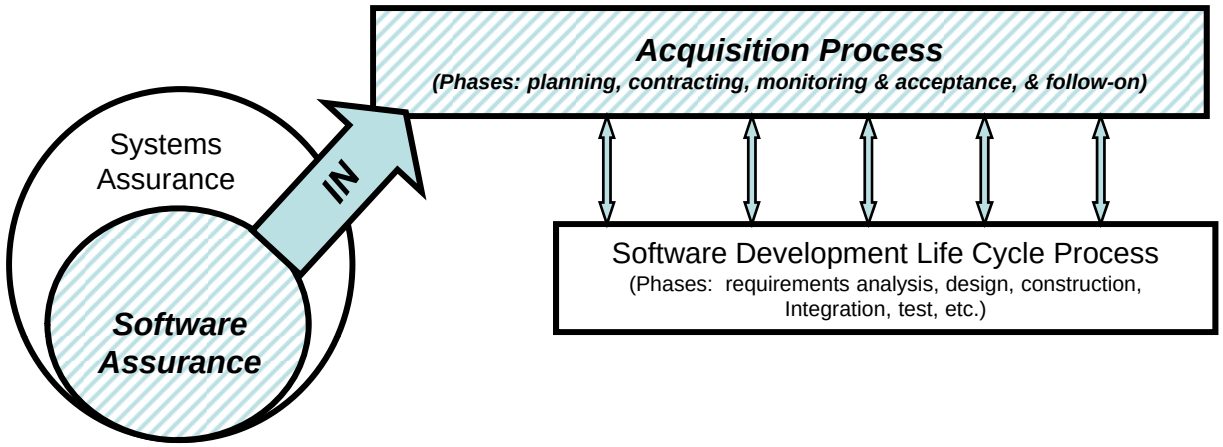


Stan Wisseman

***Co-Chair, DHS Software Assurance Working Group on Acquisition and Outsourcing***


21 April 2009

# The Acquisition and Outsourcing Working Group's goal is to help acquirers obtain SW that is more resistant to attack in order to minimize operational risks



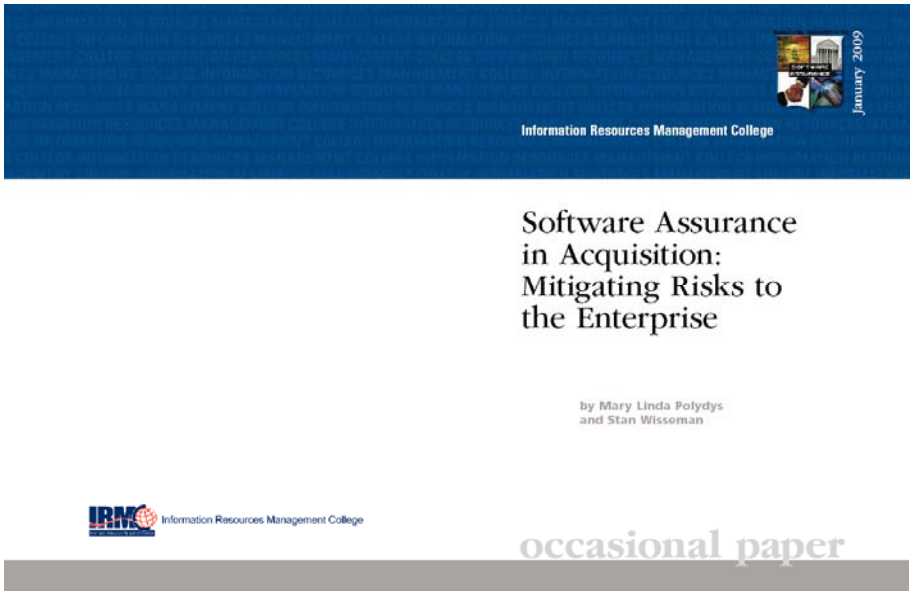

- Stakeholders need justifiable confidence that the software that enables their core mission operations can be trusted to function as expected
- Responsibility for software assurance must be shared by Acquirers in the software supply chain
- Therefore, acquirers involved in purchasing software products or services have a responsibility to factor in Software Assurance to minimize software risks
- The Working Group initial objective was to publish information that helps acquirers apply a risk-based approach to software acquisition/outsourcing.
- Co-chaired by Mary Polydys (NDU IRMC) and Stan Wisseman (Booz Allen)

# Software Assurance in Acquisition: Mitigating Risks to the Enterprise

Document was published through the National Defense University Press (NDU)

# Software Assurance in Acquisition TOC (continued)






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

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

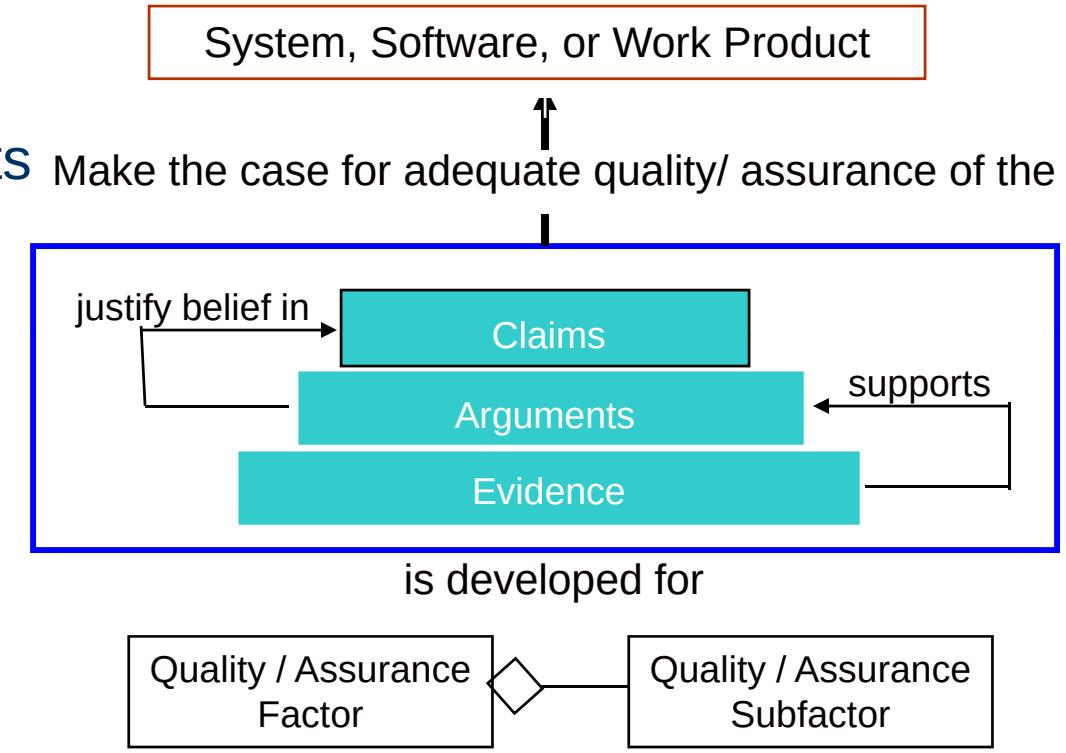
- Acquirers should ask and have answered the following questions*:
  - What is the value we need to protect?
  - To sustain this value, what software and information assets need to be protected? Why do they need to be protected? What happens if they're not protected?
  - What is the impact if the software 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?"*

# 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?




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

# 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.

# 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? |

## 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.

# Integration services sometimes 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.

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

- Risk management
  - Acquirers 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  Use of CWEs in acceptance criteria is an example.
- Assurance case management
  - The Assurance Case must be managed as part of the risk management strategy for the acquisition
  - Security measures can be used to demonstrate progress on maintaining assurance case
- Independent software testing
  - Acquirers should consider independent software test
  - This testing organization can test either in a white or black box scenario depending on need
  - OWASP Application Security Verification Standard can be leveraged

# 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

**Stan Wisseman**
Senior Associate

**Booz | Allen | Hamilton**

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