Software Assurance in Education, Training & Certification:

SwA WET Pocket Guide (Purple Book)

Robin A. Gandhi

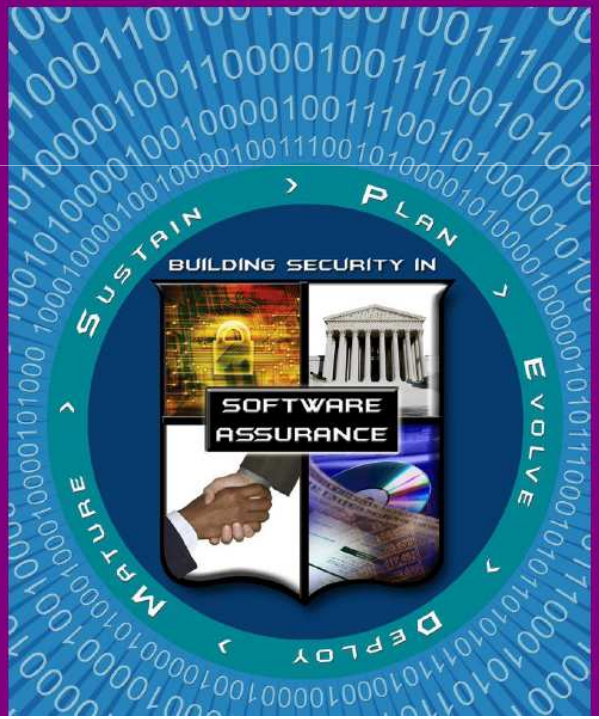
School of Interdisciplinary Informatics (Si2)
Nebraska University Center on Information Assurance (NUCIA)
University of Nebraska at Omaha
College of Information Science and Technology

Acknowledgement

- Joe Jarzombek for giving me the opportunity to lead this effort
- Members of the SwA WG on Education and Training for insightful comments, reviews and content (Dan, Carol, Nancy, Art)
- EC-Council
- Susan Morris and Walter Houser
- And many others

Software Assurance in Education, Training & Certification

Software Assurance Pocket Guide Series:
Life Cycle Support, Volume I
Version 1, (Draft)



Software Assurance (SwA) Pocket Guide Resources

This is a resource for 'getting started' in educating, training and certifying a workforce with regards to their awareness about the engineering activities and knowledge areas in building software that is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software operates as expected. As part of the Software Assurance (SwA) Pocket Guide series, this resource is offered for informative use only; it is not intended as directive or presented as being comprehensive since it references and summarizes material in the source documents that provide detailed information. When referencing any part of this document, please provide proper attribution and reference the source documents, when applicable.

This volume of the SwA Pocket Guide series focuses on enumerating education, training and certification resources. It identifies the most effective strategies to inject software assurance topics into existing college curriculums and workforce training and certification programs.

At the back of this pocket guide are references, limitation statements, and a listing of topics addressed in the SwA Pocket Guide series. All SwA Pocket Guides and SwA-related documents are freely available for download via the SwA Community Resources and Information Clearinghouse at https://buildsecurityin.us-cert.gov/swa .

Acknowledgements

The SwA Forum and Working Groups function as a stakeholder mega-community that welcomes additional participation in advancing software security and refining SwA-related information resources that are offered free for public use. Input to all SwA resources is encouraged. Please contact Software.Assurance@dhs.gov for comments and inquiries.

The SwA Forum is composed of government, industry, and academic members. The SwA Forum focuses on incorporating SwA considerations in acquisition and development processes relative to potential risk exposures that could be introduced by software and the software supply chain.

Participants in the SwA Forum's Workforce Education and Training Working Group contributed to developing the material used in this pocket guide as a step in raising awareness on how to incorporate SwA topics in education, training and certification of a workforce that is knowledgeable to perform engineering activities or aspects of activities relevant for promoting software assurance throughout the Software Development Life Cycle (SDLC).

Theme

- Educating the Educator/Trainer on available SwA resources

- Purpose:
  - A resource for “getting started” in educating, training and certifying a workforce
  - An index to the vast amount of resources, tools, sample curricula, certification and training opportunities for software assurance

Updates

- Tabular listing of BOK and Curriculum guides, Workforce guides and Strategies to inject SwA materials
- Removed training and cost estimates from the list of certifications
- Additions
  - References added to CMU VTE training materials
  - ISC^2 resource guide
  - Updates to SAFEcode guides
  - Linkedin SwA Education
  - SwA MS Curriculum Podcast, Stevens SwA program

SwA Curriculum and Training Development Guides

Table 1– SwA Curriculum and Training Development Guides		
Identifier	**Relevant Documents and Links**	**Purpose**
• **SwA Curriculum Project**	Volume I: Master of Software Assurance Reference Curriculum. Mead, Nancy R. et al. SEI/CMU. http://www.cert.org/mswa/ ; http://www.cert.org/podcast/show/20101026mead.html ;	Offers a core body of knowledge from which to create a master's level degree program in software assurance, as a standalone offering and as a track within existing software engineering and computer science master's degree programs. Last updated **2010.**
	Volume II: Undergraduate Course Outlines. Mead, Nancy R. et al. SEI/CMU. http://www.cert.org/mswa/	Focuses on an undergraduate curriculum specialization for software assurance. Intended to provide students with fundamental skills for either entering the field directly or continuing with graduate level education. Last updated **2010.**
• **Software Security Assurance SOAR**	Software Security Assurance: A State-of-the-Art Report. Goertzel, Karen Mercedes, et al, IATAC of the DTIC. http://iac.dtic.mil/iatac/download/security.pdf	Identifies the current "state-of-the-art" in software security assurance. Last updated July **2007**.
	Enhancing the Development Life Cycle to Produce Secure Software: A Reference Guidebook on Software Assurance. Goertzel, Karen et al. For DHS and DTIC https://www.thedacs.com/techs/enhanced_life_cycles/	Complements the Software Security Assurance: A State-of-the-Art Report with further details. Last updated October **2008**
• **SwA CBK**	Software Assurance Body of Knowledge. Version 1.2, Samuel T. Redwine, Jr. (Editor), DHS, https://buildsecurityin.us-cert.gov/bsi/dhs/927-BSI.html	A comprehensive set of principles and guidelines from the disciplines of software engineering, systems engineering, information system, computer science, safety, security, testing, information assurance, and project management. Last updated October **2007**.
	Towards an Organization for Software System Security Principles and Guidelines. Version 1.0, Samuel T. Redwine, Jr, https://buildsecurityin.us-cert.gov/bsi/dhs/927-BSI.html	An extensive set of software system security principles and guidelines organized in a logical, in-depth fashion. Last updated February **2008**.

Workforce Development and Improvement

Table 2– Workforce Development and Improvement		
Identifier	**Relevant Documents and Links**	**Purpose**
• **EBK**	IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development. DHS US-CERT http://www.us-cert.gov/ITSecurityEBK/	Characterizes the IT security workforce and provides a national baseline representing the essential knowledge and skills that IT security practitioners should have to perform specific roles and responsibilities. Last updated September **2008.**
• **DoD 8570.01-M**	Information Assurance Workforce Improvement Program. Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer. http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf	Provides guidance and procedures for the training, certification, and management of the DoD workforce conducting Information Assurance (IA) functions in assigned duty positions. Last update: Incorporating Change 2, April 20, **2010**.

Strategies for Injecting SwA Knowledge Areas in existing Education and Training Programs

Table 3– Strategies

Strategy	Relevant Documents and Links
• **Degree programs and specializations in SwA**	Reference curriculums available from the Software Engineering Institute, Carnegie Mellon University can be used as recommendations for designing Masters of Software Assurance degree program and undergraduate curriculum specialization in software assurance. These reference curriculum are available at http://repository.cmu.edu/sei/3/ and http://repository.cmu.edu/sei/4/
• **Stand-alone Courses**	New course offerings based on SwA knowledge areas complement existing Software Engineering courses. Examples: http://www.cs.jmu.edu/sss https://www.securecoding.cert.org/confluence/display/sci/S08+15392+Secure+Programming Other examples include graduate-level Software Assurance courses that cover the secure software engineering activities during the SDLC, being offered at the University of North Carolina at Charlotte, and The University of Nebraska at Omaha
• **Augmenting Existing Courses**	The SwA CBK and State-of-the-Art reports are catalogs of secure software development practices, processes, and techniques that can be mapped to topics relevant to current curriculums. The identified gaps can then be filled using relevant materials.
• **Micro-Modules**	Problem-based learning exercises, in class workshops or short talks can be conducted to inject topics such as Mis-use cases and Assurance Cases in existing software engineering or information security courses.
• **Capstone and Class Projects**	Software Engineering capstone courses or class projects can be geared towards a security critical domain such as designing a software system for the Department of Defense, Cyber-physical systems or for a Credit Card transaction processing company. These domains will facilitate the exploration of security needs throughout the SDLC.
• **Online Courses**	The Adaptive Cyber-Security Training Online (**ACT-Online**) courses are available on the TEEX Domestic Preparedness Campus. Ten courses are offered through three discipline specific tracks targeting everyday non-technical computer users, technical IT professionals, and business managers and professionals. These courses are offered at no cost and students earn a DHS/FEMA Certificate of completion along with Continuing Education Units (CEU) at the completion of each course. http://www.teexwmdcampus.com/index.k2
	The **CERT Virtual Training Environment (VTE)** combines the components of traditional classroom training with the convenience of web-based training. Over 200 hours of course material focused around the technical, policy, and management implications of information security – including preparatory courses for commercial certifications, core skills courses, role-based courses for managers and technical staff, and vendor-developed courses. Open access is provided to individual DoD personnel (Active Duty, DoD Civilian and contractors) and members of the Federal Civilian Workforce through specific sponsorships from DISA, and DHS in conjunction with the Department of State Foreign Service Institute. Sponsored accounts can be requested at www.vte.cert.org. Public access to many of the materials is provided through the VTE Library at https://www.vte.cert.org/vteweb/Library/Library.aspx
• **Awareness and Self-study Resources**	**SAFECode**: Software Assurance Forum for Excellence in Code. http://www.safecode.org **Fundamental Practices for Secure Software Development** http://www.safecode.org/publications/SAFECode_Dev_Practices1108.pdf **Security Engineering Training** http://www.safecode.org/publications/SAFECode_Training0409.pdf **Software Assurance: An Overview of Current Industry Best Practices** http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf **Framework for Software Supply Chain Integrity** http://www.safecode.org/publications/SAFECode_Supply_Chain0709.pdf **Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain.** http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf
	Rugged Software http://www.ruggedsoftware.org/
• **Community Support**	**Linkedin SwA Education Discussion Group** Nancy Mead, SwA Curriculum Team lead The objective of the SwA Curriculum Development Team in establishing this group is to provide a venue for dialog about software assurance education. http://www.linkedin.com/groups?mostPopular=&gid=3430456

Find me

- Robin A. Gandhi, Ph.D.
  Assistant Professor of Information Assurance
  University of Nebraska at Omaha

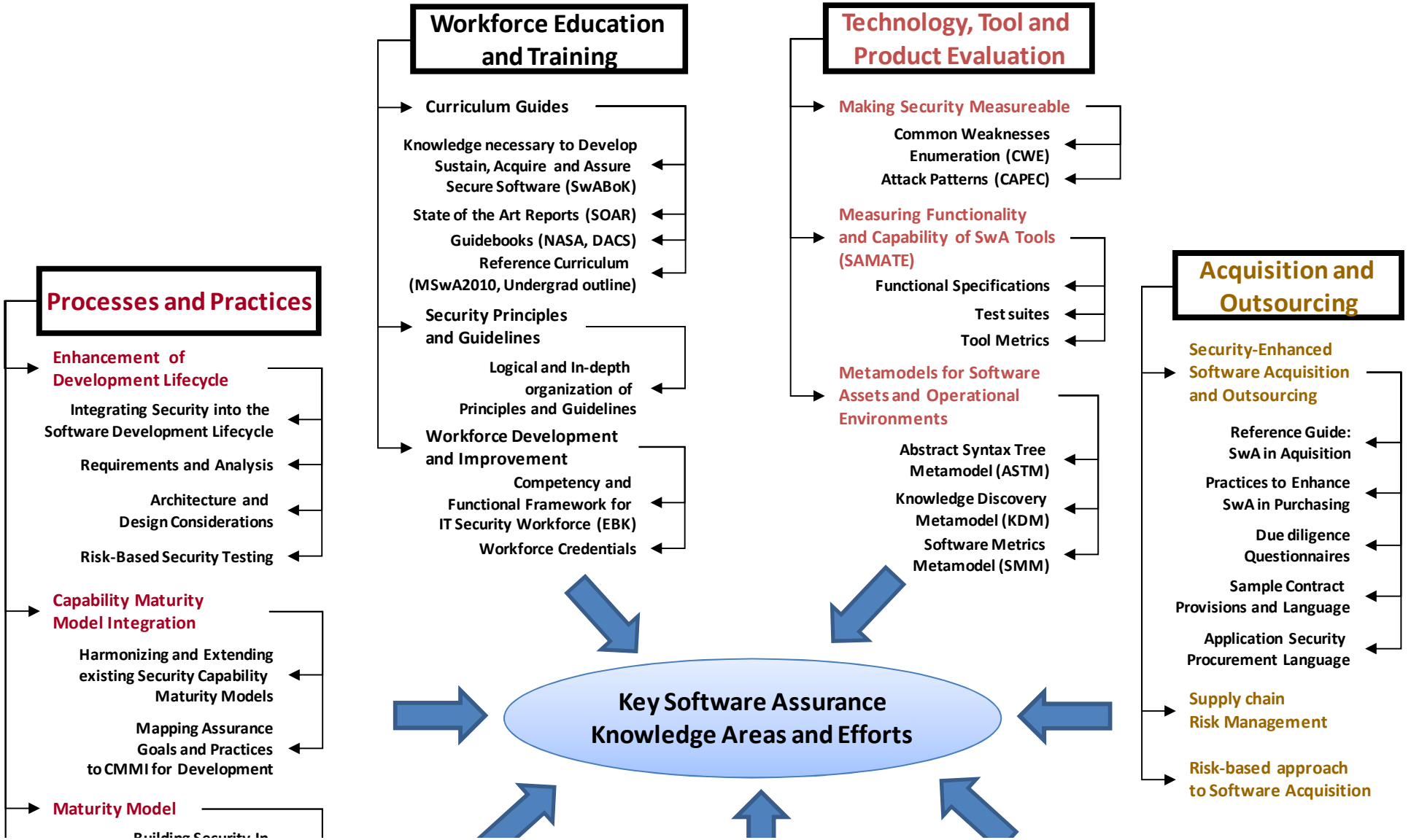
  rgandhi@unomaha.edu

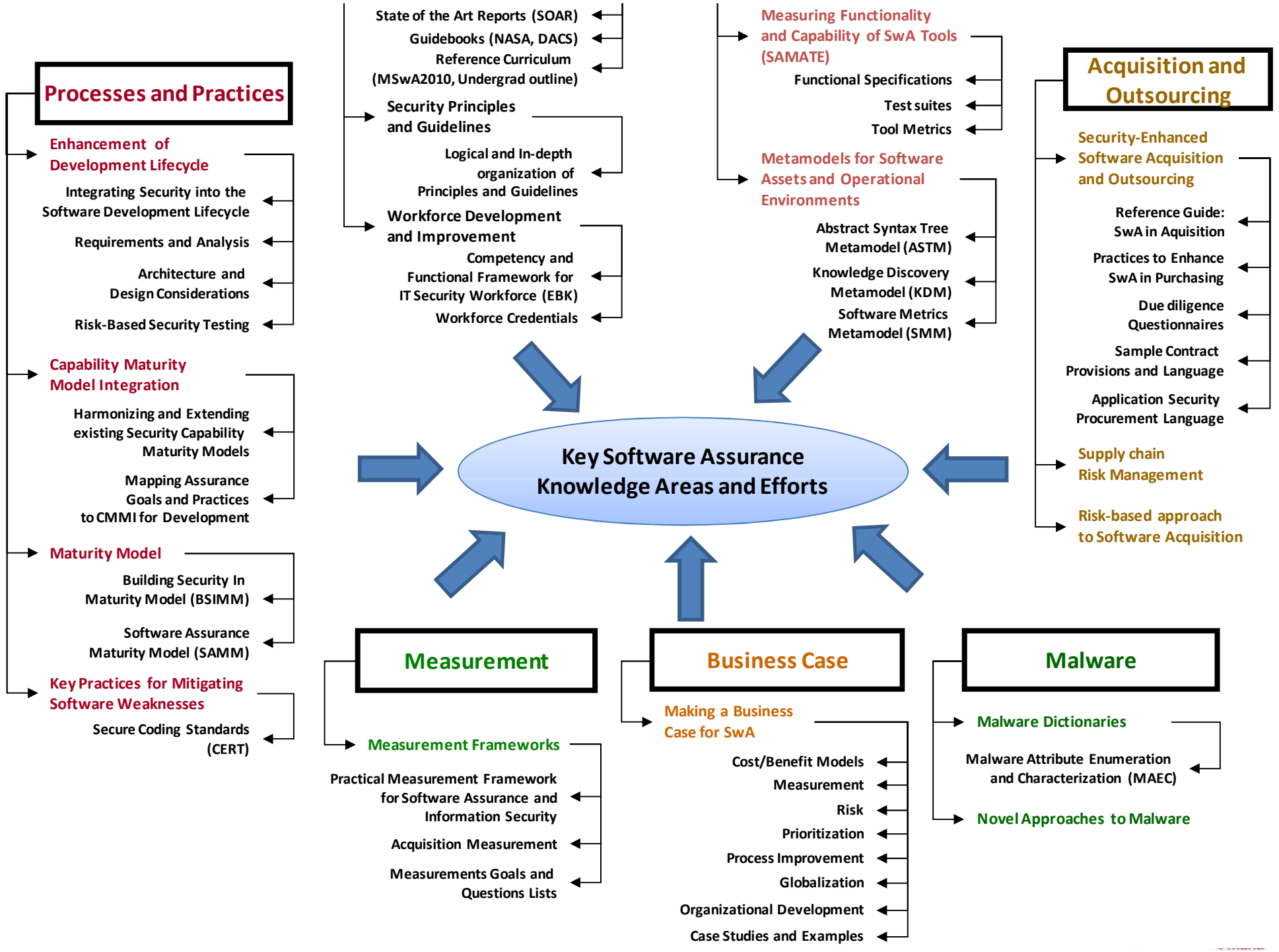
  Voice: (402) 554 3363, Fax: (402) 554-3284

  http://faculty.ist.unomaha.edu/rgandhi

The Various WGs and Deliverables

The Various WGs and Deliverables




Key Software Assurance Knowledge Areas and Efforts
Processes and Practices
Enhancement of Development Lifecycle
Integrating Security into the Software Development Lifecycle
Requirements and Analysis
Architecture and Design Considerations
Risk-Based Security Testing
Capability Maturity Model Integration
Harmonizing and Extending existing Security Capability Maturity Models
Mapping Assurance Goals and Practices to CMMI for Development
Maturity Model
Building Security In Maturity Model (BSIMM)
Software Assurance Maturity Model (SAMM)
Key Practices for Mitigating Software Weaknesses
Secure Coding Standards (CERT)
State of the Art Reports (SOAR)
Guidebooks (NASA, DACS)
Reference Curriculum (MSwA2010, Undergrad outline)
Security Principles and Guidelines
Logical and In-depth organization of Principles and Guidelines
Workforce Development and Improvement
Competency and Functional Framework for IT Security Workforce (EBK)
Workforce Credentials
Measuring Functionality and Capability of SwA Tools (SAMATE)
Functional Specifications
Test suites
Tool Metrics
Metamodels for Software Assets and Operational Environments
Abstract Syntax Tree Metamodel (ASTM)
Knowledge Discovery Metamodel (KDM)
Software Metrics Metamodel (SMM)
Acquisition and Outsourcing
Security-Enhanced Software Acquisition and Outsourcing
Reference Guide: SwA in Aquisition
Practices to Enhance SwA in Purchasing
Due diligence Questionnaires
Sample Contract Provisions and Language
Application Security Procurement Language
Supply chain Risk Management
Risk-based approach to Software Acquisition
Measurement
Measurement Frameworks
Practical Measurement Framework for Software Assurance and Information Security
Acquisition Measurement
Measurements Goals and Questions Lists
Business Case
Making a Business Case for SwA
Cost/Benefit Models
Measurement
Risk
Prioritization
Process Improvement
Globalization
Organizational Development
Case Studies and Examples
Malware
Malware Dictionaries
Malware Attribute Enumeration and Characterization (MAEC)
Novel Approaches to Malware

Topics

- **SwA Curriculum and Training Development Guides**
  - SwA CBK
  - Organization of Principles and Guidelines
  - Software Security Assurance: SOAR
  - Enhancing the Development lifecycle to produce Secure Software
  - Master of Software Assurance Reference Curriculum
  - Undergraduate Course Outlines
  - IT Security Essential Body of Knowledge (EBK)
  - DoD 8570.01-M: Information Assurance Workforce Improvement Program
  - Build Security In website

Topics

- **Strategies for Injecting SwA Knowledge Areas in existing Education and Training Programs**
  - Worked Examples of Injecting SwA concepts
  - Themes for Graduate or Undergraduate Curriculums and Courses
  - List of existing courses, curriculums and training programs
  - Online courses and tutorials for training
  - Conferences and workshops

Topics

- **SwA Tools in Education and Training**

Table 1 – Tools for hands-on classroom experience with SWA Concepts		
Tool Name	**Tool Description**	**Possible Classroom Uses**
ASCE	ASCE supports the key assurance case notations: Goal Structuring Notation and Claims-Arguments-Evidence. Academic license available upon request. URL: http://www.adelard.com/web/hnav/ASCE/index.html	Assurance case documentation for class assignments and projects, Demonstration of worked examples used on real projects.
FindBugs™	A program which uses static analysis to look for bugs in Java code http://findbugs.sourceforge.net/	Scan java code repositories for bugs; Introduction to static code checking activities
SAMATE Reference Dataset	The purpose of the SAMATE Reference Dataset (SRD) is to provide users, researchers, and software security assurance tool developers with a set of known security flaws. This will allow end users to evaluate tools and tool developers to test their methods. http://samate.nist.gov/index.php/Main_Page.html	A reference data set can be used in class to reflect upon known flaws in software

Hands on training

Web Resources		
OWASP Learning Environments	http://www.owasp.org/index.php/Phoenix/Tools	Comprehensive collection of security tools, exploits, vulnerability scanners, defensive tools, application security.
OWASP Web Goat	http://www.owasp.org/index.php/OWASP_WebGoat_Project	WebGoat is a deliberately insecure J2EE web application maintained by OWASP designed to teach web application security lessons.
Google Code University	http://jarlsberg.appspot.com/	Web application exploits and defenses. Topics include cross-site scripting, cross site request forgery, AJAX vulnerabilities, denial of service, etc.
Software Assurance (SwA) Tools Overview	https://buildsecurityin.us-cert.gov/swa/swa_tools.html	A collection of SwA tools inspired by the NIST Software Assurance Metrics And Tool Evaluation (SAMATE) project.

Books

Table 2 – A List of SwA focused Books for Use in Education and Training		
Topic	**Title and Publisher**	**Summary and Possible Use**
• **Software Assurance in SDLC**	» **Secure Coding: Principles and Practices**, Mark G. Graff and Kenneth R. van Wyk, O'Reilly, 2003	A practical approach to integrating SwA topics into the SDLC. Great for assignment of additional readings that complement classroom materials. http://www.securecoding.org/
• **Information Security**	» **Building a Secure Computer System**, Morrie Gasser, 1988	Good reading for Information Security basics.
• **Activities to improve SwA during the SDLC**	» **Software Security: Building Security In**, Gary McGraw, Addison-Wesley Professional, 2006.	Introduction to Software Security Touchpoints during software development. Possible use a textbook or additional reference material
• **Principles and guidelines** • **Implementation level issues**	» **Building Secure Software: How to Avoid Security Problems the Right Way**, John Viega and Gary McGraw, Addison Wesley, 2002	Software Assurance principles and guidelines and Implementation level issues Possible use a textbook or additional reference material
• **Attack Patterns** • **Reverse Engineering** • **Implementation level issues**	» **Exploiting Software: How to Break Code** by Greg Hoglund and Gary McGraw, Addison Wesley, 2004	Understanding attack strategies to build better defenses. Case studies for class discussion http://www.exploitingsoftware.com/
• **Design Principles and Techniques**	» **High-Assurance Design: Architecting Secure and Reliable Enterprise Applications**, Clifford J. Berg, Addison-Wesley Professional 2005.	Basic principles and techniques that can be applied to the development of business applications.
• **Static Analysis**	» **Secure Programming with Static Analysis,** Brian Chess, Jacob West, Addison Wesley, 2007.	Detailed discussion of security issues in several open source applications; steps in the static analysis process
• **Software Assurance in SDLC**	» **Software Security Engineering: A Guide for Project Managers**, Julia Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, Addison-Wesley, 2008 (ISBN 032150917X).	Software Security Engineering draws extensively on the systematic approach developed for the Build Security In (BSI) Web site. http://www.softwaresecurityengineering.com

Standards of Practice

Table 3– Domain-specific SwA standards used in practice

Standard	Community of practice	Purpose
• **MISRA C**	Motor Industry Software Reliability Association (MISRA). http://www.misra.org.uk/	A software development standard for the C programming language developed by MISRA. Its aims are to facilitate code safety, portability and reliability in the context of embedded systems, specifically those systems programmed in ISO C. There is also a set of guidelines for MISRA C++.
• **The Building Security In Maturity Model (BSIMM2)**	http://bsimm2.com/	Pronounced "bee simm" was created by observing and analyzing real-world data from thirty leading software security initiatives. The BSIMM can help you determine how your organization compares to other real-world software security initiatives and what steps can be taken to make your approach more effective.
• **openSAMM: The Software Assurance Maturity Model**	http://www.opensamm.org/	An open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

Workforce Credentials

Table 4 – Options for Workforce Credentials (In alphabetical order)

Certification Authority	SwA Relevant Certificates	Training Duration	Training Fee*	Resources
EC-Council	» EC-Council Certified Secure Programmer (**ECSP**) (Technologies Covered: C/C++, Java, .Net, PHP, SQL)	5 days	$ 2,500*	http://www.eccouncil.org/certification.htm
	» Certified Secure Application Developer (**CSAD**)	–		
	» Certified Ethical Hacker (**CEH**)	5 days	$ 2,500	
	» Licensed Penetration Tester (**LPT**)	5 days	$ 2,500	
GIAC - Global Information Assurance Certification	» GIAC Secure Software Programmer - .NET (**GSSP-NET**)	4 days	$ 3,045	http://www.giac.org/certifications/
	» GIAC Secure Software Programmer - Java (**GSSP-JAVA**)	4 days	$ 3,045	
	» GIAC Web Application Penetration Tester (**GWAPT**)	6 days	$ 3,845	
	» GIAC Certified Penetration Tester (**GPEN**)	6 days	$ 4,295	
IEEE Computer Society	» Certified Software Development Professional (**CSDP**)	–	$445	http://www.computer.org/portal/web/certification
ISC²	» **CSSLP**CM - Certified Secure Software Lifecycle Professional	5 days	$2695	http://www.isc2.org/csslp-certification.aspx

*Approximate Prices. Please check the respective websites for more details.

Topics

- **Other SwA Education and Training Topics**
  - Jobs and career planning
    - http://www.sans.org/20coolestcareers

#18 - Security-savvy Software Developer*

"Kool, because this is VERY rare."

Job Description

The security-savvy software developer leads all developers in the creation of secure software, implementing secure programming techniques that are free from logical design and technical implementation flaws. This expert is ultimately responsible for ensuring customer software is free from vulnerabilities that can be exploited by an attacker.

#2 - System, Network, and/or Web Penetration Tester* - Top Gun Job

"You can be a hacker, but do it legally and get paid a lot of money!"

Sample Job Descriptions

» Cyber Software Assurance Developer/Integrator

- Experience with applying security activities within SDLC
- Experience with security, including CISSP or SANS secure programming assessments
- Experience with security standards, including SSE-CMM, NIST SPs, ISO 15408 Common Criteria, or client-specific software assurance guides

» Software Assurance Engineer

- Provide technical leadership in all aspects of software assurance and computer systems engineering support
- Lead and actively participate in the evaluation and analyses of activities related to all phases of the secure software life cycle from initial planning, requirements definition, design and development through integrated system testing and sustaining operations.

Got Content?

- The pocket guide is a “work in progress”
- Plenty of opportunity to contribute content
- Join the Effort !
  - Your comments, suggestions, criticism/praise are all very welcome

Other Themes

- **Working Professionals and Student focused:**
  - What programs are available from a university setting
  - What is available in terms of certifications and training programs
  - What classes can I sign up for?
  - What does the career path look like?
  - What organizations currently require SwA capabilities?

Other Themes

- **Organization focused:**
  - What roles and responsibilities need to be enacted in the SwA oriented SDLC?
  - What capabilities are required for each role?
  - How can we enable SwA training programs within the organization?
  - What are fortune 500 type companies doing regarding SwA education and training?
  - How to assess SwA credentials?

Where to find the PocketGuide?

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