

# Software Assurance in Education, Training & Certification:

## SwA WET Pocket Guide (Purple Book)

Robin A. Gandhi, Ph.D.

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

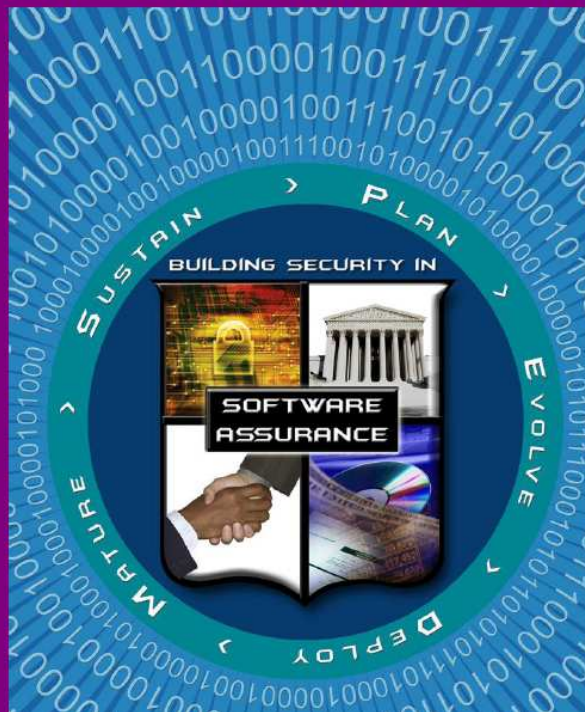


# Acknowledgement

- 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
- 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](mailto: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).

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

Software Assurance in Education, Training & Certification  
1

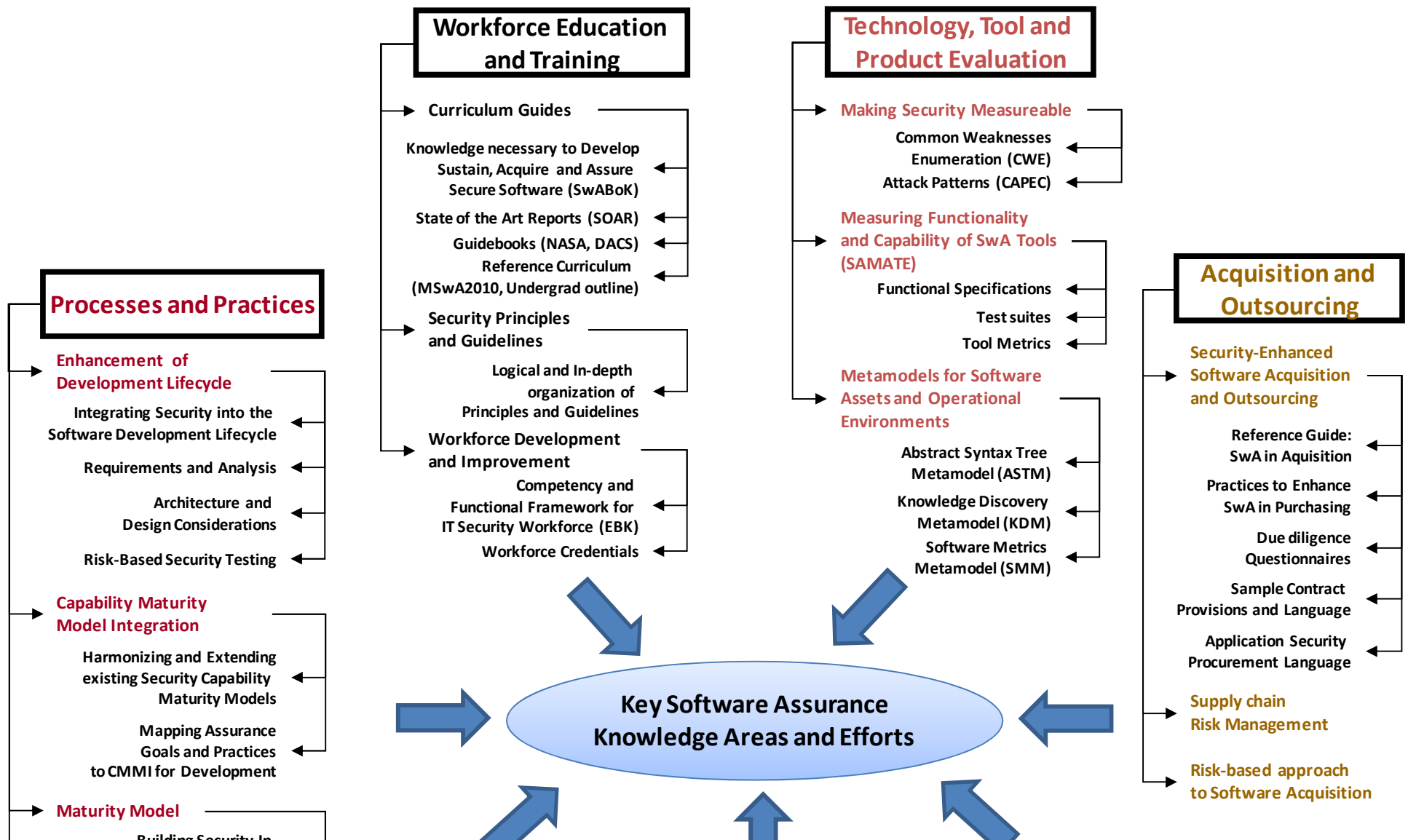
# Theme

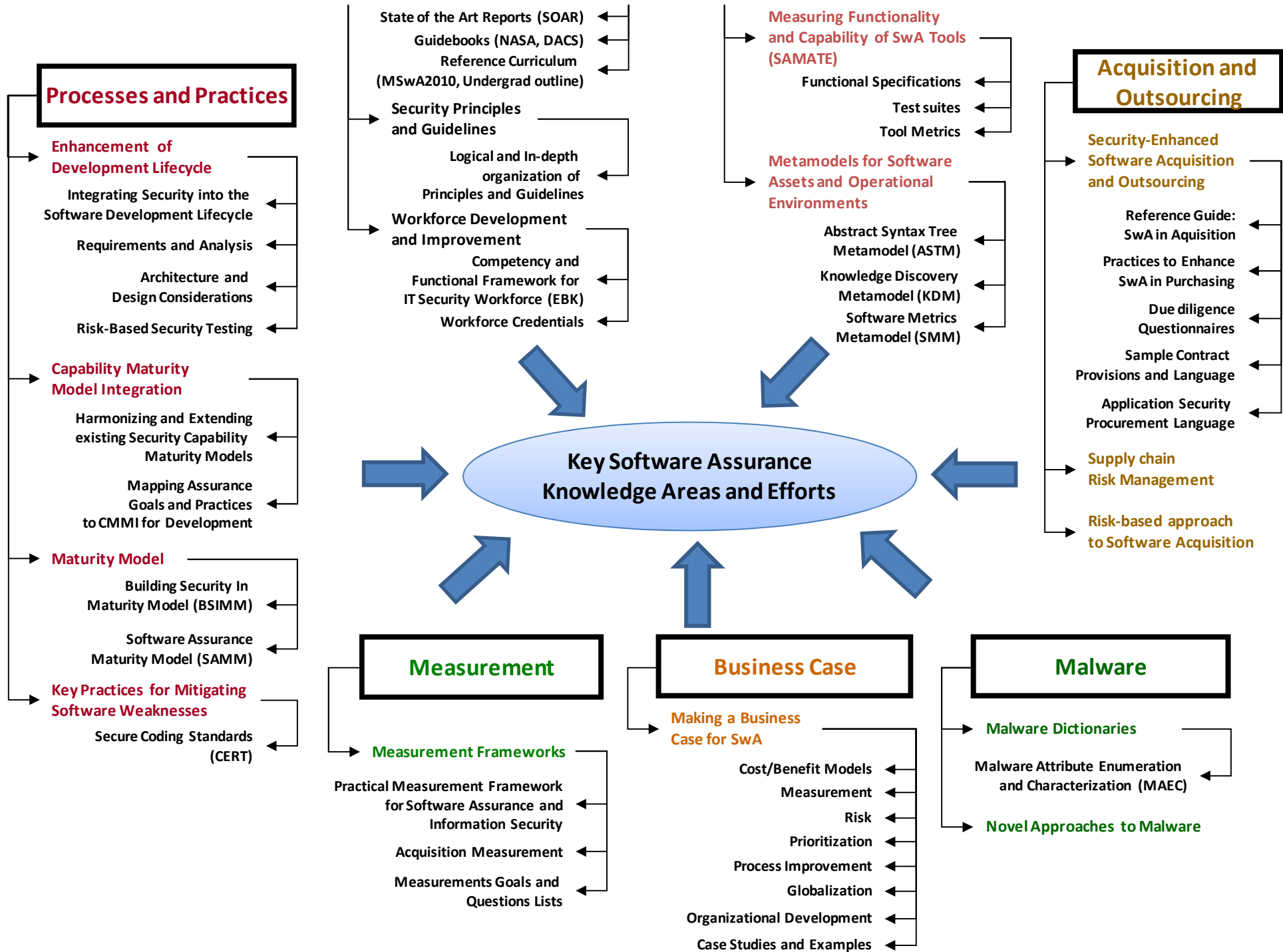
- Educating the Educator/Trainer on available SwA resources
- Purpose:
  - A resource for “getting started” in educating, training and certifying a workforce
  - An index to the vast amount of resources, tools, sample curricula, certification and training opportunities for software assurance

# The Various WGs and Deliverables



# The Various WGs and Deliverables







# 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**

<i>Table 1 – Tools for hands-on classroom experience with SWA Concepts</i>		
<b>Tool Name</b>	<b>Tool Description</b>	<b>Possible Classroom Uses</b>
<b>ASCE</b>	ASCE supports the key assurance case notations: Goal Structuring Notation and Claims-Arguments-Evidence. Academic license available upon request. URL: <a href="http://www.adelard.com/web/hnav/ASCE/index.html">http://www.adelard.com/web/hnav/ASCE/index.html</a>	Assurance case documentation for class assignments and projects, Demonstration of worked examples used on real projects.
<b>FindBugs™</b>	A program which uses static analysis to look for bugs in Java code <a href="http://findbugs.sourceforge.net/">http://findbugs.sourceforge.net/</a>	Scan java code repositories for bugs; Introduction to static code checking activities
<b>SAMATE Reference Dataset</b>	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. <a href="http://samate.nist.gov/index.php/Main_Page.html">http://samate.nist.gov/index.php/Main_Page.html</a>	A reference data set can be used in class to reflect upon known flaws in software

# Hands on training

Web Resources		
<b>OWASP Learning Environments</b>	<a href="http://www.owasp.org/index.php/Phoenix/Tools">http://www.owasp.org/index.php/Phoenix/Tools</a>	Comprehensive collection of security tools, exploits, vulnerability scanners, defensive tools, application security.
<b>OWASP Web Goat</b>	<a href="http://www.owasp.org/index.php/OWASP_WebGoat_Project">http://www.owasp.org/index.php/OWASP_WebGoat_Project</a>	WebGoat is a deliberately insecure J2EE web application maintained by OWASP designed to teach web application security lessons.
<b>Google Code University</b>	<a href="http://jarlsberg.appspot.com/">http://jarlsberg.appspot.com/</a>	Web application exploits and defenses. Topics include cross-site scripting, cross site request forgery, AJAX vulnerabilities, denial of service, etc.
<b>Software Assurance (SwA) Tools Overview</b>	<a href="https://buildsecurityin.us-cert.gov/swa/swa_tools.html">https://buildsecurityin.us-cert.gov/swa/swa_tools.html</a>	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
<ul style="list-style-type: none"> <li>• <b>Software Assurance in SDLC</b></li> </ul>	<ul style="list-style-type: none"> <li>» <b>Secure Coding: Principles and Practices</b>, Mark G. Graff and Kenneth R. van Wyk, O'Reilly, 2003</li> </ul>	<p>A practical approach to integrating SwA topics into the SDLC. Great for assignment of additional readings that complement classroom materials.</p> <p><a href="http://www.securecoding.org/">http://www.securecoding.org/</a></p>
<ul style="list-style-type: none"> <li>• <b>Information Security</b></li> </ul>	<ul style="list-style-type: none"> <li>» <b>Building a Secure Computer System</b>, Morrie Gasser, 1988</li> </ul>	<p>Good reading for Information Security basics.</p>
<ul style="list-style-type: none"> <li>• <b>Activities to improve SwA during the SDLC</b></li> </ul>	<ul style="list-style-type: none"> <li>» <b>Software Security: Building Security In</b>, Gary McGraw, Addison-Wesley Professional, 2006.</li> </ul>	<p>Introduction to Software Security Touchpoints during software development. Possible use a textbook or additional reference material</p>
<ul style="list-style-type: none"> <li>• <b>Principles and guidelines</b></li> <li>• <b>Implementation level issues</b></li> </ul>	<ul style="list-style-type: none"> <li>» <b>Building Secure Software: How to Avoid Security Problems the Right Way</b>, John Viega and Gary McGraw, Addison Wesley, 2002</li> </ul>	<p>Software Assurance principles and guidelines and Implementation level issues Possible use a textbook or additional reference material</p>
<ul style="list-style-type: none"> <li>• <b>Attack Patterns</b></li> <li>• <b>Reverse Engineering</b></li> <li>• <b>Implementation level issues</b></li> </ul>	<ul style="list-style-type: none"> <li>» <b>Exploiting Software: How to Break Code</b> by Greg Hoglund and Gary McGraw, Addison Wesley, 2004</li> </ul>	<p>Understanding attack strategies to build better defenses. Case studies for class discussion</p> <p><a href="http://www.exploitingsoftware.com/">http://www.exploitingsoftware.com/</a></p>
<ul style="list-style-type: none"> <li>• <b>Design Principles and Techniques</b></li> </ul>	<ul style="list-style-type: none"> <li>» <b>High-Assurance Design: Architecting Secure and Reliable Enterprise Applications</b>, Clifford J. Berg, Addison-Wesley Professional 2005.</li> </ul>	<p>Basic principles and techniques that can be applied to the development of business applications.</p>
<ul style="list-style-type: none"> <li>• <b>Static Analysis</b></li> </ul>	<ul style="list-style-type: none"> <li>» <b>Secure Programming with Static Analysis</b>, Brian Chess, Jacob West, Addison Wesley, 2007.</li> </ul>	<p>Detailed discussion of security issues in several open source applications; steps in the static analysis process</p>
<ul style="list-style-type: none"> <li>• <b>Software Assurance in SDLC</b></li> </ul>	<ul style="list-style-type: none"> <li>» <b>Software Security Engineering: A Guide for Project Managers</b>, Julia Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, Nancy R. Mead, Addison-Wesley, 2008 (ISBN 032150917X).</li> </ul>	<p>Software Security Engineering draws extensively on the systematic approach developed for the Build Security In (BSI) Web site.</p> <p><a href="http://www.softwaresecurityengineering.com">http://www.softwaresecurityengineering.com</a></p>

# Standards of Practice

<i>Table 3– Domain-specific SwA standards used in practice</i>		
Standard	Community of practice	Purpose
<ul style="list-style-type: none"> <li>• <b>MISRA C</b></li> </ul>	Motor Industry Software Reliability Association (MISRA). <a href="http://www.misra.org.uk/">http://www.misra.org.uk/</a>	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++.
<ul style="list-style-type: none"> <li>• <b>The Building Security In Maturity Model (BSIMM2)</b></li> </ul>	<a href="http://bsimm2.com/">http://bsimm2.com/</a>	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.
<ul style="list-style-type: none"> <li>• <b>openSAMM: The Software Assurance Maturity Model</b></li> </ul>	<a href="http://www.opensamm.org/">http://www.opensamm.org/</a>	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
<b>EC-Council</b>	» EC-Council Certified Secure Programmer ( <b>ECSP</b> ) (Technologies Covered: C/C++, Java, .Net, PHP, SQL )	5 days	\$ 2,500*	<a href="http://www.eccouncil.org/certification.htm">http://www.eccouncil.org/certification.htm</a>
	» Certified Secure Application Developer ( <b>CSAD</b> )	–		
	» Certified Ethical Hacker ( <b>CEH</b> )	5 days	\$ 2,500	
	» Licensed Penetration Tester ( <b>LPT</b> )	5 days	\$ 2,500	
<b>GIAC - Global Information Assurance Certification</b>	» GIAC Secure Software Programmer - .NET ( <b>GSSP-NET</b> )	4 days	\$ 3,045	<a href="http://www.giac.org/certifications/">http://www.giac.org/certifications/</a>
	» GIAC Secure Software Programmer - Java ( <b>GSSP-JAVA</b> )	4 days	\$ 3,045	
	» GIAC Web Application Penetration Tester ( <b>GWAPT</b> )	6 days	\$ 3,845	
	» GIAC Certified Penetration Tester ( <b>GPEN</b> )	6 days	\$ 4,295	
<b>IEEE Computer Society</b>	» Certified Software Development Professional ( <b>CSDP</b> )	–	\$445	<a href="http://www.computer.org/portal/web/certification">http://www.computer.org/portal/web/certification</a>
<b>ISC<sup>2</sup></b>	» <b>CSSLP<sup>CM</sup></b> - Certified Secure Software Lifecycle Professional	5 days	\$2695	<a href="http://www.isc2.org/csslp-certification.aspx">http://www.isc2.org/csslp-certification.aspx</a>

# 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

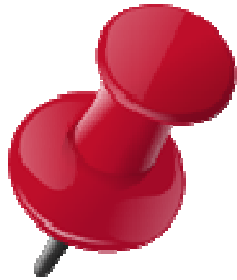
- **Organization focused:**
  - What roles and responsibilities need to be enacted in the SwA oriented SDLC?
  - What capabilities are required for each role?
  - How can we enable SwA training programs within the organization?
  - What are fortune 500 type companies doing regarding SwA education and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

# Where to find the PocketGuide?

- [https://buildsecurityin.us-cert.gov/swa/pocket\\_guide\\_series.html](https://buildsecurityin.us-cert.gov/swa/pocket_guide_series.html)

▶ <b>SwA in Acquisition and Outsourcing</b>	
▶ <b>SwA in Development</b>	
▼ <b>SwA Life Cycle</b>	
	<p><b>Software Assurance in Education, Training &amp; Certification</b> <i>Life Cycle Support Volume I – (Version 1.0, May 28, 2010)</i></p> <p>Current events related to cybersecurity encourage a fundamental shift in the way we think about educating and training a workforce prepared to address security issues in all phases of a software system. Software assurance education and training is aimed to ensure adequate coverage of requisite knowledge areas in contributing disciplines such as software engineering (including its many subdisciplines), systems engineering, project management, etc., to identify and acquire competencies associated with secure software. The primary audiences for this pocket guide are educators and trainers who can use this guide to identify resources to supplement their efforts as well as identify strategies to inject software assurance related topics in the existing education and training programs.</p>
8.5" x 11" version <a href="#">PDF File</a>	
▶ <b>Future SwA Pocket Guides</b>	

# Find me



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

**[rgandhi@unomaha.edu](mailto:rgandhi@unomaha.edu)**

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

**<http://faculty.ist.unomaha.edu/rgandhi>**