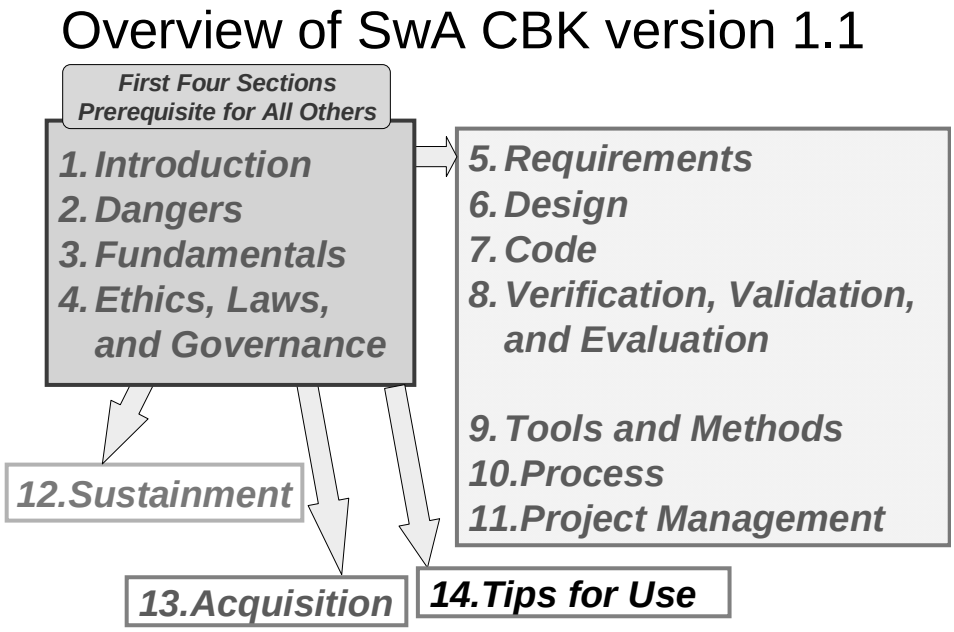
Backgrounder on the Guide to the Common Body of Knowledge

Introduction

The Workforce Education and Training Working Group's first major product has been a body of knowledge for software security titled *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire, and Sustain Secure Software.* It was edited by Sam Redwine and authored by him and other members of the Working Group with the aid of experts from the US and elsewhere as well as oversight by Joe Jarzombek at the Department of Homeland Security. It identifies the additional body of knowledge necessary to develop, sustain, acquire, and assure secure software beyond that normally required for software where safety and security are not concerns.

As security is now a "normal" software concern, portions of this knowledge has become essential for most individuals and organizations involved in software. The knowledge areas identified and their related references provide a foundation for producing education and training curricula and products as well as being useful to standards developers, evaluators and testers, practitioners, managers, and others wishing to be knowledgeable in all or part of software-related security. It contains 14 sections plus a bibliography and an index.



Mainly intended for persons with knowledge of software but not security or assurance, this document introduces them to the surface of the field of software-security-related knowledge and points to references for deeper knowledge. It supplies the background they need to meaningfully recognize the topic that a reference covers and which

references might be of interest. Given this, while a guide and not a textbook, this document's text can function as a high-level introduction -- and some may choose to use it that way. However, in its primary role, its high-level description and context combines with the numerous references to serve as a guide for educators and trainers as well as others to the software-security-related knowledge relevant to their work (no job requires it all).

The primary audiences for this guide are educators and trainers who can use this guide to help identify both appropriate curricular content and references that detail it. Other audiences include evaluators and testers, acquisition personnel, program managers, and standards developers for whom it can help provide a better appreciation of the breadth of subject matter and issues involved. In addition, studious practitioners could use it to obtain overviews or to guide their learning.

Document History

Two years in the making and15 months in the writing, the guide represents a major leap forward by achieving a comprehensive and integrated overview of the body of knowledge. An outline of the history of its development over the two years is:

- Spring 2005
  - Collected lists of added or changed activities
  - Formed subgroups & assigned authors
- Summer2005
  - Started writing in June
  - Many iterations within Working Group
  - Draft distributed at October 2-3 Software Assurance Forum
- 2006 versions
  - January 23
  - March 14
  - April 17
  - May
  - July
  - September 25 version 1.1
    - Mature and ready for wide use

Work is underway to produce a new version adding recent developments and benefiting from experiences in its use.

Editor and Authors

This document was developed by:

Editor:

Samuel T. Redwine, Jr.

Authors:

Samuel T. Redwine, Jr.

Rusty O. Baldwin

Mary L. Polydys

Daniel P. Shoemaker

Jeffrey A. Ingalsbe

Larry D. Wagoner

Additional contributors included: Martin Croxford of Praxis High Integrity Systems Ltd; John McDermid, University of York; Jim Moore, MITRE; Mary Ann Davidson, Oracle; Karen Goertzel, Booz Allen Hamilton; and the Ford Motor Company whose staff helped in the production of the section on Sustainment particularly its reference list.