



Common Criteria Developer Training Course Outline

Common Criteria version 3.1

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301
www.atsec.com



Course Audience

This course is aimed at software development team members who will be involved in a Common Criteria evaluation in the NIAP CCEVS evaluation scheme.

Prerequisites: Basic knowledge of software development life cycle.

Course Goals

After completing this course, the developer will have the knowledge and skills to:

- understand and use the CC Parts 1,2, 3, the CEM, and additional CCEVS guidance
- understand his or her responsibilities in an evaluation process
- contribute to evaluation projects as a member of the evidence development team
- contribute to authoring a Security Target and provide other evaluation evidence

Course Objectives

Knowledge of CC history

Knowledge of CC organizations

- International
- U.S.

General knowledge of the overall CC standard structure

- Knowledge of the functional assurance paradigm
- Knowledge of how functional components cover functional requirements
- Knowledge of Evaluation Assurance Levels

Ability to understand security functional components as described in CC Part 2

- Knowledge of the functional requirements paradigm
- Knowledge of SFR class structure
 - o Ability to describe the purpose of each SFR class
- Knowledge of SFR family structure
 - o Ability to describe the purpose of each SFR family
 - o Ability to navigate component hierarchy
 - o Ability to trace Management requirements
 - o Ability to trace Audit requirements
- Knowledge of SFR component structure
 - o Ability to describe purpose of each SFR component
 - o Ability to describe purpose of each SFR element
 - o Ability to trace Dependencies
- Knowledge of component operations

Knowledge of CC evaluation process

- Understand the assurance concept



- Understand the information flow
- Understand the general certification process

Ability to apply security assurance components as described in CC Part 3

- Knowledge of the functional assurance paradigm
- Knowledge of SAR class structure
 - o Ability to describe the purpose and application of each SAR class
- Knowledge of SAR family structure
 - o Ability to describe the purpose of each SAR family
 - o Ability to navigate component hierarchy
- Knowledge of SAR component structure
 - o Ability to describe purpose & application of each SAR component
 - o Ability to trace Dependencies
 - o Ability to identify and describe application of assurance elements
 - o Ability to trace Dependencies
- Knowledge of Evaluation Assurance Levels
 - o Ability to describe the application of an EAL
 - o Ability to differentiate the EALs

Course Duration and Style

This course is targeted for two full days in duration.

This course will be taught in workshop style, with presentations, instructor-led discussions, and hands-on exercises.



Course Outline

1. Statements of course
2. Brief Introduction to evaluations
 - 2.1. Business value of CC
3. International standard and documents
 - 3.1.1. History
 - 3.1.2. International CC organization
 - 3.1.3. CC documentation
4. U.S. National Scheme
 - 4.1. U.S. CCTL
 - 4.2. NVLAP
 - 4.2.1. Handbook 150
 - 4.3. NIAP, NSA
 - 4.4. CCEVS organization
 - 4.4.1. Definition
 - 4.4.2. CCTL
 - 4.4.3. Key resources within NIAP – Director, Deputy Director
 - 4.4.4. CCEVS publications
 - 4.4.4.1. Guidance documents
 - 4.4.4.2. Policy letters
5. Evaluation process overview
6. CC structure overview
 - 6.1. CC documentation
 - 6.2. Key documents produced for evaluation
 - 6.2.1. TOE overview
 - 6.2.2. ST overview
 - 6.2.3. PP overview
7. Evaluation of Protection Profiles and Security Targets
 - 7.1. Functional assurance paradigm
 - 7.2. Previews of simple development life cycle and class example TOE
 - 7.3. Discussion of PP and ST
 - 7.3.1. Purpose
 - 7.3.2. Dissection of document structures
 - 7.3.2.1. Introduction
 - 7.3.2.2. TOE description
 - 7.3.2.3. TOE security environment
 - 7.3.2.3.1. Threats
 - 7.3.2.3.2. OSPs



- 7.3.2.3.3. Assumptions
- 7.3.2.4. Security objectives
- 7.3.2.5. IT security requirements
- 7.3.2.6. TOE summary specification
- 7.3.2.7. PP claims
- 7.3.2.8. Rationale
- 7.3.2.9. Review / summation
- 8. Introduction to functional families
 - 8.1. Structure of functional classes
 - 8.2. Learning to read Part 2
 - 8.2.1. naming conventions
 - 8.2.2. component leveling
 - 8.2.3. component dependencies
 - 8.2.4. component operations
 - 8.3. Introduction to each functional class
- 9. Introduction to assurance families
 - 9.1. The concept of assurance
 - 9.2. Learning to read Part 3
 - 9.2.1. naming conventions
 - 9.2.2. component dependencies
 - 9.2.3. component operations
 - 9.3. Introduction to assurance classes
 - 9.3.1. Protection Profile
 - 9.3.2. Security Target
 - 9.4. Assurance components for EAL4
 - 9.4.1. Look into each assurance component
 - 9.4.2. Include experiential learning
- 10. Course Review
- 11. Additional materials
 - 11.1. Handouts to students
 - 11.1.1. Common Criteria version 3.1 including CEM
 - 11.1.2. Glossary
 - 11.1.3. Example TOE
 - 11.1.4. Simple development life cycle
 - 11.1.5. Policy letters 10, 12, 13
 - 11.1.6. Assurance packages shown as EALs
 - 11.1.7. Index of external documentation
 - 11.1.8. Completed evaluation resources
 - 11.1.8.1. Red Hat Enterprise Linux 4 Update 1 High-level design



- 11.1.8.2. Red Hat Enterprise Linux 4 Update 1 Functional specification
- 11.1.8.3. Red Hat Enterprise Linux 4 Update 1 CAPP configuration guide
- 11.1.8.4. Red Hat Enterprise Linux 4 Update 1 Security target
- 11.1.8.5. fs.h
- 11.1.8.6. inotify.c
- 11.1.8.7. super.c
- 11.1.9. Class feedback form
- 11.2. Instructional resources for instructor
 - 11.2.1. Example TOE
- 11.3. Marketing brief
- 12. Workshops within the course
 - 12.1. Review recent NIAP Policy Letters (10,12,13)
 - 12.2. Discuss simple product development lifecycle
 - 12.3. Read a Security Target
 - 12.4. Embedded tasks as questions to students
 - 12.4.1. SFR component leveling question