Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Applying the Common Criteria to the Certification &; Accreditation of Department of Defense Unclassified Information Technology Systems

Perhaps the greatest challenge Information Technology (IT) professionals face today is providing evidence that the systems they develop are secure'. To provide this evidence, they must use a standardized process that will foster a high level of confidence in the security features of the IT system. This process must provide a means to quantify and measure the extent to which the security of the IT system has been evaluated and assessed. No matter what type of system is to be developed, there must be assurance that the d...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Applying the Common Criteria to the Certification & Accreditation of Department of Defense Unclassified Information Technology Systems

Arthur F. Roubik Jr.
1.4b

Abstract / Summary

Perhaps the greatest challenge Information Technology (IT) professionals face today is providing evidence that the systems they develop are 'secure'. To provide this evidence, they must use a standardized process that will foster a high level of confidence in the security features of the IT system. This process must provide a means to quantify and measure the extent to which the security of the IT system has been evaluated and assessed. No matter what type of system is to be developed, there must be assurance that the data and data processing resources are protected and the security mechanisms will operate in the manner in which they were designed to operate. Besides being a good business practice, there are numerous laws and regulations, which define and explain why one must be concerned with the adequacy of IT security.

One community of interest that is very concerned about the security of it's IT systems is the Department of Defense (DOD). The DOD uses a standardized process known as 'DITSCAP' for evaluating the security of it's information systems. In order for this process to be successful, there must be a standard set of evaluation criteria used. The current evaluation criteria used by the DOD was developed in 1985 and has become outdated. This paper will discuss how the adoption of a more recently developed evaluation criteria known as the 'Common Criteria' (CC) may be applied to DITSCAP process.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

DITSCAP INTRODUCTION **4**
COMMON CRITERIA INTRODUCTION **4**
ORIGIN OF THE COMMON CRITERIA **4**
CC ORGANIZATION **5**
EVALUATION ASSURANCE LEVELS **6**
THE C&A PROCESS **7**
USING THE CC DURING THE C&A PROCESS **7**
SYSTEM DEVELOPMENT 7
SYSTEM EVALUATION 8
SYSTEM TESTING 9
SYSTEM ACCREDITATION 11
POST ACCREDITATION 11
CONCLUSION **11**
APPENDIX A - LIST OF REFERENCES **12**
APPENDIX B – SECURITY FUNCTIONAL REQUIREMENTS **14**
APPENDIX C – SECURITY ASSURANCE REQUIREMENTS **15**
APPENDIX D - EVALUATION ASSURANCE LEVELS (EALS) **16**
APPENDIX E – EAL MAPPING TO SOURCE CRITERIA **17**
APPENDIX F – ACRONYM LIST **18**

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Figures

Figure 1- CC Contructs[6] 5
Figure 2 – TCSEC to CC Mapping[9] 6
Figure 3 – Security Functional Classes 14
Figure 4 – Security Assurance Classes 15
Figure 5 – Evaluation Assurance Levels 16

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

DITSCAP Introduction

The DOD ensures confidence in the security of it's IT systems by using a standard methodology known as the DOD Information Technology Security Certification and Accreditation Process (DITSCAP). Department of Defense Instruction (DODI) 5200.40 mandates the use of this process. The instruction "implements policy, assigns responsibilities, and describes the procedures"[1] to be used during the Certification and Accreditation (C&A) of information system operated on behalf of the DOD.

Certification is a comprehensive evaluation of the technical and non-technical security features of an IT system, made in support of the accreditation process. This evaluation is used to establish the extent that a particular design and implementation of an IT system meets a set of specified information security requirements. The current evaluation criteria used by the DOD is called the Trusted Computer System Evaluation Criteria (TCSEC) and is known as the 'Orange Book'.

Accreditation is a formal declaration that the IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. This declaration is usually made by a senior operational commander with the authority to approve IT system operation in view of the security risks that it may contain.

Common Criteria Introduction

The Common Criteria for Information Technology Security Evaluation (CC) defines the general concepts and principles of information security, identifies requirements for the security of an IT system or product, and presents a general model of evaluation using categories of functional requirements and assurance requirements. Functional requirements represent desired security behavior. Assurance requirements are the basis for establishing confidence that the security measures are effective and implemented correctly. The CC represents the outcome of efforts to develop a criteria for the evaluation of IT security that could be used within the international community. It is an alignment of a number of similar source criteria from the United States (US), Europe, and Canada that resolved the conceptual and technical differences between them. Essentially, the CC is meant to be used as the basis for the evaluation of the security properties of IT system and products.

Origin of the Common Criteria

During the 1980s, the United Kingdom's Communications-Electronics Security Group (CESG), Germany's Bundesamt für Sicherheit in der Informationstechnik (BSI), France's Central Service for Information System Security (SCSSI) and the National Communication Security Agency (NLNCSA) from the Netherlands each produced versions of their own national security certification criteria. These European criteria were later combined and published as the Information Technology Security Evaluation Criteria (ITSEC). "The current issue, Version 1.2, was published by the European Commission in June 1991".[2]

1. DODI 5200.40, Page 1
2. The National Technical Authority for Information Assurance

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Canada also had it's own security certification criteria known as the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC). CTCPEC version 3.0 was published in early 1993 "as a combination of the ITSEC and TCSEC approaches".[3] The CTCPEC is "somewhat more flexible than the TCSEC (along the lines of the ITSEC) while maintaining fairly close compatibility with individual TCSEC requirements.[4]

In the early 1990's development efforts originated on the CC with the goal of combining the existing evaluation criteria from North America and Europe into a single internationally recognized standard. In 1996, the CPCTEC, ITSEC, and TCSEC were combined to form the first version of the CC. After extensive public review and the development of additional revisions to the original document, version 2.0 of the CC was produced in April of 1998. In 1999, this version became known as International Standards Organization (ISO) 15408 - Evaluation Criteria for Information Technology Security. The CC Project subsequently "incorporated minor changes and produced CC version 2.1 in August 1999".[5]

CC Organization

The CC is broken up into 3 parts. Part 1 is "an introduction of the general model" for the CC and defines the terms and concepts used throughout the evaluation process. Part 2 "establishes a set of security functional components" that describe the security requirements for an IT system or product. Part 3 "establishes a set of assurance components" that are used to rate the effectiveness of the security controls.

Figure 1 shows how the CC defines a set of constructs, for classifying security requirements.

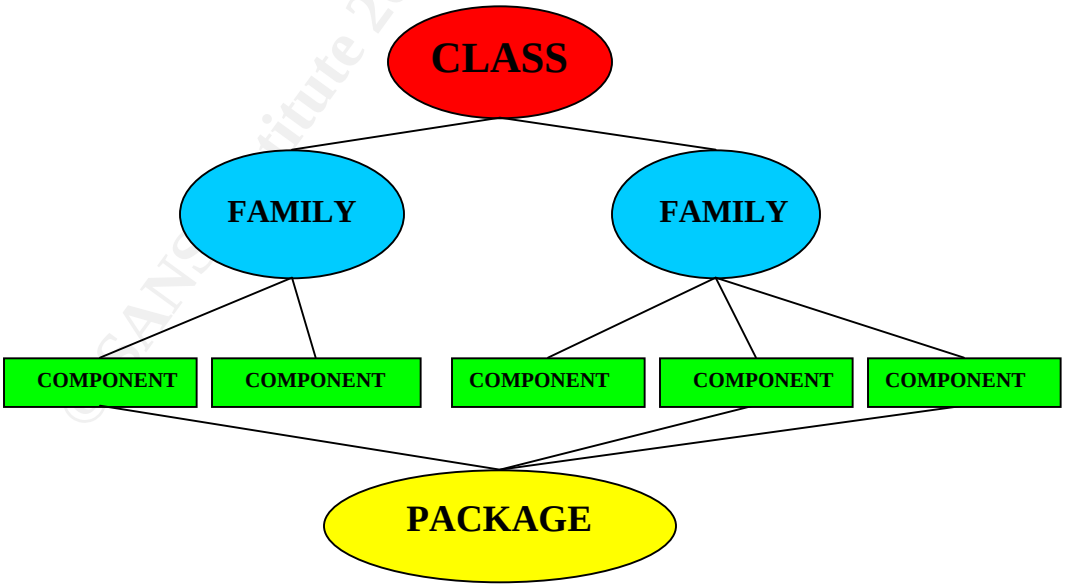

Figure 1- CC Contructs[6]

3. Common Criteria Org - Origins of the Common Criteria
4. Trusted Product Evaluation Program - Computer Security Evaluation FAQ
5. Computer Security Resource Center - Common Criteria for IT Security Evaluation
6. Syntegra, Common Criteria – An Introduction

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As shown in Figure 1, the organization of the CC begins with **Classes.** Classes are a way of grouping security features that describe similar or common functional security requirements. Examples include Identification and Authentication, Security Management, Data Protections, Communications Security, and Auditing. Each class contains **Families** of security requirements that meet a specific security objective. As an example, the Audit Security Class contains families for audit collection, audit storage and analysis, and audit file protection. Finally within each family there are **Components**. Component definitions further breakdown the security objectives of a family into specific tasks that must be performed to meet the objective. Components may be tailored in order to meet a specific security policy or counter a specific threat. The combination of the actual set of requirements, used for meeting an identifiable subset of security objectives is termed a **Package**.

Evaluation Assurance Levels

An Evaluation Assurance Level (EAL) is defined as "a package consisting of assurance components that represents a point on the CC predefined assurance scale".[8] There are seven predefined assurance packages or EALs defined in Part 3 of the common criteria and each is briefly described Appendix D. The EALs are defined on a rising scale of assurance and were developed provide approximate mappings to the class ratings of the ITSEC and TCSEC for defining levels of assurance. For additional information, see Appendix E.

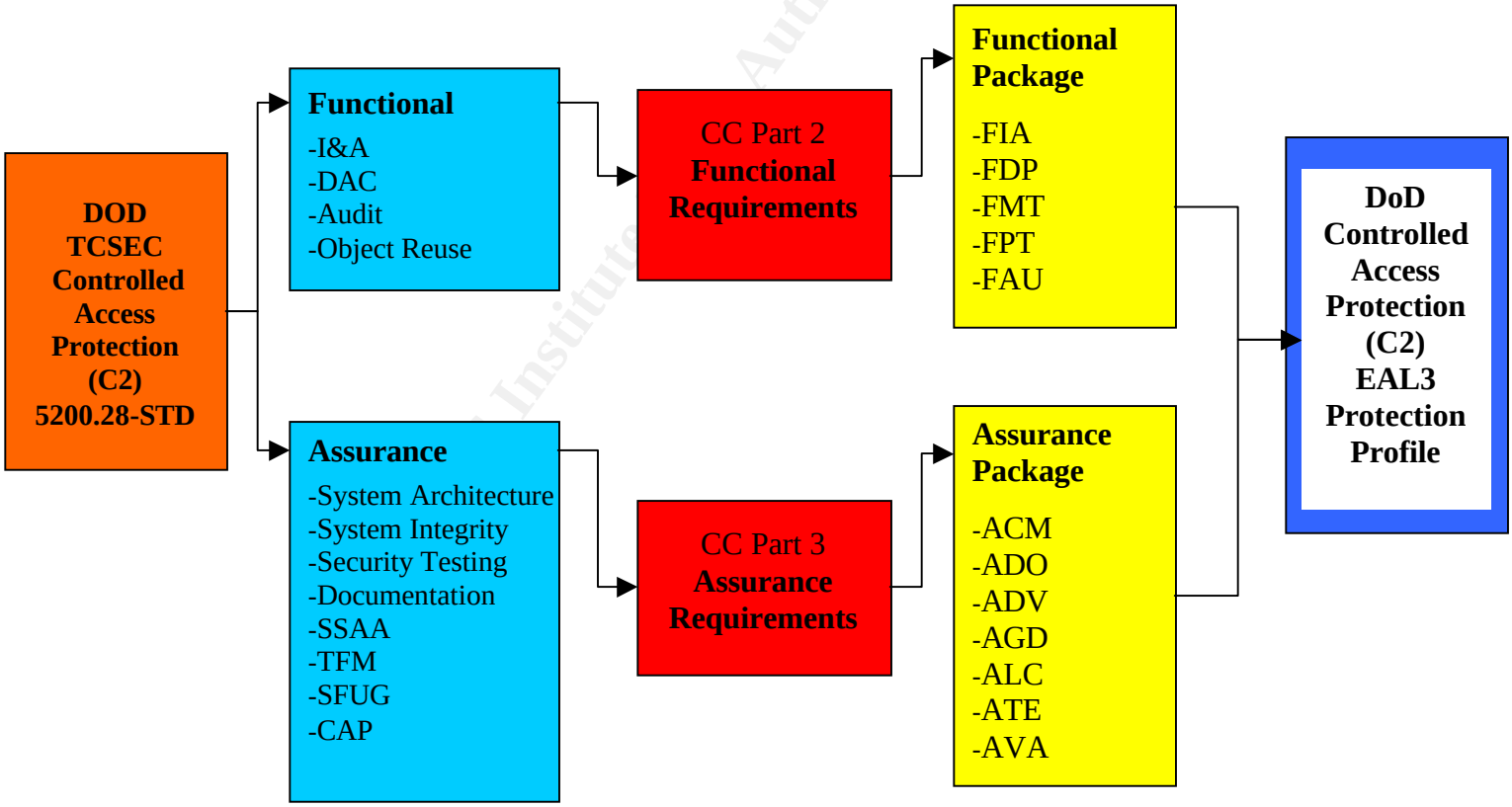

Figure 2 – TCSEC to CC Mapping[9]

8. Common Criteria Org - Evaluation Assurance Levels
9. National Institute for Standards and Technology – Common Criteria Familiarization, Page 7

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Figure 2 provides a diagram of how the TCSEC is mapped to the Common Criteria. As shown in figure 2 above, the TCSEC Class C2 level of protection, maps to EAL3 in the CC. All DOD unclassified IT systems must currently meet a TCSEC Class C2 level of protection. Class C2 security requirements mandate the use of Identification and Authentication (I&A), Discretionary Access Controls (DAC), and User Level Auditing (ULA) in order for the IT system to be compliant. EAL3 is defined as "methodically tested and checked" and is applicable when there is a requirement for a moderate level of independently assured security that must include a thorough investigation of the IT system and its operational environment. An EAL3 evaluation also requires confirmation of the security requirements using test results and evidence that an evaluator has searched for obvious vulnerabilities.

The C&A Process

Within each DOD command there is a Designated Approving Authority (DAA) who will mandate that certain security standards must be present in the IT systems for which they are responsible. These individuals are known as 'accreditors' and they will delegate tasking to a Certification Authority (CA) to perform the C&A process. The purpose of performing the C&A process is to determine if the evaluated IT system is capable of protecting the confidentiality, integrity, and availability of it's resources and data and report this information to the accreditor. The security mechanisms in place must provide an acceptable level of risk that the information contained in the IT system is protected from unauthorized disclosure, modification, or loss of use.

The process of certifying a DOD IT system begins with a review of the security requirements mandated by various National and DOD policies and described in the IT systems supporting documentation. The supporting documentation will define the system's functions, architecture, and interfaces. The next step in the certification of an IT system is a security analysis of the physical, personnel, and administrative security controls in place. The last step is validating that the IT system is in compliance with the mandated security requirements and is done by performing Security Test and Evaluation (ST&E) procedures.

Using the CC During the C&A process

System developers supporting the user community, system evaluators supporting the CA, and the individual accreditor are all involved during the C&A process. Each has specific responsibilities during the process and they all may benefit by using the CC.

System Development

System developers may use the CC during their design of the system. The CC provides developers with Protection Profiles (PP) for clearly identifying the required security features that the IT system must meet. A PP defines an "implementation-independent set of security requirements and objectives for an IT system and/or product"[10] and addresses the threats that exist in a specified environment. The PP

10. Common Criteria Org – Abbreviations and Definitions

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

construct allows the user community to work together with developers to create standardized reusable sets of security requirements, which will meet their identified security objectives. A PP may be used in the following scenarios:

- A user group wishes to specify security requirements for an application type (e.g. naval ship maintenance)
- A government wishes to specify security requirements for a class of security products (e.g. firewalls)
- An organization wishes to purchase an IT system to address its security requirements (e.g. patient records for a hospital)

The federal government and commercial industries have already developed multiple PPs, however the PPs most important to our discussion are the PPs that have been developed to replicate TCSEC Class C2 requirements. In defining the security requirements for an IT system, the developers must also consider the threats to the operational environment. The CC contains a catalogue of components that the developers of PPs can collate to form the security requirements definition. The organization of these components into a hierarchy helps the developer to locate the right components to combat their specific threats.

In order to document compliance of the IT system with previously agreed upon security requirements derived from PPs, a System Security Authorization Agreement (SSAA) will be developed. The SSAA, with its appendices, is intended to provide a reasonably complete description of the IT system and its security posture along with descriptions of the security test and evaluation procedures to be performed. During system development, the SSAA is used to specify information assurance requirements and document the operational environment. For example, if the operating system provides a method for Identification and Authentication, the SSAA will document how this is performed. If there are requirements for audit functions that detect and record the occurrences of such events, descriptions of these audit functions would also be part of SSAA. This SSAA is a living document, so any discrepancies that are identified later during the evaluation and testing phase will be corrected and the SSAA would be updated appropriately.

System Evaluation

During the system evaluation phase of the DITSCAP process, evaluators (who are normally assigned by the CA) will perform a review of the system to determine if each of the threats identified in the development PPs are properly mitigated and to verify that organization policies are being enforced. The principal inputs to the evaluation portion of the C&A process are the PPs, the SSAA, and the Target of Evaluation (TOE). A TOE is defined as “an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.”.[11] So essentially, the TOE is that part of the IT system which is subject to evaluation and could include networks, operating systems, and computer applications.

11. Common Criteria Org – Abbreviations and Definitions

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The Security Target ST is the description of a product or a system. The Security Target (ST) contains the IT security objectives and requirements of a specific TOE and defines the functional and assurance measures offered by that TOE to meet stated requirements. As such it is expected to identify the security functions, and possibly the security mechanisms that enforce the defined organizational security policies and counter any identified threats. The evaluator must check that the installation, configuration, and start-up procedures that must be performed in order to secure the TOE are also described in the ST. A ST may claim conformance to one or more PPs, and forms the basis for the security evaluation of an IT system. The expected result of the evaluation process is a confirmation that the ST is satisfied for the TOE, with one or more reports documenting the evaluation findings.

The TOE description, the security environment, and the IT security requirements information should be included in the SSAA. The evaluator must examine the SSAA and determine if the security features are described in a level of detail that is sufficient to give the reader a general understanding of those features. The SSAA will also include assumptions about the environment in which the TOE will operate. The evaluator must verify the physical, personnel, and connectivity security controls of the environment that are outlined in the SSAA. Physical security controls may include administrator consoles that are in an area restricted to only administrator personnel. An example of a personnel control is that all system users must have a certain minimum clearance. Connectivity controls include secure connections between the TOE and other IT systems.

System Testing

The largest and most complex activity during the C&A process is the development and execution of the test procedures, which will test the IT system's compliance with the defined security requirements. Therefore, the TOE security requirements and the security requirements for the IT environment must be described completely and consistently in the SSAA, and they must provide an adequate basis for development of the test and evaluation procedures.

The system tester will use the CC functional and assurance requirements to determine via testing if the TOE actually meets the defined security requirements. Security functional and assurance requirements are grouped into classes. As stated earlier, classes are just a grouping of security requirements that have a similar focus. Part 2 of the CC contains the listing of the eleven functionality requirements classes. Examples include Identification and Authentication, Security Management, Data Protections, Communications Security, and Auditing. Part 3 of the CC contains the listing of the eight assurance requirements classes. Examples include Configuration Management, Vulnerability Assessment, and Delivery and Operation. Two additional classes contain the assurance requirements specifically for PPs and STs. Once again each of these classes contains a number of families. The requirements for each family share similar security objectives, but differ in emphasis. For example, the Development class

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

contains seven families dealing with various aspects of design documentation (e.g. functional specification, high-level design and representation correspondence). Appendices B & C respectively each describe the functional and assurance requirement classes.

The CC also describes the security requirements the evaluator must develop test procedures for and the security functions on which to perform these tests. The evaluator will develop the ST&E procedures using the CC functional and assurance classes that apply to an EAL3 level of assurance. The functional classes that would apply to an unclassified system include the Identification and Authentication (FIA), User Data Protection (FDP), Audit (FAU), and Security Management (FMT).

The FIA class describes requirements for determining and verifying user identity, determining user authorization with respect to the TOE, and correctly associating security attributes to an authorized user. The FDP class may be used to develop test procedures to verify the protection of user data within the TOE during import, export and storage. The FAU class identifies the test requirements for auditing. Auditing is performed to associate processing actions to authorized users and involves capturing information related to security activities. The class lists the requirements for auditable events, the analysis of audit records, and the protection and storage of the audit information. The FMT specifies the requirements for management of security attributes, data and functions associated with the IT system and list the requirements for testing separation of duties security features.

The assurance classes that would apply to an unclassified system include the Development (ADV), Guidance Documents (AGD), Configuration Management (ACM), Delivery and Operation (ADO), Life Cycle Support (ALC), and Vulnerability Assessment (AVA)

The requirements in the ADV class would be used to map the security requirements from their lowest level representation to their actual implementation. The class of AGD requirements would be used to build test steps to verify the secure operational use of the IT system by both users and administrators. The system tester would use the requirements in the ACM class to determine if the configuration management procedures in place preserve the integrity of the IT system and provide confidence that the TOE and DITSCAP documentation used for evaluation will also be used in production. The ADO class requirements would be used to build test procedures that verify that the security protection features built into IT system are not compromised during delivery, installation, and operation. The requirements in the ALC class support testing procedures to evaluate the security of the development environment and the mitigation of vulnerabilities identified by users. The evaluator would use the requirements AVA in order to examine the strength of the security mechanisms, identify vulnerabilities and discover flaws introduced during development of the IT system.

After the completion of security testing a formal report of the results will be developed and all discrepancies identified during testing shall be included in the report. Hopefully most of the discrepancies can be corrected and then re-tested. If the discrepancy

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

cannot be corrected or the solution is not cost effective, it shall be identified as a 'residual risk'. The CA will then present to the accreditor a Certification Package that includes the SSAA and supporting documentation, the results of system testing, and a listing of any residual risk that the IT system may contain.

System Accreditation

The CC is also useful to system accreditors because they are sometimes closely involved in the determination of functional and assurance requirements for an IT system. System Accreditors must also understand how the different EALs can be used as objective measures of risk reduction, when applied to critical security functions in an IT system and therefore should be familiar with CC Part 3. Accreditors can review the results of the test and evaluation to determine if the system meets their security requirements and can operate at an acceptable level of risk. If this is the case then the IT system will be given the "Authority to Operate" otherwise known as accreditation. If it is determined that the system does not meet all security requirements (contains discrepancies), then an "Interim Authority to Operate" may be issued for a period of ninety (90) days by which time all discrepancies would be resolved.

Post Accreditation

Accreditation is a continuing life cycle function. Accordingly, this includes activities to monitor system management and operation to ensure the system preserves an acceptable residual risk level. Once a TOE is in operation vulnerabilities may surface, or environmental assumptions may require revision. Security personnel must determine the security impact, if any, of these vulnerabilities and reports may then be made to the developer requiring changes to the TOE. After the changes are made reevaluation of the system may be required.

Conclusion

The CC provides great flexibility in the specification of secure information systems or products and in my opinion it may be appropriately applied to the DOD C&A process for unclassified IT systems. The CC may be used during the C&A process to define security requirements, identify security threats to a system, and to develop test plans & evaluation procedures. In my own experience, I have found that both user communities and developers most often will only focus of the functional features of an IT system and will fail to address security requirements during system planning and definition. I believe using the CC provides these communities with an effective method for specifying the security functionality of their systems in terms of standard protection profiles. System evaluators who independently examine the system to ensure that it's meets the EAL3 requirements will also benefit from using the CC because the process will provide clear evidence as to whether the IT system developed is in fact secure.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix A - List of References

1. Department of Defense Instruction 5200.40, "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)", 30 Dec 1997 URL: http://www.dtic.mil/whs/directives/corres/pdf/i520040_123097/i520040p.pdfm (13 Apr 2003)

2. CommonCriteria.org. ", URL: http://www.commoncriteria.org/docs/origins.html (10 Apr 2003)

3. The National Technical Authority for Information Assurance, "ITSEC and Common Criteria", URL: http://www.cesg.gov.uk/, (9 Apr 2003)

4. CommonCriteria.org. "Origins of the Common Criteria", URL: http://www.commoncriteria.org/docs/origins.html (10 Apr 2003)

5. Trusted Product Evaluation Program, "Computer Security Evaluation FAQ Version 2.1", URL: http://isc.faqs.org/faqs/computer-security/evaluations, (10 Apr 2003)

6. Computer Security Resource Center, "Common Criteria for IT Security Evaluation", http://www.csrc.nist.gov/cc, (12 Apr 2003)

7. CommonCriteria.org. "Common Criteria Documentation", URL: http://www.commoncriteria.org/cc/cc.html (10 Apr 2003)

8. Syntegra, "Common Criteria – An Introduction", URL: http://www.common.criteria.org/introductory/CCIntroduction.pdf , *Apr 19 2003)

9. CommonCriteria.org. "Security Functional Requirements", URL: http://www.commoncriteria.org/docs/ccbb.html (10 Apr 2003)

10. CommonCriteria.org. "Common Criteria Abbreviations and Definitions", URL: http://www.commoncriteria.org/faq/definitions.html (10 Apr 2003)

11. National Information Assurance Partnership, http://www.niap.nist.gov/cc-scheme, (12 Apr 2003)

12. CommonCriteria.org. "Evaluation Assurance Levels", URL: http://www.commoncriteria.org/docs/eals.html (10 Apr 2003)

13. National Institute of Standards and Technology (NIST), "Using Common Criteria Protection Profiles", URL: http://csrc.nist.gov/cc/Documents/Guidance/Using_PPs.ppt, (24 Apr 2003)

14. John Pike, Federation of American Scientists, "cryptologie et commerc electronique" (26 Nov 97) URL: http://www.fas.org/irp/world/france/defense/scssi/ (1 May 03)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

15. Richard Walzer (The Mitre Group) – Murray G. Donaldson (Communication Electronic Security Group – CSEG), "Using the Common Criteria Version 2.1" URL:http://www.acsac.org/1999/tutorials.html

16. National Institute of Standards and Technology (NIST), "Common Criteria Familiarization", URL: http://csrc.nist.gov/cc/Documents/Guidance/CC_Overview.ppt (24 Apr 2003)

17. National Institute of Standards and Technology (NIST), "Using Common Criteria Protection Profiles", URL: http://csrc.nist.gov/cc/Documents/Guidance/Using_PPs.ppt, (24 Apr 2003)

18. CommonCriteria.org. "Evaluation Assurance Levels", URL: http://www.commoncriteria.org/docs/eals.html (10 Apr 2003)

19. International Standards Organization, "Common Criteria for Information Security Technical Evaluation – Introduction and General Model", (Aug 1999), Ver 2.1, CCIMB-99-031, URL: http://www.commoncriteria.org/docs, (18 Apr 2003)

20. International Standards Organization, "Common Criteria for Information Security Technical Evaluation – Security Functional Requirements", (Aug 1999), Ver 2.1, CCIMB-99-032, URL: http://www.commoncriteria.org/docs, (18 Apr 2003)

21. International Standards Organization, "Common Criteria for Information Security Technical Evaluation – Security Assurance Requirements", URL: http://www.commoncriteria.org/docs, (Aug 1999), Ver 2.1, CCIMB-99-033, (18 Apr 2003)

22. Department of Defense Instruction 8500.2, "Information Assurance (IA) Implementation ", 6 Feb 2003 URL: www.dtic.mil/whs/directives/corres/ pdf/i85002_020603/i85002p.pdf (7 May 2003)

23. CommonCriteria.org, Common Evaluation Methodology Ver 1.0 Part 2, (Aug 1999), URL: http://www.commoncriteria.org/cem/cem_html/cem2_ch3.html#33837 (4 May 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix B – Security Functional Requirements

Figure 3 below describes each of the eleven (11) security functional requirement classes contained in Part 2 of the CC.

Class Name	Description
Identification and Authentication (FIA)	This class contains families that deal with determining and verifying user identity, determining user authorization with respect to the TOE, and correctly associating security attributes to an authorized user.
TOE Access (FTA)	This class specifies functional requirements for controlling the establishment of a user's session. This include limiting the number of user sessions, limiting user access capabilities, user access history and the modification of access controls.
User Data Protection (FDP)	This class contains families specifying requirements relating to the protection of user data within the TOE during import, export and storage
Communications (FCO)	The communications class provides two families concerned with assuring the identity of a party participating in data exchange. The families are concerned with non-repudiation by the originator and by the recipient of data.
Cryptographic Support (FCS)	This class contains two families describing the operational use and management of cryptographic keys. This class is used when the TOE implements cryptographic functions to support communications, identification and authentication, or data separation.
Audit (FAU)	This class contains families that define the requirements for the selection of auditable events, the analysis of audit records, and the protection and storage of the audit information. Auditing is performed to associate processing actions to authorized users and involves capturing information related to security activities.
Security Management (FMT)	The class deals with the management aspects of the other functional classes and is to specify the management of TSF security attributes, data and functions. The interaction of different management roles (i.e. separation of duties) is also defined.
Privacy (FPR)	This class contains families dealing with anonymity, pseudonymity, unlinkability and unobservability. Privacy requirements protects the user identity from others.
Protection of the TOE Security Functions (FPT)	This class is focused on the integrity management, and protection of TSF (TOE security functions) data, rather than of user data.
Resource Utilization (FRU)	This class contains three (3) families, which support the availability of resources (i.e. processing capability and storage capacity). The families identify requirements for fault tolerance, service priority and resource allocation.
Trusted Path/Channels (FTP)	This class is concerned with trusted communications paths between the users and the TSF. Trusted paths are constructed from trusted channels, which exist for inter-TSF communications

Figure 3 – Security Functional Classes

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix C – Security Assurance Requirements

Figure 4 below describes the ten (10) security assurance requirement classes defined in Part 3 of the CC.

Class Name	Description
Configuration Management (ACM)	The families in this class are concerned with the capabilities of the Configuration Management (CM), its scope and automation. CM is concerned with preserving the integrity of the TOE and provides confidence that the TOE and documentation used for evaluation will also be used in production
Delivery and Operation (ADO)	This families in this class deal with the procedures for secure delivery, installation and operational of the TOE and to ensure that the security protection offered by the TOE is not compromised during these events.
Maintenance of Assurance (AMA)	This class provides requirements that are intended to be applied after a TOE has been certified against the CC. These requirements are aimed at assuring that the TOE will continue to meet its security target as changes are made to the TOE or its environment. The class contains four families. The first covers the content of the assurance maintenance plan, which covers the nature of proposed changes and the controls which govern them.
Protection Profile Evaluation (APE)	The families in this class deal with the TOE Description, the Security Environment, the Security Objectives and the TOE Security Requirements. The class is used to verify that the PP is consistent , complete, and technically sound.
Development (ADV)	The families in this class involve mapping from the security requirements to their lowest level representation and refining the TSF from the specification defined in the ST to it's actual implementation.
Guidance Documents (AGD)	This class is concerned with the secure operational use of the TOE by both users and administrators.
Life Cycle Support (ALC)	The families in this class involve the life-cycle of the TOE include lifecycle definition, tools and techniques, security of the development environment and the remediation of vulnerabilities identified by TOE users.
Security Target Evaluation (ASE)	The families in this class deal with TOE Description, the Security Environment, the Security Objectives, any PP Claims, the TOE Security Requirements and the TOE Summary Specification. The goal here is to demonstrate that the ST is complete, consistent and technically sound, and is a suitable basis for the TOE evaluation.
Tests (ATE)	The families in this class address developer testing, and the requirements for independent testing. This class is concerned with demonstrating that the TOE meets its functional requirements.
Vulnerability Assessment (AVA)	The families in this class involve identifying vulnerabilities through covert channel analysis, analysis of the configuration of the TOE, examining the strength of mechanisms of the security functions, and identifying flaws introduced during development of the TOE. This class defines requirements directed at the identification of exploitable vulnerabilities, which could be introduced by construction, operation, misuse or incorrect configuration of the TOE.

Figure 4 – Security Assurance Classes

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix D - Evaluation Assurance Levels (EALs)

There are seven (7) EALs defined in Part 3 of the common criteria and each is briefly described Figure 5 below.

Name	Description
EAL1	EAL1 is defined as "functionally tested" and is applicable where threats to security are not viewed as serious but some confidence in correct operation is required. EAL1 requires independent assurance that due care has been exercised with respect to the protection of personal or similar information.
EAL2	EAL2 is defined as "structurally tested" and requires the developer to use consistent and good commercial practice in terms of the delivery of design information and test results. EAL2 is applicable in situations where developers or users require a low / moderate level of independently assured security such as with legacy systems and where access to the developer may be limited.
EAL3	EAL3 is defined as "methodically tested and checked" and is applicable when developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development. An EAL3 evaluation requires confirmation of test results and evidence that a developer has searched for obvious vulnerabilities.
EAL4	EAL4 is defined as "methodically designed, tested and reviewed" and requires rigorous testing based on good commercial development practices that are supported by an independent search for vulnerabilities. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security.
EAL5	EAL5 is defined as "semiformally designed and tested" and is applicable when circumstances developers or users require a high level of independently assured security in a planned development and require rigorous development approach. Vulnerabilities must be identified to "ensure resistance to attackers with a moderate attack potential"[12]. Covert channel analysis and design are also required.
EAL6	EAL6 is defined as "semiformally verified design and tested", requires a rigorous development environment, and is applicable in the development of security TOEs for applications which are "protecting high value assets against significant risks."[13] An independent search for vulnerabilities must be conducted to ensure resistance to attackers with a high attack potential.
EAL7	EAL7 is defined as "formally verified design and tested" and is applicable to the development of security TOEs for application in extremely high risk situations with high value assets. EAL7 is for TOEs that require extensive formal analysis of the security functionality, yet the "complexity of the design must be minimized"[14].

Figure 5 – Evaluation Assurance Levels

12. Common Criteria Org – Evaluation Assurance Levels
13. Common Criteria Org – Evaluation Assurance Levels
14. Common Criteria Org – Evaluation Assurance Levels

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix E – EAL Mapping to Source Criteria

Figure 6 shows the relationship between the CC EAL's and the ITSEC / TCSEC Class Ratings.

CC Level	Brief Description	ITSEC Equivalent	ITSEC Equivalent
EAL1	functionally tested	EO	D: Minimal Protection
EAL2	structurally tested	-	-
EAL3	methodically tested and checked	E1	C1: Discretionary Security Protection
EAL4	methodically designed, tested and reviewed	E2	C2: Controlled Access Protection
EAL5	semiformally designed and tested	E3	B1: Labeled Security Protection
EAL6	semiformally verified design and tested	E4	B2: Structured Protection
EAL7	formally verified design and tested	E5	B3: Security Domains
-	-	E6	A1: Verified Design

Figure 6 – Evaluation Assurance Levels

Note: Some of the EAL's do not derive assurance using the same methodologies as the ITSEC and TCSEC and therefore exact mappings do not exist.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Appendix F – Acronym List

BSI	Bundesamt für Sicherheit in der Informationstechnik
C&A	Certification and Accreditation
CA	Certification Authority
CAP	Controlled Access Protection
CC	Common Criteria
CESG	Communications-Electronics Security Group
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DITSCAP	Department of Defense Information Technology Security Certification & Accreditation Process
DOD	Department of Defense
DODI	Department of Defense Instruction
EAL	Evaluation Assurance Level
I&A	Identification and Authentication
ISO	International Standards Organization
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
NLNSCA	Netherlands National Communication Security Agency (NLNCSA)
PP	Protection Profile
SCSSI	Central Service for Information System Security
SFUG	Security Features Users Guide
SSAA	System Security Authorization Agreement
ST	Security Target
TCSEC	Trusted Computer Security Evaluation Criteria
TFM	Trusted Facility Manual
TOE	Target of Evaluation
ULA	User Level Auditing
US	United States

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 29th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

FOR578 Cyber Threat Intelligence	**Tysons Corner, VAUS**	**Aug 31, 2015 - Sep 04, 2015**	**Live Event**
SANS Milan 2015	**Milan, IT**	**Sep 07, 2015 - Sep 12, 2015**	**Live Event**
SANS Crystal City 2015	**Crystal City, VAUS**	**Sep 08, 2015 - Sep 13, 2015**	**Live Event**
SANS Network Security 2015	**Las Vegas, NVUS**	**Sep 12, 2015 - Sep 21, 2015**	**Live Event**
SANS Seoul 2015	**Seoul, KR**	**Sep 14, 2015 - Sep 19, 2015**	**Live Event**
SANS Tallinn 2015	**Tallinn, EE**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Perth 2015	**Perth, AU**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS Baltimore 2015	**Baltimore, MDUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
Data Breach Investigation Summit & Training	**Dallas, TXUS**	**Sep 21, 2015 - Sep 26, 2015**	**Live Event**
SANS ICS Amsterdam 2015	**Amsterdam, NL**	**Sep 22, 2015 - Sep 28, 2015**	**Live Event**
SANS Bangalore 2015	**Bangalore, IN**	**Sep 28, 2015 - Oct 17, 2015**	**Live Event**
SANS DFIR Prague 2015	**Prague, CZ**	**Oct 05, 2015 - Oct 17, 2015**	**Live Event**
SANS Seattle 2015	**Seattle, WAUS**	**Oct 05, 2015 - Oct 10, 2015**	**Live Event**
SOS: SANS October Singapore 2015	**Singapore, SG**	**Oct 12, 2015 - Oct 24, 2015**	**Live Event**
SANS Tysons Corner 2015	**Tysons Corner, VAUS**	**Oct 12, 2015 - Oct 17, 2015**	**Live Event**
SANS Gulf Region 2015	**Dubai, AE**	**Oct 17, 2015 - Oct 29, 2015**	**Live Event**
SANS Cyber Defense San Diego 2015	**San Diego, CAUS**	**Oct 19, 2015 - Oct 24, 2015**	**Live Event**
SANS Tokyo Autumn 2015	**Tokyo, JP**	**Oct 19, 2015 - Oct 31, 2015**	**Live Event**
SANS South Florida 2015	**Fort Lauderdale, FLUS**	**Nov 09, 2015 - Nov 14, 2015**	**Live Event**
SANS Sydney 2015	**Sydney, AU**	**Nov 09, 2015 - Nov 21, 2015**	**Live Event**
SANS London 2015	**London, GB**	**Nov 14, 2015 - Nov 23, 2015**	**Live Event**
Pen Test Hackfest Summit & Training	**Alexandria, VAUS**	**Nov 16, 2015 - Nov 23, 2015**	**Live Event**
SANS Hyderabad 2015	**Hyderabad, IN**	**Nov 24, 2015 - Dec 04, 2015**	**Live Event**
SANS Chicago 2015	**OnlineILUS**	**Aug 30, 2015 - Sep 04, 2015**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**