



Common Criteria Evaluation and Validation Scheme

Publication #6

Assurance Continuity: Guidance for Maintenance and Re-evaluation

8 September 2008
Version 2.0

Foreword

The Common Criteria Evaluation and Validation Scheme (CCEVS) was established to ensure the ready availability of independently evaluated and validated IT products that meet the security needs of the United States Government.

Audrey M. Dale
Director, CCEVS

All correspondence in connection with this document should be addressed to:

National Security Agency
Common Criteria Evaluation and Validation Scheme
9800 Savage Road, Suite 6757
Fort George G. Meade, MD 20755-6757
E-mail: scheme-comments@missi.ncsc.mil
<http://www.niap-ccevs.org/cc-scheme>

Amendment record

Version	Date	Description
2.0	8 September 2008	Initial release

(Page intentionally left blank)

Table of Contents

1 Introduction.....	1
1.1 Purpose of this document.....	1
1.2 Organization and scope.....	2
2 Technical Concepts	2
2.1 Purpose of Assurance Continuity.....	2
2.2 Terminology.....	3
2.3 Assumptions.....	4
2.4 Assurance Continuity paradigm.....	5
2.4.1 Maintenance.....	7
2.4.2 Re-evaluation.....	9
2.5 Oversight for Assurance Continuity of a Validated TOE.....	11
2.5.1 Roles and responsibilities.....	11
2.5.2 IAR submission review process.....	12
3 Characterization of Changes	14
3.1 Typical minor changes.....	15
3.2 Typical major changes.....	16
3.3 Changes requiring additional analysis.....	17
3.4 Interpretations and criteria updates.....	18
4 Performing an Impact Analysis.....	18
4.1 Input.....	18
4.2 Preliminary work.....	18
4.3 Steps in performing the impact analysis.....	19
4.4 Output.....	21
5 Impact Analysis Report (IAR).....	22
5.1 Introduction.....	22
5.2 Description of the change(s).....	23
5.3 Affected developer evidence.....	23
5.4 Description of the developer evidence modifications.....	23
5.5 Conclusions.....	23
5.6 Annex: Updated developer evidence.....	24
Annex A: References.....	25
Annex B: Acronyms.....	26
Annex C: Glossary.....	28
Annex D: Checklist for IAR author.....	31

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS) for Information Technology Security was established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to validate conformance of Information Technology (IT) products and Protection Profiles (PP) to international standards. The CCEVS oversees the evaluations performed by Common Criteria Testing Labs (CCTLs) on information technology products and PP's against the *Common Criteria for Information Technology Security Evaluation (CC)*.

The principal participants in the CCEVS program are the:

- **Sponsor/Developer:** The Sponsor may be a product developer, a Protection Profile developer, a value-added reseller of an IT security-enabled product, or another party that wishes to have a product or PP evaluated. The sponsor requests that a Common Criteria Testing Laboratory (CCTL) conduct a security evaluation of an IT product or PP.
- **Common Criteria Testing Laboratory (CCTL):** The CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS to perform security evaluations against the *Common Criteria for Information Technology Security Evaluation (CC)* using the *Common Methodology for Information Technology Security Evaluation (CEM)*.
- **Common Criteria Evaluation and Validation Scheme (CCEVS):** The CCEVS is the government organization established to maintain and operate the scheme for the U.S. Government and to oversee and validate the evaluations performed by the CCTLs.

1.1 Purpose of this document

The purpose of this document is to define the CCEVS approach to maintenance and re-evaluation activities, which together are termed Assurance Continuity. *Assurance Continuity: CCRA Requirements version 1.0 released February 2004* was used as the basis for defining the CCEVS assurance continuity process. It describe the minimum set of requirements for the maintenance and re-evaluation of CC validated products and is intended to provide sponsors/vendors of evaluated products with the basic information required for them to submit an Impact Analysis Report (IAR) for maintenance of a previously evaluated product.

1.2 Organization and scope

This document is one of a series of technical and administrative CCEVS publications that describes how the scheme operates. It consists of five chapters and several supporting annexes. Chapter 1 provides a general description of maintenance and re-evaluation, chapter 2 describes the technical concepts underpinning the assurance continuity paradigm including a description of the processes involved in both maintenance and re-evaluation along with the roles and responsibilities of the participants, chapter 3 describes how changes to the product are categorized, chapter 4 describes how an impact analysis is performed and chapter 5 defines the required contents of the Impact Analysis Report (IAR). The supporting annexes include a list of acronyms, a glossary, references and an IAR checklist.

This document complements or references other CCEVS publications and documents used in the operation of the CCEVS. These other publications include:

[Publication #1](#), *Common Criteria Evaluation and Validation Scheme -- Organization, Management, and Concept of Operations*

[Publication #2](#), *Common Criteria Evaluation and Validation Scheme – Quality Manual and Standard Operating Procedures*

[Publication #3](#), *Common Criteria Evaluation and Validation Scheme -- Guidance to Validators*

[Publication #4](#), *Common Criteria Evaluation and Validation Scheme -- Guidance to Common Criteria Testing Laboratories*

[Publication #5](#), *Common Criteria Evaluation and Validation Scheme - Guidance to Sponsors*

This *Assurance Continuity Guidance* also references other documents such as Common Criteria, NVLAP and ISO publications in describing requirements to evaluation sponsors. The reader of this document will need to be familiar with these reference documents to gain a clear understanding of the guidance provided herein.

CCEVS related publications and information are available on the CCEVS web site <http://www.niap-ccevs.org/cc-scheme/index.cfm>.

2 Technical Concepts

2.1 Purpose of Assurance Continuity

The purpose of Assurance Continuity is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner.

The awarding of a Common Criteria evaluation certificate signifies that all necessary evaluation work has been performed, the TOE meets all the defined assurance requirements, and the CCEVS has confidence that the IT product or system meets its security objectives.

Assurance Continuity recognizes that as changes are made to a validated TOE or its environment, evaluation work previously performed need not all be repeated. Assurance Continuity defines an approach to minimizing redundancy in IT Security evaluations, allowing a determination to be made as to whether independent evaluator actions need to be re-performed.

It is important to note that the date on which the Assurance Continuity submission is received by CCEVS must be no later than two years from the completion date of the original evaluation for the validated TOE.

2.2 Terminology

For clarity, the following terms are used in this paradigm description:

- a) The *validated TOE* refers to the version of the TOE that has been evaluated and for which a certificate has been issued;
- b) The *changed TOE* refers to a version that differs from the validated TOE; for example:
 - a new release of the TOE or of the product in which the TOE is a subset of functionality.
 - the validated TOE with patches applied to correct discovered bugs.
 - the same version of the validated TOE, but in a new operational environment (e.g. on a different hardware or software platform) as reflected in a new Security Target.
- c) The *maintained TOE* refers to a changed TOE that has undergone the maintenance process and to which the certificate for the validated TOE also applies. This signifies that assurance gained in the validated TOE also applies to the maintained TOE.
- d) The *Maintenance Addendum* refers to a notation on the Validated Products List (VPL) ,that serves as an addendum to the certificate for a validated TOE. The Maintenance Addendum lists the maintained versions of the TOE. There is no implied issuance of an updated certificate.

- e) The *Impact Analysis Report (IAR)* refers to a report which records the analysis of the impact of changes to the validated TOE. The IAR is generated by the developer who is requesting a Maintenance Addendum. Note: The developer may elect to have a CCTL or CC consultant generate or assist in the generation of the IAR. It is assumed that the CCTL or CC consultant has access to the original evaluation evidence and the current TOE changes.
- f) The *Maintenance Report* refers to a publicly available report that describes all changes made to the validated TOE which have been accepted under the maintenance process.
- g) The *assurance baseline* refers to the culmination of activities performed by both the evaluator and developer resulting in a validated TOE, recorded or submitted as evidence and measurable by change to that evidence.
- h) The *developer evidence* refers to all items made available to the evaluators in support of an evaluation of a TOE.
- i) *Maintenance* refers to the process of recognizing that a set of one or more changes made to a validated TOE have not adversely affected assurance in that TOE.
- j) *Re-evaluation* refers to the process of recognizing that changes made to a validated TOE require independent evaluator activities to be performed in order to establish a new assurance baseline. The re-evaluation process will attempt to reuse results from a previous evaluation.

We refer to the product or system throughout its original evaluation as a TOE. Once the original evaluation is completed and a certificate awarded, it becomes the validated TOE. After a subsequent version of the validated TOE (changed TOE) has been added to the Maintenance Addendum, that version is considered to be a maintained TOE.

2.3 Assumptions

This document was written with the following assumptions:

- a) The CCEVS has an appropriate level of trust in the developer and in any developer supplied evidence.
- b) The CCEVS will use ‘Assurance Continuity: CCEVS Requirements’ as the basis for implementation of Assurance Continuity.
- c) For maintenance under the CCRA, a developer can only submit an IAR to the same scheme under which the original evaluation was conducted.

- d) The developer may elect to have a CCTL or consultant generate or assist in the generation of the IAR and it is assumed that the CCTL or consultant has access to the original evaluation evidence and the current TOE changes.
- e) There exists a means to ensure consistency among CCTLs in the characterization of major and minor changes.
- f) The updated product complies with all CCEVS policies in effect at the time of the Assurance Continuity submission.

2.4 Assurance Continuity paradigm

Assurance Continuity takes advantage of the fact that as changes are made to a validated TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. The Assurance Continuity paradigm therefore defines the processes for *maintenance* and *re-evaluation* such that both attempt to recognize previous evaluation work.

Maintenance refers to the process undertaken by a developer in order to have a unique TOE identifier change (e.g. version increment), resulting from a changed TOE, listed in the Maintenance Addendum for that TOE. It must be demonstrated that the changes to the TOE do not adversely affect the assurance baseline.

Re-evaluation refers to the evaluation of a changed TOE, such that the developer could not (or chose not to) demonstrate that changes to the validated TOE did not adversely affect the assurance baseline.

It is important to note that the maintenance process is not intended to provide assurance in regard to the resistance of the TOE to new vulnerabilities or attack methods discovered since the date of the initial certificate. Such assurance can only be gained through re-evaluation. Maintenance only considers the affect of TOE changes on the assurance baseline; it does not consider an evolving threat environment. All publicly known vulnerabilities must, however, be mitigated prior to submitting an updated TOE through the maintenance process.

Figure 2.1 shows the primary paths through assurance continuity. Both the maintenance and re-evaluation processes have an equivalent starting point: when a change is made to the validated TOE [box 1]. This change might be a patch designed to correct a discovered flaw, an enhancement to a feature, the addition of a new feature, a clarification in the guidance documentation, or any other change to the validated TOE.

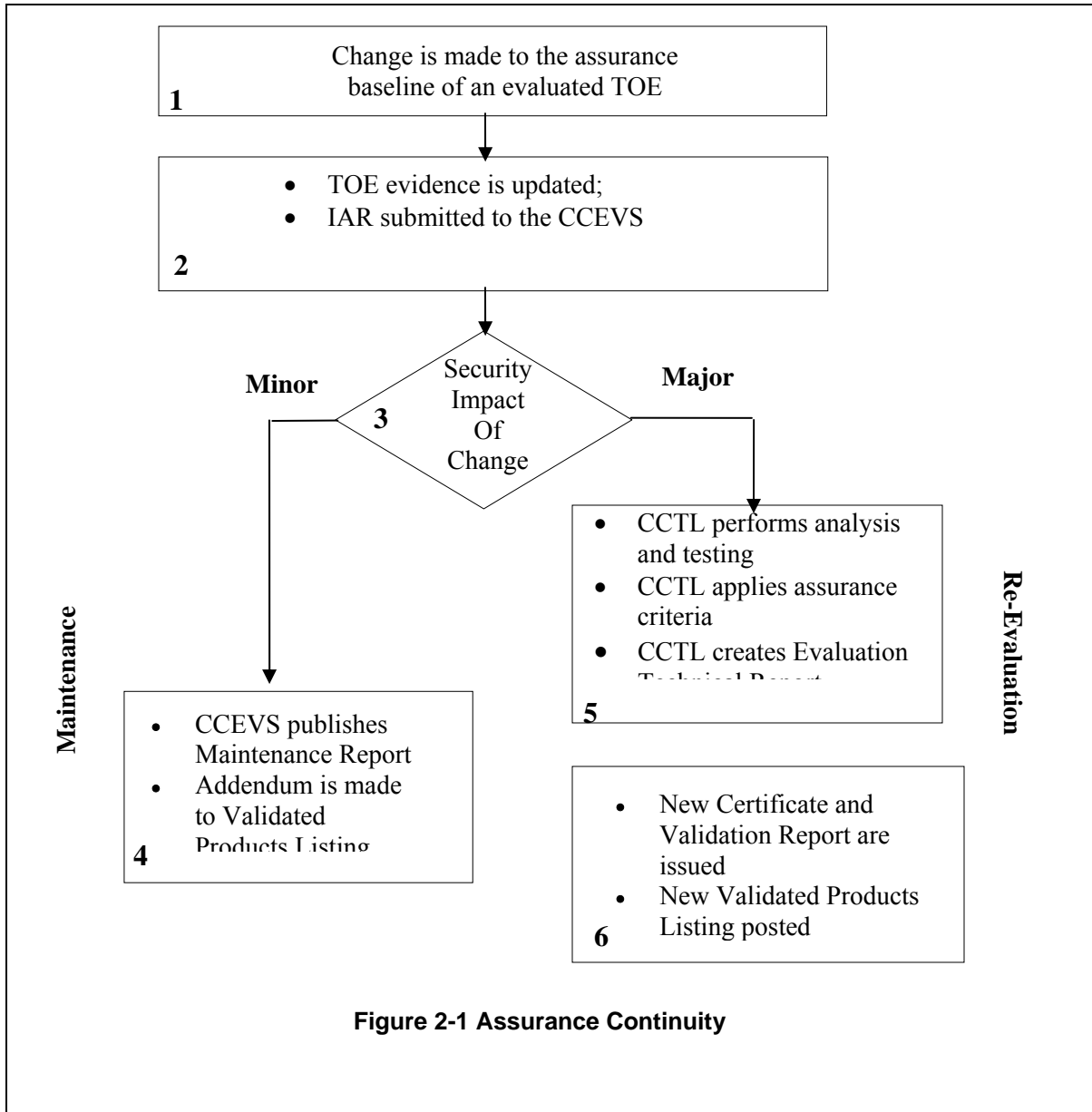


Figure 2-1 Assurance Continuity

As a result of this change, a recommendation by the developer or CCTL (acting as agent on behalf of the developer) needs to be made in regard to its resulting impact on assurance [box 2]. This includes an analysis of the evaluation evidence that would have to be updated to reflect the change, and *regression testing* of the code to be sure that it works when incorporated into the TOE (e.g. all previous security tests need to be re-run). The basis for making this recommendation is called *impact analysis*, which is performed by the TOE developer and recorded in an Impact Analysis Report (IAR). See [Chapter 5](#) for more detail on the content of the IAR.

The CCEVS uses the IAR¹ to determine whether [box 3] the changes have a minor or major impact on assurance baseline.

The CCEVS might use other factors (e.g. elapsed time since validation) other than the changes being major or minor in determining whether maintenance or re-evaluation is to be used. See Sections 3.2-3.3 for additional details.

If the CCEVS agrees that the change has a minor impact, then [box 4] a Maintenance Report is produced from the IAR, and an addendum to the Validated Products List (VPL) is created. The Maintenance Report is made publicly available where it will serve as an addendum to the Validation Report of the original validated TOE.

If the CCEVS finds that the change has a major impact, then the changed TOE must undergo re-evaluation. This evaluation [box 5] makes maximum use of previously generated evidence, as well as the IAR, resulting in [box 6] a new Validated Product with a new Validation Report and a new certificate. See [Chapter 2.4.2](#) for additional details regarding re-evaluations.

This new validated TOE will then serve as the baseline against which any future changes will be compared [back to box 1].

2.4.1 Maintenance

The purpose of Maintenance, under Assurance Continuity, is to allow for minor changes (those that can be shown to have little or no affect on assurance) to be made to a validated TOE and have the resulting TOE version recognized as maintaining the same level of assurance as the validated TOE.

To achieve this aim, maintenance provides a mechanism which enables developers and/or its selected CCTL to analyze the effects of the change and present their findings to the CCEVS. This means that when a change occurs, developers must conduct relevant action items in order to confirm that the assurance baseline has not been adversely affected. This process places an obligation on the developer to maintain all developer evidence (recording sufficient information in the IAR about changes to documentary evidence would be considered maintaining that evidence); to conduct, record, and provide evidence of appropriate testing; and to confirm that previous analysis results have not been affected by changes to the TOE. Chapter 4: *Performing an Impact Analysis* further describes these types of activities. The maintenance process is described below.

2.4.1.1 Process description

The maintenance process can be defined in terms of the necessary inputs, actions and outputs that lead to a Maintenance Addendum for a Common Criteria certificate. The

¹ Strictly speaking, the IAR is necessary only in cases where the Maintenance path is desired. Although no IAR need be submitted if a developer were to elect the re-evaluation path, the developer might elect to provide a high-level report of the changes to serve as useful input to the re-evaluation effort.

provisions of the certificate apply to all versions of the TOE that are listed in the Maintenance Addendum.

In order for CCEVS to review the developer's analysis, and begin the process, the developer must ensure that the following inputs are available to the CCEVS:

- a) Certificate for the TOE (including Maintenance Addendum)
- b) Validation Report
- c) Security Target for the validated TOE
- d) Security Target for the updated TOE (with tracked changes)
- e) Impact Analysis Report (IAR)

Once the CCEVS has the required inputs, a review of the IAR and other relevant evidence will commence in order to determine what impact the changes described in the IAR will have on the assurance baseline.

The review process performed by the CCEVS will likely involve consultation with the developer and/or the CCTL generating the IAR. This consultation should result in a complete and consistent IAR. That is, the analysis recorded is complete and the IAR meets all requirements for content and presentation (see [Chapter 5](#)), to the satisfaction of the CCEVS. The IAR review is conducted in accordance with this document and with any relevant guidance issued by the CCEVS.

There are two possible outcomes from the IAR review:

- i) The CCEVS determines that the impact of changes on the TOE are major and the Maintenance Addendum will not be created.
- ii) The CCEVS determines that the impact of changes on the TOE are minor and the Maintenance Addendum is created to show that the certificate also applies to the maintained TOE. See [Chapter 2.5](#) for further details.

Once this determination is made, the CCEVS will inform the developer of the outcome. If the impact of changes is considered minor, a Maintenance Report and updated Maintenance Addendum is published on the CCEVS VPL. The complete IAR is shared only between the developer and the CCEVS.

The CCEVS will record the underlying rationale for their decisions in accordance with their quality assurance processes.

2.4.1.3 Maintenance Report

The Maintenance Report is considered to be an addendum to the Validation Report for the validated TOE. It provides details of all changes made to the validated TOE that have been accepted under the maintenance process.

The information contained in the Maintenance Report is a subset of the IAR content. The following sections of the IAR should be included in the Maintenance Report:

- a) Introduction
- b) Description of changes
- c) Affected developer evidence

The content of each of these sections is described in Chapter 5 *Impact Analysis Report*. These sections may be sanitized when reproduced in the Maintenance Report by the removal or paraphrasing of proprietary technical information.

The Maintenance Report will also contain a reference to the Validation Report for which it is an addendum.

2.4.1.2 Maintenance Addendum

The Maintenance Addendum serves as an addendum to the certificate for a validated TOE that lists the maintained TOEs derived from that validated TOE.

2.4.2 Re-evaluation

When a change to a validated TOE has been determined to have a major impact on the assurance of that TOE, additional analysis, performed by an independent evaluator, is required to assess the assurance of the changed TOE. A re-evaluation is performed in the context of an earlier evaluation; reusing any results from that earlier evaluation that still apply.

This re-evaluation is the same as a new evaluation except the previous evaluation results and evidence are used to the maximum extent possible to minimize duplication of effort. Furthermore, the re-evaluation must comply with all current CCEVS policies.

The developer may opt to move directly into re-evaluation without ever creating an IAR (for example, if the changes are so substantial that the changed TOE bears only a minimal resemblance to the evaluated TOE).

If the developer conducted and documented a security impact analysis of the differences between the changed TOE and the evaluated TOE and if this IAR was provided to the CCTL, it would be used as the basis for identifying those parts of the changed TOE remaining unchanged from the previously-evaluated TOE. As with all evaluations,

analysis that has already been performed on parts of a TOE that remain unchanged need not be performed again, thereby maximizing the results of previous effort that can be re-used.

The minimum components necessary for building upon a previously conducted evaluation, regardless of where it was conducted, re-utilizing previous analysis and evidence are:

- a) Product and supporting documentation
- b) New Security Target
- c) Original Security Target
- d) Original Evaluation Technical Report
- e) Original Certification/Validation Report
- f) Original Common Criteria Certificate
- g) Original Evaluation Work Packages (if available)

The CCTL will be required to perform an analysis of the changes between the new ST and the original ST to determine the impact of those changes on the analysis and evidence from the original evaluation. During the re-evaluation the CCTL must only repeat analysis previously conducted when requirements have changed or where requirements were impacted by another change. Thus, many of the requirements previously met during the original evaluation may still be satisfied and new work packages for these requirements will not be required. Work packages, which are developed from a previous evaluation, may be helpful in providing information on how the previous evaluation team reached their conclusions and may also provide helpful information in assessing compliance to the new requirements. With this in mind, if the previous evaluation work packages are available they should be used to the maximum extent possible. Generally, the CCTL conducting the current evaluation should use any evidence from the prior evaluation where beneficial, either to reduce costs or to help ensure a technically sound evaluation. When generating a new ETR for the current evaluation, the CCTL can use a combination of previous work packages or ETR sections (in the absence of work packages) coupled with new evaluation work packages

At the completion of the evaluation of the changed TOE, a new ETR is produced, along with a new Validation Report and new certificate. This changed TOE becomes the basis for any future assurance continuity activities.

2.5 Oversight for Assurance Continuity of a Validated TOE

2.5.1 Roles and responsibilities

There are three parties that participate in a CC evaluation: Developer (Sponsor), CCTL, and CCEVS. This document describes the responsibilities for each of these parties in the Assurance Continuity process. Note: In cases where the sponsor of an evaluation is not the developer of the product, the sponsor needs to obtain the cooperation of the developer for any technical materials and essential deliverables.

2.5.1.1 Developer

The developer of the validated TOE is responsible for:

- a) producing the updated TOE;
- b) regression testing of the updated TOE;
- c) updating all evidence that is affected by changes to the validated TOE₁;
- d) performing an impact analysis of the changes to the validated TOE, and documenting the results in an Impact Analysis Report; and
- e) providing the CCEVS with a complete Assurance Continuity submission.

2.5.1.2 CCTL

Under the Assurance Continuity process, the CCEVS interacts directly with the developer, and thus there may be no explicit role for the CCTL. However, the developer may choose to enlist the services of a CCTL or CC consultant when preparing for Assurance Continuity.

CCTLs or CC consultants providing Assurance Continuity assistance are considered to be acting as agents on behalf of the developer.

2.5.1.3 CCEVS

The CCEVS is responsible for:

- a) ensuring that the Impact Analysis Report sufficiently documents the changes to the TOE, the analysis of the impact of those changes to the validated TOE, and that all results are substantiated;
- b) confirming whether changes to the validated TOE are major or minor;
- c) documenting the findings arising from the review and analysis of the Assurance Continuity submission; and

- d) if changes are deemed minor, producing a Maintenance Report, and a Maintenance Addendum that is consistent with the results documented in the Impact Analysis Report.

2.5.2 IAR submission review process

There are three stages to the submission review process for Assurance Continuity:

- a) the submission review stage, during which the CCEVS checks the developer's submission for completeness;
- b) the submission analysis stage, during which the CCEVS analyzes the developer's maintenance claim;
- c) the conclusion stage, during which the CCEVS produces a Maintenance Report and a Maintenance Addendum.

In the sections that follow, each stage of submission and review process is described in detail.

2.5.2.1 IAR submission review stage

The CCEVS acknowledges receipt of the submission and reviews the submission to verify that there are no input items missing, and that there are no readily apparent inconsistencies or anomalies. There are two possible results:

- a) the CCEVS informs the developer that the submission package contains all the required deliverables, and that the CCEVS will now proceed to the submission analysis stage. The CCEVS also provides an estimated timeframe for the analysis stage; or
- b) the CCEVS informs the developer that the submission is incomplete, identifies the missing elements, and may recommend that the developer contact a CCTL or CC consultant for assistance in producing an updated Assurance Continuity submission.

2.5.2.2 IAR submission analysis stage

The CCEVS examines the changes described in the Impact Analysis Report in order to determine their impact upon the assurance of the validated TOE.

- a) if the developer has provided sufficient supporting rationale describing the impact of each change;

- b) whether the impact of each change has a minor or major impact on assurance;
- c) whether, taking the culmination of changes into consideration, the overall impact of the changes are minor or major.

The CCEVS may also selectively sample the affected developer evidence to verify that the required updates have been applied.

The CCEVS informs the developer, in writing, of the results of the submission analysis. There are four possible results:

- a) all changes are assessed as minor, all affected developer evidence has been updated, and the maintained TOE qualifies for assurance maintenance. In this case, the process enters into the conclusion stage,
- b) all changes appear to be minor, but some affected developer evidence has not been adequately updated. In this case, the developer is required to update the evidence. Once all affected developer evidence has been updated, the maintained TOE qualifies for assurance maintenance. The process then enters into the conclusion stage.
- c) one or more sections of the Impact Analysis Report contain inadequate detail. In this case, the developer is required to provide the additional details, which may require additional impact analysis activity on the part of the developer. This may result in a significant rewrite and re-submission of the Impact Analysis Report. Once all affected developer evidence has been updated, the maintained TOE qualifies for assurance maintenance. The process then enters into the conclusion stage, or
- d) one or more changes are assessed as major, and re-evaluation is required.

2.5.2.3 IAR submission conclusion stage

The CCEVS uses the Impact Analysis Report as the basis for producing a Maintenance Report and Maintenance Addendum. The CCEVS is the final authority for the content of the Maintenance Report.

2.5.2.3.1 Maintenance Report

The Maintenance Report is an addendum to the Validation Report for the validated TOE. It identifies the changes made to the validated TOE that have been accepted under the maintenance process.

The Maintenance Report contains the following information, taken from the Impact Analysis Report, and sanitized as appropriate by removing or paraphrasing proprietary technical information:

- a) introduction;
- b) description of changes;
- c) affected developer evidence.

The Maintenance Report also contains a reference to the Validation Report for the validated TOE.

2.5.2.3.2 Maintenance Addendum

The Maintenance Addendum serves as an addendum to the certificate for the evaluated TOE. The Maintenance Addendum includes the following information:

- a) a unique identifier for the most recent version of the maintained TOE;
- b) the date of maintenance completion;
- c) unique identifiers for all previous maintained TOEs that are based on the validated TOE;
- d) the unique reference for the validated TOE;
- f) the Maintenance Report.

3 Characterization of Changes

The CCEVS examines the changes described in the Impact Analysis Report in order to determine their impact upon the assurance of the validated TOE. A *minor change* is one whose impact is sufficiently minimal that it does not affect the assurance to the extent that the evaluator activities need to be independently reapplied (although the developer is expected to have tested the changes as part of their standard regression testing). By contrast, a change deemed *major* has an impact that is substantial enough that it does affect the assurance and would consequently warrant independent re-application of the evaluator activities. Therefore, minor changes are addressed under *maintenance*, which can be performed solely by the developer, while major changes are addressed under *re-evaluation*, which is performed by the CCTL.

It is important to note the difference between a change's impact upon the validated TOE and a change's impact upon the assurance of the validated TOE. A given change that is widespread and affects many parts of the TOE might have no effect upon the assurance of the TOE, or it could have far-reaching effects upon the assurance of the TOE. Similarly, a given change that affects only a very small part of the TOE might have no effect upon the assurance of the TOE, or it could have far-reaching effects upon the assurance of the TOE.

It is impossible to predict all possible changes to all possible TOEs and, therefore, to identify the impact of all possible changes (and whether a given possible change is minor or major). Consequently, there is no concrete method for identifying whether the security impact of a change is major or minor. The following offers a general guideline on the differences between major and minor changes, and also offers examples of exceptions.

3.1 Typical minor changes

Minor changes typically consist of changes to the TOE that have no effect on any claims about the TOE. Examples of minor changes that are therefore suitable to be addressed under maintenance are:

- **Changes to the IT environment that do not affect the validated TOE.** For example, a change to the underlying hardware (where the hardware is not part of the TOE) or to software parts of the product that are outside the TOE boundary would likely be minor if the interface remains unchanged. In addition, moving to a later version of an underlying platform is usually minor, unless there are major interface changes to the underlying platform. Moving to a distinctly different underlying platform (e.g., from a Windows-based platform to a Linux-based platform) is often major just because of the potential impact on the lower interface. Adequate retesting would have to be performed to ensure that the new underlying platform does not introduce vulnerabilities.
- **Changes to the validated TOE that do not affect the assurance evidence.** For example, if a TOE has been validated to EAL1, a change to the source code and/or hardware schematics would not have an impact upon the assurance documentation. Nevertheless, the developer would have to test the changes as part of their standard regression testing.
- **Non-security relevant changes to TOE functionality.** Changes to or the addition of non-security relevant functionality are considered minor. Changes or additions of security relevant functionality may be minor or major.
- **Editorial changes** (grammatical, typographical, formatting) to any of the assurance evidence. For example, editorial changes to a functional specification that provide additional clarification would be minor.
- **Changes to non-executable text in the source code** (such as comments) would typically be minor changes. But, a change to compiler instructions would likely be considered a major change, as in cases when ALC_TAT is being claimed.
- **Changes to the development environment** that have no notable effect upon assurance. For example, an update to the configuration management tool would be minor if the update did not affect the results of tracking the evolution of the TOE. However, if an update to the configuration management tool produced entirely new results that would therefore have to be re-evaluated, then the change would be considered major.

- **Changes to the ST front-matter.** A change to the ST's identification or to the TOE identifier (e.g. product name change) would be minor. If any of the statements of Threats, OSPs, Assumptions, or Security Objectives change, without necessitating a change to the Security Requirements, these would likely be minor changes. If, however, any of the requirements statements do change, these would be major changes.
- **Claiming compliance to a new PP.** Although making changes in order to claim compliance to a PP will likely be major, it is possible that no changes to the TOE, to the ST front-matter, or to the claimed requirements will occur. This often happens when the PP is being developed simultaneously with the ST, but the ST evaluation completes before the PP is finalized. If the two have been developed in concert, mere addition of the PP compliance claim – by itself – would be considered minor.

3.2 Typical major changes

Major changes typically consist of changes to the claims about the TOE. Examples of major changes that should be addressed under re-evaluation include:

- **Changes to the set of claimed assurance requirements.** This includes both claiming families that were not claimed in the original evaluation as well as a claim of a higher component within the same family. While the deletion of an assurance requirement could arguably be considered a “minor” change, the result would require the production of a new certificate, which is done only under re-evaluation and therefore must be considered a major change.
- **Changes to the set of claimed functional requirements.** This would likely change the TOE boundary, which would have to be re-assessed for correctness and soundness under re-evaluation.
- **Use of procedures not assessed in the original evaluation.** The use of new procedures that were not used in the original evaluation, such as delivery procedures different from those examined for the delivery requirements, would constitute a major change.
- **Changes to the TOE boundary.** Adding a new security function or mechanism that changes a claimed SFR or contributes to a new SFR. Removing a security function or mechanism that contributes to enforcing a claimed SFR.
- **A set of minor changes that together have a major impact upon the security of the TOE.** Although changes might be of minor impact in isolation, the collection of minor changes could have a major security impact, and so the combination of these would have to be re-evaluated.

- **The accumulation of maintenance iterations collectively result in the maintained version being too different from the original version such that a single change cannot be meaningfully analyzed in isolation.** If the accumulation of changes is so substantial that the result no longer resembles the original (as in cases where each update is a change to a different portion of the TOE), then a meaningful examination of only the change becomes infeasible to the point that the entire TOE would have to be re-evaluated.
- **Addition of PP compliance claims.** Adding a PP compliance claim will likely involve adding claimed assurance or functional requirements, redefining the assumptions or threat statements, or changing the TOE boundary to include portions necessary to fulfill all of the PP's requirements. Such changes would have to be assessed under re-evaluation.
- **Changes to the TOE after a prolonged elapsed time since the assurance baseline was evaluated or maintained.** If a change is made to the TOE and more than two years have passed since the evaluation or latest maintenance activity, CCEVS's corporate knowledge about the product will have diminished to the point that the minimal oversight that maintenance entails would be insufficient to readily catch any problems. Therefore, re-evaluation would be required.
- **Assurance Continuity of higher assurance components.** There are some CC assurance components above EAL 4 that require internal NSA evaluation resources in addition to those provided by the CCTL. For evaluations containing such components, re-evaluations may be required. See CCEVS [Policy #19](#) for details.

Migration to new criteria. The CC is updated in terms of both major and minor reissues. Minor revisions result from the incorporation of changed text as defined in Requests for Interpretation or change proposals, and are denoted by either a change to the minor part of the version number (from version 2.1 to version 2.3). Major reissues result from drastic rewriting and are denoted by a new version number (e.g. from version 2 to version 3). The results of a TOE evaluation against one version cannot be readily migrated to another version within the scope of maintenance; a re-evaluation will be required.

3.3 Changes requiring additional analysis

There are some kinds of changes that are not clearly major or minor and must be decided on a case-by-case basis. The description of these changes in the IAR should contain sufficient explanatory text to provide a basis on which a sound judgment may be made. These include:

- Adding extended security functional requirements (security functional requirements that are not contained in the CC, part 2)
- Modifying refinements in the original set of claimed CC components.

- Adhering to international interpretations (CCEVS and the other schemes will determine which interpretations are considered major or minor).
- Bug fixes. A bug fix has no predictable extent of change to the validated TOE, nor a predictable effect upon the assurance of the validated TOE.

3.4 Interpretations and criteria updates

For full TOE evaluations, the CCEVS requires developers and CCTLs to apply all international interpretations that are in effect at the start date of the evaluation. All CCEVS interpretations that are final at the start date of the evaluation must likewise be considered.

During assurance maintenance, all final interpretations must be discussed within the IAR, including an explanation of how they are met or why they do not apply.

If the CCRA signatories adopt a new version of the CC, there will be an associated migration timetable that establishes deadlines by which evaluations can no longer use the previous version of the criteria. This timetable will also include a date by which maintenance activities can no longer be made against the older criteria. All CCEVS evaluations will be required to adhere to these deadlines.

4 Performing an Impact Analysis

4.1 Input

The following are the primary inputs required for the impact analysis process:

- a) developer evidence associated with the Validated TOE;
- b) change(s) description (probably generated from life cycle quality processes and procedures).

4.2 Preliminary work

Security categorization of the TOE may be used as a tool to help assess if a change is within the scope of maintenance. For example, when a change is described in an impact analysis, the security categorization may be consulted to identify the influence of the change on the developer evidence provided in the assurance baseline.

Security categorization may include any security relevant development tools, secure delivery procedures, developer security procedures, development life-cycle activities, or the security relevant procedures affecting the use or administration of the configuration management system.

It should be noted that any additions to the TOE will need to be security categorized, according to the chosen approach, and any modified portions may need to have their security categorization reviewed.

4.3 Steps in performing the impact analysis

During maintenance, it is the developer's responsibility to confirm that content and presentation verdicts for modified developer evidence can still be met. Having identified the effect of the change on the developer evidence, the developer is then able to conclude the security effect of the change.

Step 1 - Identify Validated TOE

Determine the developer evidence provided for the validated TOE assurance baseline, including the validated TOE. All changes are applied against this baseline.

Step 2 - Identify and describe change(s)

Describe the change(s) to the product relevant to the product associated with the validated TOE.

Identify and describe the change(s) to the development environment relevant to the development environment of the validated TOE.

These changes must be described to the level of detail necessary to understand what was done, but not necessarily how it was done.

Step 3 - Determine impacted developer evidence

The objective of this step is to determine, considering each change from the previous step, which items of the developer evidence need to be updated. This step should be conducted in a systematic way, considering in turn each assurance component included in the assurance package for the validated TOE, the effect of the change on the assurance component, and the evidence provided for that component. The following list can be used to facilitate such an approach.

For a change to the product, the following should be considered:

- a) Has it affected the Security Target?
- b) Does it meet all applicable CCEVS Policies?
- c) Has it affected the reference for the TOE?
- d) Has it affected the list of configuration items for the TOE?
- e) Has it affected any of the TSF abstraction levels, (such as the functional specification, the implementation representation, etc.) or the correspondence between them?
- f) Has it affected the TSP model?

- g) Has it affected the guidance documentation?
- h) Has it affected the testing documentation, that is, the analysis of test coverage, the analysis of the depth of testing or the test documentation?
- i) Has it affected the covert channel analysis, the analysis of guidance documentation, the vulnerability analysis?

For a change to the development environment, the following should be considered:

- a) Has it affected the Security Target?
- b) Does it meet all applicable CCEVS policies?
- c) Has it affected the configuration management documentation?
- d) Has it affected the delivery procedures?
- e) Has it affected the procedures necessary for the secure installation, generation, and start-up of the TOE?
- f) Has it affected the developer security procedures?
- g) Has it affected the flaw remediation procedures?
- h) Has it affected the life cycle model?
- i) Has it affected the development tools?

The impacts on all the developer evidence should be considered, based on the change description, in order to verify that all potential impacts have been identified.

Note that the ST is likely to be affected, even if it is substantially similar to the original ST. If the TOE has changed, then at a minimum, the ST must be updated to include a change to the TOE version number.

Previous versions of the IAR may be used as input to this analysis.

For some developer action elements, this determination may be simple (e.g. a new graphical user interface for the changed TOE, to be delivered in the same manner used for the TOE, will not have an adverse impact on *delivery* requirements), while for other requirements it may be more difficult (e.g. whether the introduction of the new GUI changes the list of the TSF interfaces).

The output of this step is a list of affected developer action elements.

Step 4 - Perform required modifications to developer evidence.

The objective of this step is to determine how the affected developer evidence (identified during the previous step) should be modified in order to address the corresponding elements for content and presentation of evidence. It is sufficient to collect together changes required to developer evidence before actually implementing those changes.

Testing (regression testing) may be necessary in order to update the evidence. For instance, the developer may repeat a sample of the developer tests delivered for the evaluation.

Regarding the IAR, sufficient information about how the developer testing was updated would be required, commensurate with the testing components in the assurance baseline. If new tests were written to address a change, these are identified, with the test purpose, in the impact analysis report. However, the details of the tests in terms of providing the test scripts including the individual test steps, are not required.

If the change to the TSF is “invisible” at the lowest TSF abstraction available (e.g. the lowest level of TSF decomposition in the assurance baseline was the high-level design, and some source code is changed during maintenance, but the changes do not require modification to the high-level design), then the developer should show how the change was tested. The IAR would then describe why this was adequate.

The output of this step is a list of updated evidence (this could take the form of a list of changes to the evidence - where, why, what).

Step 5 – Conclusion

Determine the overall impact of the identified changes on the assurance of the validated TOE and make the conclusion as a minor or major impact.

See [Chapter 3](#) for a discussion on the characterization of changes.

Step 6 – Report

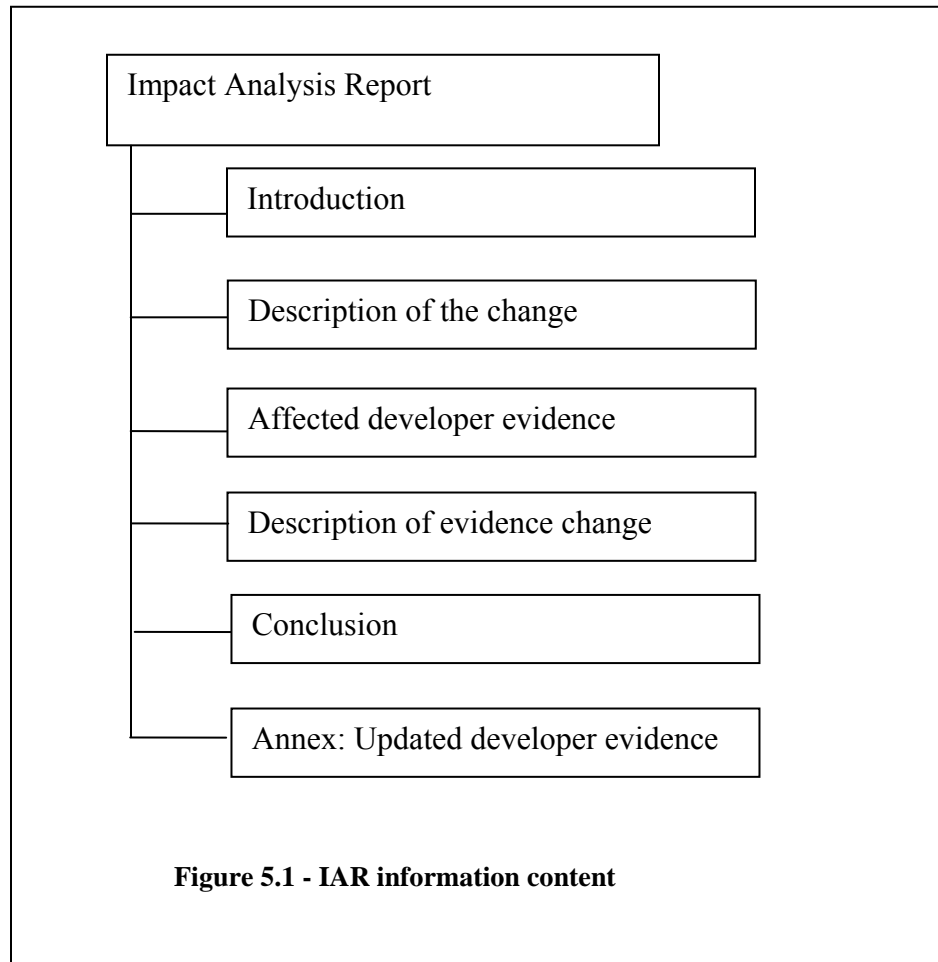
The analysis performed and findings are captured in the Impact Analysis Report (See [Chapter 5](#)). This is reviewed by CCEVS for concurrence.

4.4 Output

- a) Impact Analysis Report (IAR)
- b) Updated developer evidence.

5 Impact Analysis Report (IAR)

This chapter describes the minimum content of the IAR. The contents of the IAR are portrayed in Figure 5.1; this figure may be used as a guide when constructing the outline of the IAR document. The IAR is a required input for the maintenance process.



5.1 Introduction

The developer **shall report** the IAR configuration control identifiers.

The IAR configuration control identifiers contain information that identifies the IAR (e.g. name, date and version number).

The developer **shall report** the current TOE configuration control identifiers.

The TOE configuration control identifiers identify the current version of the TOE that reflects changes to the validated TOE.

The developer **shall report** the configuration control identifiers for the ETR, VR, and validated TOE.

These configuration control identifiers are required to identify the assurance baseline and its associated documentation as well as any other changes that may have been made to this baseline.

The developer **shall report** the configuration control identifiers for the version of the ST related to the validated TOE.

The developer **shall report** the identity of the developer.

The identity of the TOE developer is required to identify the party responsible for producing the TOE, performing the impact analysis and updating the evidence.

The developer may include information in relation to legal or statutory aspects, for example related to the confidentiality of the document.

5.2 Description of the change(s)

The developer **shall report** the changes to the product.

The identified changes are with regard to the product associated with the validated TOE.

The developer **shall report** the changes to the development environment.

The identified changes are with regard to the development environment of the validated TOE.

5.3 Affected developer evidence

For each change, the developer **shall report** the list of affected items of the developer evidence.

For each change to the product associated with the validated TOE or to the development environment of the validated TOE, any item of the developer evidence that need to be modified in order to address the developer action elements shall be identified.

5.4 Description of the developer evidence modifications

The developer **shall briefly describe** the required modifications to the affected items of the developer evidence.

For each affected item of the developer evidence, the modifications required to address the corresponding content and presentation of evidence elements shall be briefly described.

5.5 Conclusions

For each change the developer **shall report** whether the impact on assurance is considered minor or major. *(The checklist in Appendix A can be used to ensure that all areas that will be evaluated are included in the IAR.)*

For each change the developer should provide a supporting rationale for the reported impact.

The developer ***shall report*** whether the overall impact is considered minor or major.

The developer should include a supporting rationale, taking the culmination of changes into consideration.

5.6 Annex: Updated developer evidence

The developer ***shall report*** for each updated item of developer evidence the following information:

- the title;
- the unique reference (e.g. issue date and version number).

Only those items of evidence that are notably changed need to be listed; if the only update to an item of evidence is to reflect the new identification of the TOE, then it does not need to be included.

Annex A: References

The Report of the [President's Commission on Critical Infrastructure Protection](#) (PCCIP), Critical Foundations: Protecting America's Infrastructures, October, 1997.

The White House, The Clinton Administration's Policy on Critical Infrastructure Protection: [Presidential Decision Directive 63, May 1998](#).

CEMEB (Common Evaluation Methodology Editorial Board), [Common Methodology](#) for Information Technology Security Evaluation, Version 3.1, September 2007.

CCMB (Common Criteria Maintenance Board), [Common Criteria](#) for Information Technology Security Evaluation, Version 3.1, September 2007.

- Part 1 Introduction and general model
- Part 2 Security functional components
- Part 3 Security assurance components

[NIST Handbook 150:2005](#) Edition, *Procedures and General Requirements*

[NIST Handbook 150-20](#), *Information Technology Security Testing—Common Criteria*

[ISO/IEC 17025](#) (formerly ISO Guide 25)—General Requirements for the Competence of Calibration and Testing Laboratories, 2005

[ISO/IEC Guide 65](#) — General Requirements for Bodies Operating Product Certification Systems, 1996

Annex B: Acronyms

C	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CCMB	Common Criteria Maintenance Board
CEM	Common Evaluation Methodology
CCRA	Common Criteria Recognition Arrangement
CCTL	Common Criteria Testing Laboratory
EAL	Evaluation Assurance Level
EAP	Evaluation Acceptance Package
ETR	Evaluation Technical Report
FVOR	Final Validation Oversight Review
ISO	International Organization for Standardization
IVOR	Initial Validation Oversight Review
NIAP	National Information Assurance Partnership
MR	Memorandum for Record
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
OD	Observation Decision
OR	Observation Report
ODRB	Observation Decision Review Board
PP	Protection Profile
ST	Security Target

TOE	Target of Evaluation
TTAP	Trust Technology Assessment Program
TOP	Technical Oversight Panel
TVOR	Test Validation Oversight Review
VID	Validation Identification
VOR	Validation Oversight Review
VPL	Validated Products List
VR	Validation Report

Annex C: Glossary

This glossary contains definitions of terms used in the Common Criteria Scheme. These definitions are consistent with the definitions of terms in ISO Guide 2 and are also broadly consistent with the Common Criteria and Common Methodology.

Accreditation Body: An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Agreement Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security: An agreement in which the Parties (i.e., signatories from participating nations) agree to commit themselves, with respect to IT products and protection profiles, to recognize the Common Criteria certificates which have been issued by any one of them in accordance with the terms of the agreement.

Appeal: The process of taking a complaint to a higher level for resolution.

Approved Test Methods List: The list of approved test methods maintained by the CCEVS which can be selected by a CCTL in choosing its scope of accreditation, that is, the types of IT security evaluations that it will be authorized to conduct using CCEVS-approved test methods.

Assurance Maintenance: The process of recognizing that a set of one or more changes made to a validated TOE has not adversely affected assurance in that TOE.

Assurance maintenance addendum: A notation, such as on the listing of evaluated products, that serves as an addendum added to the certificate for a validated TOE. The maintenance addendum lists the maintained versions of the TOE.

Impact Analysis Report (IAR): A report which records the analysis of the impact of changes to the validated TOE.

Assurance Continuity Maintenance Process: A program within the Common Criteria Scheme that allows a sponsor to maintain a Common Criteria certificate by providing a means (through specific assurance maintenance requirements) to ensure that a validated TOE will continue to meet its security target as changes are made to the IT product or its environment.

Assurance Maintenance Report: A publicly available report that describes all changes made to the validated TOE which have been accepted under the maintenance process.

Common Criteria (CC): Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Criteria Certificate: A certificate issued by the CCEVS which confirms that an IT product or protection profile has successfully completed evaluation by an accredited CCTL in conformance with the Common Criteria standard.

Common Criteria Evaluation and Validation Scheme (CCEVS): The program developed to establish an organizational and technical framework to evaluate the trustworthiness of IT products and protection profiles.

Common Criteria Testing Laboratory (CCTL): Within the context of the Common Criteria Evaluation and Validation Scheme, an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS to conduct Common Criteria-based evaluations.

Common Evaluation Methodology (CEM): Common Methodology for Information Technology Security Evaluation, the title of a technical document which describes a particular set of IT security evaluation methods.

Evaluation Evidence: Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.

Evaluation Technical Report: A report giving the details of the findings of an evaluation, submitted by the CCTL to the CCEVS as the principal basis for the validation report.

Evaluation Work Plan: A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

Interpretation: Expert technical judgment, when required, regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Methodology.

National Voluntary Laboratory Accreditation Program (NVLAP): The U.S. accreditation authority for CCTLs operating within the NIAP Common Criteria Evaluation and Validation Scheme.

National Information Assurance Partnership (NIAP): The partnership that included the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) which established a program to evaluate IT product conformance to international standards. Currently, NIST is responsible for the National Voluntary Laboratory Accreditation Program (NVLAP) and NSA is responsible for the Common Criteria Evaluation and Validation Scheme (CCEVS).

Observation Decision (OD): The formal documented response from the CCEVS that provides clarification/guidance to the CCTL on a submitted Observation Report.

Observation Reports (OR): A report issued to the CCEVS by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

Protection Profile (PP): An implementation independent set of security requirements for a category of IT products which meet specific consumer needs.

Re-evaluation: A process of recognizing that changes made to a validated TOE require independent evaluator activities to be performed in order to establish a new assurance baseline. Re-evaluation seeks to reuse results from a previous evaluation.

Security Target (ST): A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Target of Evaluation (TOE): A TOE is defined as a set of software, firmware and/or hardware possibly accompanied by guidance.

Technical Oversight Panel: A panel composed of scheme validators to ensure technical consistency across evaluations and validations performed under CCEVS.

Validation: The process carried out by the CCEVS leading to the issue of a Common Criteria certificate.

Validation Oversight Review: The process for CCEVS to provide validation oversight and to ensure the technical quality of evaluations.

Initial VOR: To ensure that the ST is accurate and clearly specified, meets CCEVS Policies 1, 9, 10, 13, their respective addendums, and the evaluation team correctly performed the Assurance Security Target Evaluation (ASE) analysis

Test VOR: The Test VOR shall be conducted after the TOE passes all the work units except those dependent on team testing. Examples of these exceptions include some (not all) of the guidance documents, testing and vulnerability analysis work units.

Final VOR: The focus of the Final VOR is to ensure all issues have been resolved and to discuss the evaluation team's testing activities.

Validated Products List (VPL): A publicly available listing maintained by the CCEVS Scheme of every IT product/system or protection profile that has been issued a Common Criteria certificate by the CCEVS.

Validation Report (VR): A document issued by the CCEVS and posted on the VPL which summarizes the results of an evaluation and confirms the overall results.

Annex D: Checklist for IAR author

<p>TSF Interfaces. Changes to the TSF Interfaces are of interest because they affect the mapping of SFRs to interfaces. New or changed interfaces require testing to ensure they are implemented correctly (although at EAL2 and below the testing isn't required, but the lack of testing must be noted). New or changed interfaces also required design analysis.</p>		
<input type="checkbox"/> New TSF Interfaces <input type="checkbox"/> Changed TSF Interfaces <input type="checkbox"/> No changes to TSF Interfaces	Describe:	
<p>TSF Platform (TOE Hardware). Changes to the TOE hardware may be major or minor, depending on the change. Faster equipment is not usually a concern, unless covert channels are part of the equation. New components may create new undocumented interfaces, if they are accessible to untrusted users. A new operating system (OS) is more significant, again due to potentially new interfaces.</p>		
<input type="checkbox"/> Faster hardware <input type="checkbox"/> New components <input type="checkbox"/> New OS <input type="checkbox"/> No hardware changes	Describe:	
<p>SFRs. Changes to SFRs in the ST mean the ASE evaluation must be re-accomplished, as it affects mappings, consistency, and the TSS. These changes also propagate throughout all the assurance evidence.</p>		
<input type="checkbox"/> SFR changes <input type="checkbox"/> No SFR changes	Describe:	
<p>New Security Functions. New security functions (i.e., security functionality not covered by SFRs) provided by the product (i.e., what is delivered the product is ordered, even though technically the features may not be in the TSF) must be assessed per Scheme Policy. Based on this assessment and any rationale for exclusion provided in the IAR, CCEVS management must decide whether the new features would be reasonably considered part of the product. If they are, this constitutes a major change and these new security features must be covered by <i>this</i> maintenance action. Further, publicly available literature must be considered to determine if there are other security features that would be reasonably expected to be part of the product.</p>		
<input type="checkbox"/> New security features <input type="checkbox"/> No new security features	Describe:	
<p>Assumptions and Objectives. Changes to assumptions and objectives may either create the need for new SFRs, or create contradictions with existing SFRs. If such changes occur, they should be examined for such effects.</p>		
<input type="checkbox"/> Changes to Assumptions and Objectives <input type="checkbox"/> No changes to assumptions and objectives	Describe:	

<p>Assurance Documents. There should be changes to assurance documents, at minimum to indicate changed CM lists. Changes in other documents are more significant and may require incremental evaluation. New interfaces or features may change guidance documents. New hardware or OSs may change installation procedures. There may also be updates to vulnerability assessments to capture new vulnerabilities.</p>		
<input type="checkbox"/> ACM changes <input type="checkbox"/> AGD, ADO changes <input type="checkbox"/> ATE changes <input type="checkbox"/> AVA changes <input type="checkbox"/> ALC changes <input type="checkbox"/> No new assurance evidence	Describe:	
<p>New Features. The product may include new non-security features. These need to be reviewed to ensure that they are categorized correctly, and that they would have no interference with the TSF.</p>		
<input type="checkbox"/> New non-security features <input type="checkbox"/> No new non-security features	Describe:	
<p>Bug Fixes. Updates often contain bug fixes. If these fixes were security relevant (either to security relevant software, or security vulnerabilities that were discovered in seemingly non-security-relevant software), they should be reviewed to ensure they were corrected. AVA may also require consideration for similar problems in other programs.</p>		
<input type="checkbox"/> Security-relevant fixes <input type="checkbox"/> Non-security-relevant fixes <input type="checkbox"/> No fixes	Describe:	
<p>TOE Environment. Changes to the IT environment typically are not significant, as long as they are acknowledged in the ST and do not violate assumptions. A large change (i.e., to a significantly different underlying operating system) may require retesting to ensure proper integration and ADO instructions.</p>		
<p>Conclusions:</p> <input type="checkbox"/> Clear maintenance action. Only ST updates required. <input type="checkbox"/> Minor maintenance action. Retesting required, but nothing more. <input type="checkbox"/> Reevaluation required. Reuse of evidence is possible. <input type="checkbox"/> Evaluation required. Evidence cannot be reused.		