



Canadian Common Criteria Evaluation and
Certification Scheme (CCS)

CCS-Guide-006 Version 1.2

Technical Oversight for
Assurance Continuity of
a Certified TOE

Foreword

This document describes the process by which the Certification Body (CB) of the Canadian Common Criteria Evaluation and Certification Scheme (CCS) performs technical oversight for Common Criteria assurance continuity. Technical oversight is the quality assurance process for evaluations conducted by CCS-accredited evaluation facilities.

Table of contents

Foreword.....	i
1 Introduction.....	1
1.1 References.....	1
1.2 Objective.....	2
1.3 Audience.....	2
1.4 Document organization.....	2
2 Roles and responsibilities.....	3
2.1 Developer.....	3
2.2 Evaluator.....	3
2.3 Certifier.....	4
2.4 Evaluation sponsor.....	4
3 The submission.....	5
4 Technical oversight process for assurance continuity.....	6
4.1 Submission review stage.....	6
4.2 Submission analysis stage.....	6
4.2.1 Certifier analysis of the Impact Analysis Report.....	6
4.2.2 Certifier analysis of affected developer evidence.....	9
4.2.3 Establishing and communicating the verdict.....	9
4.3 Conclusion stage.....	9
4.3.1 Maintenance Addendum.....	10
4.3.2 Maintenance Report.....	10
5 Confidentiality of reports.....	11
5.1 Impact Analysis Report.....	11
Annex A – Trademarks.....	12

1 Introduction

1. The purpose of Assurance Continuity is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner.
2. The awarding of a Common Criteria evaluation certificate signifies that all necessary evaluation work has been performed to convince the evaluation authority that the TOE meets all the defined assurance requirements as grounds for confidence that an IT product or system meets its security objectives.
3. Assurance Continuity recognises that as changes are made to a certified TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. Assurance Continuity therefore defines an approach to minimising redundancy in IT security evaluation, allowing a determination to be made as to whether independent evaluator actions need to be re-performed.
4. In February 2004, version 1.0 of the document Assurance Continuity: CCRA Requirements [AC: CCRA] was released. [AC: CCRA] defines an accepted baseline approach to assurance maintenance and re-evaluation activities (together termed Assurance Continuity) for use by Common Criteria Recognition Arrangement (CCRA) participants.
5. The Communications Security Establishment, as the certification body (CB) for the Canadian Common Criteria Scheme (CCS), has a responsibility to put into place an Assurance Continuity process that is compliant with the baseline requirements described in [AC: CCRA].
6. This document describes the technical oversight process that will be followed by the CB for Assurance Continuity activities within the CCS.

1.1 References

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000: is the arrangement between its signatories for the recognition of evaluations performed by any of the signatories;

[AC: CCRA] Assurance Continuity: CCRA Requirements, Version 1.0, February 2004: defines an accepted baseline approach to assurance maintenance and re-evaluation activities, for use by CCRA participants;

1.2 Objective

7. The objective of this document is to describe the technical oversight process that is carried out under the CCS for the Assurance Continuity of a Target of Evaluation (TOE), including the necessary input to, and output from, the process.

1.3 Audience

8. The primary audience of this document is the developer, as they are responsible for providing input to the Assurance Continuity process and because they have a vested interest in maintaining assurance in their TOE.
9. Secondary audiences of this document include CC evaluation facilities and advice providers who may provide support to the developer as part of the Assurance Continuity process, as well as consumers who may have an interest in how assurance is maintained for specific TOEs.

1.4 Document organization

10. This document is organized into the following chapters and annexes:
 - a) Chapter 2 describes the Assurance Continuity roles and responsibilities;
 - b) Chapter 3 identifies requirements on the developer's Assurance Continuity submission;
 - c) Chapter 4 describes the technical oversight process employed by the CB;
 - d) Chapter 5 discusses the confidentiality of reports related to the Assurance Continuity process; and
 - e) Annex A identifies all logos that are required to be displayed on reports.

2 Roles and responsibilities

11. There are four parties to a CC evaluation: developer, evaluator, certifier, and sponsor. This document describes the degree of involvement of each of these parties in the Assurance Continuity process.

2.1 Developer

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

2.2 Evaluator

13. Under the Assurance Continuity process, the CB interacts directly with the developer, and thus there is no explicit role for the evaluator. However, the developer may choose to enlist the services of a CCS evaluation facility (or other CC advice provider) when preparing for Assurance Continuity. Such assistance is limited to assisting the developer in performing the impact analysis, and assisting in documenting the results in an Impact Analysis Report.
14. CCS evaluation facilities or advice providers providing Assurance Continuity assistance are considered to be acting as agents on behalf of the developer. The CB places no restrictions on who may provide assistance to the developer in preparing for Assurance Continuity.
15. CCS evaluation facilities should take note that Assurance Continuity assistance provided to the developer could result in a future conflict of interest, should the same individuals serve as evaluators for a future evaluation of the changed TOE. The CB will determine, on a case-by-case basis, whether a conflict of interest exists, based on the nature and degree of assistance provided.

¹ as defined in section 2.2 of version 1.0 of the CCRA Assurance Continuity Guide

2.3 Certifier

16. The main responsibilities of the certifier are:
 - a) to ensure that the Impact Analysis Report documents the analysis of the impact of changes to the certified TOE, and that the results are substantiated;
 - b) to confirm whether changes to the certified TOE are major or minor;
 - c) document their findings arising from the review and analysis of the Assurance Continuity submission; and
 - d) if changes are deemed minor, to produce a Maintenance Addendum, and a Maintenance Report that is consistent with the results documented in the Impact Analysis Report.

2.4 Evaluation sponsor

17. During a TOE evaluation, the role of the evaluation sponsor lies in their interaction with the evaluator, whether to fund the evaluation work or to ensure that the evaluator has access to all required developer assurance evidence. However, since the evaluator has no explicit role under the Assurance Continuity process, neither does the evaluation sponsor.

3 The submission

18. [AC: CCRA] provides specific guidance to the developer in preparing for Assurance Continuity. Within [AC: CCRA], chapter 3 provides guidance on the characterization of major and minor changes to the TOE, chapter 4 provides guidance on performing an impact analysis, and chapter 5 defines content requirements for the Impact Analysis Report.
19. In preparing the Assurance Continuity submission, the developer may wish to consider enlisting the assistance of a CC evaluation facility or advice provider.
20. In addition to content requirements defined in [AC: CCRA], the CB levies the following requirements on the Assurance Continuity submission:
 - a) the certified TOE must have received a CC certificate issued by the CCS;
 - b) the date on which the Assurance Continuity submission is received must be no later than two years from the date on the CC certificate that was issued by the CCS for the certified TOE; and
 - c) the submission shall include:
 - 1) the Evaluation Technical Report;
 - 2) the Impact Analysis Report;
 - 3) revised versions of all affected developer evidence;
 - 4) a reference to the CC certificate for the certified TOE; and
 - 5) identification of those persons that assisted in the preparation of the submission, together with a brief description of their respective roles.
21. Even though [AC: CCRA] mandates the inclusion of the Certification Report and Security Target for the original TOE in the Assurance Continuity submission, the CB does not require that these be explicitly included, since the CB already has access to these public documents.

4 Technical oversight process for assurance continuity

22. There are three stages to the technical oversight process. They are: the submission review stage, during which the certifier checks the developer's submission for completeness; the submission analysis stage, during which the certifier analyses the developer's maintenance claim; and the conclusion stage, during which the certifier produces a Maintenance Addendum and a Maintenance Report.
23. In the sections that follow, each of the stages of technical oversight is described in detail.

4.1 Submission review stage

24. The certifier acknowledges receipt of the submission, and within two working days, provides an estimate for when a verdict will be returned.
25. The certifier 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 verdicts:
 - a) the certifier informs the developer that the submission package contains all the required deliverables, and that the CB will now proceed to the submission analysis stage. The certifier also provides an estimated timeframe for the analysis stage; or
 - b) the certifier informs the developer that the submission is incomplete, identifies or characterizes the missing elements of the submissions, and may recommend that the developer contact a CC evaluation facility or advice provider for assistance in producing an updated Assurance Continuity submission.

4.2 Submission analysis stage

26. The submission analysis stage comprises three activities: analysis of the Impact Analysis Report; analysis of the affected developer evidence; and the establishing and communicating of the analysis verdict to the developer.

4.2.1 Certifier analysis of the Impact Analysis Report

27. The certifier examines each of the following sections of the Impact Analysis Report against the content requirements defined in chapter 5 of [AC: CCRA].

4.2.1.1 Introduction

28. The certifier verifies that:

- a) the developer has reported the Impact Analysis Report's configuration control identifiers and that the identifiers contain information that identifies the Impact Analysis Report (name, date and version number);
- b) the developer has reported the current TOE configuration control identifiers and that the identifiers identify the current version of the TOE that reflects changes to the certified TOE;
- c) the developer has reported the configuration control identifiers for the Evaluation Technical Report, the certified TOE, and the Certification Report for the certified TOE;
- d) the developer has reported the configuration control identifiers for the version of the Security Target related to the certified TOE; and
- e) the developer has reported the identity of the developer.

4.2.1.2 Description of the change(s)

29. The certifier verifies that:

- a) the developer has reported the changes to the product and that the identified changes are with regard to the product associated with the certified TOE; and
- b) the developer has reported the changes to the development environment and that the identified changes are with regard to the development environment of the certified TOE.

4.2.1.3 Affected developer evidence

30. The certifier verifies that:

- a) for each change, the developer has reported the list of affected items of the developer evidence; and
- b) for each change to the product associated with the certified TOE or to the development environment of the certified TOE, any item of the developer evidence that needs to be modified in order to address the developer action elements has been identified.

4.2.1.4 Description of the developer evidence modifications

31. The certifier verifies that:
- a) the developer has described the required modifications to the affected items of the developer evidence and that for each affected item of the developer evidence, the modifications required to address the corresponding content and presentation of evidence elements have been briefly described; and
 - b) for EAL 4 certified products, the developer has described changes to the source code in terms of whether or not the subset of implementation representation viewed during evaluation has been modified. In cases where the subset has been subject to modifications the developer has identified whether or not any code that implements an SFR has been modified.

4.2.1.5 Conclusions

32. The certifier verifies that:
- a) for each change the developer has reported whether the impact on assurance is considered minor or major and that for each change, the developer has provided supporting rationale for the reported impact; and
 - b) the developer has reported if the overall impact is considered minor or major and that the developer has included a supporting rationale, taking the culmination of changes into consideration.
33. In addition to verifying that the developer has provided supporting rationale for the reported impact of each change, the certifier will independently assess the impact of each change, applying the guidance contained in chapter 3 of [AC: CCRA], together with other guidance that may be made available to CSE through its participation on committees such as the CCRA Scheme Directors or CCRA Executive Subcommittee.

4.2.1.6 Annex: Updated developer evidence

34. The certifier verifies that the developer has reported for each updated item of developer evidence the following information:
- a) the title; and
 - b) the unique reference (e.g., issue date and version number).

4.2.2 Certifier analysis of affected developer evidence

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

4.2.3 Establishing and communicating the verdict

36. The certifier informs the developer in writing of the results of the submission analysis. There are four possible verdicts:
 - 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 (see Section 4.3 – 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 remedy the shortcoming. When all changes are assessed as minor and all affected developer evidence has been updated, the maintained TOE qualifies for assurance maintenance. The process then enters into the conclusion stage (see Section 4.3 – Conclusion stage);
 - c) one or more sections of the Impact Analysis Report contain inadequate detail. In this case, the developer is required to remedy the shortcoming, which may in turn 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. When all changes are assessed as minor and all affected developer evidence has been updated, the maintained TOE qualifies for assurance maintenance. The process then enters into the conclusion stage (see Section 4.3 – Conclusion stage);
or
 - d) one or more changes are assessed as major, and re-evaluation is required. Reference is made to [AC: CCRA] section 2.4.2 for an explanation of the next steps in the process.

4.3 Conclusion stage

37. The certifier uses the Impact Analysis Report as the basis for producing a Maintenance Addendum that contains a Maintenance Report. The Maintenance Report is provided to the developer for review prior to finalization. The Head of the CB is the final authority for the content of Maintenance Reports.

Technical Oversight for Assurance Continuity of a certified TOE

38. Additional activities include updating the Canadian Certified Products List with the Maintenance Addendum, and notifying clients and other interested parties; however such activities are outside the scope of this document.

4.3.1 Maintenance Addendum

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

- a) a unique identifier for the most recent version of the maintained TOE;
- b) date of maintenance completion;
- c) unique identifiers for all previous maintained TOEs that are based on the certified TOE;
- d) the unique reference for the certified TOE;
- e) the Security Target associated with the maintained TOE (note that if the only change to the Security Target is to the version of the TOE then the Security Target for the certified TOE may be referenced instead); and
- f) the Maintenance Report.

4.3.2 Maintenance Report

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

41. The Maintenance Report contains the following information, taken from the Impact Analysis Report, and sanitized as appropriate to remove or paraphrase proprietary technical information:

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

42. The Maintenance Report also contains a reference to the Certification Report for the certified TOE.

5 Confidentiality of reports

43. This section outlines the responsibilities of the developer and the certifier to ensure that sensitive information is not disclosed to unauthorized parties.

5.1 Impact Analysis Report

44. The Impact Analysis Report is produced by the developer and may contain developer-sensitive information. It is the responsibility of the developer to clearly indicate the level of sensitivity of the information contained therein, through appropriate markings.
45. The Impact Analysis Report is not considered to be a public document. Both the developer and certifier shall safeguard the Impact Analysis Report from disclosure to unauthorized parties. The certifier may receive requests from other parties that desire access to the Impact Analysis Report. In such cases, the certifier will first seek permission from the developer who has a claim to sensitive information in the Impact Analysis Report, and will only release the Impact Analysis Report in cases where permission has been granted. If permission cannot be granted, then the certifier may elect, in some cases, to work with the developer to produce a sanitized Impact Analysis Report.

Annex A – Trademarks

CCS Logo: This mark distinguishes the CCS from other CC evaluation schemes. It should be used by the developer to mark deliverables to the CB that are related to Assurance Continuity. It is also used by certifiers to mark deliverables that are output from the CB.



CC Certificate Logo: This mark confirms that a CC evaluation is certified as having been performed in conformance with the [CCRA]. No party to an evaluation shall use this mark, except evaluation sponsors who are issued a certificate from the CCS, or other authorities who are participants of the [CCRA]

