National Information Assurance Partnership /Common Criteria Evaluation and Validation Scheme

Publication #6

Assurance Continuity: Guidance for Maintenance and Re-evaluation

12 September 2016
Version 3.0

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

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme
9800 Savage Road, Suite 6940
Fort George G. Meade, MD 20755-6940
E-mail: niap@niap-ccevs.org
http://www.niap-ccevs.org/

Amendment record

Version	Date	Description
2.0	8 September 2008	Initial release
3.0	July 2016	Updated to reflect current evaluation paradigm

(Page intentionally left blank)

Table of Contents

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS), hereafter referred to as The National Information Assurance Partnership (NIAP), Common Criteria Scheme, or Scheme, 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 to international standards. NIAP oversees the evaluations of IT products performed by Common Criteria Testing Laboratories (CCTLs) against the *Common Criteria for Information Technology Security Evaluation* (CC).

The principal participants in the NIAP program are the:

a) **Sponsor/Developer**: The Sponsor may be a product developer, a value-added reseller of an IT security-enabled product, or another party that wishes to have a product evaluated. The sponsor requests that a Common Criteria Testing Laboratory (CCTL) conduct a security evaluation of an IT product.

b) **Common Criteria Testing Laboratory (CCTL)**: The CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by NIAP to perform security evaluations against the *Common Criteria for Information Technology Security Evaluation* (CC) using the Assurance Activities defined in the Protection Profile, and where appropriate the procedures defined in the *Common Methodology for Information Technology Security Evaluation* (CEM).

c) **National Information Assurance Partnership (NIAP**): NIAP is the U.S. government organization established by NIST and NSA 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

This document defines the NIAP approach to maintenance and re-evaluation activities, which together are termed Assurance Continuity. *Assurance Continuity: CCRA Requirements version 2.1 released June 2012* was used as the basis for defining the NIAP assurance continuity process. It describes the minimum set of requirements for the maintenance and re-evaluation of CC validated products and is intended to provide sponsors/developers 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 NIAP publications that describe how the Scheme operates. Copies of NIAP-related publications and information are available through the NIAP web site: https://www.niap-ccevs.org/Documents_and_Guidance/guidance_docs.cfm.

This document 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.
- 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.

2 Technical Concepts

2.1 Purpose of Assurance Continuity

Assurance Continuity enables developers to provide assured products to the IT consumer community in a timely and efficient manner.

Assurance Continuity recognizes that as changes are made to a validated TOE or its environment, evaluation work previously performed does not need to be repeated entirely. Assurance Continuity defines an approach to minimizing redundancy in IT Security evaluations.

Note: Assurance Continuity submissions must be submitted to NIAP at least 30 days prior to the Assurance Maintenance Date of the original evaluation for the validated TOE (see Section 2.4.6).

2.2 Terminology

The following terms are used throughout this document:

a) *Validated TOE:* the version of the TOE previously evaluated and for which a certificate has been issued.

b) *Changed TOE:* a version differing from the validated TOE that may include:

- 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).

c) *Maintained TOE:* a changed TOE that has undergone the Assurance 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) *Maintenance Addendum:* a notation on the Product Compliant List (PCL), serving as an addendum to the certificate for a validated TOE. The Maintenance Addendum lists the maintained version(s) of the TOE. There is no issuance of an updated certificate.

e) *Updated Security Target (ST):* an updated implementation-dependent statement of security needs for a specific identified TOE. The updated ST is generated by the developer who is requesting a Maintenance Addendum.

f) *Impact Analysis Report (IAR):* a report that records the analysis of the impact of changes to the validated TOE. The IAR is generated by the developer who is requesting an addition to the Maintenance Addendum.

g) *Assurance Continuity Maintenance Report (ACMR):* a publicly available report, considered to be an addendum to the Validation Report, describing all changes made to the validated

TOE that have been accepted under the Maintenance process.

h) *Assurance Baseline:* the culmination of activities performed by both the evaluator and developer resulting in a validated TOE, recorded or submitted as evidence.

i) *Developer Evidence:* all items made available to the evaluators in support of an evaluation of a TOE.

j) *Assurance Maintenance:* the process of recognizing a set of one or more changes made to a validated TOE since its original evaluation.

k) *Re-evaluation:* 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 should attempt to reuse results from a previous evaluation.

l) *Sunset:* status of a PP when it is no longer used for product evaluations and is listed on the Archived Protection Profile List.

2.3 Assumptions

This document was written with the following assumptions:

a) NIAP has an appropriate level of trust in the developer and in any developer-supplied evidence.

b) For maintenance under the CCRA, a developer can only submit for Assurance Continuity to the same Scheme under which the original evaluation was conducted.

c) The updated product complies with all NIAP 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 does not need to be repeated in all circumstances. The Assurance Continuity paradigm recognizes previous applicable evaluation work for both the maintenance and re-evaluation process.

Maintenance refers to the process, undertaken by a developer, in updating the product and documentation for a changed 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 because the changes to the validated TOE did not adversely affect the Assurance Baseline.

It is important to note the Maintenance process is not intended to provide assurance that the original validated TOE is resistant 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 effect of TOE changes on the Assurance Baseline. However, all

publicly known vulnerabilities, as of the date of the release of the updated version, must be mitigated before the developer submits a changed TOE through the Maintenance process since it is assumed that adversaries can easily exploit any such vulnerability[1].

Figure 1 shows the Assurance Continuity process flow. The starting point for both the Maintenance and Re-evaluation processes is when a change is made to the validated TOE (Figure 1, 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.

[1] See NIAP/CCEVS Policy #17, "Effects of Vulnerabilities in Evaluated Products."

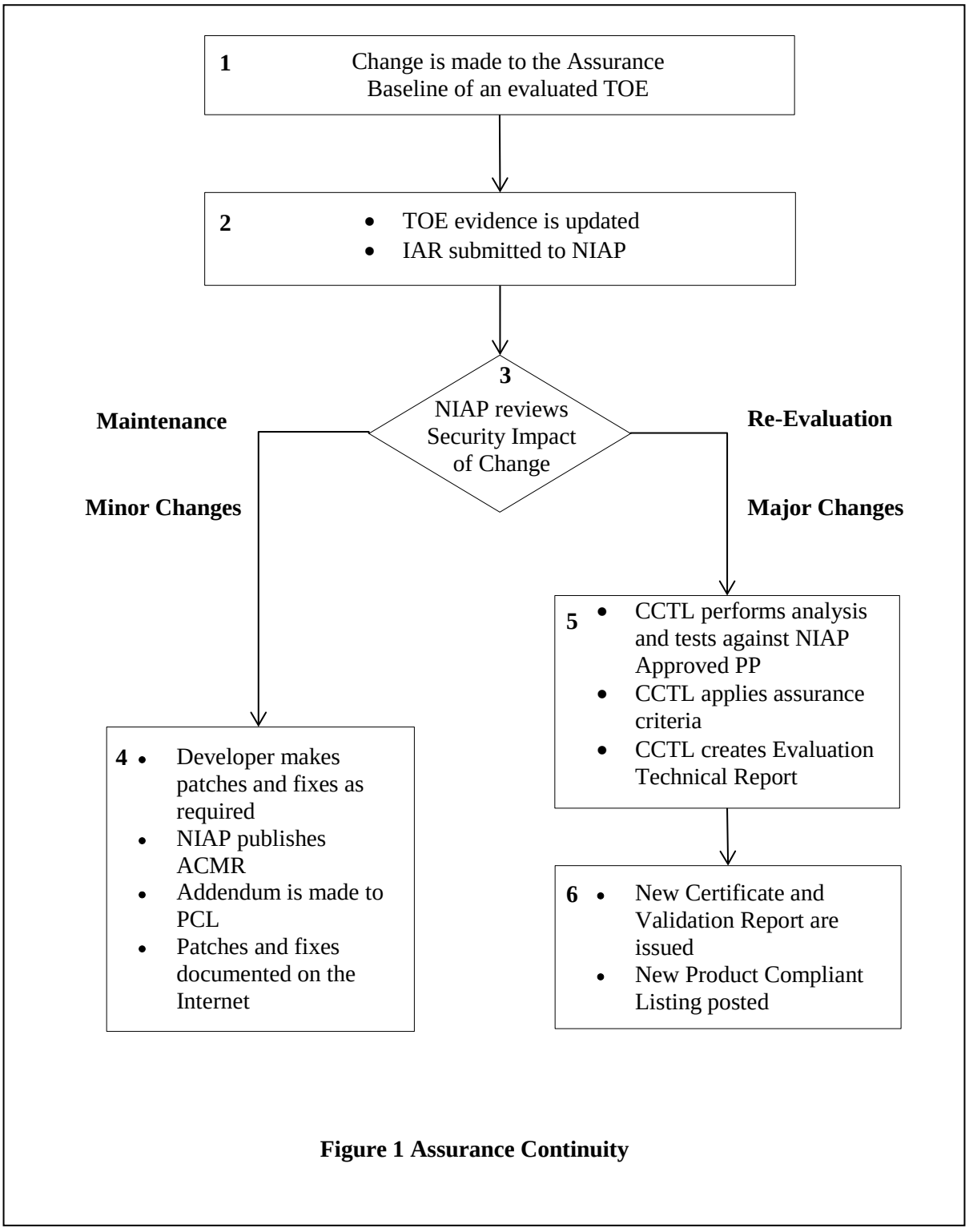

Figure 1 Assurance Continuity

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 (Figure 1, box 2). This includes an analysis of the evaluation evidence reflecting the change. The developer (or CCTL) must submit an IAR for the product at least 30 days prior to the Assurance Maintenance Date. NIAP uses the IAR to determine the impact (Figure 1, box 3) the changes have on the

Assurance Baseline.

The NIAP review process may include consultation with the developer and/or the CCTL that generated the IAR in order to ensure the recorded analysis is complete and the IAR meets all requirements for the content and presentation, resulting in a complete and consistent IAR (see Chapter 5), to the satisfaction of NIAP. The IAR review is conducted in accordance with this document and with any relevant guidance issued by NIAP.

2.4.1 IAR Submission Review Process

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

a) The **Submission Review** stage, during which NIAP reviews the developer's submission for completeness;

b) The **Submission Analysis** stage, during which NIAP analyzes the developer's maintenance claim; and

c) The **Conclusion** stage, during which NIAP produces the Assurance Continuity Maintenance Report (ACMR) and a Maintenance Addendum if the impact of changes are minor, or determines that the impact of changes are major and the product would need re-evaluation.

2.4.1.1 IAR Submission Review Stage

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

a) NIAP informs the developer that the submission package contains all the required deliverables and NIAP will proceed to the Submission Analysis stage. NIAP also provides an estimated timeframe for the Analysis stage.

(Or)

b) NIAP informs the developer that the submission is incomplete, identifies the missing elements, and may recommend the developer contact a CCTL or CC consultant for assistance in producing an updated Assurance Continuity submission.

2.4.1.2 IAR Submission Analysis Stage

NIAP examines the changes described in the IAR to determine their impact upon the assurance of the validated TOE with the following possible results:

a) The developer has provided sufficient supporting rationale describing the impact of each change.

b) The impact of each change has a minor or major impact on assurance.

c) The overall culmination of changes has security impacts that are minor or major.

d) All publicly-known security vulnerabilities applicable to releases prior to the changed TOE have been mitigated in the changed TOE.

NIAP may also selectively sample the affected developer evidence to verify the required updates have been applied. 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 sections of the IAR have been updated, the maintained TOE qualifies for Assurance Maintenance. The process then enters into the Conclusion stage.

c) One or more sections of the IAR contain inadequate detail. In this case, the developer is required to provide the additional details, which may require that the developer perform additional impact analysis, resulting in a significant rewrite and re-submission of the IAR. Once all affected sections of the IAR have been updated, the maintained TOE qualifies for Assurance Maintenance. The process then enters into the Conclusion stage.

d) One or more changes are assessed as major, and Re-evaluation is required.

2.4.1.3 IAR Submission Conclusion stage

There are two possible outcomes from the IAR review:

1. NIAP determines that the impact of changes on the TOE is **MINOR**, and the Maintenance process will be followed. See Section 3.1 for more details.

2. NIAP determines that the impact of the changes on the TOE is **MAJOR**, and re-evaluation is needed. See Section 3.2.

Once the review is complete, NIAP will inform the developer, in writing, of the outcome and will record the underlying rationale for their decisions in accordance with their quality assurance processes.

2.4.2 Maintenance Process

Maintenance, under Assurance Continuity, allows for minor changes or patches to a validated TOE, and the resulting TOE version recognized as maintaining the same level of assurance as the validated TOE.

When NIAP determines the change has a minor impact (Figure 1, box 4), then an ACMR is produced from the IAR, and an addendum to the Product Compliant List (PCL) is created. The ACMR is made publicly available where it will serve as an addendum to the Validation Report of the original validated TOE. The maintained TOE will then serve as the baseline against which any future changes will be compared.

2.4.2.1 Process Description

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

certificate apply to all versions of the TOE published in the Maintenance Addendum.

The developer must ensure the following documents are available to NIAP in order to begin the Assurance Maintenance process:

a) Security Target for the changed TOE (with tracked changes)

b) Impact Analysis Report (IAR)

IARs will be accepted for a validated product up to 30 days prior to the Assurance Maintenance Date; after that date, no IARs will be accepted for the product. IARs will be reviewed by NIAP and the product will remain on the PCL until the Assurance Maintenance review is completed. A successful Assurance Maintenance activity must be completed or the product will be moved from the PCL to the Archived Product Compliant List (APCL) after the Assurance Maintenance Date.

2.4.2.2 Assurance Continuity Maintenance Report (ACMR)

The information contained in the ACMR is a subset of the IAR content that may be sanitized when reproduced in the ACMR by removing or paraphrasing proprietary technical information. The ACMR may also summarize information in the IAR with respect to the regression testing of the product and the publicly-disclosed vulnerabilities that have been mitigated in the product. The following sections of the IAR should be included in the ACMR:

a) Introduction

b) Summary description of changes[2]

c) Affected developer evidence

The ACMR includes NIAP concurrence/non-concurrence of the overall assessment of the totality of changes as major or minor, and the rationale for that position. If NIAP concurred that the totality of changes was minor and Assurance Maintenance was permitted, then the ACMR will also include:

a) An assessment of the regression testing performed and an assessment of whether the Assurance Activities remain satisfied.

b) A confirmation that all vulnerabilities publicly-disclosed prior to the changed TOE have been mitigated.

The ACMR also contains a reference to the Validation Report**.** NIAP is the final authority for the content of the ACMR.

2.4.2.3 Maintenance Addendum

The Maintenance Addendum to the certificate for a validated TOE includes the following information:

[2] The description of the changes is at a high- and non-proprietary summary level.

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.

e) The unique reference for the ACMR.

The Maintenance Addendum is published to the PCL.

2.4.3 Re-evaluation Process

Re-evaluation, under Assurance Continuity, is necessary when changes to a validated TOE have been determined to have a major assurance impact to the Assurance Baseline (Figure 1, box 5). Re-evaluation is performed by an independent CCTL, against a NIAP-approved PP in accordance with all current NIAP policies, including re-use of previous evaluation results to the maximum extent possible to minimize duplication of effort.

Upon successful completion of re-evaluation, NIAP issues a new certificate and Validation Report, and the product is posted to the PCL (Figure 1, box 6). This new validated TOE becomes the basis for any future Assurance Continuity activities.

2.4.4 Maintenance Against a Sunset PP

NIAP determines if the product is eligible for Assurance Maintenance against a sunset PP. This determination is based upon how long the product has been listed on the PCL. NIAP will not update the Assurance Maintenance Date for any products with sunset PPs.

2.4.5 Bug Fixes and Security Patches

User installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; and with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration, thus, an IAR is not required.

2.4.6 Assurance Maintenance Date

Each product on the NIAP PCL will be assigned an Assurance Maintenance Date. Assurance Maintenance Dates will typically be two years after completion of the evaluation, but may vary depending on the technology. The Assurance Maintenance Date will only be updated for products complying with a current NIAP-approved PP. The product will be given an Assurance Maintenance Date no longer than one year after successful completion of Maintenance.

2.5 Oversight for Assurance Continuity of a Validated TOE

Normally, there are three parties that participate in a CC evaluation: (1) Developer (usually the Sponsor), (2) CCTL, and (3) NIAP. This section 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.

2.5.1Developer

The developer of the validated TOE is responsible for:

a) Producing the changed TOE.

b) Regression testing of the changed TOE.

c) Providing an argument that the regression testing was sufficient to address the testing Assurance Activities for the SFRs/SARs affected by the changes.

d) Updating all evidence (including Administrative Guidance) that is affected by changes to the validated TOE.

e) Performing an impact analysis of the changes to the validated TOE, and documenting the results in an Impact Analysis Report.

f) Ensuring that all publicly-disclosed vulnerabilities for versions prior to the updated release version have been mitigated in the changed TOE.

g) Providing NIAP with a complete Assurance Continuity submission.

2.5.2 CCTL

Under the Assurance Continuity process, NIAP may interact directly with the developer, possibly requiring 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.

2.5.3 NIAP

NIAP is responsible for:

a) Ensuring the Impact Analysis Report sufficiently documents the changes to the TOE, the impact of those changes to the validated TOE, and that all results are substantiated.

b) Determining whether changes to the validated TOE are major or minor.

c) Confirming that all publicly-disclosed vulnerabilities in releases prior to the changed TOE have been mitigated in the changed TOE.

d) Documenting the findings arising from the review and analysis of the Assurance Continuity submission.

e) If changes are deemed minor, producing an Assurance Continuity Maintenance Report (ACMR) and a Maintenance Addendum consistent with the results documented in the Impact Analysis Report (IAR).

3 Characterization of Changes

NIAP examines the changes described in the IAR in order to determine their impact upon the assurance of the validated TOE.

- A *minor* change has an impact that is sufficiently minimal to not affect the assurance to the extent that the product needs to be re-evaluated (Note: The developer is expected to have tested the changes as part of their standard regression testing).

- A *major* change has an impact that is substantial enough that it does affect the overall assurance and would consequently warrant *independent* re-application of the evaluator activities.

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. It is possible that a widespread change could have little or no impact upon the overall assurance of the TOE, while a small change to the TOE could greatly impact the assurance of the TOE. NIAP is primarily concerned with changes that affect the overall assurance of the TOE.

Because there is no concrete method to identify whether the security impact of a change is major or minor, the following sections offer a general guideline on the differences between major and minor changes.

3.1 Typical Minor Changes

Minor changes typically consist of changes to the TOE that do not affect any assurance claims about the TOE. In addition to those found in *Assurance Continuity: CCRA Requirements version 2.1 released June 2012*, examples of minor changes that can be addressed under Maintenance are:

- **Claiming compliance to an updated PP.** Although making changes in order to claim compliance to an updated PP is probably major, it is possible that no changes to the TOE, the ST front-matter, or the claimed requirements will occur. If the PP and ST have been developed simultaneously, mere addition of the PP compliance claim – by itself – would be considered minor. This simultaneous development often happens but the ST evaluation is completed before the PP is finalized. In this case, the PP must be reviewed to determine if there are significant changes in the new Assurance Activities; such changes may be sufficient to require re-evaluation by an independent CCTL as opposed to a claim of test equivalence by the developer, and thus would make the overall change major.

3.2 Typical Major Changes

Major changes typically consist of changes to the claims about the TOE. In addition to those found in *Assurance Continuity: CCRA Requirements version 2.1 released June 2012*, examples of major changes that would require re-evaluation include:

- **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, may constitute a major change.

- **Changes to the TOE boundary.** Examples include the following:

- Adding a new security function or mechanism that results in a claim of a new optional Security Functional Requirement (SFR) or new SFR iteration from the PP.

- Changes to a security function or mechanism that requires changes in the assignment or selection of an existing SFR, and may require new selection-based SFRs.

- 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 each have minor impact alone, the aggregated collection of minor changes could have a major security impact overall, therefore the combination of these changes would require re-evaluation.

- **Addition of PP compliance claims.** Claiming compliance to a new PP requires adding claimed assurance and/or functional requirements, redefining the assumptions or threat statements, or changing the TOE boundary to include portions necessary to fulfill all of the new PP's requirements, and adding new Assurance Activities. Such changes would have to be assessed under re-evaluation.

- **Migration to new criteria.** The CC is updated through both major and minor reissuances. A minor revision occurs when text changes are made, as defined in Requests for Interpretation or change proposals, and are reflected as a minor version number change (e.g., from version 2.1 to version 2.3). Major reissue occurs when substantial rewrites have occurred and are reflected as 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 the new version within the scope of Maintenance; a re-evaluation will be required.

  If the CCRA signatories adopt a new version of the CC, an associated migration timetable establishes deadlines when evaluations can no longer use the previous version of the Common Criteria. This timetable also includes a date when Maintenance activities can no longer be made against the older criteria. All NIAP evaluations are required to adhere to these deadlines.

3.3 Changes Requiring Additional Analysis

Changes that are not clearly major or minor (as defined above) must be decided on a case-by-case basis. The description of these changes in the IAR must contain sufficient explanatory text to provide a basis to determine whether the change is major or minor. These include, but are not limited to:

- Modifying refinements in the original set of claimed CC components.

- Adhering to international interpretations and NIAP Technical Decisions (NIAP and the other Schemes will determine which interpretations are considered major or minor).

- Bug fixes. It is difficult to predict the extent to which a bug fix may change the validated TOE or have an effect upon the assurance of the validated TOE.

- Equivalency claims. The similarities and differences between the validated TOE and the changed TOE must be identified in order to define the evaluation activities required for product updates. This includes both system software and platform hardware equivalency justifications.

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).

c) Evidence of regression testing of the change as part of normal life-cycle regression testing.

d) List of publicly-disclosed flaws for the product (as might be found in the National Vulnerability Database).

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.

Note: Any additions to the TOE must 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, the developer is responsible to confirm that the Assurance Activities and associated verdicts for modified developer evidence can still be met. Once the impact of the change on the developer evidence is identified, the developer can then determine the security impact 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) relevant to the product associated with the validated TOE.

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

Note: 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 developer evidence needs to be updated. This step should be conducted systematically, considering each Assurance Activity (AA) included in the PP for the validated TOE, the effect of the change on the AA component, and the evidence provided for the component. The following list can be used to facilitate such an approach.

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

a) Does it meet all applicable NIAP Policies?

b) Has it affected the Security Target, particularly the TSS?

c) Has it affected the reference for the TOE (and how)?

d) Has it affected the list of configuration items for the TOE?

e) Has it affected any of the TSF abstraction levels called out in the PP, such as the functional specification?

f) Has it affected the Guidance documentation?

g) Is the change likely to affect the result of an Assurance Activity test?

h) Has it affected the analysis of guidance documentation, or (if required) the vulnerability analysis?

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

a) Does it meet all applicable NIAP policies?

b) Has it affected the Security Target?

c) Has it affected any visible the configuration management documentation?

d) If ALC_DEL is included, has it affected the delivery procedures?

e) Has it affected the procedures necessary for the secure installation, generation, and start-up of the TOE?

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

Note: 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 [GUI] for the changed TOE, to be delivered in the same manner used for the TOE, will not have an adverse impact on *delivery* requirements). 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 AAs and any elements for content and presentation of evidence.[3] It is sufficient to collect these changes required for developer evidence before actually implementing those changes.

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 – Review Any Regression Testing

The developer is assumed to have performed regression testing to commercial standards (e.g., not specifically for CC evaluation) as part of approving changes implemented. If the changes covered by the IAR relate to any SFR/SAR in the PP, the changes should be reviewed for the testing portion of the Assurance Activity for the SFR/SAR. The developer regression test(s) should then be reviewed and an argument provided detailing how those tests sufficiently address the Assurance Activity testing.

Step 6 – Conclusion

Determine the overall impact of the identified changes on the assurance of the validated TOE and determine whether they have minor or major impact.

See Chapter 3 for a discussion on the characterization of changes.

Step 7 – Report

The analysis performed and findings are captured in the IAR (See Chapter 5). This is reviewed by NIAP for concurrence.

4.4 Output

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

a) Impact Analysis Report (IAR).

b) Updated developer evidence.

[3] Typically, the CEM is only applied for the ASE work units.

5 Impact Analysis Report (IAR)

This chapter describes the minimum content of the IAR. The contents of the IAR are portrayed in Figure 2; 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.

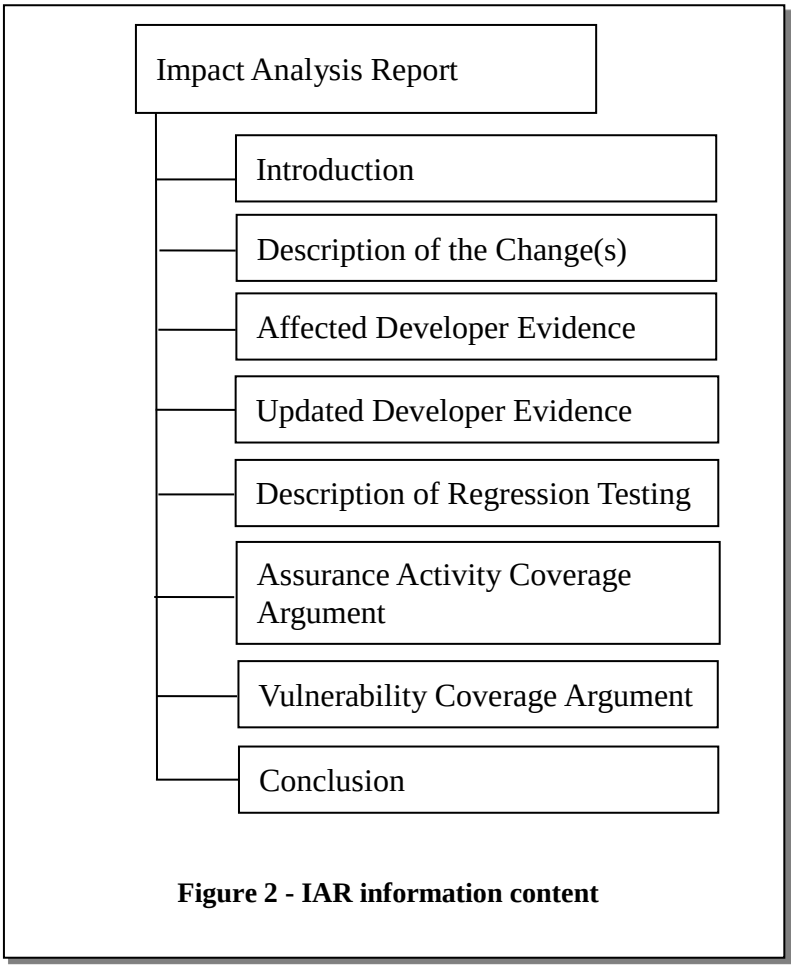

Figure 2 - IAR information content

5.1 Introduction

The developer ***shall report***:

- The IAR configuration control identifiers that contain information identifying the IAR (e.g., name, date and version number).
- The current TOE configuration control identifiers that identify the current version of the TOE reflecting changes to the validated TOE.
- The configuration control identifiers for the ETR, VR, and validated TOE, which are required to identify the Assurance Baseline and its associated documentation as well as any other changes possibly made to this Baseline.

- The configuration control identifiers for the version of the ST related to the validated TOE.

- The identity of the developer, which 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 content (e.g., related to the confidentiality of the document).

5.2 Description of the Change(s)

The developer ***shall report***:

- The changes to the product associated with the validated TOE.

- The changes to the development environment of the validated TOE.

- Whether the impact on assurance is considered minor or major and a supporting rationale for the reported impact, for each change or group of changes. (The checklist in Annex D can be used to ensure all areas that will be evaluated are included in the IAR.)

5.3 Affected Developer Evidence

For each change to the product associated with the validated TOE or to the development environment of the validated TOE, the developer ***shall report*** the list of the affected developer evidence items that need to be modified in order to address Assurance Activities or, for any SARs using CEM work units, the developer action elements.

The developer ***shall briefly describe*** the required modifications to each of the affected developer evidence items and the modifications required to address the corresponding Assurance Activities or, for any SARs using CEM work units, the content and presentation of evidence elements.

Note: This item may be included in the previous section.

5.4 Updated Developer Evidence

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

- The title.
- The unique reference (e.g., issue date and version number).

Only those changed items of evidence 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.

5.5 Description of Regression Testing

The developer ***shall describe*** the regression testing performed, to ensure the product still performed correctly after the described changes.

Note: This description *does not* need to be at the level of *each* individual change, but can be addressed in a summary paragraph.

5.6 Assurance Activity Coverage Argument

The developer ***shall present*** a convincing argument as to why regression testing sufficiently addressed the Assurance Activities for any changes related to an SFR or SAR.

5.7 Vulnerability Coverage Argument

The developer ***shall present*** a statement that all publicly-disclosed cybersecurity vulnerabilities applicable to versions of the TOE prior to the changed TOE have been mitigated.

5.8 Conclusions

The developer ***shall report*** whether the assurance impact is considered minor or major, and provide a supporting rationale, taking the totality of changes into consideration.

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.

Current versions of the CC/CEM, Common Criteria for Information Technology Security Evaluation and Assurance Continuity.

Current versions of the NIST Handbook 150, *NVLAP Procedures and General Requirements* and *NVLAP Common Criteria Testing*.

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

ISO/IEC 17065:2012 — General Requirements for Bodies Operating Product Certification Systems, 1996

Annex B: Acronyms

ACMR	Assurance Continuity Maintenance Report
ALC	Assurance Life-Cycle Support
APCL	Archived Product Compliant List
AGD	Assurance Guidance Documents
ASE	Assurance Security Target Evaluation
ATE	Assurance Tests
AVA	Assurance Vulnerability Assessment
CC	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
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IAR	Impact Analysis Report
ISO	International Organization for Standardization
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Accreditation Program
OS	Operating System
PCL	Product Compliant List
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
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.

Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security: An arrangement in which the Parties (e.g., 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.

Assurance Continuity Maintenance Process: A program within the Common Criteria Scheme that allows a sponsor/developer 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. Note: A new Common Criteria certificate is not awarded after successful completion of this process.

Assurance Maintenance: The process of verifying and documenting that the total set of 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.

Assurance Continuity Maintenance Report (ACMR): A publicly available report that describes all changes made to the validated TOE which has 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 NIAP which confirms that an IT product has successfully completed evaluation by an accredited CCTL against a NIAP-approved Protection Profile 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): An IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP to conduct Common Criteria-based evaluations.

Common Evaluation Methodology (CEM): Common Methodology for Information Technology Security Evaluation, the title of a technical document that 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 (ETR): A report giving the details of the findings of an evaluation, submitted by the CCTL to the NIAP as the principal basis for the validation report.

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

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

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

National Information Assurance Partnership (NIAP): The partnership that includes 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 NVLAP and NSA is responsible for the CCEVS.

National Institute of Standards and Technology (NIST): A federal technology agency that works with industry to develop and apply technology, measurements, and standards.

National Voluntary Laboratory Accreditation Program (NVLAP): The U.S. accreditation authority for CCTLs operating within the NIAP CCEVS. NVLAP is a part of the National Institute of Standards and Technology (NIST).

Product Compliant List (PCL): A publicly available listing maintained by the NIAP Scheme of every IT product/system that has been issued a Common Criteria certificate by the NIAP.

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 TOE, used as a baseline for evaluation under the Common Criteria. The ST 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, which will be evaluated.

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

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

Annex D: Checklist for IAR Author

<table>
<tr><td colspan="2">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. New or changed interfaces also required design analysis.</td></tr>
<tr><td>[ ] New TSF Interfaces
[ ] Changed TSF Interfaces
[ ] No changes to TSF Interfaces</td><td>Describe:</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>[ ] Faster hardware
[ ] New components
[ ] New OS
[ ] No hardware changes</td><td>Describe:</td></tr>
<tr><td colspan="2">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.</td></tr>
<tr><td>[ ] SFR changes
[ ] No SFR changes</td><td>Describe:</td></tr>
<tr><td colspan="2">New Security Functions. New security functions, given exact compliance, are typically minor. However, new functions may result in the incorporation of optional SFRs from the PP to which compliance is claimed would constitute a major change.</td></tr>
<tr><td>[ ] New security features
[ ] No new security features</td><td>Describe:</td></tr>
<tr><td colspan="2">Assumptions and Objectives. Changes to assumptions and objectives may have an impact on exact compliance. either create the need for new SFRs, or create contradictions with existing SFRs. If such changes occur, they should be examined for such effects.</td></tr>
<tr><td>[ ] Changes to Assumptions and Objectives
[ ] No changes to assumptions and objectives</td><td>Describe:</td></tr>
<tr><td colspan="2">Assurance Documents. There should be changes to assurance documents. 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. Depending on the SARs included in the PP to which compliance is claimed, there may also be updates to vulnerability assessments to capture new vulnerabilities.</td></tr>
</table>

[ ] AGD changes [ ] ATE changes [ ] AVA changes [ ] ALC changes [ ] ADV_FSP changes [ ] ASE changes [ ] No new assurance evidence	Describe:
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.	
[ ] New non-security features [ ] No new non-security features	Describe:
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.	
[ ] Security-relevant fixes [ ] Non-security-relevant fixes [ ] No fixes	Describe:
TOE Environment. Changes to the IT operational environment typically are not significant, as long as they are acknowledged in the ST and do not violate assumptions. A large change (e.g., to a significantly different underlying operating system) may require retesting to ensure proper integration.	
Conclusions: [ ] **Clear maintenance action**. Only ST updates required. [ ] **Minor maintenance action**. Retesting required, but nothing more. [ ] **Reevaluation required**. Reuse of evidence is possible. [ ] **Evaluation required**. Evidence cannot be reused.	