

IC3S

**Assurance Continuity Guidance for
Maintenance and Re-evaluation of CC
Certification under IC3S
(STQC/CC/D10)
Issue : 04**



CC Certification Body, STQC Directorate,
Indian Common Criteria Certification Scheme (IC3S),
MeitY, Government of India
INDIA

	<h1>Indian CC Certification Scheme</h1>	
	Issue : 04	
	Date : 25-05-2021	
		Page : 2 of 27

Table of Contents

0.1	Approval and Issue.....	4
0.2	Amendment Record	6
1.0	Introduction	7
1.1	Purpose of the document	7
1.2	Organization and scope	7
2.0	Reference	8
3.0	Assurance Continuity framework	8
3.1	Purpose.....	8
3.2	Terminology	9
3.3	Assumption.....	10
3.4	Roles and responsibility	10
3.4.1.	Developer/ Sponsor	10
3.4.2.	CCTL	11
3.4.3.	The Certification Body (CB).....	11
4.0	Assurance Continuity Process	12
4.1	Process overview	12
4.2	Process steps	14
4.3	Maintenance	15
4.4	Re-evaluation.....	16
4.5	Characterization of changes	18
4.5.1.	Typical minor changes	18
4.5.2.	Typical major changes	20
4.6	Performing Impact Analysis.....	20
5.0	Annexure:	22
A1.	Impact Analysis Report (IAR) format.....	22
A2.	Checklist for IAR author.....	25

 <p>STQC ॥ गुणोत्कर्षं समृद्धिः ॥</p>	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
		Page : 3 of 27

 STQC ॥ गुणोत्कर्षं समृद्धिः ॥	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
		Page : 4 of 27

0.1 Approval and Issue

This document is the property of Indian Common Criteria Certification Scheme (IC3S) and should not be reproduced in part or full without the written consent.

Reviewed by : Management Representative

Approved by : Head, CC Scheme

Note:

- Management Representative is responsible for issue and distribution of this document including amendments.
- Holder of this copy is responsible for incorporation of all the amendments and currency of the document.

 <p>STQC ॥ गुणोत्कर्षं समृद्धिः ॥</p>	<h2>Indian CC Certification Scheme</h2>	
		Issue : 04
		Date : 25-05-2021
		Page : 5 of 27

	<h1>Indian CC Certification Scheme</h1>	
	Issue : 04	
	Date : 25-05-2021	
Page : 7 of 27		

--	--	--	--

1.0 Introduction

Assurance continuity is the process by which changes to a previously-certified IT Products is assessed to determine whether assurance certificate can be maintained through impact assessment of the changes rather than going through detailed and costly re-evaluation. This document describes an accepted baseline approach to assurance maintenance and re-evaluation activities under the Indian Common Criteria Certification Scheme (IC3S).

1.1 Purpose of the document

The purpose of this document is to define the approach of Indian Common Criteria Certification Scheme (IC3S), for maintenance and re-evaluation activities (which together are termed ‘Assurance Continuity’) for the previously certified products under this scheme. It describes minimum set of requirements for Assurance Continuity of CC certified products and is intended to provide developer/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 publications of Indian Common Criteria Certification Scheme (will be identified as CB, now onwards) that describes how the scheme operates. It consists of four chapters and supporting annexure. Chapter 1 provides a general description of maintenance and re-evaluation, chapter 2 describes the references, chapter 3 describes the assurance continuity framework, under which this activity is supposed to operate, chapter 4 describes the process as a whole and the Annexure to this document contains the outlines of the Impact Analysis Report (IAR) and the Checklist for IAR authors. This document complements or references other CB publications and documents used in the operation of Indian Common Criteria Certification Scheme.

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
		Page : 8 of 27

2.0 Reference

STQC/CC/D01	: CC Scheme Organization, Management and operations
STQC/CC/DO2	: Quality Manual of the Certification Body
[CC Part 1]	: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model
[CC Part 2]	: Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements
[CC Part 3]	: Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements
[CEM]	: Common Methodology for Information Technology Security Evaluation,
[CCIMB-2004-02-009]	: Assurance Continuity: CCRA Requirements

3.0 Assurance Continuity framework

3.1 Purpose

The Assurance Continuity framework of CB enables the developers to develop CC Certified 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 works have been performed; the TOE meets all the defined assurance requirements, and the CB has confidence that the IT product or system meets its security objectives.

This Assurance Continuity Framework recognizes that it is not always necessary to repeat all the previously carried out evaluation works, in the event of changes are made to already certified TOE or its operational environment.

Assurance Continuity framework defines an approach to minimize the redundancies in evaluation effort and creates a basis of determination that whether additional evaluator actions need to be re-performed.

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 9 of 27	

It is important to note that the date of receipt of the application for assurance continuity by CB, must be within one year of completion of the original certification of the TOE.

3.2 Terminology

The following terms are used in this framework:

The 'Certified TOE' refers to the version of the TOE that has been evaluated and for which a certificate has been issued.

The 'Changed TOE' refers to a version of the TOE that is different from the certified TOE; for example:

- a new release of the product in which the TOE is a subset of functionality.
- the certified TOE with patches applied to correct discovered(after previous evaluation) bugs /security vulnerabilities.
- the same version of the certified TOE, but in a new operational environment (e.g. on a different hardware or software platform) as reflected in a new Security Target.

The 'Maintained TOE' refers to a changed TOE that has undergone through the maintenance process, as defined in this document and to which the certificate for the previously certified TOE also applies. This signifies that assurance gained in the previously certified TOE also applies to the maintained TOE.

The Maintenance Addendum refers to a notation on the Certified Products List that serves as an addendum to the certificate/certification report for a certified TOE. The Maintenance Addendum lists the maintained versions of the TOE.

The Impact Analysis Report (IAR) refers to a report which records the analysis of the impact of changes to the certified TOE. The IAR is generated by the developer who is requesting a Maintenance Addendum.

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 10 of 27	

The Maintenance Report refers to a publicly available report that describes all the changes made to the certified TOE which have been accepted under the Assurance Continuity Program

The Assurance baseline refers to the culmination of activities performed by both the evaluator and developer resulting in a certified TOE, recorded or submitted as evidence and measurable by change to that evidence.

Re-evaluation refers to the process of recognizing that changes made to a certified TOE require additional 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.

Evaluation work outputs refer to the evaluation work sheets and observation reports associated with an evaluation project.

3.3 Assumption

For maintenance of assurance certification under the CCRA, a developer can only submit an IAR to the same scheme under which the original evaluation was conducted

3.4 Roles and responsibility

There are three stake holders; those participate in a CC evaluation: Developer / Sponsor, CCTL, and CB. The roles & responsibilities are summarized as below.

3.4.1. Developer/ Sponsor

The developer of the certified TOE is responsible for:

- producing the updated TOE;
- regression testing of the updated TOE;
- updating all evaluation evidence that is affected by changes to the certified TOE;
- performing an impact analysis of the changes to the certified TOE, and documenting the results in an Impact Analysis Report; and

	<h2 style="color: blue;">Indian CC Certification Scheme</h2>	
		Issue : 04
		Date : 25-05-2021
	Page : 11 of 27	

- providing the CB with a complete Assurance Continuity submission.

3.4.2. CCTL

Under the Assurance Continuity process, the CB interacts directly with the developer, and thus there may be no explicit role for the CCTL. However, the CB may choose to avail the services of a CCTL while analyzing IAR.

CCTLs or CC consultants providing Assurance Continuity assistance are considered to be acting as agents on behalf of the developer and should not be associated with actual evaluation.

3.4.3. The Certification Body (CB)

The CB is responsible for:

- Ensuring that sufficient documentation towards the changes to the TOE is available in the Impact Analysis Report
- Analysis of the results of impact of those changes to the certified TOE are properly substantiated
- Confirming whether changes to the certified TOE are **major** or **minor**;
- Producing a Maintenance Report and a Maintenance Addendum that is consistent with the results documented in the Impact Analysis, in case the changes are categorized as **minor**.
- Guidance to concern CCTL for limited evaluation of the changed TOE, in case the changes are categorized as **major**
- Validation of work outputs of CCTL, in case of re-evaluation applying the principle of CC.
- Listing of re-evaluated TOE

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
		Page : 12 of 27

4.0 Assurance Continuity Process

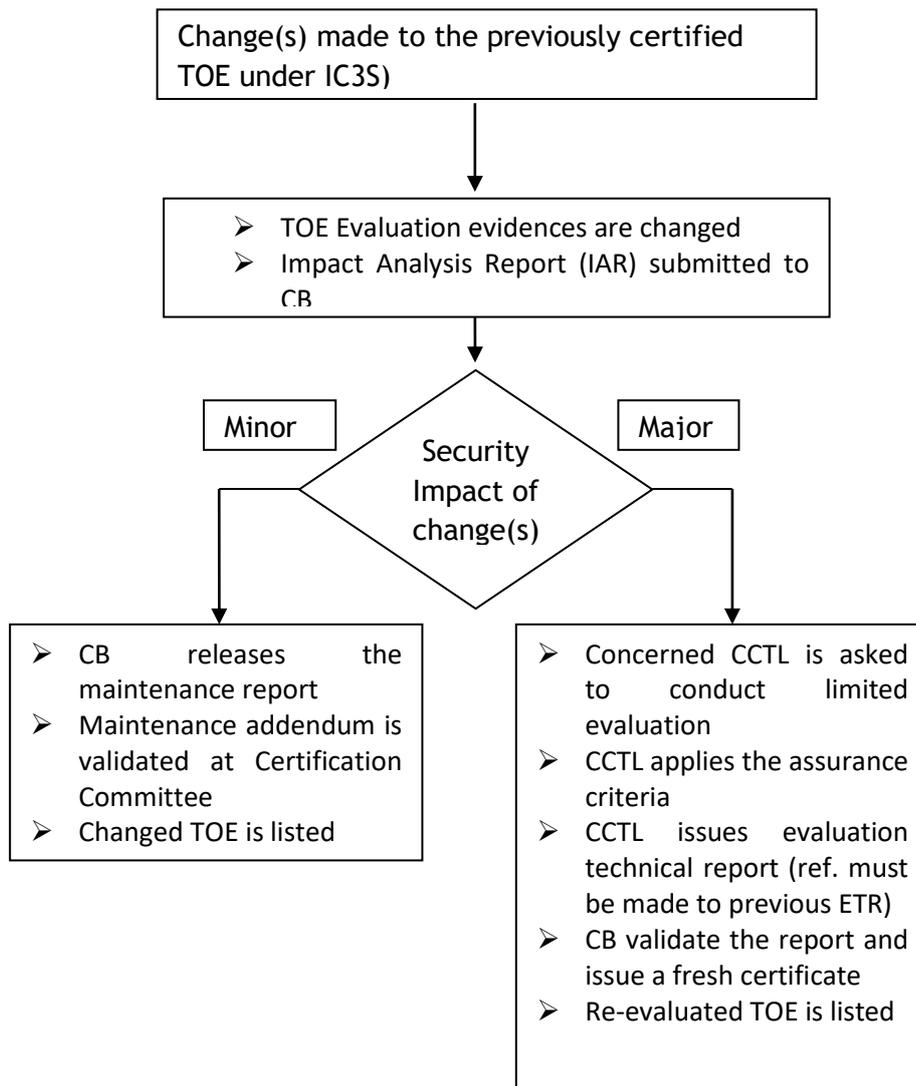
4.1 Process overview

Maintenance of assurance of a previously certified TOE deals with the changes of the TOE those are not resulted out of the change(s) in the assurance baseline of the TOE but the result of upgraded version of the TOE as its natural process on improvement. Maintenance of assurance is not intended to provide assurance regarding resilience of the TOE to new vulnerabilities /attacks discovered since issuance of certificate. Assurance of the certified TOE in respect of its resistance to new attacks can only be drawn from the process of re-evaluation.

Re-evaluation of a previously certified TOE is necessary when the developer is unable to demonstrate that the changes in the certified TOE do not have any impact on the assurance baseline.

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 13 of 27	

Figure below shows the primary paths through assurance continuity.



	<h1 style="color: blue;">Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 14 of 27	

4.2 Process steps

Step1: Both the maintenance and re-evaluation processes have an equivalent starting point; when change(s) is made to the already certified TOE under Indian Certification Scheme. This change(s) might be a patch(s) designed to correct a discovered flaw, an enhancement to feature(s), the addition of a new feature(s), clarification in the guidance documentations, or any other changes to the certified TOE.

Step 2: At this step of assurance continuity, an analysis of the evaluation evidence that would have to be updated to reflect the change and the regression testing is performed on the TOE to ensure that the change(s) works (e.g. all previous security tests need to be re-run). The output of the analysis of the evaluation evidences and regression testing form the basis of IAR. Impact Analysis Report is prepared by the TOE developer and the same is submitted to CB for review. CB analyzes the IAR through the validator, who was originally involved in the evaluation of the TOE. Outcome of this step is a decision whether the change(s) leads to 'Major' or 'Minor' impact on the assurance baseline of the certified TOE. Following section of this document indicates the how the change(s) will be characterized.

Step3 – option 1: If the CB agrees that the change has a minor impact, then a Maintenance Report is produced from the IAR, and an addendum to the Certified Products List is created. The Maintenance Report is made publicly available where it will serve as an addendum to the Certification Report of the originally certified TOE.

Step3 – option 2: If the CB finds that the change has a major impact, then the changed TOE must undergo re-evaluation. This evaluation makes maximum use of previously generated evidences, as well as the IAR. The outcome of this step results into a new Certified Product with a new Certification Report and a new Certificate. This new validated TOE will then serve as the baseline against which any future changes will be compared.

	<h1 style="color: blue;">Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 15 of 27	

4.3 Maintenance

The purpose of Maintenance, under Assurance Continuity, is to allow for minor changes (those that can be shown to have little or no effect on assurance baseline) to a certified TOE and to maintain the same level of assurance as the previously certified TOE, even if there is a change in TOE version.

Maintenance provides a mechanism which enables developers to analyze the effects of the change and present their findings to the CB. This means that when a change occurs, developers must conduct an analysis to confirm that the assurance baseline has not been adversely affected. This process places an obligation on the developer to maintain all previous and present evaluation evidences.

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 provisions of the certificate apply to all versions of the TOE that are listed in the Maintenance Addendum. The developer must ensure that the following inputs are available to the CB, for review.

- Security Target for the already certified TOE
- Security Target for the updated TOE (with tracked changes)
- Impact Analysis Report (IAR)

Once the CB has the required inputs, a review of the IAR and other relevant evidence will commence in order to determine the impact on the changes described in the IAR on the assurance baseline. The review process performed by the CB will likely involve the validators and/or the developer who generated the IAR. This exercise should result in a complete and consistent IAR. The IAR review is conducted in accordance with this document. There are two possible outcomes from the IAR review:

The CB determines that the impact of changes on the TOE is major and the Maintenance Addendum will not be created.

The CB determines that the impacts of changes on the TOE are minor and the Maintenance Addendum is created to show that the certificate also

	<h1 style="color: blue;">Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 16 of 27	

applies to the maintained TOE. If the impact of changes is considered minor, a **Maintenance Report** and updated **Maintenance Addendum** are published. The complete IAR is shared only between the developer and the CB. The CB will record the underlying rationale for the decisions.

Maintenance Report 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:

- Introduction
- Description of changes
- Affected developer evidences

The Maintenance Addendum serves as an addendum to the certificate/certification report (CR) for a certified TOE that lists the maintained TOEs and associated certified from which the same is derived.

4.4 Re-evaluation

If the CB finds that the changes to an already certified TOE have a major impact, on the assurance base line of that TOE, additional analysis to be performed by an independent evaluator. A re-evaluation is performed in the context of an earlier evaluation; reusing any results from that earlier applicable evaluation. This re-evaluation is as good as a new evaluation, except the previous evaluation results and evidences are re-used to the maximum extent possible. Furthermore, the re-evaluation must comply with all current CB policies. The developer may opt to move directly into re-evaluation without even creating an IAR (for example, if the changes are so substantial that the changed TOE bears only a minimal resemblance to the evaluated TOE).

The developer shall conduct a security impact analysis of the differences between the changed TOE and the evaluated TOE and document the same in IAR. This IAR will be used as the basis for identifying those parts of the changed TOE remaining unchanged from the previously-evaluated TOE. As with all evaluations, not be performed again, thereby maximizing the results of previous effort that can be re-used. The minimum components necessary

	<h2 style="color: blue;">Indian CC Certification Scheme</h2>	
		Issue : 04
		Date : 25-05-2021
		Page : 17 of 27

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

- Product and supporting documentation
- New Security Target
- Original Security Target
- Original Evaluation Technical Report
- Original Certification/Validation Report
- Original Common Criteria Certificate
- Original Evaluation Evidences
- Changed Evaluation Evidences

The concerned 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.

Thus, many of the requirements previously met during the original evaluation may still be satisfied and new evaluation work out put for these requirements will not be required.

Evaluation work outputs, which are available 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. 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 evaluation work outputs.

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

	<h2 style="color: blue;">Indian CC Certification Scheme</h2>	
	Issue : 04	
	Date : 25-05-2021	
		Page : 18 of 27

4.5 Characterization of changes

The CB examines the changes described in the Impact Analysis Report in order to determine their impact upon the assurance of the certified 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). A change deemed to be *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 the impact of change on the certified TOE and the same on the assurance of the certified 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.

4.5.1. 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 as follows:

- a. **Changes to the IT environment that do not affect the validated TOE**

	<h1 style="color: blue;">Indian CC Certification Scheme</h1>	
	Issue : 04	
	Date : 25-05-2021	
		Page : 19 of 27

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.

b. Changes to the certified TOE that do not affect the evaluation assurance evidence

For example, a change to the source code and/or hardware schematics would not have any impact upon the assurance documentation of a certified TOE for EAL 1. However, the developer would have to test the changes as part of their standard regression testing and result of the testing to be submitted along with IAR.

c. Non-security relevant changes to TOE functionality

d. Editorial changes

e. Changes to non-executable text (such as comments) in the source code

f. Changes to the development environment

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

g. Changes to the ST front-matter

Changes to the ST's identification or to the TOE identifier (e.g. product name change) would be minor. If there is any in 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.

h. Claiming compliance to a new PP

*Although making changes in order to claim compliance to a PP will likely be **major**; however, changes may be limited, to the ST front-matter, or to the claimed requirements, then such changes would be categorized as **minor**.*

	<h1 style="color: blue;">Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 20 of 27	

4.5.2. 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 are as follows:

- a) Changes to the set of claimed evaluation assurance requirements
- b) Changes to the set of claimed evaluation functional requirements**
- c) Use of procedures not assessed in the original evaluation**
 - i. *For example, delivery procedures are different from those examined for the delivery requirements.*
- d) Changes to the TOE boundary**
 - i. *For example, adding a new security function or mechanism or removing the same which leads to the changes to an already claimed SFR or contributes to a new SFR.*
- e) A set of minor changes that together have a major impact upon the security of the TOE**
 - a. Addition of PP compliance claims**

Adding a PP compliance claim will likely involve adding claimed evaluation 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.

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. Major reissues result from drastic rewriting and are denoted by a new version number. 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.

4.6 Performing Impact Analysis

Security categorization of the TOE may be used as a tool to help assess if a change is within the scope of maintenance. Security categorization may

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 21 of 27	

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.

Steps in performing the impact analysis :

Step 1 - Identify Validated/certified TOE

- the developer evidence provided for the certified/validated TOE (to establish assurance baseline)

Step 2 - Identify and describe change(s)

- Changes related to the product associated with the certified/validated TOE.
- Changes to the development environment relevant to the certified/validated TOE.

Step 3 - Determine impacted developer evidence

- The impacts on all the developer evidence should be considered, based on the change description (both TOE related and as well related to TOE environment)

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 necessary to collect the changes required to developer evidences 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. 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

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
		Page : 22 of 27

terms of providing the test scripts including the individual test steps are not required.

Step 5 – Conclusion

Determination of the overall impact of the identified changes on the assurance of the certified/validated TOE and making the conclusion as a **minor** or **major** impact.

Step 6 – Report

The analysis performed and findings are captured in the Impact Analysis Report. This is reviewed by CB for concurrence.

5.0 Annexure:

A1. Impact Analysis Report (IAR) format

The minimum contents of the IAR are as below; 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.

- **Introduction**

In this section of IAR, the developer will report about the configuration control identifiers for the IAR, current TOE, certified TOE, ST of the certified TOE, ETR, and Certification report. 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.

[IAR configuration control identifiers contain information that identifies the IAR (e.g. name, date and version number). The TOE configuration control identifiers identify the current version of the TOE that reflects changes to the validated TOE.]

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 23 of 27	

This section will also contain, 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.

- **Description of the changes**

In this section of IAP, the developer will report

- *the identified changes to the product associated with the certified TOE*
- *the changes to the development environment and*
- *the changes are with regard to the development environment of the validated TOE*

- **Affected developer's evidences and associated changes**

In this section of IAR, the developer will report, the affected items of the developer evidences, indicating the modifications those are required to address the corresponding content and presentation of evidence elements.

- **Conclusion**

*For each change the developer will provide statement on whether the impact on assurance is considered minor or major. (The checklist in Annexure5.2 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 will report whether the overall impact is considered **minor** or **major**, along with supporting rationale (considering all changes).*

- **Annexure: updated developer evidence**

For each updated item of developer evidence the following information are required in IAR.

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

 <p>STQC ॥ गुणोत्कर्षं समृद्धिः ॥</p>	<h2>Indian CC Certification Scheme</h2>	
		Issue : 04
		Date : 25-05-2021
		Page : 24 of 27

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
	Page : 25 of 27	

A2. Checklist for IAR author

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). New or changed interfaces also required design analysis.

<i>Tick which one is applicable</i>	Description:
<input type="checkbox"/> New TSF Interfaces <input type="checkbox"/> Changed TSF Interfaces <input type="checkbox"/> No changes to TSF Interfaces	

TSF Platform (TOE Hardware): Changes to the TOE hardware may be **major** or **minor**, depending on the change. 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.

<i>Tick which one is applicable</i>	Description:
<input type="checkbox"/> Faster hardware <input type="checkbox"/> New components <input type="checkbox"/> New OS <input type="checkbox"/> No hardware changes	

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.

<i>Tick which one is applicable</i>	Description:
<input type="checkbox"/> SFR changes <input type="checkbox"/> No SFR changes	

	<h1>Indian CC Certification Scheme</h1>	
		Issue : 04
		Date : 25-05-2021
		Page : 26 of 27

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.

<i>Tick which one is applicable</i>	Description:
<input type="checkbox"/> Changes to Assumptions and Objectives <input type="checkbox"/> No changes to assumptions and objectives	

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.

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.

<i>Tick which one is applicable</i>	Description:
<input type="checkbox"/> New non-security features <input type="checkbox"/> No new non-security features	

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.

<i>Tick which one is applicable</i>	Description:
<input type="checkbox"/> Security-relevant fixes <input type="checkbox"/> Non-security-relevant fixes <input type="checkbox"/> No fixes	

	<h2 style="color: blue;">Indian CC Certification Scheme</h2>	
		Issue : 04
		Date : 25-05-2021
	Page : 27 of 27	

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

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.