Joint Interpretation Library

Assurance Continuity

Object: Define re-assessment concept for use within SOG-IS while the CCRA finalizes the update of Assurance Continuity

Version 1.0
November 2019

This page is intentionally left blank

Table of contents

Appendices

1 Introduction

This document seeks to define a temporary mutually recognizable process for re-assessment under the SOG-IS agreement until the Common Criteria Recognition Arrangement (CCRA) has finalized the update of Assurance Continuity. The approach defined in this version of 'Assurance Continuity' is only intended to set the minimum technical requirements for the mutual recognition of activities performed in relation with changes affecting a certified TOE or its environment.

This document does not preclude signatories nations from having further requirements in their implementation of Assurance Continuity. This document has been updated to correspond to Common Criteria version 3.1.

1.1 Scope

This document draws on the concepts of the CC and is designed to be used by signatory nations of the SOG-IS as the minimum set of requirements for the maintenance, re-evaluation and re-assessment of CC certified products.

1.2 Approach

This document covers the following aspects of Assurance Continuity

a) Description of technical concepts underpinning the assurance continuity paradigm including a description of the processes involved in both maintenance, re-evaluation and re-assessment.

b) Guidance on the characterisation of change, where applicable.

c) Guidance on performing impact analysis, where applicable.

d) Requirements for content and presentation of the impact analysis report, where applicable.

1.3 Contents

This document contains five chapters: this introduction (Chapter 1), the technical concepts underlying this document (Chapter 2), a discussion of the characterisation of change (Chapter 3), how to perform an impact analysis (Chapter 4), and the requirements for content and presentation of an Impact Analysis Report (Chapter 5).

2 Technical Concepts

2.1 Assurance Continuity Purpose

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

The awarding of a Common Criteria evaluation certificate signifies that all necessary evaluation work has been performed 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.

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.

2.2 Terminology

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

a) the *certified TOE* refers to the version of the TOE that has been evaluated and for which a certificate has been issued.

b) the *changed TOE* refers to a version that differs in some respect from the certified TOE; this could be, for example:

   - a new release of the TOE or of the product in which the TOE is a subset of functionality.
   - the certified TOE with patches applied to correct discovered bugs.
   - the same basic 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.

c) the *maintained TOE* refers to a changed TOE that has undergone the maintenance process and to which the certificate for the certified TOE also applies. This signifies that assurance gained in the certified TOE also applies to the maintained TOE.

d) The *reassessed TOE* refers to a previously *certified TOE* that has undergone a *re-*

assessment.

e) the *maintenance addendum* refers to a notation, such as on the listing of evaluated products, that serves as an addendum added to the certificate for a certified TOE. The maintenance addendum lists the maintained versions of the TOE. There is no implied issuance of an updated certificate.

f) 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 an addition to a maintenance addendum.

g) the *Maintenance Report* refers to a publicly available report that describes the changes made to the certified TOE which have been accepted under the maintenance process.

h) the *re-assessment report* refers to a report that identifies the version of the TOE, the list of applicable guidance and the reached AVA_VAN level. Depending on the choice of the sponsor this report may be made public.

i) 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.

j) the *developer evidence* refers to all items made available to the evaluators in support of an evaluation of a TOE.

k) *maintenance* refers to the process of recognising that a set of one or more changes made to a certified TOE (or to aspects of the *development environment*) have not adversely affected assurance in that TOE.

l) *re-evaluation* refers to the process of recognising that changes made to a certified TOE (or to other assurance measures) 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.

m) *re-assessment* refers to the processof updating the vulnerability analysis of the initially certified product, at the same level as initially requested within the security target, including when necessary the associated penetration tests. *Re-assessment* can be peformed *ad hoc* or on a periodical basis. It can be seen as a particular case of *re-evaluation* where the TOE has not changed, but where the changes in the threat environment need to be assessed to check if the TOE still reaches the same level of resistance as initially certified.

n) the *development environment* addresses all procedures relating to development, delivery, start-up and flaw remediation of the TOE. It includes all concepts covered by the ALC class, together with the AGD_PRE family.

o) A *subset evaluation* is applicable where minor changes to the TOE include changes to the development environment. A qualified CC evaluation facility identifies those assurance components that are impacted by the changes to the development environment, and re-evaluates only those assurance components in light of the changes, producing a *partial ETR.*

p) a *partial ETR* is an output from the *subset evaluation*. It is created by the qualified CC evaluation facility that performed the *subset evaluation* and provides, for the impacted assurance components, a level of detail that is commensurate with the corresponding sections of the ETR for the original certified TOE.

q) the *evaluation authority* is a body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community. When this term is used, it can mean the evaluation authority itself or another appointed party on behalf of the evaluation authority.

A product or system throughout its original evaluation is referred to as a TOE. Once the original evaluation is completed and a certificate awarded, it becomes the certified TOE. After a subsequent version of the certified TOE (changed TOE) has been added to the maintenance addendum, that version is considered to be a maintained TOE.

2.3 Assumptions

This document is written taking the following assumptions into consideration:

a) It is assumed that evaluation authorities have an appropriate level of trust in the developer and in any developer-supplied evidence.

b) It is assumed that evaluation authorities will use ‘Assurance Continuity’ as the basis for a scheme specific implementation of Assurance Continuity which may include requirements beyond those described in this document.

c) It is assumed that for maintenance, a developer can only submit an IAR to the same evaluation authority under which the original evaluation was conducted.

d) It is assumed that there exists a means to ensure consistency among evaluation authorities in the characterisation of major and minor changes.

2.4 Assurance continuity paradigm

Assurance continuity seeks to exploit the fact that as changes are made to a certified

TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. The assurance continuity paradigm therefore defines the processes for *maintenance*, *re-evaluation* and *re-assessment* such that each seeks to recognise previous evaluation work.

Maintenance refers to the process undertaken by a developer in order to have a TOE, listed in the maintenance addendum for that TOE. It must be demonstrated that the changes to the TOE, the IT environment and/or the *development environment* do not adversely affect the assurance baseline.

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

Re-assessment refers to the evaluation of a previously *certified TOE* against a changed threat environment.

It is important to note that the maintenance process is not intended to provide assurance in regard to the resistance of the TOE to new vulnerabilities or attack methods discovered since the date of the initial certificate. Such assurance can only be gained through re-evaluation or re-assessment. Maintenance only considers the effect of TOE changes on the assurance baseline; it does not consider an evolving threat environment.

Figure 2.1 and 2.2 show the primary paths through assurance continuity. Both the maintenance and re-evaluation processes have an equivalent starting point: when a change is made to the certified TOE [box 1]. This change might be a patch designed to correct a discovered flaw, an enhancement to a feature, the addition of a new feature, a clarification in the guidance documentation, or any other change to the certified TOE. For the specific case of re-assessment, no change has been made to the certified TOE but new threats or attack techniques are considered.

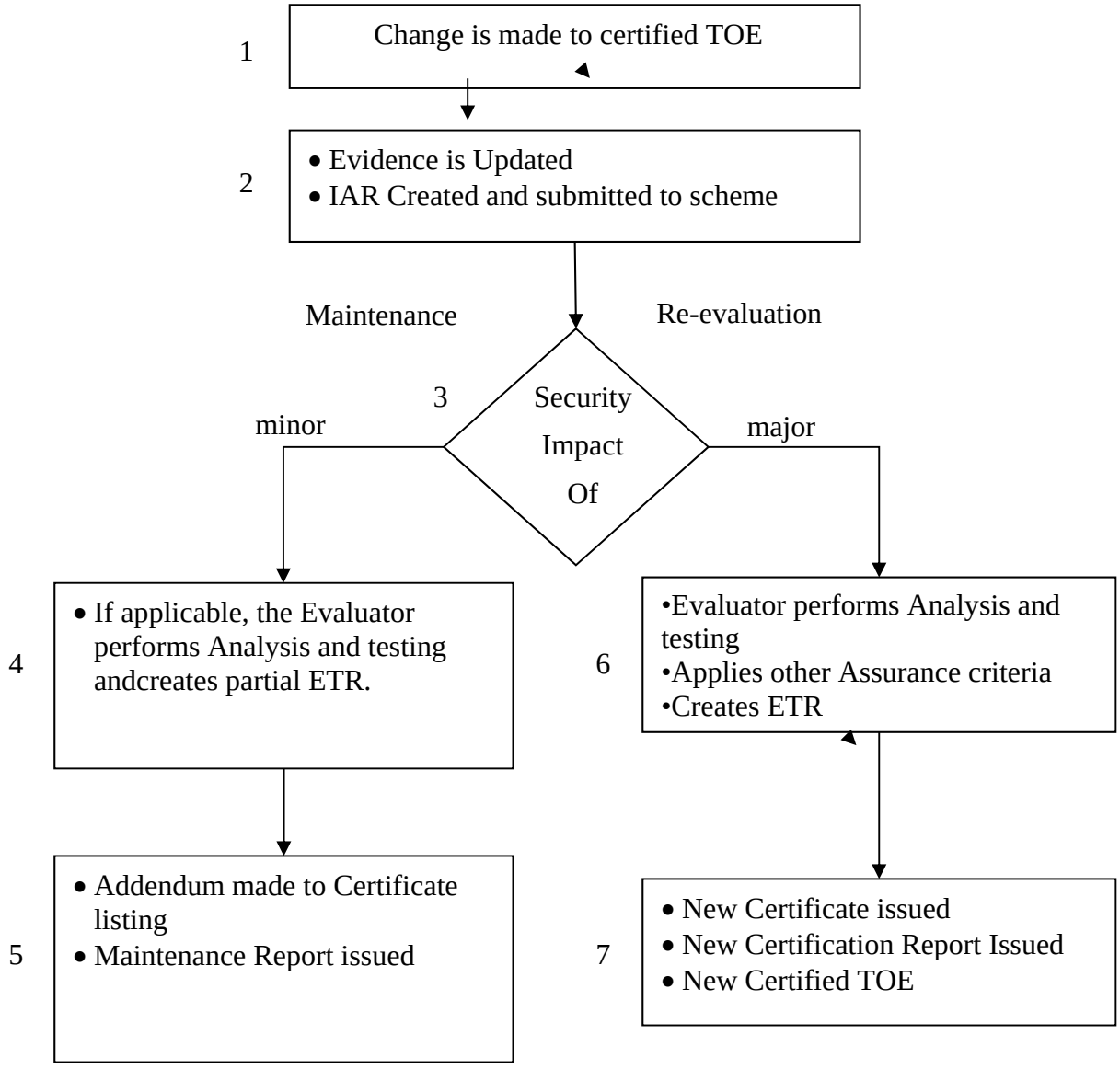


Figure 1 - Maintenance and re-evaluation

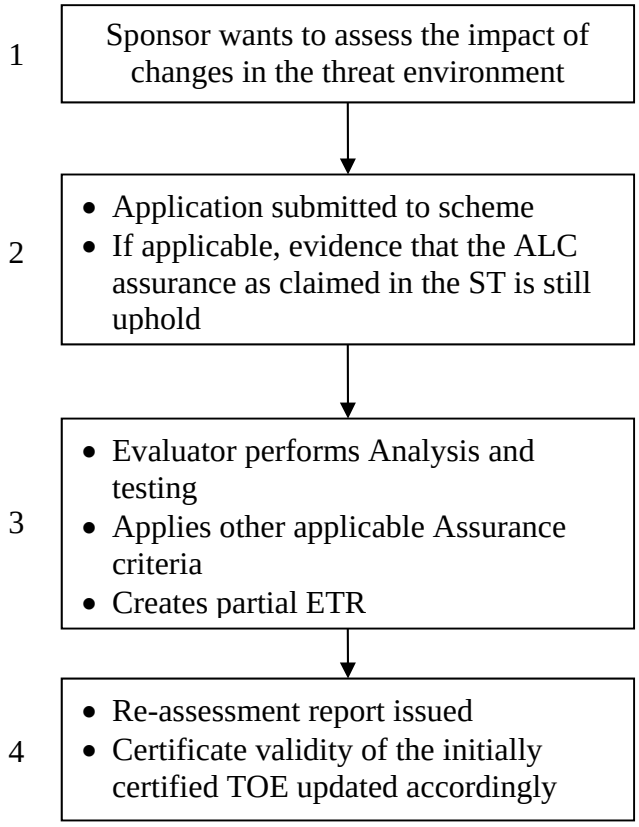
As a result of this change, a judgement needs to be made in regard to its resulting impact on assurance [box 2]. This includes an analysis of the evaluation evidence that would have to be updated to reflect the change, and regression testing of the code to be sure that it works when incorporated into the TOE. The basis for making this judgement is called impact analysis, which is performed by the TOE developer and recorded in an Impact Analysis Report (IAR); see Chapter 5 for more detail on the content of the IAR.

The evaluation authority uses the IAR[1] to determine whether [box 3] each of the changes can be included under maintenance, or whether it has a major impact on assurance and is therefore considered sufficiently substantial that it requires re-evaluation. It should be noted that an evaluation authority might use factors other than whether the changes are major or minor in determining whether maintenance or re-evaluation is to be used (e.g. elapsed time since certification).

If the evaluation authority agrees that the changes to the TOE are of minor impact, then it may be necessary (if there have been changes to the assurance measures in the *development environment*) for a qualified CC evaluation facility to [box 4] perform a subset evaluation of those assurance measures, and provide the evaluation authority with a partial ETR covering those assurance components that were affected. Once the evaluation authority is in agreement that the assurance baseline has not been adversely affected, then [box 5] an addendum to the certification listing is created, and a Maintenance Report is produced from the IAR and made publicly available where it will serve as an addendum to the certification report of the original certified TOE.

If the evaluation authority finds that the change has a major impact on the assurance baseline, then the changed TOE must undergo re-evaluation in order for it to have an associated certification. This evaluation [box 6] makes maximum use of previously generated evidence, as well as the IAR, resulting in [box 7] a new ETR and hence a new certification report; in addition, the evaluation authority issues a new certificate. This new certified TOE will then serve as the baseline against which future changes will be compared [back to box 1].

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



In the specific case where a sponsor wants to assess the impact of changes to the threat environment on a certified TOE, a re-assessment request is submitted to the evaluation authority [box 2]. No IAR is needed, but evidence that the assurance on the development environment is still uphold should be provided at this stage if available to avoid unnecessary evaluation work. The TOE then goes through evaluator analysis and testing [box 3]. Only the assurance activities impacted by the evolution of the threat environment are re-opened, namely the AVA_VAN family, and, if sufficient evidence could not be provided, the ALC class as well.

Upôn reception of the ETR from the evaluator, the Evaluation Authority issues a re-assessment report that can be made public if the sponsor wishes so. A new certificate need not be issued after a re-assessment.

2.4.1 Process Description

The Assurance Continuity processes can be defined in terms of the necessary inputs, actions and outputs that results in an update to the evaluation authority's certified products list, to reflect :

1. the assurance gained for the changed TOE, or,
2. the impact on certificate validity for the initially certified TOE.

To achieve aim 1, Assurance Continuity provides a mechanism which enables

developers to analyse the effect of changes and present their findings to an evaluation authority. This means that when a change occurs, developers must conduct relevant action items in order to determine whether the assurance baseline has been adversely affected. This process places an obligation on the developer to maintain all developer evidence (recording sufficient information in the IAR about changes to documentary evidence would be considered maintaining that evidence), conduct and record appropriate testing and confirm that previous analysis results have not been affected by changes to the TOE. Chapter 4: *Performing an Impact Analysis* further describes these types of activities. The Assurance Continuity process is described below.

In order for an evaluation authority to review the developer's analysis, and in order to begin the process, the developer must ensure that the following inputs are available to the evaluation authority (the authority will most likely already have some of these inputs):

a) Certificate for the TOE (including maintenance addendum)

b) Certification Report

c) Evaluation Technical Report

d) Security Target for the certified TOE

e) Impact Analysis Report (IAR)

Once the evaluation authority is satisfied that it has the required inputs, it will proceed with a review of the IAR and other relevant inputs in order to determine what impact the changes described in the IAR have on the assurance baseline.

The review process performed by the evaluation authority will most likely involve consultation with the developer and this consultation should result in a complete and consistent IAR. That is, the analysis recorded is complete and the IAR meets all requirements for content and presentation (see Chapter 5), to the satisfaction of the evaluation authority. The IAR review is conducted in accordance with this document and with any relevant guidance documentation that may be issued by the evaluation authority, and a key focus of this review is to determine whether the changes (to the TOE, the IT environment and/or the *development environment*) can be considered major or minor, based on their apparent impact on the assurance baseline.

There are two possible outcomes from the IAR review:

i) The evaluation authority determines that the impact of changes on the assurance baseline are considered minor and the maintenance addendum is

subsequently updated to show that the certificate also applies to the maintained TOE. Section 2.4.2 provides further detail regarding the maintenance process.

ii) The evaluation authority determines that the impact of changes on the assurance baseline are considered major and the maintenance addendum will not be updated. Such changes would need to be considered during re-evaluation. Section 2.4.3 provides further detail regarding the re-evaluation process.

Once this determination is made, the evaluation authority will inform the developer of the outcome. In either case, major or minor, the evaluation authority will record the underlying rationale for their decision in accordance with their quality assurance processes. Such information may feed into a consistency process undertaken by Common Criteria Recognition Arrangement participating nations. The Executive Subcommittee (ES), at the time of writing, was identified as the body that would undertake to administer any such consistency process.

2.4.2 Maintenance

The purpose of Assurance Continuity - Maintenance is to allow for minor changes (those that can be shown to have little or no affect on assurance) to be made to a certified TOE, the IT environment and/or the development *environment*, and have the resulting TOE version recognised as maintaining the same level of assurance as the certified TOE.

If the impact of changes to the TOE are considered to be minor, then the evaluation authority must also determine that the scope of any changes to the *development environment* do not have a follow-on effect on any assurance components outside of the *development environment*. For any changes to *development environment* assurance measures, it is necessary to have a qualified evaluation laboratory conduct a partial evaluation (see Section 2.4.2.1) of the applicable assurance components in the Security Target. Subsequent to the successful completion of any such partial evaluation, an updated maintenance addendum (see Section 2.4.2.2) and a Maintenance Report (see Section 2.4.2.3) are published on the evaluation authority's Certified Products List. The complete IAR is considered an output shared only between the developer and the evaluation authority.

Maintenance may, in general, continue for up to 2 years beyond the certification date. However, the certificate-issuing Scheme may, as circumstances warrant, either lengthen or shorten this maintenance period, based on the IT product type and the needs of the consumer.

2.4.2.1 Evaluating changes to the *development environment*

A qualified evaluation laboratory performs a partial evaluation, focussing only on those *development environment* assurance components for which the assurance measures have been modified. The evaluation laboratory conducts this evaluation in the same way that they would normally perform a CC evaluation for that functionality, and produces a partial ETR that provides sufficient evidence to the evaluation authority that the assurance baseline has been preserved, for those changes to the *development environment*.

2.4.2.2 Maintenance Addendum

The maintenance addendum serves as an addendum to the certificate for a certified TOE that lists the maintained TOEs derived from that certified TOE.

The exact form of the maintenance addendum is not specified in this document. The most likely form of the addendum will be an addition of maintained TOE identifiers to each evaluation authority's Certified Product List.

Information required in the addendum is as follows:

a) Unique TOE identifier for each maintained TOE related to the certified TOE.

b) Reference to 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 original Security Target may be referenced).

c) Reference to the Maintenance Report, which should be publicly available.

2.4.2.3 Maintenance Report

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

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

a) Introduction

b) Description of changes

c) Affected developer evidence

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

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

Evaluation authorities may wish to provide users with useful information in regard to a maintained TOE. Such information could also be included in the Maintenance Report.

2.4.3 Re-evaluation

When a change to a certified TOE has been determined to be of major impact, the implication is that a more concerted analysis, and by an independent evaluator, is required to assess the assurance of the changed TOE. A re-evaluation is performed in the context of an earlier evaluation, reusing any results from that earlier evaluation that still apply.

It is possible that the developer may opt directly for re-evaluation without ever creating an IAR (for example, if the changes are so substantial that the changed TOE bears only a minimal resemblance to the evaluated TOE). Alternatively, even with substantial changes, the developer still may have conducted a security impact analysis of the differences between the changed TOE and the evaluated TOE.

If an IAR has been provided, this would be used as the basis for identifying those parts of the changed TOE remaining unchanged from the previously-evaluated TOE. As with all evaluations, analysis that has already been performed on parts of a TOE that remain unchanged need not be performed again, thereby maximizing the amount of results of previous effort that can be re-used. To this end, the new ETR is derived from the ETR of the original TOE.

At the completion of the evaluation of the changed TOE, a new ETR is produced, along with a certification report and certificate for the changed TOE. This changed TOE becomes the updated basis for any future changes that might be made.

2.4.4 Re-assessment

When the threat environment has changed since the initial certification of a TOE, the

certificate holder may want the TOE's resistance to be re-assessed. Re-assessment is performed by the same evaluator who performed the initial evaluation, reusing all results from that earlier evaluation that still apply. Only tasks pertaining to the AVA_VAN family are reopened, as well as, when relevant, those of the ALC class for which sufficient evidence that they are still fulfilled cannot be provided.

When updating the vulnerability analysis of the product, the ITSEF may consider the following : :

- The list of potential vulnerabilities established during the initial evaluation is reused to update the vulnerability analysis. Attack methods and attack potential can evolve over time, thus the attack ratings may be changed from the initial certification. New penetration testing may also be performed to assess vulnerabilities initially considered as residual.

- New potential vulnerabilities which were not addressed during the initial certification, and associated attack methods are identified through examination of publicly available sources of information (see CEM work unit AVA_VAN.*-3) and any other evaluation evidence (see CEM work unit AVA_VAN.2-4 and higher) These new potential vulnerabilities are used to update the vulnerability analysis in accordance with the initial AVA_VAN level.

As *re-assessment* is based on the initial Security Target, no change to the security problem can be made and only new or evolved attack techniques are covered.

At the completion of the re-assessment of the TOE, a new ETR is produced, along with a re-assessment report for the reassessed TOE.

The validity of the initial certificate is then updated according to the following table :

Re-assessment results	Publication of the re-assessment report	No publication of the re-assessment report
Positive[2]	The validity of the initial certificate is extended	No change

[22] Positive here means that the TOE is re-assessed conformant to the same AVA_VAN component as initially claimed in the Security Target.

Negative	The validity of the initial certificate is not change. The AVA_VAN level reached by the re-assessed TOE shall be made public	The initial certificate is considered as no more valid and moved to the archived certificates list

When the validity of the certificate is extended, the new validity period is established in respect of the applicable rule adopted by the SOG-IS.

3 Characterisation of changes

The evaluation authority 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 be independently reapplied (although the developer is expected to have tested the changes as part of his standard regression testing) or a change to the development environment in which the change can be shown to have no follow-on effect on the other assurance measures that were in place at the time of the original evaluation. By contrast, a change deemed major has an impact that is substantial enough that it does affect the assurance (except as noted above for the development environment) and would consequently warrant independent re-application of the evaluator activities. Therefore, minor changes are addressed under maintenance, which is performed solely by the developer, while major changes are addressed under re-evaluation, which is performed by the evaluator.

It is important to note the difference between a change's impact upon the certified TOE and a change's impact upon 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 fixed method for identifying whether the security impact of a change is major or minor. The following offers a general guideline on the differences between major and minor changes, and also offers examples of exceptions.

3.1 Typical minor changes

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

- **Changes to the IT environment that do not change the certified TOE.** For example, a change to the underlying hardware (where the hardware is not part of the TOE) or to software parts of the product that are outside the TOE boundary would likely be minor if the interface remains unchanged. However if the interface also changes, then it is likely a major change.

- Changes to the Certified TOE that do not affect the assurance evidence. For example, if a TOE has been certified to EAL1, a change to the source code and/or hardware schematics would not have an impact upon the assurance documentation. Nevertheless, the developer would have tested the changes as part of the standard regression testing.

- Editorial changes (grammatical, typographical, formatting) to any of the assurance evidence. For example, editorial changes to a functional specification that provide additional clarification would probably be minor. However, if a PP were to specify *exact* compliance[3] as the degree of conformance, then even an editorial change to the ST's security objectives statements or environment description would be major.

- Changes to Development Environment. A change to the *development environment* that can be shown to have no follow-on effect on other assurance measures would typically be a minor change. An example of this would be where a developer has passed a certification that claimed ALC_CMC.2 and for whatever reason changed Configuration Management Tool. If the developer can provide, in the Impact Analysis Report, a convincing rationale that this process does not have follow-on effects on the other assurance measures that were in place originally, then this could be considered minor.

- Changes to the ST front matter. A change to the ST's identification or to the TOE identifier (e.g. product name change) would be minor. If any of the statements of Threats, OSPs, Assumptions, or Security Objectives change, without necessitating a change to the Security Requirements, these would likely be minor changes. If, however, any of the requirements statements do change, these would be major changes.

3.2 Typical major changes

Major changes typically consist of changes to the claims about the TOE and may (yet need not) result in changes to the TOE. Examples of major changes that are therefore suitable to be addressed under re-evaluation are:

- Changes to the set of claimed assurance requirements. This includes both the addition of new assurance measures and the deletion of existing assurance measures.

- Changes to the set of claimed functional requirements. This would likely change

[3] *Exact* compliance refers to the case where a PP author specifies precisely what is required; any deviation from the content and text of the PP would mean that the ST could not claim compliance. (See the ASE Update for Trial Use for more details on degrees of compliance).

the TOE boundary, which would have to be re-assessed for correctness and soundness under re-evaluation.

- **A set of minor changes that together have a major impact upon the security.** Although changes might be of minor impact in isolation, the collection of minor changes could have a major security impact. The combination of these would have to be re-evaluated.

It should be noted that a bug fix has no predictable extent of change to the certified TOE, nor a predictable effect upon the assurance of the certified TOE. Therefore, a “bug fix” might constitute either a major or minor change.

4 Performing an Impact analysis

4.1 Input

The following are inputs to the impact analysis process:

a) developer evidence associated with the Certified TOE;

b) change(s) description (probably generated from life cycle quality processes and procedures).

4.2 Preliminary work

Security categorisation 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 categorisation may be consulted to identify the influence of the change on the developer evidence provided in the assurance baseline.

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

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

4.3 Steps in performing the impact analysis

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

Step 1 - Identify Certified TOE

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

Step 2 - Identify and describe change(s)

Describe the change(s) to the product with regard to the product associated with the certified TOE.

Identify and describe the change(s) to the development environment with regard to the development environment of the certified TOE.

These changes are listed to the level of detail necessary to understand what was done, but not necessarily how it was done.

Step 3 - Determine impacted developer evidence

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

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

a) Has it affected the Security Target?

b) Has it affected the reference for the TOE?

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

d) Has it affected any of the TSF abstraction levels, that is, the functional specification, the TOE design, or the implementation representation?

e) Has it affected the architectural description (if the assurance baseline includes a component from the ADV_ARC family)?

f) Has it affected the mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design (if the assurance baseline contains a component from the ADV_TDS family), and to the implementation representation (if the assurance baseline contains a component from the ADV_IMP family)?

g) Has it affected the guidance documentation (if the assurance baseline includes a component from the AGD class)?

h) Has it affected the testing documentation, that is, the analysis of test coverage, the analysis of the depth of testing or the test documentation (if the assurance baseline includes a component from the ATE class)?

i) Has it affected the vulnerability analysis?

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

a) Has it affected the Security Target?

b) Has it affected the CM documentation?

c) Has it affected the delivery procedures (if the assurance baseline includes a component from the ALC_DEL family)?

d) Has it affected the procedures necessary for the secure acceptance of the delivered TOE, secure installation of the TOE, and secure preparation of the operational environment?

e) Has it affected the developer security procedures (if the assurance baseline includes a component from the ALC_DVS family)?

f) Has it affected the flaw remediation procedures (if the assurance baseline includes a component from the ALC_FLR family)?

g) Has it affected the life cycle model (if the assurance baseline includes a component from the ALC_LCD family)?

h) Has it affected the development tools (if the assurance baseline includes a component from the ALC_TAT family)?

i) Have there been changes to the manufacturing process (in particular for hardware components)?

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

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

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

For some developer action elements this determination may be simple (e.g. a new graphical user interface for the changed TOE, to be delivered in the same manner used for the TOE, will not have an adverse impact on ALC_DEL), while for other requirements it may be more difficult (e.g. has the TOE design for the user interface subsystem changed through the introduction of the new GUI and the effect on the material provided for ADV_TDS?

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

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

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

If the change to the TSF is “invisible” at the lowest TSF abstraction available (e.g., the lowest level of TSF decomposition is represented by the ADV_TDS.2 component, and some source code is changed during maintenance, but the changes do not require modification to the subsystems in the TOE design), then it suffices for the developer to show how the change was tested, and provide associated rationale in the IAR.

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 – Conclude

Determine the overall impact of the identified changes on the assurance of the certified TOE. Conclude: minor or major impact.

See Chapter 3 for a discussion on the characterisation of change.

4.4 Output

a) Impact Analysis Report (IAR);

b) Updated developer evidence.

5 Impact Analysis Report (IAR)

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

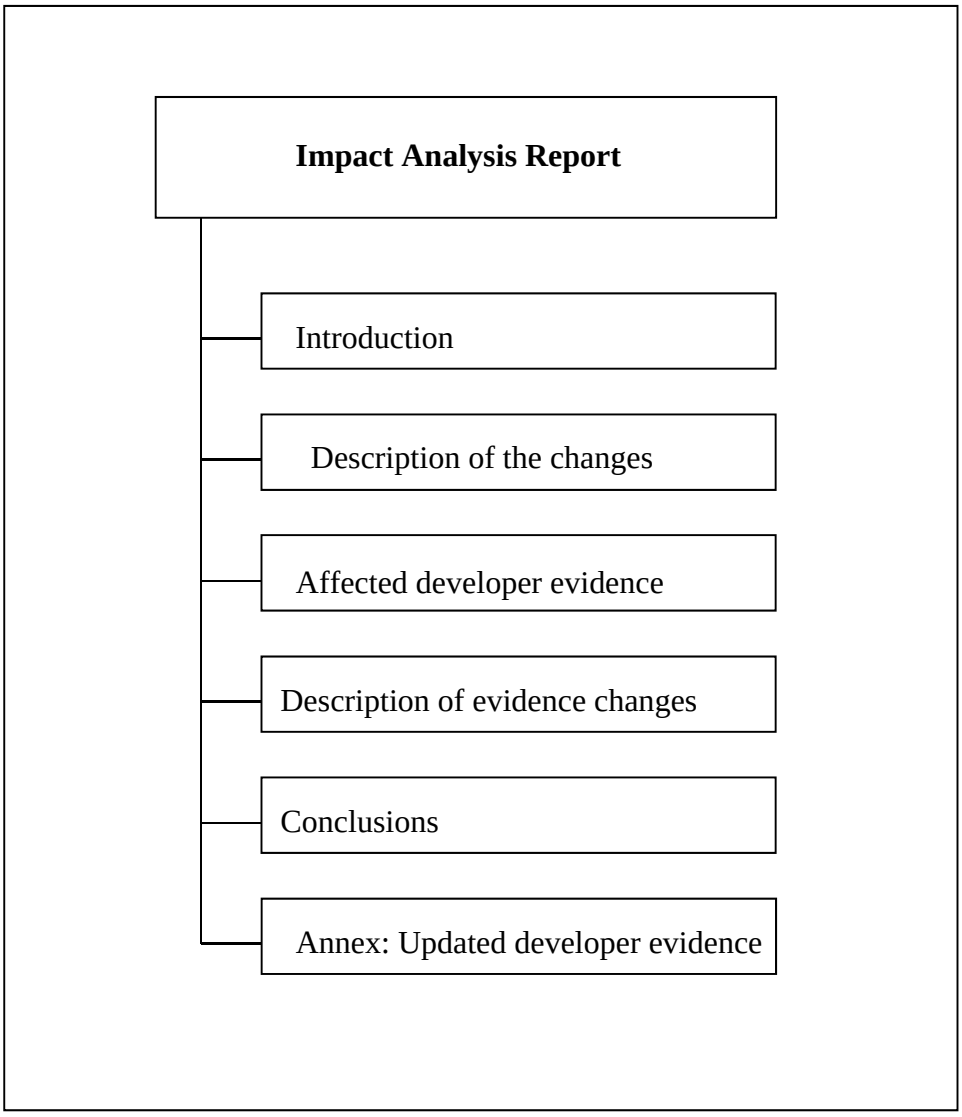


Figure 3 - IAR information content

5.1 Introduction

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

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

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

The developer ***shall report*** the configuration control identifiers for the ETR, CR, and certified TOE. *These configuration control identifiers are required to identify the assurance baseline and its associated documentation as well as any other changes that may have been made to this baseline.*

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

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

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

5.2 Description of the change(s)

The developer ***shall report*** the changes to the product. *The identified changes are with regard to the product associated with the certified TOE.*

The developer ***shall report*** the changes to the development environment. *The identified changes are with regard to the development environment of the certified TOE.*

5.3 Affected developer evidence

For each change, the developer ***shall report*** the list of affected items of the developer evidence. *For each change to the product associated with the certified TOE or to the development environment of the certified TOE, any item of the developer evidence that*

need to be modified in order to address the developer action elements shall be identified.

5.4 Description of the developer evidence modifications

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

5.5 Conclusions

For each change the developer ***shall report*** if the impact on assurance is considered minor or major. F*or each change the developer should provide a supporting rationale for the reported impact. In the event that the change is to the development environment, the rationale will show that there is no follow-on impact on other assurance measures.*

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

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

5.6 Annex: Updated developer evidence

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

- the title;

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

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