

CCIMB-2004-02-009

Assurance Continuity:

CCRA Requirements

Version 1.0

February 2004

# 1 Introduction

1 In August 1999 the Common Criteria for Information Technology Security Evaluation, Parts 1, 2 and 3, v2.1 (CC 2.1) were released along with a companion document, the Common Methodology for Information Security Evaluation, Part 2, v1.0 (CEM). The CC Recognition Arrangement (CCRA) has been established to use the CC as the basis for mutual recognition of evaluation results performed by signatory nations.

2 This document seeks to define a mutually recognisable approach to maintenance and re-evaluation activities, together termed Assurance Continuity. In defining this approach, ‘Assurance Continuity: CCRA Requirements’ seeks only to define the minimum technical requirements expected of CCRA signatory nations for conducting Assurance Continuity activities that are to be mutually recognised. This document does not preclude such nations from having further requirements in their implementation of Assurance Continuity.

## 1.1 Scope

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

## 1.2 Approach

4 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 and re-evaluation.
- b) Guidance on the characterisation of change.
- c) Guidance on performing impact analysis.
- d) Requirements for content and presentation of the impact analysis report.

## 1.3 Contents

5 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

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

7 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.

8 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

9 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 *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.

- e) 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.
- f) the *Maintenance Report* refers to a publicly available report that describes all changes made to the certified TOE which have been accepted under the maintenance process.
- g) the *assurance baseline* refers to the culmination of activities performed by both the evaluator and developer resulting in a certified TOE, recorded or submitted as evidence and measurable by change to that evidence.
- h) the *developer evidence* refers to all items made available to the evaluators in support of an evaluation of a TOE.
- i) *Maintenance* refers to the process of recognising that a set of one or more changes made to a certified TOE have not adversely affected assurance in that TOE.
- j) *Re-evaluation* refers to the process of recognising that changes made to a certified 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.
- k) 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.

10 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

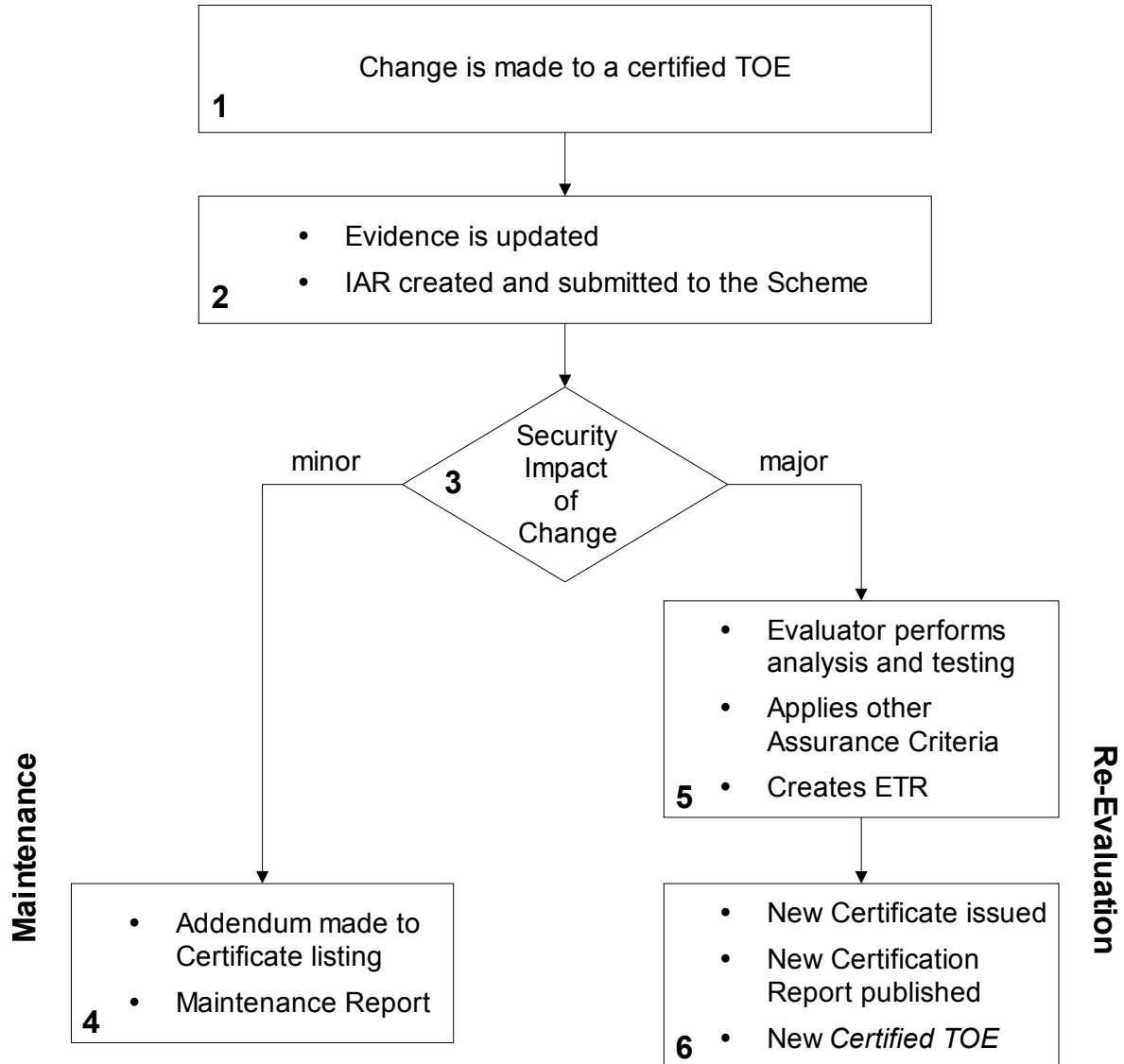
11 This document is written taking the following assumptions into consideration:

- 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: CCRA Requirements' as the basis for a scheme specific implementation of Assurance Continuity which may include requirements beyond that described in this document.

- c) It is assumed that for maintenance under the CCRA, 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

- 12 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* and *re-evaluation* such that each seeks to recognise previous evaluation work.
- 13 Maintenance refers to the process undertaken by a developer in order to have a unique TOE identifier change (e.g. version increment), resulting from a changed TOE, listed in the maintenance addendum for that TOE. It must be demonstrated that the changes to the TOE do not adversely affect the assurance baseline.
- 14 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.
- 15 It is important to note that the maintenance process is not intended to provide assurance in regard to the resistance of the TOE to new vulnerabilities or attack methods discovered since the date of the initial certificate. Such assurance can only be gained through re-evaluation. Maintenance only considers the affect of TOE changes on the assurance baseline, it does not consider an evolving threat environment.
- 16 Figure 2.1 shows the primary paths through assurance continuity. Both the maintenance and re-evaluation processes have an equivalent starting point: when a change is made to the 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.



**Figure 2.1 - Assurance Continuity**

17

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.

- 18 The evaluation authority uses the IAR<sup>1</sup> 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).
- 19 If the evaluation authority agrees that the change is of minor impact, then [box 4] 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.
- 20 If the evaluation authority finds that the change has a major impact, then the changed TOE must undergo re-evaluation in order for it to have an associated certification. This evaluation [box 5] makes maximum use of previously generated evidence, as well as the IAR, resulting in [box 6] 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 any changes will be compared [back to box 1].

#### 2.4.1 Maintenance

- 21 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 and have the resulting TOE version recognised as maintaining the same level of assurance as the certified TOE.
- 22 To achieve this aim, maintenance provides a mechanism which enables developers to analyse the affect of change and present their findings to an evaluation authority. This means that when a change occurs, developers must conduct relevant action items in order to confirm that the assurance baseline has not been adversely affected. This process places an obligation on the developer to maintain all developer evidence (recording sufficient information in the IAR about changes to documentary evidence would be considered maintaining that evidence), 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 maintenance process is described below.

##### 2.4.1.1 Process Description

- 23 The maintenance process can be defined in terms of the necessary inputs, actions and outputs that lead to a new entry to the 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.

---

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.

- 24 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)
- 25 The time relationship between the issuing of a certificate and performing an update to the maintenance addendum is undefined. That is, if a certificate is valid, there is no defined time limit for requesting an update to the maintenance addendum.
- 26 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.
- 27 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.
- 28 There are two possible outcomes from the IAR review:
- i) The evaluation authority determines that the impact of changes on the TOE are considered major and the maintenance addendum will not be updated. Such changes would need to be considered during re-evaluation.
  - ii) The evaluation authority determines that the impact of changes on the TOE are considered minor and the maintenance addendum is subsequently updated to show that the certificate also applies to the maintained TOE.
- 29 Once this determination is made, the evaluation authority will inform the developer of the outcome. If the impact of changes is considered minor, a Maintenance Report and updated maintenance addendum is published on the evaluation authority's Certified Products List. The complete IAR is considered an output shared only between the developer and the evaluation authority.



30 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.

#### 2.4.1.2 Maintenance Addendum

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

32 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.

#### 2.4.1.3 Maintenance Report

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

34 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

35 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.

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

37 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.

#### **2.4.2 Re-evaluation**

38 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.

39 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.

40 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.

41 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.

### 3 Characterisation of changes

42 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 re-applied (although the developer is expected to have tested the changes as part of his standard regression testing). By contrast, a change deemed *major* has an impact that is substantial enough that it does affect the assurance and would consequently warrant independent re-application of the evaluator activities. Therefore, minor changes are addressed under *maintenance*, which is performed solely by the developer, while major changes are addressed under *re-evaluation*, which is performed by the evaluator.

43 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.

44 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

45 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 his 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<sup>2</sup> 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 non-executable text in the source code** (such as comments) would typically be minor changes. But a change to compiler instructions would likely be a major change, as in cases when ALC\_TAT is being claimed.
- **Changes to the development environment** that have no notable effect upon assurance. For example, an update to the configuration management tool would be minor if the update did not affect the results of tracking the evolution of the TOE, or when ACM is not being claimed. However, if ACM is being claimed and an update to the configuration management tool produced entirely new results that would therefore have to be re-evaluated, then the change would be considered major.
- **Changes to the ST frontmatter.** 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

46 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 changes to the families (for example, where ADV\_HLD is the highest design abstraction claimed for the Certified TOE, and there is a desire to add a claim for ADV\_LLD) as well as a claim of a higher component within the same family. While the deletion of an assurance could arguably be considered a "minor" change, the result would require the production of a new certificate, which is done only under re-evaluation.
- **Changes to the set of claimed functional requirements.** This would likely change the TOE boundary, which would have to be re-assessed for correctness and soundness under re-evaluation.

---

2. *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).

- **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 ADO\_DEL) would constitute a major change.
- **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.

47

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

48 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

49 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.

50 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.

51 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

52 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 affect of the change on the developer evidence, the developer is then able to conclude the security affect of the change.

#### Step 1 - Identify Certified TOE

53 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)

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

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

56 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

57 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 affect 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.

58 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 (if the assurance baseline includes a component from the ACM\_CAP family)?
- c) Has it affected the list of configuration items for the TOE (if the assurance baseline includes a component from the ACM\_SCP family)?
- d) Has it affected any of the TSF abstraction levels, that is, the functional specification, the high level design, the low level design or the implementation representation (if the assurance baseline includes a component from the ADV class)?
- e) Has it affected the architectural description (if the assurance baseline includes a component from the ADV\_INT family)?
- f) Has it affected the analysis of correspondence (if the assurance baseline includes a component from the ADV\_RCR family)?
- g) Has it affected the TSP model (if the assurance baseline includes a component from the ADV\_SPM family)?
- h) Has it affected the guidance documentation (if the assurance baseline includes a component from the AGD class)?
- i) 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)?
- j) Has it affected the covert channel analysis, the analysis of guidance documentation, the vulnerability analysis (if the assurance baseline includes a component from the AVA class)?

- 59 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 (if the assurance baseline includes a component from the ACM class)?
  - c) Has it affected the delivery procedures (if the assurance baseline includes a component from the ADO\_DEL family)?
  - d) Has it affected the procedures necessary for the secure installation, generation, and start-up of the TOE (if the assurance baseline includes a component from the ADO\_IGS family)?
  - 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)?
- 60 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.
- 61 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.
- 62 Previous versions of the IAR may be used as input to this analysis.
- 63 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 ADO\_DEL.1.1D), while for other requirements it may be more difficult (e.g. has the high level design for the user interface subsystem changed through the introduction of the new GUI and the affect on the material provided for ADV\_HLD.1.1D).
- 64 The output of this step is a list of affected developer action elements.
- Step 4 - Perform required modifications to developer evidence.**
- 65 The objective of this step is to determine how should each of the affected developer evidence (identified during the previous step) 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.

66 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.

67 *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.*

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

69 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

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

71 *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)

72 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.

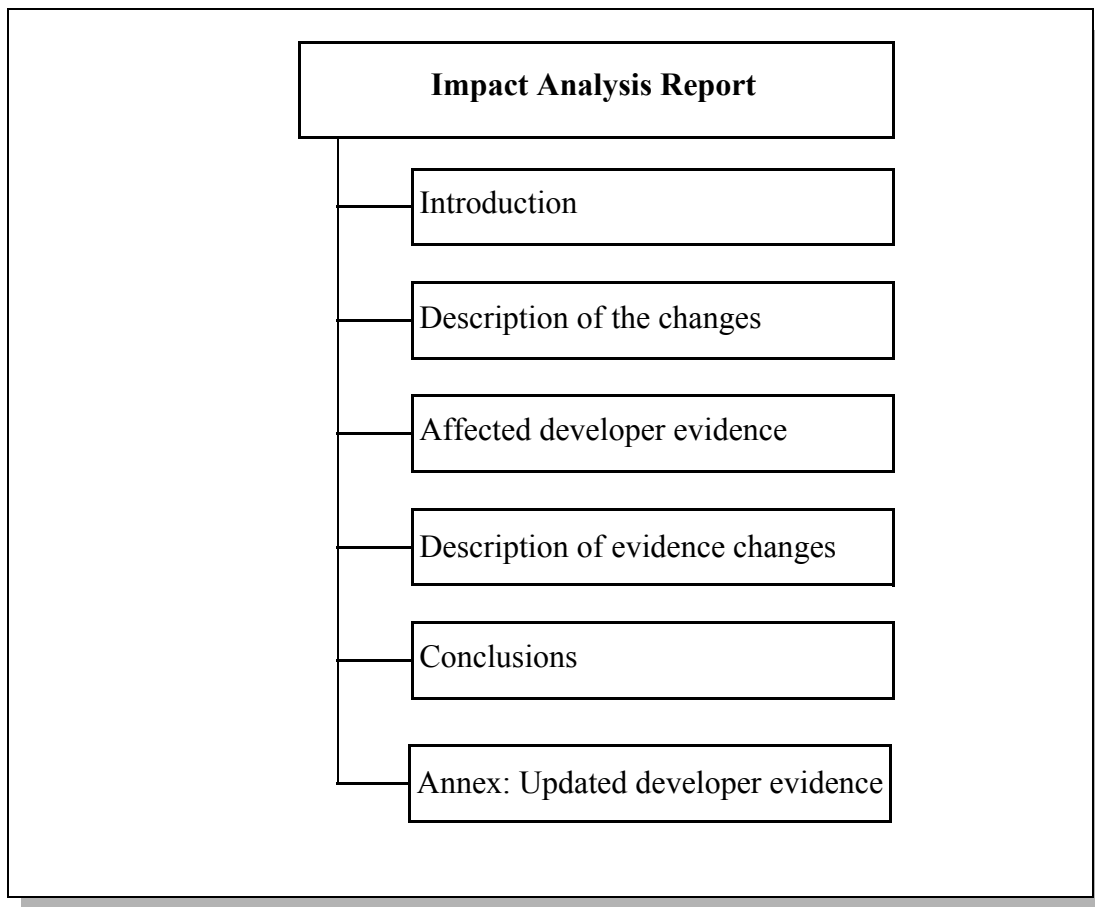


Figure 5.1 - IAR information content

### 5.1 Introduction

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

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

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

- 76 *The TOE configuration control identifiers identify the current version of the TOE that reflects changes to the certified TOE.*
- 77 The developer **shall report** the configuration control identifiers for the ETR, CR, and certified TOE.
- 78 *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.*
- 79 The developer **shall report** the configuration control identifiers for the version of the ST related to the certified TOE.
- 80 The developer **shall report** the identity of the developer.
- 81 *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.*
- 82 *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)

- 83 The developer **shall report** the changes to the product.
- 84 *The identified changes are with regard to the product associated with the certified TOE.*
- 85 The developer **shall report** the changes to the development environment.
- 86 *The identified changes are with regard to the development environment of the certified TOE.*

## 5.3 Affected developer evidence

- 87 For each change, the developer **shall report** the list of affected items of the developer evidence.
- 88 *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

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

90 *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

91 For each change the developer *shall report* if the impact on assurance is considered minor or major.

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

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

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

## 5.6 Annex: Updated developer evidence

95 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).

96 *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.*