Common Methodology for Information Technology Security Evaluation

CEM-2001/0015R

Part 2: Evaluation Methodology

Supplement: ALC_FLR - Flaw Remediation

Version 1.1

February 2002

Foreword

This document is issued by the Common Criteria sponsoring organisations to the international IT security evaluation community for use. It is a supplement to the Common Methodology for Information Technology Security Evaluation, Part 2, version 1.0 (CEM) and can therefore be considered as part of that document. The publication of this supplement does not alter the terms of the Common Criteria Recognition Arrangement but provides a basis for common methodology for evaluations containing the ALC_FLR family in the Security Target.

This version of the supplement has this updated Foreword and a small number of editorial changes. These are identified via ‘change bars’ in the left margin.

Any comments on this document should be communicated via the Request for Interpretation process defined at http://www.commoncriteria.org.

Chapter 1

Introduction

1 In August 1999 the Common Methodology for Information Technology Security Evaluation, Part 2, v1.0 (CEM) was released, describing the methodology to be used in applying the assurance components for evaluation assurance levels (EALs) 1 through 4, as defined in the Common Criteria for Information Technology Security Evaluation v2.1 (CC). However, the CEM defines no methodology for applying the rest of the assurance requirements, other than those of the APE and ASE classes.

2 This document supplements the CEM by providing a methodology for applying the CC assurance requirements of the ALC_FLR family (Flaw remediation), including interpretations CCIMB-INTERP-062 and CCIMB-INTERP-092. This supplement supercedes CCIMB-INTERP-094. While the assurance components of this family are not included in any CC Part 3 EAL, they may be incorporated into any PP and ST.

3 It is planned that, when the CEM is updated, the contents of this document will be incorporated into the new version of the CEM.

1.1 Application

4 The ALC_FLR requirements are not used in the EALs defined in the CC. Because the assurance requirements in PPs and STs need not be restricted to defined EALs, it is possible to include other assurance components, including those from the ALC_FLR family. That is, any of the ALC_FLR components may be used as part of an PP/ST in combination with any of the assurance packages in the CC.

1.2 Contents

5 This document contains four sections: this introduction to the document, technical concepts underlying this document, the methodology for components ALC_FLR.1, ALC_FLR.2, and ALC_FLR.3, and an annex containing the replacement text for the ALC_FLR family in the CC.

6 For each of these components, the associated evaluator actions are described: the objectives of the component are given, along with the inputs upon which the evaluator work units are performed. This is then followed by the evaluator actions called for by the CC evaluator action elements or implied by the CC developer action elements. Each of these CC content and presentation of evidence elements, or developer action elements, is included in italicised text, followed by the methodology work units for that element and any additional guidance. Within this supplement, the first occurrence of each work unit is presented in boldface type.

7 Work units are identified in the left margin by a symbol such as *ALC_FLR.1-2*. In this symbol, the string *ALC_FLR.1* indicates the CC component (i.e. the CEM sub-activity), and the final digit *(2)* indicates that this is the second work unit in the ALC_FLR.1 sub-activity.

8 Readers are reminded to consult the CC for additional details on the objectives and application notes associated with these requirements.

Chapter 2

Underlying technical concepts

9 This chapter contains the technical concepts upon which the remainder of this document are based. These concepts are divided into two categories, terms that are defined and application notes, all of which apply to the methodology for the components described in Chapter 3. Other terms and acronyms are those used and explained in the CC and CEM.

2.1 Terminology

10 The phrase *TOE* stands for *target of evaluation*; however, there is the connotation that a target is no longer a target once the goal it was aiming for is achieved. That is, once the evaluation of a TOE is complete, it is no longer the target for an evaluation. The CC offers no means of referring to a TOE once the evaluation has completed. The ALC_FLR requirements, by their nature of dealing with post-evaluation events, have produced a need for additional post-evaluation terms. Additionally, for the sub-activities described in this document, other terms have been used with precise meaning. The following terms are therefore defined:

11 Certified TOE - a product or system and its associated guidance that, having been a TOE (under evaluation), has completed the evaluation, its ST, certification report, and certificate having been published.

12 Release of a TOE - a product or system that is a release of a certified TOE to which changes have been applied. (Consider: the original certificate does not apply to the changed versions, regardless of the reasons for the changes.)

13 Tracking a security flaw - knowing the security flaw's current status and history (that is, where it has been along its timeline of existence).

14 TOE user - the focal point in the user organisation that is responsible for receiving and implementing fixes to security flaws. This is not necessarily an individual user (e.g. as is used in the AGD_USR requirements), but may be an organisational representative who is responsible for the handling of security flaws. The use of the term *TOE user* recognises that different organisations have different procedures for handling flaw reporting, which may be done either by each individual user or by a central administrative body.

15 TOE guidance - the administrator guidance, user guidance, flaw remediation guidance, delivery procedures, and installation, generation, and start-up procedures.

16 Security flaw - a condition that, alone or in concert with others, provides an exploitable vulnerability. TSP violations that occur not from a problem with the

hardware, software, or firmware portion of a TOE, but from a problem in the TOE guidance are also recognised as *security flaws*. Any paths of execution that result in a violation of the TSP when the product or system is used outside the intended environment would be nonexploitable and, therefore, not considered a security flaw.

2.2 Application notes

17 Remediation of security flaws is performed upon security flaws discovered after the completion of the evaluation of the TOE. (Correction of security flaws discovered before or during the evaluation is a matter for configuration management, vulnerability analysis, testing, etc.)

18 A TOE developer's responsibility for *reporting* flaws extends to those discovered in the TOE environment; the developer's responsibility for *correcting* flaws does not extend to those in the environment. For example, the developer of a trusted application would identify the underlying operating system as the IT environment. Flaws found in the application would be reported, tracked, and corrected by the developer. Flaws discovered in the operating system need only be reported by the developer (perhaps simply in terms of "Don't run this application on operating system X"). TOE users, who are informed that the operating system no longer fulfills the requirements (or meets the assumptions) levied upon the TOE environment, would then need to find another operating system meeting those requirements/assumptions until the operating system flaws are corrected by the operating system developer. This scenario underscores the importance of the knowledge of the TOE user when combining TOEs from different developers.

19 It should be noted that, in this sub-activity, the flaw remediation procedures address the developer's procedures to be followed when security flaws are found in certified TOEs and releases of TOEs, but they contain no provision to verify that such procedures are being followed; the ACM_SCP.2 and AMA_EVD.1 workunits can be used in support of this verification. Because the correction of such flaws requires the modification of the evaluated TOE, the TOE would no longer be a certified version.

20 A reported security flaw can be considered only a 'suspected' security flaw until such time that investigation determines either that it is not a security flaw (in which case it need not be tracked further), or that it is a security flaw (in which case it continues to be tracked until such time it is resolved).

Chapter 3

Flaw remediation sub-activities

3.1 Evaluation of flaw remediation (ALC_FLR.1)

3.1.1 Objectives

21 The objective of this sub-activity is to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users.

3.1.2 Input

22 The evaluation evidence for this sub-activity is:

a) the flaw remediation procedures documentation.

3.1.3 Evaluator actions

23 This sub-activity comprises one CC Part 3 evaluator action element:

a) ALC_FLR.1.1E.

3.1.3.1 Action ALC_FLR.1.1E

ALC_FLR.1.1C - *The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.*

ALC_FLR.1-1 The evaluator shall examine the flaw remediation procedures documentation to determine that it describes the procedures used to track all reported security flaws in each release of the TOE.

24 The procedures describe the actions that are taken by the developer from the time each suspected security flaw is reported to the time that it is resolved. This includes the flaw's entire timeframe, from initial detection through ascertaining the flaw is a security flaw, to resolution of the security flaw.

25 If a flaw is discovered not to be security-relevant, there is no need (for the purposes of the ALC_FLR requirements) for the flaw remediation procedures to track it further; only that there be an explanation of why the flaw is not security-relevant.

26 While these requirements do not mandate that there be a publicised means for TOE users to report security flaws, they do mandate that all security flaws that are

reported be tracked. That is, a reported security flaw cannot be ignored simply because it comes from outside the developer's organisation.

ALC_FLR.1.2C - *The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.*

ALC_FLR.1-2 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would produce a description of each security flaw in terms of its nature and effects.

27 The procedures identify the actions that are taken by the developer to describe the nature and effects of each security flaw in sufficient detail to be able to reproduce it. The description of the nature of a security flaw addresses whether it is an error in the documentation, a flaw in the design of the TSF, a flaw in the implementation of the TSF, etc. The description of the security flaw's effects identifies the portions of the TSF that are affected and how those portions are affected. For example, a security flaw in the implementation might be found that affects the identification and authentication enforced by the TSF by permitting authentication with the password 'BACKDOOR'.

ALC_FLR.1-3 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would identify the status of finding a correction to each security flaw.

28 The flaw remediation procedures identify the different stages of security flaws. This differentiation includes at least: suspected security flaws that have been reported, suspected security flaws that have been confirmed to be security flaws, and security flaws whose solutions have been implemented. It is permissible that additional stages (e.g. flaws that have been reported but not yet investigated, flaws that are under investigation, security flaws for which a solution has been found but not yet implemented) be included.

ALC_FLR.1.3C - *The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.*

ALC_FLR.1-4 The evaluator shall check the flaw remediation procedures to determine that the application of these procedures would identify the corrective action for each security flaw.

29 *Corrective action* may consist of a repair to the hardware, firmware, or software portions of the TOE, a modification of TOE guidance, or both. Corrective action that constitutes modifications to TOE guidance (e.g. details of procedural measures to be taken to obviate the security flaw) includes both those measures serving as only an interim solution (until the repair is issued) as well as those serving as a permanent solution (where it is determined that the procedural measure is the best solution).

30 If the source of the security flaw is a documentation error, the corrective action consists of an update of the affected TOE guidance. If the corrective action is a procedural measure, this measure will include an update made to the affected TOE guidance to reflect these corrective procedures.

ALC_FLR.1.4C - *The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to the TOE users.*

ALC_FLR.1-5 The evaluator shall examine the flaw remediation procedures documentation to determine that it describes a means of providing the TOE users with the necessary information on each security flaw.

31 The *necessary information* about each security flaw consists of its description (not necessarily at the same level of detail as that provided as part of work unit ALC_FLR.1-2), the prescribed corrective action, and any associated guidance on implementing the correction.

32 TOE users may be provided such information, correction, and documentation updates in any of several ways, such as their posting to a website, their being sent to TOE users, or arrangements made for the developer to install the correction. In cases where the means of providing this information requires action to be initiated by the TOE user, the evaluator examines any TOE guidance to ensure that it contains instructions for retrieving the information.

33 The only metric for assessing the adequacy of the method used for providing the information, corrections and guidance is that there be a reasonable expectation that TOE users can obtain or receive it. For example, consider the method of dissemination where the requisite data is posted to a website for one month, and the TOE users know that this will happen and when this will happen. This may not be especially reasonable or effective (as, say, a permanent posting to the website), yet it is feasible that the TOE user could obtain the necessary information. On the other hand, if the information were posted to the website for only one hour, yet TOE users had no way of knowing this or when it would be posted, it is infeasible that they would ever get the necessary information.

3.2 Evaluation of flaw remediation (ALC_FLR.2)

3.2.1 Objectives

34 The objective of this sub-activity is to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users. Additionally, this sub-activity determines whether the developer's procedures provide for the corrections of security flaws, for the receipt of flaw reports from TOE users, and for assurance that the corrections introduce no new security flaws.

35 In order for the developer to be able to act appropriately upon security flaw reports from TOE users, TOE users need to understand how to submit security flaw reports to the developer, and developers need to know how to receive these reports. Flaw remediation guidance addressed to the TOE user ensures that TOE users are aware of how to communicate with the developer; flaw remediation procedures describe the developer's role is such communication

3.2.2 Input

36 The evaluation evidence for this sub-activity is:

a) the flaw remediation procedures documentation;

b) flaw remediation guidance documentation.

3.2.3 Evaluator actions

37 This sub-activity comprises one CC Part 3 evaluator action element:

a) ALC_FLR.2.1E.

3.2.3.1 Action ALC_FLR.2.1E

ALC_FLR.2.1C - *The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.*

ALC_FLR.2-1 The evaluator shall examine the flaw remediation procedures documentation to determine that it describes the procedures used to track all reported security flaws in each release of the TOE.

38 The procedures describe the actions that are taken by the developer from the time each suspected security flaw is reported to the time that it is resolved. This includes the flaw's entire timeframe, from initial detection through ascertaining the flaw is a security flaw, to resolution of the security flaw.

39 If a flaw is discovered not to be security-relevant, there is no need (for the purposes of the ALC_FLR requirements) for the flaw remediation procedures to

track it further; only that there be an explanation of why the flaw is not security-relevant.

ALC_FLR.2.2C - *The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.*

ALC_FLR.2-2 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would produce a description of each security flaw in terms of its nature and effects.

40 The procedures identify the actions that are taken by the developer to describe the nature and effects of each security flaw in sufficient detail to be able to reproduce it. The description of the nature of a security flaw addresses whether it is an error in the documentation, a flaw in the design of the TSF, a flaw in the implementation of the TSF, etc. The description of the security flaw's effects identifies the portions of the TSF that are affected and how those portions are affected. For example, a security flaw in the implementation might be found that affects the identification and authentication enforced by the TSF by permitting authentication with the password 'BACKDOOR'.

ALC_FLR.2-3 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would identify the status of finding a correction to each security flaw.

41 The flaw remediation procedures identify the different stages of security flaws. This differentiation includes at least: suspected security flaws that have been reported, suspected security flaws that have been confirmed to be security flaws, and security flaws whose solutions have been implemented. It is permissible that additional stages (e.g. flaws that have been reported but not yet investigated, flaws that are under investigation, security flaws for which a solution has been found but not yet implemented) be included.

ALC_FLR.2.3C - *The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.*

ALC_FLR.2-4 The evaluator shall check the flaw remediation procedures to determine that the application of these procedures would identify the corrective action for each security flaw.

42 *Corrective action* may consist of a repair to the hardware, firmware, or software portions of the TOE, a modification of TOE guidance, or both. Corrective action that constitutes modifications to TOE guidance (e.g. details of procedural measures to be taken to obviate the security flaw) includes both those measures serving as only an interim solution (until the repair is issued) as well as those

serving as a permanent solution (where it is determined that the procedural measure is the best solution).

43 If the source of the security flaw is a documentation error, the corrective action consists of an update of the affected TOE guidance. If the corrective action is a procedural measure, this measure will include an update made to the affected TOE guidance to reflect these corrective procedures.

ALC_FLR.2.4C - *The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to the TOE users.*

ALC_FLR.2-5 The evaluator shall examine the flaw remediation procedures documentation to determine that it describes a means of providing the TOE users with the necessary information on each security flaw.

44 The *necessary information* about each security flaw consists of its description (not necessarily at the same level of detail as that provided as part of work unit ALC_FLR.2-2), the prescribed corrective action, and any associated guidance on implementing the correction.

45 TOE users may be provided such information, correction, and documentation updates in any of several ways, such as their posting to a website, their being sent to TOE users, or arrangements made for the developer to install the correction. In cases where the means of providing this information requires action to be initiated by the TOE user, the evaluator examines any TOE guidance to ensure that it contains instructions for retrieving the information.

46 The only metric for assessing the adequacy of the method used for providing the information, corrections and guidance is that there be a reasonable expectation that TOE users can obtain or receive it. For example, consider the method of dissemination where the requisite data is posted to a website for one month, and the TOE users know that this will happen and when this will happen. This may not be especially reasonable or effective (as, say, a permanent posting to the website), yet it is feasible that the TOE user could obtain the necessary information. On the other hand, if the information were posted to the website for only one hour, yet TOE users had no way of knowing this or when it would be posted, it is infeasible that they would ever get the necessary information.

ALC_FLR.2.5C - *The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.*

ALC_FLR.2-6 The evaluator shall examine the flaw remediation procedures to determine that they describe procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.

47 The procedures ensure that TOE users have a means by which they can communicate with the TOE developer. By having a means of contact with the developer, the user can report security flaws, enquire about the status of security flaws, or request corrections to flaws. This means of contact may be part of a more general contact facility for reporting non-security related problems.

48 The use of these procedures is not restricted to TOE users; however, only the TOE users are actively supplied with the details of these procedures. Others who might have access to or familiarity with the TOE can use the same procedures to submit reports to the developer, who is then expected to process them. Any means of submitting reports to the developer, other than those identified by the developer, are beyond the scope of this work unit; reports generated by other means need not be addressed.

ALC_FLR.2.6C - *The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.*

ALC_FLR.2-7 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would help to ensure every reported flaw is corrected.

49 The flaw remediation procedures cover not only those security flaws discovered and reported by developer personnel, but also those reported by TOE users. The procedures are sufficiently detailed so that they describe how it is ensured that each reported security flaw is corrected. The procedures contain reasonable steps that show progress leading to the eventual, inevitable resolution.

50 The procedures describe the process that is taken from the point at which the suspected security flaw is determined to be a security flaw to the point at which it is resolved.

ALC_FLR.2-8 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would help to ensure that the TOE users are issued corrective actions for each security flaw.

51 The procedures describe the process that is taken from the point at which a security flaw is resolved to the point at which the corrective action is provided. The procedures for delivering corrective actions should be consistent with the security objectives; they need not necessarily be identical to the procedures used for delivering the TOE, as documented to meet ADO_DEL, if included in the assurance requirements. For example, if the hardware portion of a TOE were originally delivered by bonded courier, updates to hardware resulting from flaw remediation would likewise expected to be distributed by bonded courier. Updates unrelated to flaw remediation would follow the procedures set forth in the documentation meeting the ADO_DEL requirements.

ALC_FLR.2.7C - *The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.*

ALC_FLR.2-9 **The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would result in safeguards that the potential correction contains no adverse effects.**

52 Through analysis, testing, or a combination of the two, the developer may reduce the likelihood that adverse effects will be introduced when a security flaw is corrected. The evaluator assesses whether the procedures provide detail in how the necessary mix of analysis and testing actions is to be determined for a given correction.

53 The evaluator also determines that, for instances where the source of the security flaw is a documentation problem, the procedures include the means of safeguarding against the introduction of contradictions with other documentation.

ALC_FLR.2.8C - *The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.*

ALC_FLR.2-10 **The evaluator shall examine the flaw remediation guidance to determine that the application of these procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.**

The guidance ensures that TOE users have a means by which they can communicate with the TOE developer. By having a means of contact with the developer, the user can report security flaws, enquire about the status of security flaws, or request corrections to flaws.

3.3 Evaluation of flaw remediation (ALC_FLR.3)

3.3.1 Objectives

54 The objective of this sub-activity is to determine whether the developer has established flaw remediation procedures that describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users. Additionally, this sub-activity determines whether the developer's procedures provide for the corrections of security flaws, for the receipt of flaw reports from TOE users, for assurance that the corrections introduce no new security flaws, for the establishment of a point of contact for each TOE user, and for the timely issue of corrective actions to TOE users.

55 In order for the developer to be able to act appropriately upon security flaw reports from TOE users, TOE users need to understand how to submit security flaw reports to the developer, and developers need to know how to receive these reports. Flaw remediation guidance addressed to the TOE user ensures that TOE users are aware of how to communicate with the developer; flaw remediation procedures describe the developer's role is such communication.

3.3.2 Input

56 The evaluation evidence for this sub-activity is:

a) the flaw remediation procedures documentation;

b) flaw remediation guidance documentation.

3.3.3 Evaluator actions

57 This sub-activity comprises one CC Part 3 evaluator action element:

a) ALC_FLR.3.1E.

3.3.3.1 Action ALC_FLR.3.1E

ALC_FLR.3.1C - *The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.*

ALC_FLR.3-1 The evaluator shall examine the flaw remediation procedures documentation to determine that it describes the procedures used to track all reported security flaws in each release of the TOE.

58 The procedures describe the actions that are taken by the developer from the time each suspected security flaw is reported to the time that it is resolved. This includes the flaw's entire timeframe, from initial detection through ascertaining the flaw is a security flaw, to resolution of the security flaw.

59 If a flaw is discovered not to be security-relevant, there is no need (for the purposes of the ALC_FLR requirements) for the flaw remediation procedures to

track it further; only that there be an explanation of why the flaw is not security-relevant.

60 ALC_FLR.3.2C - *The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.*

ALC_FLR.3-2 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would produce a description of each security flaw in terms of its nature and effects.

61 The procedures identify the actions that are taken by the developer to describe the nature and effects of each security flaw in sufficient detail to be able to reproduce it. The description of the nature of a security flaw addresses whether it is an error in the documentation, a flaw in the design of the TSF, a flaw in the implementation of the TSF, etc. The description of the security flaw's effects identifies the portions of the TSF that are affected and how those portions are affected. For example, a security flaw in the implementation might be found that affects the identification and authentication enforced by the TSF by permitting authentication with the password 'BACKDOOR'.

ALC_FLR.3-3 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would identify the status of finding a correction to each security flaw.

62 The flaw remediation procedures identify the different stages of security flaws. This differentiation includes at least: suspected security flaws that have been reported, suspected security flaws that have been confirmed to be security flaws, and security flaws whose solutions have been implemented. It is permissible that additional stages (e.g. flaws that have been reported but not yet investigated, flaws that are under investigation, security flaws for which a solution has been found but not yet implemented) be included.

ALC_FLR.3.3C - *The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.*

ALC_FLR.3-4 The evaluator shall check the flaw remediation procedures to determine that the application of these procedures would identify the corrective action for each security flaw.

63 *Corrective action* may consist of a repair to the hardware, firmware, or software portions of the TOE, a modification of TOE guidance, or both. Corrective action that constitutes modifications to TOE guidance (e.g. details of procedural measures to be taken to obviate the security flaw) includes both those measures serving as only an interim solution (until the repair is issued) as well as those

serving as a permanent solution (where it is determined that the procedural measure is the best solution).

64 If the source of the security flaw is a documentation error, the corrective action consists of an update of the affected TOE guidance. If the corrective action is a procedural measure, this measure will include an update made to the affected TOE guidance to reflect these corrective procedures.

ALC_FLR.3.4C - *The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to the TOE users.*

ALC_FLR.3-5 The evaluator shall examine the flaw remediation procedures documentation to determine that it describes a means of providing the TOE users with the necessary information on each security flaw.

65 The *necessary information* about each security flaw consists of its description (not necessarily at the same level of detail as that provided as part of work unit ALC_FLR.3-2), the prescribed corrective action, and any associated guidance on implementing the correction.

66 TOE users may be provided such information, correction, and documentation updates in any of several ways, such as their posting to a website, their being sent to TOE users, or arrangements made for the developer to install the correction. In cases where the means of providing this information requires action to be initiated by the TOE user, the evaluator examines any TOE guidance to ensure that it contains instructions for retrieving the information.

67 The only metric for assessing the adequacy of the method used for providing the information, corrections and guidance is that there be a reasonable expectation that TOE users can obtain or receive it. For example, consider the method of dissemination where the requisite data is posted to a website for one month, and the TOE users know that this will happen and when this will happen. This may not be especially reasonable or effective (as, say, a permanent posting to the website), yet it is feasible that the TOE user could obtain the necessary information. On the other hand, if the information were posted to the website for only one hour, yet TOE users had no way of knowing this or when it would be posted, it is infeasible that they would ever get the necessary information.

68 For TOE users who register with the developer (see work unit ALC_FLR.3-12), the passive availability of this information is not sufficient. Developers must actively send the information (or a notification of its availability) to registered TOE users.

ALC_FLR.3.5C - *The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.*

ALC_FLR.3-6 The evaluator shall examine the flaw remediation procedures to determine that they describe procedures for the developer to accept reports of security flaws or requests for corrections to such flaws.

69 The procedures ensure that TOE users have a means by which they can communicate with the TOE developer. By having a means of contact with the developer, the user can report security flaws, enquire about the status of security flaws, or request corrections to flaws. This means of contact may be part of a more general contact facility for reporting non-security related problems.

70 The use of these procedures is not restricted to TOE users; however, only the TOE users are actively supplied with the details of these procedures. Others who might have access to or familiarity with the TOE can use the same procedures to submit reports to the developer, who is then expected to process them. Any means of submitting reports to the developer, other than those identified by the developer, are beyond the scope of this work unit; reports generated by other means need not be addressed.

ALC_FLR.3.6C - *The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.*

ALC_FLR.3-7 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would help to ensure that every reported flaw is corrected.

71 The flaw remediation procedures cover not only those security flaws discovered and reported by developer personnel, but also those reported by TOE users. The procedures are sufficiently detailed so that they describe how it is ensured that each reported security flaw is corrected. The procedures contain reasonable steps that show progress leading to the eventual, inevitable resolution.

72 The procedures describe the process that is taken from the point at which the suspected security flaw is determined to be a security flaw to the point at which it is resolved.

ALC_FLR.3-8 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would help to ensure that the TOE users are issued corrective actions for each security flaw.

73 The procedures describe the process that is taken from the point at which a security flaw is resolved to the point at which the corrective action is provided. The procedures for delivering corrective actions should be consistent with the security objectives; they need not necessarily be identical to the procedures used for

delivering the TOE, as documented to meet ADO_DEL, if included in the assurance requirements. For example, if the hardware portion of a TOE were originally delivered by bonded courier, updates to hardware resulting from flaw remediation would likewise expected to be distributed by bonded courier. Updates unrelated to flaw remediation would follow the procedures set forth in the documentation meeting the ADO_DEL requirements.

ALC_FLR.3.7C - *The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.*

ALC_FLR.3-9 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would result in safeguards that the potential correction contains no adverse effects.

74 Through analysis, testing, or a combination of the two, the developer may reduce the likelihood that adverse effects will be introduced when a security flaw is corrected. The evaluator assesses whether the procedures provide detail in how the necessary mix of analysis and testing actions is to be determined for a given correction.

75 The evaluator also determines that, for instances where the source of the security flaw is a documentation problem, the procedures include the means of safeguarding against the introduction of contradictions with other documentation.

ALC_FLR.3.8C - *The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.*

ALC_FLR.3-10 The evaluator shall examine the flaw remediation guidance to determine that the application of these procedures would result in a means for the TOE user to provide reports of suspected security flaws or requests for corrections to such flaws.

The guidance ensures that TOE users have a means by which they can communicate with the TOE developer. By having a means of contact with the developer, the user can report security flaws, enquire about the status of security flaws, or request corrections to flaws.

ALC_FLR.3.9C - *The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.*

ALC_FLR.3-11 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would result in a timely means of providing the registered TOE users who might be affected with reports about, and associated corrections to, each security flaw.

76 The issue of timeliness applies to the issuance of both security flaw reports and the associated corrections. However, these need not be issued at the same time. It is recognised that flaw reports should be generated and issued as soon as an interim solution is found, even if that solution is as drastic as 'Turn off the TOE'. Likewise, when a more permanent (and less drastic) solution is found, it should be issued without undue delay.

77 It is unnecessary to restrict the recipients of the reports and associated corrections to only those TOE users who might be affected by the security flaw; it is permissible that all TOE users be given such reports and corrections for all security flaws, provided such is done in a timely manner.

ALC_FLR.3-12 The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would result in automatic distribution of the reports and associated corrections to the registered TOE users who might be affected.

78 *Automatic distribution* does not mean that human interaction with the distribution method is not permitted. In fact, the distribution method could consist entirely of manual procedures, perhaps through a closely monitored procedure with prescribed escalation upon the lack of issue of reports or corrections.

79 It is unnecessary to restrict the recipients of the reports and associated corrections to only those TOE users who might be affected by the security flaw; it is permissible that all TOE users be given such reports and corrections for all security flaws, provided such is done automatically.

ALC_FLR.3.10C - *The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.*

ALC_FLR.3-13 The evaluator shall examine the flaw remediation guidance to determine that it describes a means of enabling the TOE users to register with the developer.

80 *Enabling the TOE users to register with the developer* simply means having a way for each TOE user to provide the developer with a point of contact; this point of contact is to be used to provide the TOE user with information related to security flaws that might affect that TOE user, along with any corrections to the security flaw. Registering the TOE user may be accomplished as part of the standard procedures that TOE users undergo to identify themselves to the developer, for the purposes of registering a software licence, or for obtaining update and other useful information.

81 There need not be one registered TOE user per installation of the TOE; it would be sufficient if there were one registered TOE user for an organisation. For example,

a corporate TOE user might have a centralised acquisition office for all of its sites. In this case, the acquisition office would be a sufficient point of contact for all of that TOE user's sites, so that all of the TOE user's installations of the TOE have a registered point of contact.

82 In either case, it must be possible to associate each TOE that is delivered with an organisation in order to ensure that there is a registered user for each TOE. For organisations that have many different addresses, this assures that there will be no user who is erroneously presumed to be covered by a registered TOE user.

83 It should be noted that TOE users need not register; they must only be provided with a means of doing so. However, users who choose to register must be directly sent the information (or a notification of its availability).

ALC_FLR.3.11C - *The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.*

ALC_FLR.3-14 The evaluator shall examine the flaw remediation guidance to determine that it identifies specific points of contact for reports and enquiries about security issues involving the TOE.

84 The guidance includes a means whereby registered TOE users can interact with the developer to report discovered security flaws in the TOE or to make enquiries regarding discovered security flaws in the TOE.

Annex A: Flaw Remediation evaluation criteria

85 This annex provides the replacement text for Clause 12.2 in the CC v2.1 Part 3, including Interpretations CCIMB-INTERP-062 and CCIMB-INTERP-092. The following text supercedes Interpretation CCIMB-INTERP-094. It is provided to aid the reader in understanding and using the methodology provided in the main body of this document. Note that the original CC paragraph numbering has been retained for reference purposes. In addition, change bars have been used to indicate where changes have taken place within the CC text.

12.2 Flaw remediation (ALC_FLR)

Objectives

388 Flaw remediation requires that discovered security flaws be tracked and corrected by the developer. Although future compliance with flaw remediation procedures cannot be determined at the time of the TOE evaluation, it is possible to evaluate the policies and procedures that a developer has in place to track and correct flaws, and to distribute the flaw information and corrections.

Component levelling

389 The components in this family are levelled on the basis of the increasing extent in scope of the flaw remediation procedures and the rigour of the flaw remediation policies.

Application notes

390 This family provides assurance that the TOE will be maintained and supported in the future, requiring the TOE developer to track and correct flaws in the TOE. Additionally, requirements are included for the distribution of flaw corrections. However, this family does not impose evaluation requirements beyond the current evaluation.

The TOE user is considered to be the focal point in the user organisation that is responsible for receiving and implementing fixes to security flaws. This is not necessarily an individual user, but may be an organisational representative who is responsible for the handling of security flaws. The use of the term “TOE user” recognises that different organisations have different procedures for handling flaw reporting, which may be done either by an individual user, or by a central administrative body.

391 The flaw remediation procedures should describe the methods for dealing with all types of flaws encountered. These flaws may be reported by the developer, by users of the TOE, or by other parties with familiarity with the TOE. Some flaws may not be reparable immediately. There may be some occasions where a flaw cannot be fixed and other (e.g. procedural) measures must be taken. The documentation provided should cover the procedures for providing the operational sites with fixes,

and providing information on flaws where fixes are delayed (and what to do in the interim) or when fixes are not possible.

Once the evaluation of a TOE is complete, it is no longer the target for evaluation. Furthermore, any changes to this evaluated TOE result in the original evaluation results being no longer applicable to the changed version. The phrase "release of the TOE" used in this family therefore refers to a version of a product or system that is a release of a certified TOE, to which changes have been applied.

ALC_FLR.1 Basic flaw remediation

Dependencies:

No dependencies.

Developer action elements:

ALC_FLR.1.1D **The developer shall provide flaw remediation procedures addressed to TOE developers.**

Content and presentation of evidence elements:

ALC_FLR.1.1C **The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.**

ALC_FLR.1.2C **The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.**

ALC_FLR.1.3C **The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.**

ALC_FLR.1.4C **The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.**

Evaluator action elements:

ALC_FLR.1.1E **The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.**

ALC_FLR.2 Flaw reporting procedures

Objectives

In order for the developer to be able to act appropriately upon security flaw reports from TOE users, and to know to whom to send corrective fixes, TOE users need to understand how to submit security flaw reports to the developer. Flaw remediation guidance from the developer to the TOE user ensures that TOE users are aware of this important information.

Dependencies:

No dependencies.

Developer action elements:

ALC_FLR.2.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.2.2D **The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.**

ALC_FLR.2.3D **The developer shall provide flaw remediation guidance addressed to TOE users.**

Content and presentation of evidence elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5C **The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.**

ALC_FLR.2.6C **The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.**

ALC_FLR.2.7C **The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.**

ALC_FLR.2.8C **The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.**

Evaluator action elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_FLR.3 Systematic flaw remediation

Objectives

In order for the developer to be able to act appropriately upon security flaw reports from TOE users, and to know to whom to send corrective fixes, TOE users need to understand how to submit security flaw reports to the developer, and how to register themselves with the developer so that they may receive these corrective fixes. Flaw remediation guidance from the developer to the TOE user ensures that TOE users are aware of this important information.

Dependencies:

No dependencies.

Developer action elements:

ALC_FLR.3.1D The developer shall provide flaw remediation procedures addressed to TOE developers.

ALC_FLR.3.2D The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

ALC_FLR.3.3D The developer shall provide flaw remediation guidance addressed to TOE users.

Content and presentation of evidence elements:

ALC_FLR.3.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

ALC_FLR.3.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.3.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

ALC_FLR.3.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.3.5C The flaw remediation procedures documentation shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

ALC_FLR.3.6C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.

ALC_FLR.3.7C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

ALC_FLR.3.8C The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

ALC_FLR.3.9C **The flaw remediation procedures shall include a procedure requiring timely responses for the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.**

ALC_FLR.3.10C **The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.**

ALC_FLR.3.11C **The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.**

Evaluator action elements:

ALC_FLR.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.