Towards Common Criteria Certification for DO-178B Compliant Airborne Software Systems[1]

Comparing Evaluation Assurance Level 5 (EAL5) to DO178

Jim Alves-Foss, Bob Rinker and Carol Taylor
Center for Secure and Dependable Systems
University of Idaho

Abstract

This document provides a mapping of the Common Criteria (CC) assurance evaluation criteria to the criteria found in DO-178B "Software Considerations in Airborne Systems and Equipment Certification." Specifically, the purpose of this document is to provide guidance for developers of DO-178B compliant software on the activities necessary to make their systems also compliant with CC evaluation assurance levels 5 (EAL 5). The target of evaluation (TOE) will be an airborne software system, and all comments contained within this document refer to only these types of systems. To that end, it is important to understand the context in which these criteria have been created, how their requirements are presented and how they can be interpreted.

[1] Not releasable to the Defense Technical Information Center per DOD directive 3200.12. This material is based upon work supported by the DOD under Contract. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the DOD.

Table of Contents

Overview

This document provides a mapping of the Common Criteria (CC) assurance evaluation criteria to the criteria found in DO-178B "Software Considerations in Airborne Systems and Equipment Certification." Specifically, the purpose of this document is to provide guidance for developers of DO-178B compliant software on the activities necessary to make their systems also compliant with CC evaluation assurance levels 5 (EAL 5). The target of evaluation (TOE) will be an airborne software system, and all comments contained within this document refer to only these types of systems. To that end, it is important to understand the context in which these criteria have been created, how their requirements are presented and how they can be interpreted.

DO-178B

This document provides guidance for developers of airborne avionics software systems to ensure that the systems perform their intended function with a level of confidence in safety that complies with standards. The document provides objectives for various software life cycle processes, descriptions of design considerations and activities for satisfying those objects and descriptions of the reporting evidence that needs to be presented to indicate that the objectives have been satisfied.

The basis of the document is to discuss software development processes and related documentation. The document refers to system requirements, but not any specific type of system or functionality.

Common Criteria (CC)

The CC focuses on security issues within systems. As such it does not have the breadth of scope of DO-178B. The criteria are a guideline for the development of protection profiles. A protection profile describes a particular device (the target of evaluation, TOE); a set of security functions that the device supports (TSF); a security policy (TSP); an interface (TSFI) and a scope of control (TSC). The CC document provides guidelines for these security functions and interactions among them. Developers of protection profiles utilize these guidelines to develop specific requirements for the security device. Any avionics device that is being defined as a security device needs to be defined within the context of a protection profile (or such a profile needs to be created and certified for these devices). This is similar to the model used by DO-178B in that the specific functions and

In addition to security functions, the CC introduces a separate context for evaluation assurance levels (EAL). These levels define the objectives, processes and evidence needed to provide a required level of confidence that the system performs its security functions and implements its security policy as defined. It is these evaluation levels that correspond to the DO-178B document. However, it is important to note that the EALs were designed with the specific purpose in mind of validating security functions and policy and not the normal operational behavior of the system. Therefore, unlike the DO-178B requirements, specific types of functionality (security functions) are specifically mentioned.

ACM – Configuration Management

The purpose of the ACM class is to establish the Configuration Management (CM) requirements. These requirements are provided the integrity of the portions of the TOE that they control, by providing a method of tracking for changes to the TOE and by ensuring that all changes are authorized.

ACM_AUT.1 CM Automation

The ACM_AUT criteria is provided to specify the use of automated tools in the development process in support of change control.

Dependencies:

ACM_CAP.3 Authorization controls

Developer action elements:

ACM_AUT.1.1D The developer shall use a CM system.

The DO-178B discusses the CM system in the following sections under configuration management, in sections 7.2.2.d, 7.2.4, and 7.2, and under software planning in sections 4.2.g and 4.4. However, there is no explicit statement for the use of a CM system (i.e, a computerized CM system). To be in compliance with CC EAL 4, the use of a CM system must be explicitly stated.

ACM_AUT.1.2D The developer shall provide a CM plan.

DO-178B discusses the CM plan in section 11.4.

Content and presentation of evidence elements:

ACM_AUT.1.1C The CM system shall provide an automated means by which authorized changes are made to the TOE implementation representation.

In DO-178B, sections 7.2.4 and 7.2.5 discuss the CM system's implementation of change control and approval while sections 11.4.b.4 and 11.4.b.5 provide for documentation for these sections. However, DO-178B does not require that the CM system use automation to achieve its purpose and would need to add the automation requirement in order to comply with EAL 4.

ACM_AUT.1.2C The CM system shall provide an automated means to support the generation of the TOE.

Section 11.4.a generally discusses the CM system but does not specifically address automation. A requirement for automation would need to be added in order to comply with CC EAL5.

ACM_AUT.1.3C The CM plan shall describe the automated tools used in the CM system.

Section 11.4.a which specifies the CM plan, mentions tools but does not specify CM automation.

ACM_AUT.1.4C The CM plan shall describe how the automated tools are used in the CM system.

Discussion of how the tools are used in the CM plan can be found in DO-178B sections 11.4.b.1 through 11.4.b.10. Again, no mention is made about CM automation.

Evaluator action elements:

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

DO-178B requires that the objectives of the CM system are satisfied for all SW level systems.

ACM_CAP.4 – CM Capabilities

The ACM_CAP criteria are to ensure that all components of the TOE have been labeled and can be uniquely identified for purposes of tracking. Also, criteria are established for controlling the changes to the TOE.

Dependencies:

ACM_SCP.1 TOE CM coverage
ALC_DVS.1 Identification of security measures

Developer action elements:

ACM_CAP.4.1D The developer shall provide a reference for the TOE.

DO-178B requires identification of the TOE in section 7.2.1.

ACM_CAP.4.2D The developer shall use a CM system.

DO-178B sections 4.2.g and 4.4 discuss the use of tools and their management in order to achieve change control and data necessary to verify integrity of the software. The use of a CM system is implied but not explicitly stated.

ACM_CAP.4.3D The developer shall provide CM documentation.

Sections 11.4.d and 11.18 of DO-178B discuss the documentation of the CM process.

Content and presentation of evidence elements:

ACM_CAP.4.1C The reference for the TOE shall be unique to each version of the TOE.
ACM_CAP.4.2C The TOE shall be labeled with its reference.

DO-178B section 7.2.1 refers to the labeling and unique identification of the software configuration items.

ACM_CAP.4.3C The CM documentation shall include a configuration list, a CM plan, and an acceptance plan.

DO-178B section 11.4 discusses the CM plan and section 11.18 outlines the SCM records and possible inclusions in those records. But, DO-178B does not specifically require an included configuration list or acceptance plan in the CM documentation.

ACM_CAP.4.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.4.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

Section 11.4.b.1 describes the configuration items and discusses the need for identification of configuration items. However, no mention is made of the method used to uniquely identify the configuration items.

ACM_CAP.4.6C The CM system shall uniquely identify all configuration items.

Section 7.2.1 of DO-178B discusses unique identification of CM configuration items.

ACM_CAP.4.7C The CM plan shall describe how the CM system is used.

Section 7.2.1 of the DO-178B document discusses the CM management plan and how the CM systems are to be used.

ACM_CAP.4.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

Section 7.2.1 of the DO-178B document discusses the CM management plan and how the CM systems are to be used.

ACM_CAP.4.9C The CM documentation shall provide evidence that all configuration items have been and are effectively maintained under the CM system.

Section 11.18 of DO-178B describes the CM records and suggestions for items to include in these records.

ACM_CAP.4.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Section 7.2.7.b.1 of DO-178B mentions the procedures for ensuring that no unauthorized changes are made.

ACM_CAP.4.11C The CM system shall support the generation of the TOE.

Section 11.4.a of DO-178B describes the CM plan and discusses the CM system but not the use of the system to generate the target.

ACM_CAP.4.12C The acceptance plan shall describe the procedures used to accept modified of newly created configuration items as part of the TOE.

Section 7.2.7 discusses the release activity but makes no mention of an acceptance plan.

Evaluator action elements:

ACM_CAP.4.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

DO-178B requires that the objectives of the CM system be satisfied for all SW level systems.

ACM_ SCP.3 – CM Scope

The ACM-SCP class specifies the scope of the CM coverage including the TOE implementation representation, the documentation, the configuration options and the development tools.

Dependencies

ACM_CAP.3 Authorization controls

Developer action elements:

ACM_SCP.3.1D The developer shall provide CM documentation.

CM documentation is discussed in three different sections of DO-178B including sections 7.2, 11.4 and 11.18.

Content and presentation of evidence elements:

ACM_SCP.3.1C The CM documentation shall show that the CM system, as a minimum, tracks the following: the TOE implementation representation, design documentation, test documentation, user documentation, security flaws, and development tools and related information.

Sections 11.4.d and 11.18 discuss the SCM records and 11.18 provides examples of the types of records that could be kept. However, neither section requires that the CM system track the TOE implementation representation, or the design, test, user and administration documentation. Also, no mention is made of CM documentation relating to security flaws since security is not the focus of DO-178B. To comply with CC EAL5, greater details will need to be added for including these specific types of documents in the CM documentation.

ACM_SCP.3.2C *The CM documentation shall describe how configuration items are tracked by the CM system.*

Sections 11.4.d and 11.18 are the sections that detail the SCM records. Neither section specifies how configuration items are tracked by the CM system. Details of how the tracking is done would need to supplement the existing requirements to bring DO-178B compliant software into compliance with CC EAL5.

Evaluator action elements:

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

DO-178B requires that the objectives of the CM system are satisfied for all SW level systems.

ADO – Deliver and Operation

This class specifies requirements for delivery, installation, generation and start-up of the TOE.

ADO_DEL.2 - Delivery

The objectives of this class specify the delivery of the TOE and provides assurance that the recipient receives the intended TOE and not a version that has been modified or tampered with.

Dependencies:

ACM_CAP.3 *Authorization controls*

Developer action elements:

ADO_DEL.2.1D *The developer shall document procedures for delivery of the TOE or parts of it to the user.*

Section 7.2.7 and section 11.4.b.7 discuss the release of the configuration items. However, details of the release procedures are missing. These details would need to be added for compliance with CC EAL5.

ASO_DEL.2.2D *The developer shall use the delivery procedures.*

Section 7.2.7 and section 11.4.b.7 discuss the release of the configuration items. However, details of the release procedures are missing and no mention is made of the developer using the delivery procedures. These details would need to be added for compliance with CC EAL5.

Content and presentation of evidence elements:

ADO_DEL.2.1C *The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.*

Details of the delivery procedures are missing and no mention is made of maintaining security when release of the software is made to the user. These procedures would need to be added for compliance with CC EAL5.

ADO_DEL.2.2C *The delivery documentation shall describe how the various procedures and technical measures provide for the detection of modifications, or any discrepancy between the developer's master copy and the version received at the user site.*

No mention is made in DO-178B of delivery documentation and how the detection of discrepancies between the developer's and the user's copies of the software is done. Requirements for these documents would need to be added for compliance with CC EAL5

ADO_DEL.2.3C *The delivery documentation shall describe how the various procedures allow detection of attempts to masquerade as the developer, even in cases in which the developer has sent nothing to the user's site.*

Again, no mention is made in DO-178B of delivery documentation that mentions these attempts at masquerading as the developer. These sections would need to be added for compliance with CC EAL5.

Evaluator action elements:

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

DO-178B requires that the objectives of the CM system are satisfied for all SW level systems.

ADO_IGS.1 Installation, Generation and Start-up Procedures

ADO_IGS ensures that installation, and start-up procedures are specified so that the TOE is installed, and started up in a secure manner.

Dependencies:

AGD_ADM.1 *Administrator guidance*

Developer action elements:

ADO_IGS.1D *The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.*

DO-178B does not have a section that details the procedures needed for secure installation, generation and start-up of the TOE. A section would need to be added to comply with CC EAL5.

Content and presentation of evidence elements:

ADO_IGS.1.1C *The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.*

DO-178B does not have a section that documents the steps needed for secure installation, generation and start-up of the TOE. A section would need to be added to comply with CC EAL5.

Evaluator action elements:

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

ADO_IGS.1.2E *The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.*

DO-178B must specify that the installation, generation and start-up procedures result in a secure configuration and the documentation details the steps necessary for secure installation, generation and start-up.

ADV - Development

The purpose of the ADV family of requirement is to specify criteria related to the development of the target security functions (TSF) at various levels of abstraction from the functional interface to the implementation representation. Also, this class has requirements for a target security policy (TSP) model, for corresponding mappings between the TSP requirements, the TSP model and the functional specification.

ADV_FSP.2 – Functional Specification

The ADV_FSP criteria are used to specify the level of formalism in the functional specification of the TOE.

Dependencies:

ADV_RCR.1 *Informal correspondence demonstration.*

Developer action elements:

ADV_FSP.2.1D *The developer shall provide a functional specification.*

The DO-178B requires the development of high-level requirements in section 5.1 to produce the documentation specified in section 11.9, *"Software Requirements Data"*.

Content and presentation of evidence elements:

ADV_FSP.2.1C *The functional specification shall describe the TSF and its external interfaces using an informal style.*

The style of specification is unspecified in DO-178B; but is assumed to be informal. However, section 11.6 *"Software Requirements Standards*" provides for defining this type of requirement. Understand that to be compliant with the CC, you must explicitly specify the security functions; this is similar to the explicit specification of safety requirements as specified in 5.1.2d. Again, these restrictions can be documented in 11.6

ADV_FSP.2.2C *The functional specification shall be internally consistent.*

This corresponds to DO-178B section 5.1.2a and to section 6.3.1b and is documented in sections 11.9 and 11.14 *"Software Verification Results"*.

ADV_FSP.2.3C *The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing complete details of all effects, exceptions and error messages.*

These requirements are satisfied in DO-178B section 11.9.

ADV_FSP.2.4C *The functional specification shall completely represent the TSF.*

This requirement corresponds with a DO-178B section 6.3.1f and is documented in 11.14.

ADV_FSP.2.5C *The functional specification shall include rationale that the TSF is completely represented.*

This requirement does not have a direct correspondence with a DO-178B requirement, however it should be included with the section 11.9 documentation.

Evaluator action elements:

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

ADV_FSP.2.2E *The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.*

DO-178B requires independent verification of coverage of the functional requirements and consistency for level A and level B systems.

ADV_HLD.2 – High-level Design

The purpose of the ADV_HLD requirement is to provide guidance for the development of the high-level design of the TSF. In DO-178B section 5.2, it is stated that "The software high-level requirements are refined through one or more iterations in the software design process to develop the software architecture and the low-level requirements that can be used to implement source code." It is our interpretation that the software architecture complies with ADV_HLD and that the low-level requirements comply with ADV_LLD.

Dependencies:

ADV_FSP.1 *Informal functional specification*

ADV_RCR.1 *Informal correspondence demonstration*

Developer action elements:

ADV_HLD.2.1D *The developer shall provide the high-level design of the TSF.*

This can be satisfied by the software architecture documentation specified in DO-178B section 11.10 "*Design Description*" which documents the architecture specified in section 5.2

Content and presentation of evidence elements:

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

DO-178B does not specify the format of the design or software architecture. However, section 11.7 "*Software Design Standards"* allows for the specification of these types of requirements.

ADV_HLD.2.2C The high-level design shall be internally consistent.

DO-178B section 6.3.3b satisfies this requirement and is documented in 11.14 "*Software Verification Results"*.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsytems.

DO-178B does not require the specific specification of subsystems, however, mention is made of components within the software architecture. This type of specific requirement can be specified within the document defined in section 11.7.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

This information should be provided in DO-178B *"Design Description"* section 11.10; however it is not required.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

This is required in DO-178B section 5.2 and documented in 11.10

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF

This is required in DO-178B section 5.2 and documented in 11.10

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

This is required in DO-178B section 5.2 and documented in 11.10

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

This is required in DO-178B section 5.2 and documented in 11.10

ADV_HLD.2.9C *The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.*

This is a new requirement, however it can be added when creating the "*Software Design Standards*" in DO-178B section 11.7

Evaluator action elements:

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

ADV_HLD.2.2E *The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.*

DO-178B requires independent verification of coverage of the software architecture only at level A.

ADV_IMP.1 – Implementation Representation

The purpose of the ADV_IMP requirement is to provide guidance in developing the actual implementation of the system. The requirements here do not specifically require that an executable system is developed, but rather that there is a model of the implementation that is sufficiently detailed to enable direct creation of executables.

Application notes:

333 *ADV_IMP.1.1D requires that the developer provide the implementation representation for a subset of the TSF. The intention is that access to at least a portion of the TSF will provide the evaluator with an opportunity to examine the implementation representation for those portions of the TOE where such an examination can add significantly to the understanding of, and assurance in, the mechanisms employed. Provision of a sample of the implementation representation will also allow the evaluator to sample the traceability evidence to gain assurance in the approach taken for refinement, and to assess the presentation of the implementation representation itself.*

334 *ADV_IMP.1.2E element defines a requirement that the evaluator determine that the least abstract TSF representation is an accurate and complete instantiation of the TOE security functional requirements. This provides a direct correspondence between the TOE security functional requirements and the least abstract TSF representation, in addition to the pairwise correspondences required*

by the representation, in addition to the pairwise correspondences required by the ADV_RCR family. It is expected that the evaluator will use the evidence provided in ADV_RCR as an input to making this determination. The least abstract TSF representation for this component is an aggregate of the implementation representation that is provided and that portion of the low-level design for which no corresponding implementation representation is provided.

Dependencies:

ADV_LLD.1	*Descriptive low-level design*
ADV_RCT.1	*Informal correspondence demonstration*
ALC_TAT.1	*Well-defined development tools*

Developer action elements:

ADV_IMP.1.1D *The developer shall provide the implementation representation for a selected subset of the TSF.*

The DO-178B section 5.3 requirements specifically discusses source code and not a possibly higher level representation of the implementation. Source code as delivered in section 11.11 "*Source Code*" is compliant with this section.

Content and presentation of evidence elements:

ADV_IMP.1.1C *The implementation representation shall unambiguously define the TSF to a level of detail such that the TSF can be generated without further design decisions.*

DO-178B section 11.11 documents source code (section 5.3) and compilation, linking and loading instructions in compliance with this requirement.

ADV_IMP.1.2C *The implementation representation shall be internally consistent.*

DO-178B section 6.3.4f satisfies this requirement and is documented in section 11.14 "*Software Verification Results*".

Evaluator action elements:

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

ADV_IMP.1.2E *The evaluator shall determine that the least abstract TSF representation provided is an accurate and complete instantiation of the TOE security functional requirements.*

DO-178B does require independent verification that the source code complies with low-level requirements.

ADV_LLD.1 – Low-level Design

The ADV_LLD requirement provides criteria for a low-level design of the software.

Dependencies:

ADV_HLD.2 *Security enforcing high-level design*
ADV_RCR.1 *Informal correspondence demonstration*

Developer action elements:

ADV_LLD.1.1D *The developer shall provide the low-level design of the TSF.*

As with ADV_HLD, we believe that this requirement is satisfied by section 5.3 and 11.10 "*Design Description*".

Content and presentation of evidence elements:

ADV_LLD.1.1C *The presentation of the low-level design shall be informal.*

DO-178B does not specifically require a presentation format but this can be specified in section 11.7 "*Software Design Standards"*.

ADV-LLD.1.2C *The low-level design shall be internally consistent.*

DO-178B section 6.3.2b satisfies this requirement as documented in section 11.14 "*Software Verification Results"*.

ADV_LLD.1.3C *The low-level design shall describe the TSF in terms of modules.*

Modularity is not strictly required in DO-178B but can be specified in 11.7

ADV_LLD.1.4C *The low-level design shall describe the purpose of each module.*

DO-178B section 11.10i satisfies this requirement.

ADV_LLD.1.5C *The low-level design shall define the interrelationships between the modules in terms of provided security functionality and dependencies on other modules.*

Although not specifically stated, this should be satisfied by DO-178B section 11.10.

ADV_LLD.1.6C *The low-level design shall describe how each TSP-enforcing function is provided.*

DO-178B section 11.10a satisfies this requirement.

ADV_LLD.1.7C *The low-level design shall identify all interfaces to the modules of the TSF.*

DO-178B section 11.10c satisfies this requirement.

ADV_LLD.1.8C *The low-level design shall identify which of the interfaces to the modules of the TSF are externally visible.*

DO-178B section 11.10c satisfies this requirement.

ADV_LLD.1.9C *The low-level design shall describe the purpose and method of use of all interfaces to the modules of the TSF, providing details of effects exceptions and error messages, as appropriate.*

DO-178B section 5.2.2e as documented in 11.10 satisfies this requirement.

ADV_LLD.1.10C *The low-level design shall describe the separation of the TOE into TSP-enforcing and other modules.*

This is a new requirement, however it can be added when creating the "*Software Design Standards*" in DO-178B section 11.7

Evaluator action elements:

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

ADV_LLD.1.2E *The evaluator shall determine that the low-level design is an accurate and complete instantiation of the TOE security functional requirements.*

DO-178B requires independent validation for levels A and B.

ADV_RCR.2 – Representation Correspondence

The purpose of the ADV_RCR requirements is to develop and demonstrate correspondence between the levels of abstraction.

Dependencies:

No dependencies.

Developer action elements:

ADV_RCR.2.1D *The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.*

DO-178B section 11.14 "*Software Verification Results*" satisfies this requirement when executed under the section 6 guidelines.

Content and presentation of evidence elements:

ADV_RCR.2.1C *For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.*

ADV_RCR.2.2C *For each adjacent pair of provided TSF representations, where portions of both representations are at least semiformally specified, the demonstration of correspondence between those portions of the representations shall be semiformal.*

DO-178B section 11.14 "*Software Verification Results*" satisfies this requirement when executed under the section 6 guidelines and completed in a "semiformal" manner.

Evaluator action elements:

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

DO-178B requires this (with or without independent verification) in levels A-C for most adjacent pairs; for level C the verification is only at the higher levels.

ADV_SPM.3 – Security Policy Modeling

Dependencies:

No dependencies.

Developer action elements:

ADV_SPM.3.1D *The developer shall provide a TSP model.*

A TSP is the security policy to be implemented by the TOE. The developer is required to develop a model of this policy. If the policy is a portion of the system high-level requirements, this will fit under the guidelines of section 5.1 as documented under section11.9.

ADV_SPM.3.2D *The developer shall demonstrate or prove, as appropriate, correspondence between the functional specification and the TSP model*

The actual demonstration/proof will be conducted under the guidelines of section 6.3 as documented in 11.14

Content and presentation of evidence elements:

ADV_SPM.3.1C *The TSP model shall be formal.*

As we have mentioned before, 178B does not directly specify a level of formality, but this requirement can be included in “Software Design Standards”, Section 11.7.

ADV_SPM.3.2C *The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled*

This is a specific sub-requirement to *ADV_SPM.3.1D* and will need to be considered.

ADV_SPM.3.3C *The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.*

ADV_SPM.3.4C *The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.*

ADV_SPM.3.5C *Where the functional specification is semiformal, the demonstration of correspondence between the TSP model and the functional specification shall be semiformal.*

ADV_SPM.3.6C *Where the functional specification is formal, the proof of correspondence between the TSP model and the functional specification shall be formal.*

This is a specific sub-requirement to *ADV_SPM.3.1D* and *ADV_SPM.3.2D* and will need to be considered.

Evaluator action elements:

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

AGD – Guidance Documents

The guidance documents class provides the requirements for user and administrator guidance documentation.

AGD_ADM.1 Administrator Guidance

Dependencies:

ADV_FSP.1 *Informal functional specification*

Developer action elements:

AGD_ADM.1.1D *The developer shall provide administrator guidance addressed to system administrative personnel.*

The DO-178B document does not directly address administrative documentation. Any such guidelines are not within the scope of that document. This could be due to either the fact that 178B focuses on the software development process, or the fact that the software is in airborne systems and not general purpose systems.

Content and presentation of evidence elements:

AGD_ADM.1.1C *The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.*

AGD_ADM.1.2C *The administrator guidance shall describe how to administer the TOE in a secure manner.*

AGD_ADM.1.3C *The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.*

AGD_ADM.1.4C *The administrator guidance shall describe all assumptions regarding user behavior that are relevant to secure operation of the TOE.*

AGD_ADM.1.5C *The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.*

AGD_ADM.1.6C *The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.*

AGD_ADM.1.7C *The administrator guidance shall be consistent with all other documentation supplied for evaluation.*

AGD_ADM.1.8C *The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.*

Evaluator action elements:

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

AGD_USR.1 – User Guidance

Dependencies:

ADV_FSP.1 *Informal functional specification*

Developer action elements:

AGD_USR.1.1D *The developer shall provide user guidance.*

The DO-178B document does not directly address user documentation. Any such guidelines are not within the scope of that document. This could be due to either the fact that 178B focuses on the software development process, or the fact that the software is in airborne systems and not general purpose systems.

Content and presentation of evidence elements:

AGD_USR.1.1C *The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.*

AGD_USR.1.2C *The user guidance shall describe the use of user-accessible security functions provided by the TOE.*

AGD_USR.1.3C *The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.*

AGD_USR.1.4C *The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behavior found in the statement of TOE security environment.*

AGD_USR.1.5C *The user guidance shall be consistent with all other documentation supplied for evaluation.*

AGD_USR.1.6C *The user guidance shall describe all security requirements for the IT environment that are relevant to the user.*

Evaluator action elements:

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

ALC - Life Cycle Support

Life-cycle support establishes discipline and control in the processes of refinement of the TOE during its development and maintenance.

ALC_DVS.1 – Identification of security measures

Dependencies:

No dependencies.

Developer action elements:

ALC_DVS.1.1D *The developer shall produce development security documentation.*

The DO-178B does not require development security documentation. Therefore, in order to comply with CC, such development security documentation must be included in addition to other requirements.

Content and presentation of evidence elements:

ALC_DVS.1.1C *The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality of the TOE design and implementation in its development environment.*

ALC_DVS.1.2C *The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.*

Evaluator action elements:

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

ALC_DVS.1.2E *The evaluator shall confirm that the security measures are being applied.*

ALC_LCD.2 – Standardized life-cycle model

Dependencies:

No dependencies.

Developer action elements:

ALC_LCD.2.1D *The developer shall establish a life-cycle model to be used in the development and maintenance of the TOE.*

The DO-178B specifies that a software planning process be used for the entire project, not just for security aspects. These requirements are discussed in section 4.0. The documentation that is required is described in general in section 11.0. Therefore, to be compliant with both CC and DO-178B, a software planning process should be identified for the entire software project, including a life-cycle model for security. The objectives for the planning process are outlined in section 4.1.

ALC_LCD.2.2D The developer shall provide life-cycle definition documentation.

The software plans required by DO-178B are listed in section 4.3. Guidance for preparing these plans is included in sections 4.3.a, 4.3.b, and 4.3.c. The life-cycle description of the software development plan is described in section 11.2.b. In order to also satisfy CC, this plan should specifically address the security aspects.

ALC_LCD.2.3D The developer shall use a standardized life-cycle model to develop and maintain the TOE.

The DO-178B does not require a standardized life-cycle model. Therefore, in order to meet the CC, a standardized model must be described as part of the Software Development plan described in section 11.2.

Content and presentation of evidence elements:

ALC_LCD.2.1C The life-cycle definition documentation shall describe the model used to develop and maintain the TOE.

The life-cycle description documentation required by DO-178B is described in section 11.2.b. In order to satisfy CC requirements, this description should specifically include a description of the life-cycle definition for security.

ALC_LCD.2.2C The life-cycle model shall provide for the necessary control over the development and maintenance of the TOE.

DO-178B requires review and assurance of the software planning process, described in section 4.6. The software development environment is described in section 4.4.1, and software development standards are described in 4.5. The software development plan, described in section 11.2, documents the standards (11.2.a) and software development environment (11.2.c) to be used. In order to be compliant with CC, this documentation should include a description of the steps taken to establish the necessary control over the development and maintenance of the security issues associated with the TOE.

ALC_LCD.2.3C The life-cycle definition documentation shall explain why the model was chosen.

The DO-179B does not require an explanation why the life-cycle model was chosen.Therefore, in order to meet the CC, such an explanation must be included in the life-cycle model description as specified in 11.2.b.

ALC_LCD.2.4C *The life-cycle definition documentation shall explain how the model is used to develop and maintain the TOE.*

The DO-178B does not require an explanation how the model is used to develop and maintain the TOE. Therefore, in order to satisfy the CC, such an explanation must be included in the life-cycle description as specified in 11.2.b.

ALC_LCD.2.5C *The life-cycle definition documentation shall demonstrate compliance with the standardized life-cycle model.*

DO-178B requires review and assurance of the software planning process. In order to satisfy the CC, this review must demonstrate compliance with the standardized life-cycle model.

Evaluator action elements:

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

DO-178B establishes a review and assurance of the software planning process in section 4.6, and requires that the outputs of each process produce evidence that can be traced to the activities and input associated with the process. In order to comply with CC, this review should also address the security aspects of the project.

ALC_TAT.2 – Compliance with implementation standards

Dependencies:

ADV_IMP.1 *Subset of the implementation of the TSF*

Developer action elements:

ALC_TAT.2.1D *The developer shall identify the development tools being used for the TOE.*

This requirement matches the documentation of tools used as presented in section 11.2.c of DO178-B. Further guidance concerning language and tool selection is described in section 4.4.2.

ALC_TAT.2.2D *The developer shall document the selected implementation-development options of the development tools.*

DO178-B outlines specific requirements for using optimizing features of compilers and other tools, as described in section 4.4.2. In order to comply with CC, this section should

also describe requirements and other consideration for any other development tools, not otherwise covered by DO178-B requirements.

ALC_TAT.2.3D The developer shall describe the implementation standards to be applied.

The documentation of specific standards of implementation is described in section 11.8 of DO178-B. Further guidance concerning development standards is provided in section 4.5.

Content and presentation of evidence elements:

ALC_TAT.2.1C All development tools used for implementation shall be well defined.

DO178-B requires that the software development environment be documented in accordance with section 11.2.c

ALC_TAT.2.2C The documentation of the development tools shall unambiguously define the meaning of all statements used in the implementation.

The documentation required by DO178-B concerning the software development environment, as described in section 11.2.c, shall be considered to be in compliance with CC if it unambiguously defines all the statements used in the implementation.

ALC_TAT.2.3C The documentation of the development tools shall unambiguously define the meaning of all implementation-dependent options.

The documentation required by DO178-B concerning the use of optimizing options of compilers and other tools, as described in section 4.4.2, shall be considered to be in compliance with CC if it unambiguously defines all the statements used in the implementation.

Evaluator action elements:

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

DO178-B provides guidance concerning the review and assurance of the software planning process in section 4.6. This section provides guidance that is consistent with this requirement of the CC.

ALC_TAT.2.2E The evaluator shall confirm that the implementation standards have been applied.

DO178-B provides guidance concerning the review and assurance of the software planning process in section 4.6. This section provides guidance that is consistent with this requirement of the CC.

ATE - Tests

Tests help to establish that the TOE security functional requirements are met. Testing provides assurance that the TOE satisfies at least the TOE security functional requirements.

ATE_COV.2 – Analysis of Coverage

Objectives:

415 *In this component, the objective is to establish that the TSF has been tested against its functional specification in a systematic manner. This is to be achieved through an examination of developer analysis of correspondence.*

Application notes:

416 *The developer is required to demonstrate that the tests which have been identified include testing of all of the security functions as described in the functional specification. The analysis should not only show the correspondence between tests and security functions, but should provide also sufficient information can be used in planning for additional evaluator tests. Although at this level the developer has to demonstrate that each of the functions within the functional specification has been tested, the amount of testing of each function need not be exhaustive.*

Dependencies:

ADV_FSP.1	*Informal functional specification*
ATE_FUN.1	*Functional testing*

Developer action elements:

ATE_COV.2.1D *The developer shall provide an analysis of the test coverage.*

DO178-B requires test coverage analysis, described in section 6.4.4. The CC requirement shall be considered to have been met if this test coverage analysis includes the security functions of the TOE.

Content and presentation of evidence elements:

ATE_COV.2.1C *The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.*

DO178-B specifies that an analysis should be done to determine that test coverage includes requirements-based coverage, described in section 6.4.4.1. The CC requirement

shall be considered to have been met if this test coverage analysis includes the security functions of the TOE.

ATE_COV.2.2C *The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.*

DO178-B specifies that an analysis should be done to determine that the test cases, procedures, and results are accurate and complete, as described in section 6.3.6. The CC requirement shall be considered to have been met if this test coverage analysis includes the security functions of the TOE.

Evaluator action elements:

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

ATE_DPT.2 – Testing low-level design

Objectives:

428 *The subsystems of a TSF provide a high-level description of the internal workings of the TSF. Testing at the level of the subsystems, in order to demonstrate the presence of any flaws, provides assurance that the TSF subsystems have been correctly realized.*

429 *The modules of a TSF provide a description of the internal workings of the TSF. Testing at the level of the modules, in order to demonstrate the presence of any flaws, provides assurance that the TSF modules have been correctly realized*

Application notes:

430 *The developer is expected to describe the testing of the high-level design of the TSF in terms of "subsystems". The term "subsystem" is used to express the notion of decomposing the TSF into a relatively small number of parts.*

431 *The developer is expected to describe the testing of the low-level design of the TSF in terms of "modules". The term "modules" is used to express the notion of decomposing each of the "subsystems" of the TSF into a relatively small number of parts.*

Dependencies:

ADV_HLD.2 *Security enforcing high-level design*
ADV_LLD.1 *Descriptive low-level design*
ATE_FUN.1 *Functional testing*

Developer action elements:

ATE_DPT.2.1D *The developer shall provide the analysis of the depth of testing.*

DO178-B describes the analysis that must be performed for the high-level requirements in section 6.3.1, and low-level requirements in section 6.3.2. Also, it requires that test cases be developed for normal-range values (section 6.4.2.1) and Robustness (section 6.4.2.2). This analysis satisfies the CC requirement if it includes an analysis for the security functions of the TOE.

Content and presentation of evidence elements:

ATE_DPT.2.1C *The depth analysis shall demonstrate that the identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design and low-level design.*

DO178-B specifies that the test cases, procedures and results be accurate and complete in section 6.3.6. The software testing process itself is discussed in section 6.4. In order to comply with the CC, this section must include the security functions of the TOE.

Evaluator action elements:

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

ATE_FUN.1 – Functional testing

Objectives:

445 *The objective is for the developer to demonstrate that all security functions perform as specified. The developer is required to perform testing and to provide test documentation.*

Dependencies:

No dependencies.

Developer action elements:

ATE_FUN.1.1D *The developer shall test the TSF and document the results.*

DO178-B describes the software testing process in section 6.4. In order to comply with the CC, this testing process must include the security functions of the TOE.

ATE_FUN.1.2D *The developer shall provide test documentations.*

DO178-B requires documentation of verification cases and procedures in section 11.13 and software verification results in section 11.14. In order to comply with the CC, these documents must include the security functions of the TOE.

Content and presentation of evidence elements:

ATE_FUN.1.1C *The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test reults.*

DO178-B describes the required software testing process in section 6.4. It requires that a software verification plan be developed in section 11.3. The required software verification cases and procedures are described in section 11.13. Software verification results are described in section 11.14. In order to comply with the CC, these documents must include the security functions of the TOE.

ATE_FUN.1.2C *The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.*

DO178-B specifies in section 11.13b that documentation for each test case, including the purpose of the test case, be specified. In order to comply with the CC, this documentation must include the security functions of the TOE.

ATE_FUN.1.3C *The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.*

DO178-B describes the test environment considerations for developing test procedures in section 6.4.1. Test case selection is discussed in section 6.4.2. Documentation of each test case should include the inputs, conditions, expected results, and pass/fail criteria, as described in section 11.13b. The step-by-step instructions for the set-up and execution of each test, including the test environment and how test results are evaluated, are described in section 11.13c. In order to comply with the CC, these documents must include the security functions of the TOE.

ATE_FUN.1.4C *The expected test results shall show the anticipated outputs from a successful execution of the tests.*

DO178-B requires documentation of expected test results, as described in sections 11.13b and 11.13c. In order to comply with the CC, these documents must include the security functions of the TOE.

ATE_FUN.1.5C *The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.*

DO178-B requires documentation of software verification test results in sections 11.14. In order to comply with the CC, these documents must include the security functions of the TOE.

Evaluator action elements:

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

ATE_IND.2 – Independent testing - sample

Objectives:

462 *The objective is to demonstrate that the security functions perform as specified. Evaluator testing includes selecting and repeating a sample of the developer tests.*

Application notes:

463 *The intent is that the developer should provide the evaluator with materials necessary for the efficient reproduction of developer tests. This may include such things as machine-readable test documentation, test programs, etc.*

464 *This component contains a requirement that the evaluator has available test results from the developer to supplement the program of testing. The evaluator will repeat a sample of the developer's tests to gain confidence in the results obtained. Having established such confidence the evaluator will build upon the developer's testing by conducting additional tests that exercise the TOE in a different manner. By using a platform of validated developer test results the evaluator is able to gain confidence that the TOE operates correctly in a wider range of conditions than would be possible purely using the developer's own efforts, given a fixed level of resource. Having gained confidence that the developer has tested the TOE, the evaluator will also have more freedom, where appropriate, to concentrate testing in areas where examination of documentation or specialist knowledge has raised particular concerns.*

Dependencies:

ADV_FSP.1	*Informal functional specification*
AGD_ADM.1	*Administrator guidance*
AGD_USR.1	*User guidance*
ATE_FUN.1	*Functional testing*

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

DO178-B requires that independent verification of test procedures and test results be performed only for software level A certification, as indicated by table A-7. Software level A is defined in section 2.2.2. Software level A also requires that all tests (not just a subset) be performed; thus, software level A certification exceeds the requirements of the CC EAL5 if the security functions of the TOE are included in the testing. For systems that are certified for other software levels of DO178-B, independent testing must be performed separately, for the security functions of the TOE, in order to meet the CC.

Content and presentation of evidence elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

DO178-B requires independent testing for software level A, but does not specify who shall provide the testing resources. It does not require independent testing for other software levels. Therefore, in order to fully comply with the CC, the developer must provide resources for testing the security functions of the TOE.

Evaluator action elements:

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

ATE_IND.2.2E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

For software level A, DO178-B requires independent testing of all functions of the software system, not just a subset. Therefore, if the security functions of the TOE are included in the test, software level A conformance also implies CC conformance. For other software levels, a subset of the security functions must be independently tested, in addition to any other DO178-B requirements.

ATE_IND2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA – Vulnerability Assesment

AVA_CCA.1 – Covert Channel Analysis

Objectives:

471 *The objective is to identify covert channels that are identifiable, through an informal search for covert channels.*

No correspondence to DO-178B.

Dependencies:

ADV_FSP.2	*Fully defined external interfaces*
ADV_IMP.2	*Implementation of the TSF*
AGD_ADM.1	*Administrator guidance*
AGD_USR.1	*User guidance*

Developer action elements:

AVA_CCA.1.1D *The developer shall conduct a search for covert channels for each information flow control policy.*

AVA_CCA.1.2D *The developer shall provide covert channel analysis documentation.*

Content and presentation of evidence elements:

AVA_CCA.1.1C *The analysis documentation shall identify covert channels and estimate their capacity.*

AVA_CCA.1.2C *The analysis documentation shall describe the procedure used for determining the existence of covert channels, and the information needed to carry out the covert channel analysis.*

AVA_CCA.1.3C *The analysis documentation shall describe all assumptions made during the covert channel analysis.*

AVA_CCA.1.4C *The analysis documentation shall describe the method used for estimating channel capacity, based on worst-case scenarios.*

AVA_CCA.1.5C *The analysis documentation shall describe the worst case exploitation scenario for each identified covert channel.*

Evaluator action elements:

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

AVA_CCA.1.2E *The evaluator shall confirm that the results of the covert channel analysis show that the TOE meets its functional requirements.*

AVA_CCA.1.3E *The evaluator shall selectively validate the covert channel analysis through testing.*

AVA_MSU.2 -- Misuse

Objectives:

492 *The objective is to ensure that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. In this component, an analysis of the guidance documentation by the developer is required to proved additional assurance that the objective has been met.*

No correspondence to DO-178B.

Dependencies:

ADO_IGS.1	*Installation, generation and start-up procedures.*
ADV_FSP.1	*Informal functional specification*
AGD_ADM.1	*Administrator guidance*
AGD_USR.1	*User guidance*

Developer action elements:

AVA_MSU.2.1D *The developer shall provide guidance documentation.*

AVA_MSU.2.2D *The developer shall document an analysis of the guidance documentation.*

Content and presentation of evidence elements:

AVA_MSU.2.1C *The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure of operational error), their consequences and implications for maintaining secure operation.*

AVA_MSU.2.2C *The guidance documentation shall be complete, clear, consistent and reasonable.*

AVA_MSU.2.3C *The guidance documentation shall list all assumptions about the intended environment.*

AVA_MSU.2.4C *The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).*

AVA_MSU.2.5C *The analysis documentation shall demonstrate that the guidance documentation is complete.*

Evaluator action elements:

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

AVA_MSU.2.2E *The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.*

AVA_MSU.2.3E *The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.*

AVA_MSU.2.4E *The evaluator shall confirm that the analysis documentation shows that guidance is provided for secure operation in all modes of operation of the TOE.*

AVA_SOF.1 – Strength of TOE Security Functions

No correspondence to DO_178B.

Dependencies:

ADV_FSP.1 *Informal functional specification*
ADV_HLD.1 *Descriptive high-level design*

Developer action elements:

AVA_SOF.1.1D *The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.*

Content and presentation of evidence elements:

AVA_SOF.1.1C *For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.*

AVA_SOF.1.2C *For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.*

Evaluator action elements:

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

AVA_SOF.1.2E *The evaluator shall confirm that the strength claims are correct.*

AVA_VLA.3 – Vulnerability Analysis

Objectives:

512 *A vulnerability analysis is performed by the developer to ascertain the presence of security vulnerabilities, and to confirm that they cannot be exploited in the intended environment for the TOE.*

513 *The evaluator performs independent penetration testing, supported by the evaluator's independent vulnerability analysis, to determine that the TOE is resistant to penetration attacks performed by attackers possessing a moderate attack potential.*

Dependencies:

ADV_FSP.1	*Informal functional specification*
ADV_HLD.2	*Security enforcing high-level design*
ADV_IMP.1	*Subset of the implementation of the TSF*
ADV_LLD.1	*Descriptive low-level design*
AGD_ADM.1	*Administrator guidance*
AGD_USR.1	*User guidance*

Developer action elements:

AVA_VLA.3.1D *The developer shall perform and document an analysis of the TOE deliverables searching for ways in which a user can violate the TSP.*

AVA_VLA.3.2D *The developer shall document the disposition of identified vulnerabilities.*

Content and presentation of evidence elements:

AVA_VLA.3.1C *The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.*

AVA_VLA.3.2C *The documentation shall justify that the TOE, with the identified vulnerabilities, is resistant to obvious penetration attacks.*

AVA_VLA.3.3C *The evidence shall show that the search for vulnerabilities is systematic.*

Evaluator action elements:

AVA_VLA.3.1E	*the evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.*
AVA_VLA.3.2E	*The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure the identified vulnerabilities have been addressed.*
AVA_VLA.3.3E	*The evaluator shall perform an independent vulnerability analysis.*
AVA_VLA.3.4E	*The evaluator shall perform independent penetration testing, based on the independent vulnerability analysis, to determine the exploitability of additional identified vulnerabilities in the intended environment.*
AVA_VLA.3.5E	*The evaluator shall determine that the TOE is resistant to penetration attacks performed by an attacker possessing a moderate attack potential.*