Doctoral Dissertation

Supporting Environment for IT System Security Evaluation based on ISO/IEC 15408 and ISO/IEC 18045

Da Bao

Graduate School of Science and Engineering,
Saitama University

Supervisor: Professor Yuichi Goto

March 2019

Abstract

The standardization of IT system security is always a common issue all over the world. The security of a system is only as strong as the weakest link. For software engineering, the link means each task in different process, such as design, implementation, test, operation, maintenance and so on. The whole security of IT systems can be guaranteed only when each task has been performed properly according to consistent standard.

ISO/IEC 15408 and ISO/IEC 18045 are a pair of international standards for information security evaluation. Rigorous evaluation based on the two ISO standards provides a unified way of comparisons among IT systems, such that the developers can rationally show the security strength of their products and the customers can easily choose suitable systems according to the evaluation results. ISO/IEC 15408 and ISO/IEC 18045 establish a trustworthy relationship with common basis among all stakeholders of the target system, wherefore ISO/IEC 15408 and ISO/IEC 18045 are widely used as national standard all over the world.

Security evaluation based on ISO/IEC 15408 and ISO/IEC 18045 is very complex. The whole security evaluation process can be summarized as evaluators receive the evaluation evidence from the developer performs the evaluation activities and provides the results of the evaluation assessment. Evaluators perform evaluation activities to verify whether the target system complies with ISO/IEC 15408 and ISO/IEC 18045. Although, two ISO standards have given a set of instructions to guide the evaluation activities and specified detailed procedures how to carry out those activities. It is not clear enough and difficult even for experienced evaluators to accomplish the security evaluation. The security evaluation process involves tens of documents and a wide variety of tasks. Such heavy work shall cost lots of time and complex evaluation activities may cause evaluators making mistakes. Moreover, to manage a lot of intermediate data in evaluation process is difficult even for experienced evaluators. It is also difficult to ensure that evaluation is fair and transparent. Although each evaluator tries to evaluate a target system earnestly, evaluation results may be different among evaluators because of evaluators' biases. These issues not only may result in consuming a lot of time, but also may affect the correctness, accuracy, and fairness of evaluation results. Thus, it is necessary to provide a supporting environment that supports all relevant tasks in the evaluation process to reduce the complexity of all evaluators' work and guarantee the quality of evaluation results at the same time. However, there is no such environment existing until now.

This thesis presents a supporting environment for IT system security evaluation based on ISO/IEC 15408 and ISO/IEC 18045 that integrates various supporting tools to perform a complete process of security evaluation on the target IT system. This supporting environment can provide facilities for evaluators to perform all tasks in the evaluation process in a guided order. This supporting environment can promote each task with locating the relevant contents in tens of documents and providing helpful information or functions for evaluators to determine whether

these relevant contents are up to the standard. The supporting environment can provide facilities for evaluator to manage all evaluation-relevant documents, intermediate information and their reviews on the target systems during the evaluation.

To provide full facilities for performing the security evaluation process, we firstly analyzed the whole security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045 and clarified 674 necessary evaluation tasks. We also clarified the procedure and detailed actions for each task. Under the consideration that tasks with similar procedural pattern can be supported by the same method, we then classified the detailed evaluation tasks into 7 groups according to the pattern in the procedures and proposed appropriate supporting methods for each group of evaluation tasks. According to these supporting methods, we designed and implemented each necessary supporting tool. Considering the complicated relationship among various evaluation tasks, we clarified the sequence of evaluation tasks and implement a supporting tool to guide evaluators perform all tasks in right order. We analyzed all evaluation-relevant documents, intermediate information and evaluators' reviews, and then designed matched formats to transfer these information into structured data that can be easily managed and used in the evaluation process.

We then evaluated the completeness, usability and efficiency of the evaluation supporting environment. We proposed an evaluation method to show the completeness of this supporting environment and evaluated it at design level and implementation level based on the method. We then discussed how this supporting environment is capable and useful to provide comprehensive facilities to perform all tasks in evaluation base ISO/IEC 15408 and ISO/IEC 18045. We also show the efficiency of this supporting environment by comparing the consumed time between evaluation with this supporting environment and a normal evaluation.

Acknowledgements

I would like to express my special thanks to my supervisors, Associate Professor Yuichi Goto and Professor Jingde Cheng for their enthusiastic guidance, understanding, and invaluable support on all aspects of academic life to help me accomplish my thesis and let me have the chance to pursue my doctoral degree.

I am very grateful to my thesis committee: Professor Norihiko Yoshida, Professor Noriaki Yoshiura, Associate Professor Jun OHKUBO for their support, invaluable feedback, and helpful advice to this research.

I would also like to thank other AISE lab members who have helped me in my PhD research. I would also like to express my special thanks to my family and friends for their unfailing support through the hard moments of my graduate studies.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

The standardization of IT system security is always a common issue all over the world. The security of a system is only as strong as the weakest link. For software engineering, the "link" means each task in different process, such as design, implementation, test, operation, maintenance and so on. The whole security of IT systems can be guaranteed only when each task has been performed properly according to consistent standard.

ISO/IEC 15408 [1][2][3] and ISO/IEC 18045 [4] are a pair of international competitive standards for information security evaluation. Rigorous evaluation based on the two ISO standards provides a unified way of comparisons among IT systems, such that the developers can rationally show the security strength of their products and the customers can easily choose suitable systems according to the evaluation results. ISO/IEC 15408 and ISO/IEC 18045 establish a trustworthy relationship with common basis among all stakeholders of the target system, wherefore ISO/IEC 15408 and ISO/IEC 18045 are widely used as national standard all over the world.

Security evaluation based on ISO/IEC 15408 and ISO/IEC 18045 is very complex. The whole security evaluation process can be summarized as evaluators receive the evaluation evidence from the developer performs the evaluation activities and provides the results of the evaluation assessment. Evaluators perform evaluation activities to verify whether the target system complies with ISO/IEC 15408 and ISO/IEC 18045. Although, two ISO standards have given a set of instructions to guide the evaluation activities and specified detailed procedures how to carry out those activities. It is not clear enough and difficult even for experienced evaluators to accomplish the security evaluation. The security evaluation process involves tens of documents and a wide variety of tasks. Such heavy work shall cost lots of time and complex evaluation activities may cause evaluators making mistakes. Moreover, to manage a lot of intermediate data in evaluation process is difficult even for experienced evaluators. It is also difficult to ensure that evaluation is fair and transparent. Although each evaluator tries to evaluate a target system earnestly, evaluation results may be different among evaluators because of evaluators' biases. These issues not only may result in consuming a lot of time,

but also may affect the correctness, accuracy, and fairness of evaluation results. Thus, it is necessary to provide a supporting environment that supports all relevant tasks in the evaluation process to reduce the complexity of all evaluators's work and guarantee the quality of evaluation results at the same time. However, there is no such environment existing until now.

1.2 Related Works

From view point of information security engineering, some approaches have been proposed.

An approach [13] was proposed to support model-based security engineering using UML (Unified Modeling Language) by providing tool-support for the analysis of UML models for security requirements. This approach utilizes the automated theorem-prover (ATP) SETHEO to verify the security properties. A threat and risk-driven methodology was proposed [14] to security requirement engineering. This methodology extends the security engineering process using patterns by a threat and risk-driven procedure to select adequate security mechanisms. Systems Security Engineering Capability Maturity Model (SSE-CMM) [10, 11] is a model that describes the essential systems security processes and management tasks in organizations. It can be used to indicate the development capability of organizations. A security engineering methodology [12] was proposed for analyzing, designing, developing, testing, and maintaining secure enterprise information systems. It combined security risk control, enterprise security architecture, and security management as an integrated framework.

ISEE [15, 16, 17], an information security engineering environment, was proposed to provide comprehensive facilities to support design, development, management, and maintenance of security facilities of information systems continuously and consistently, and guides and helps all users to perform their tasks regularly according to ISO/IEC security standards. Developing ISEE is an ongoing work [18, 19, 21, 20]. The core component of ISEE is Information Security Engineering Database ISEDS [18, 22, 23]. ISEDS manages all of information-security-relative ISO standards, such as ISO/IEC 15408, ISO/IEC 18045, ISO/IEC 15408 and ISO/IEC 18045 etc., and documents related with the standards, and provides integrated tools with the standards and documents. Each supporting tool of ISEE supports users to doing one or several tasks in software life cycle processes. Appropriate life cycle models were proposed to guide the sequence of executing tasks [19, 24]. Analysis of which tasks can be supported by software tools were done. Software supportable tasks relating to ISO/IEC 15408 [25, 26] and ISO/IEC 15408 and ISO/IEC 18045 [24] were analyzed and clarified. The supporting tools for corresponding supportable tasks [17, 26] were also proposed. Several tools were developed [28, 20, 29, 21].

However, the original purpose of ISO/IEC 15408 and ISO/IEC 18045 is to compare the security capability among different information systems. there is still no environment or software tools to support the evaluation process based on two ISO standards from view point of third party and independent IT system

evaluation.

1.3 Purpose and Objectives

This thesis presents a supporting environment for IT system security evaluation based on ISO/IEC 15408 and ISO/IEC 18045 that integrates various supporting tools to perform a complete process of security evaluation on the target IT system. This supporting environment can provide facilities for evaluators to perform all tasks in the evaluation process in a guided order. This supporting environment can promote each task with locating the relevant contents in tens of documents and providing helpful information or functions for evaluators to determine whether these relevant contents are up to the standard. This is the first supporting environment to support the whole security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045.

To provide full facilities for performing the security evaluation process, we firstly analyzed the whole security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045 and clarified 674 necessary evaluation tasks. We also clarified the procedure and detailed actions for each task. Under the consideration that tasks with similar procedural pattern can be supported by the same method, we then classified the detailed evaluation tasks into 7 groups according to the pattern in the procedures and proposed appropriate supporting methods for each group of evaluation tasks. According to these supporting methods, we designed and implemented each necessary supporting tool. Considering the complicated relationship among various evaluation tasks, we clarified the sequence of evaluation tasks and implement a supporting tool to guide evaluators perform all tasks in right order. We analyzed all evaluation-relevant documents, intermediate information and evaluators' reviews, and then designed matched formats to transfer these information into structured data that can be easily managed and used in the evaluation process.

We then evaluated the completeness, usability and efficiency of the evaluation supporting environment. We proposed an evaluation method to show the completeness of this supporting environment and evaluated it at design level and implementation level based on the method. We then discussed how this supporting environment is capable and useful to provide comprehensive facilities to perform all tasks in evaluation base ISO/IEC 15408 and ISO/IEC 18045. We also show the efficiency of this supporting environment by comparing the consumed time between evaluation with this supporting environment and a normal evaluation.

1.4 Structure of This Thesis

This thesis is organized as follows. Chapter 1 presents the background, motivation, and purpose of this research. Chapter 2 gives explanations about international standards ISO/IEC 15408 and ISO/IEC 18045, the evaluation process based on two ISO standards and the difficulties of promoting the evaluation process. Chapter 3 provides an analysis of tasks and documents in the evaluation process and provides

a set of supporting methods to perform these evaluation tasks. Chapter 4 presents the supporting environment, which integrated a series support tools to promote all evaluation tasks in the evaluation process. Chapter 5 presents an evaluation of this supporting environment, and conclusions are given in Chapter 6.

Chapter 2

Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045

2.1 Overview

ISO/IEC 15408 and ISO/IEC 18045[1][4] is a set of international competitive standards for security evaluation of IT systems. ISO/IEC 15408 and ISO/IEC 18045 establish a trustworthy relationship with common basis among all stakeholders of the target system that is evaluated and certified, and therefore ISO/IEC 15408 and ISO/IEC 18045 are widely used all over the world. ISO/IEC 15408 gives a unified vocabulary to describe security characteristics of the target systems. ISO/IEC 18045 provides a set of instructions that can be followed to conduct an ISO/IEC 15408 evaluation on the target system. These instructions describe the minimum actions to be performed in the evaluation.

The whole security evaluation schemas based on ISO/IEC 15408 and ISO/IEC 18045 can be summarized as evaluators receive the evaluation relevant document (called evaluation evidence) from the developer performs the evaluation activities and provides the results of the evaluation assessment. However, there is several difficulties in security evaluation process. This section introduces ISO/IEC 15408 and ISO/IEC 18045, explains the evaluation process based on two ISO standards and points out the difficulties of promoting the evaluation process.

2.2 ISO/IEC 15408 (Common Criteria)

ISO/IEC 15408 [1] (also known as Common Criteria, CC) is an international standard for evaluation and certification of security facilities in IT systems. The Common Criteria is the result of the integration of information technology and computer security criteria. In 1983 the US issued the Trusted Computer Security Evaluation Criteria (TCSEC), which became a standard in 1985. Criteria developments in Canada and European ITSEC countries followed the original US TCSEC work. The US Federal Criteria development was an early attempt to combine

these other criteria with the TCSEC, and eventually led to the current pooling of resources towards production of the Common Criteria. Version 1.0 of the CC was published for comment in January 1996. Version 2.0 took account of extensive review and trials during the next two years and was published in May 1998. Version 2.0 was adopted by the International Organization for Standards (ISO) as an International Standard (ISO/IEC 15408) in 1999.

In 2005, the interpretations that had been made to date were incorporated into an update, version 2.3. This was published as ISO/IEC 15408-1:2005, 15408-2:2005, and 15408-3:2005; ISO/IEC 15408 provides common criteria of security evaluation and certification for IT systems and gives a unified vocabulary to describe security characteristics of the target systems.The standard is composed of 3 parts, CC part 1 provides overview of the whole standards. CC part 2 Security functional components establishes a set of functional components as a standard template of expressing the functional requirements for target information systems. CC part 3 Security assurance components establishes a set of assurance components as a standard way of expressing the assurance requirements for target information systems.

2.3 ISO/IEC 18045 (Common Evaluation Methodology)

ISO/IEC 18045 (also known as Common Evaluation Methodology, CEM) [4] is a companion standard to the CC. The CEM defines the minimum actions to be performed by an evaluator using the criteria and evaluation evidences defined in the CC, in order to conduct a evaluation result [7-9]. This common methodology is the basis upon which the member nations have agreed to recognize the evaluation results of one another, as specified in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security. This was first signed in 2000 and additional member nations continue to join this agreement. The corresponding ISO standards was created as well and named as ISO/IEC 18045 [12].

ISO/IEC 18045 is provides a set of instructions that can be followed to conduct an ISO/IEC 15408 evaluation on the target system. ISO/IEC 18045 describe the activities, sub-activities to be performed by different participants in the evaluation process corresponding with CC.

There are direct relationships between the CC structure (i.e. class, family, component and element) and the structure of the CEM. The CC has organised the components in CC Part 2 and CC Part 3 into hierarchical structures: class component element is provided to assist consumers, developers and evaluators in locating specific components [7]. Figure 2.1 illustrates the correspondence between the CC constructs of class, family and evaluator action elements and CEM activities, sub-activities and actions. However, several CEM tasks may result from the requirements noted in CC developer action and content and presentation elements.

2.4 Security Evaluation and Certification Based on ISO/IEC 15408 and ISO/IEC 18045

The whole security evaluation schemas based on ISO/IEC 15408 and ISO/IEC 18045 can be summarized as evaluators receive the evaluation relevant document (called evaluation evidence) from the developer performs the evaluation activities and provides the results of the evaluation assessment. The Fig. 2.1 shows an evaluation process in ISO/IEC 15408 and ISO/IEC 18045 certificate schema. The

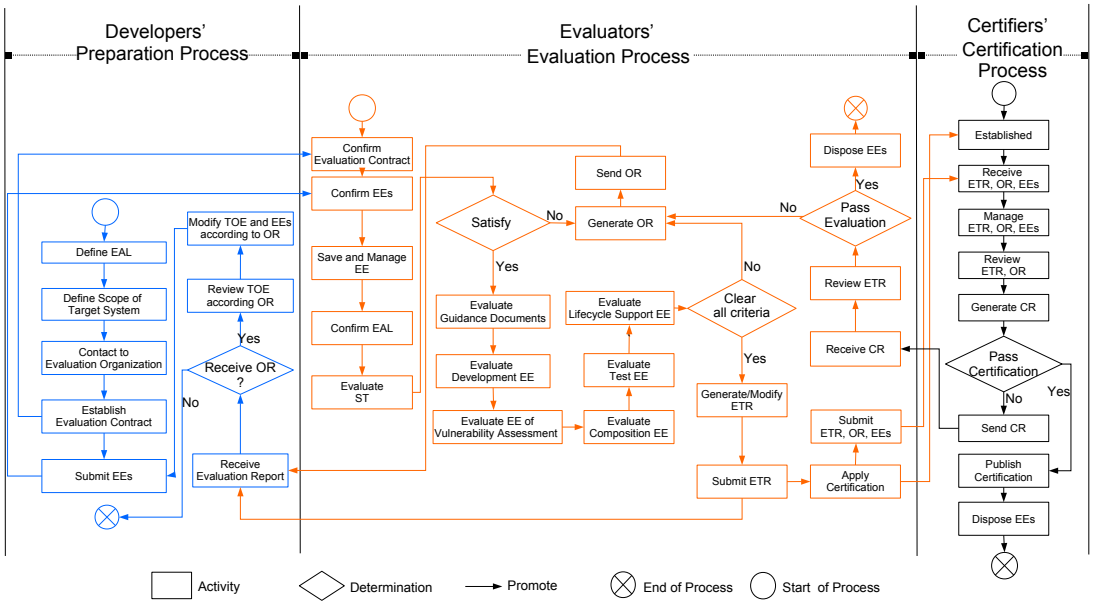


Figure 2.1: Evaluation Process Based on ISO/IEC 15408 and ISO/IEC 18045

evaluation process consists of three sub-processes: evaluation evidence preparing process, evaluation performing process, evaluation certifying process. Participants of those sub-processes are developers, evaluators and certifiers respectively.

In evaluation evidences preparing process, developers are responsible for providing and modifying evaluation evidences (EEs). At first, developers specify the evaluation assurance level (EAL) of a target system or part of security facilities of target system (Target of evaluation, target system) and submit EEs to evaluators. Then developers shall modify or improve the target system continuously based on analysis of Observation Reports (ORs) until the target systems gets certification.

In evaluation performing process, evaluators are responsible for evaluating a target system by EEs and producing evaluation results. First, evaluators save and manage EEs. Second, evaluators perform evaluation activities according to CEM to verdict whether a target system is satisfying CC. In the case of a fail verdict, the evaluator shall provide an OR to reflect the evaluation result or express clarification needs. Until there is no more fail verdict, evaluators shall provide Evaluation Technical Report (ETR) which presents technical justification of the target systems security situation to certifiers.

In evaluation certifying process, certifiers are responsible for judging ETRs and ORs and publishing certification for target system. The Certificate Authority shall verdict ETR and give Certification Review (CR), and evaluators present OR to developers according to CR.

Moreover, through the whole evaluation process, evaluators shall ensure all evaluation evidences and intermediate products are maintained the confidentiality and protected from alteration or loss. When the target system evaluation is completed, evaluators shall deliver ETR and OR (if available) to the evaluation authority, and control the disposal of evaluation evidences by returning, archiving or destroying.

2.5 Difficulties in Security Evaluation Process

Participants in an evaluation process based on ISO/IEC 15408 and ISO/IEC 18045 maybe faced with several difficulties. These difficulties may not only result in consuming a lot of time and money, but also cause the target audiences doubt the certification of evaluation result. By do research about evaluation process based on ISO/IEC 15408 and CEM certificate schema, we summarized the excising difficulties during evaluation process and divided them into 8 kinds as following:

D1: D1: It is difficult for evaluators to protect documents from loss and alteration, because the whole evaluation process involves 34 kinds of documents and 3 kinds participants, each document may be used many times by different kinds of participants.

D2: It is a challenge for evaluators to find specific document from a large number of documents. And there are some situations evaluators need to search specific information from long and complex evaluation evidences. It is hard and time-consuming work even for experienced evaluators.

D3: It is a challenge to ensure that all evaluation evidences are maintained the confidentiality because there are many participants in evaluation process and an evaluation evidence may be used times.

D4: It is a challenge for evaluation authority to ensure that their evaluators perform all activities satisfying a certain level of quality. It is difficult for evaluators to follow the ISO/IEC 18045 because the standard is not easy to understand. Different evaluators may understand the standards in different levels. Even if the evaluators understand the standards, the huge number of sub-activities cause mistakes in intermediate products and evaluation results.

D5: It is difficult to ensure that evaluation is fair and transparent. Although each evaluator tries to evaluate a target system earnestly, evaluation results may be different among evaluators because of evaluators biases.

D6: It is also a difficult for evaluation authority to ensure all evaluation activities are performed in an appropriate sequence. Because there are some dependencies between some sub-activities, and the relating sub-activities may be performed by different evaluators.

D7: It is not easy to balance their work schedule and ensure intermediate products exchanged safely.

D8: It is difficult to ensure that the generated ETRs or ORs according to the ISO/IEC 18045 requirements, because ISO/IEC 18045 is not easy to understand and evaluators may have different understanding of necessary content and regular structure of ETR or OR.

Considering of the wide use of ISO/IEC 15408 and ISO/IEC 18045 based evaluation and the complexity of evaluators work, it is necessary to provide a supporting environment which can supporting all evaluation tasks related to security evaluation and also can support management of all documents and intermediate products in the whole evaluation process to reduce human mistakes, and ensure fairness and transparency. Such that the credibility of evaluation result can be improved and the complexity of evaluation process can be reduced.

Chapter 3

Supporting Security Evaluation Process

3.1 Overview

To clarify what kind of support can be provided for the security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045, we deeply analyzed the whole process of security evaluation. ISO/IEC 18045 provided some instruction tasks to guide evaluation activities, but these instruction is not clear enough. Therefore, we proposed a set of rules to divide these instruction into detailed evaluation tasks (minimum unit of evaluation work). We also clarified the procedure of each task.

Considering detailed evaluation tasks having similar procedural pattern can be supported by the same method, we then classified the detailed evaluation tasks into 7 groups according to the pattern in the procedures and proposed appropriate supporting methods for each group of evaluation tasks. According to these supporting methods, we designed and implemented each necessary supporting tool.

Beside of containing a lot of various tasks, the complicated security evaluation process also involves many documents. We find all relevant document and proposed XML-base templates for manage them in a structured way.

3.2 Analyze and Clarify Evaluation Tasks Based on ISO/IEC 18045

Although, ISO/IEC 18045 has give a set of original evaluation tasks to guide the following evaluation activities: evaluation activities on verifying and validating Security Targets (ASE), evaluation activities on examining development process (ADV), evaluation activities on examining guidance document (AGD), evaluation activities on examining life-cycle support process (ALC), evaluation activities on examining test process (ATE), evaluation activities on examining vulnerability assessment process (AVA), and evaluation activities on examining the composition process (ACO). However, some are not clear enough to develop software supporting tools by which the evaluation works can be performed more efficiently. Therefore,

we clarified the original set of evaluation tasks by following two rules.

Some original evaluation tasks required a lot of different steps, which required each step to be separated into a separate evaluation task. Basically, we need one of the evaluation tasks to correspond to only one step of the evaluation works. Therefore, we clarified some original complicate tasks into several simple ones.

Some original evaluation tasks contains some implicit actions that the evaluators need to extract specific parts from varied documents and save them in a specific format for other evaluation tasks. These actions should be separated into an individual evaluation tasks because the extracted parts could be reused many times in other evaluation tasks. Such kind of original tasks refer to comparing and checking different parts of varied documents. The original descriptions in ISO/IEC 18045 usually include the quantifiers such as "all ...", "for each ...", etc. The extracted parts like that can be easily organized and managed as kinds of lists.

We has clarified the original evaluation tasks and found 674 detailed evaluation tasks: 168 detailed tasks about evaluation on Security Targets, 129 detailed tasks about evaluation on development process, 11 detailed tasks about evaluation on the guidance document process, 133 detailed tasks about evaluation on life-cycle support process, 70 detailed tasks about evaluation on test process, 86 detailed tasks about evaluation on vulnerability assessment process, and 77 detailed tasks about evaluation on composition process. The Appendix A listed all detailed evaluation tasks and shown the description of each task.

3.3 Classify Detailed Evaluation Tasks Based on ISO/IEC 18045

We analyzed each detailed evaluation task and found that some tasks have similar pattern with each other. Therefore we classified the detailed tasks into 7 groups.

- **Sufficiency and Necessity of Content**

  The tasks in this group is about examining whether the contents is sufficient or necessary or possible to occur misunderstanding for the documentation relating to the under-evaluation system.

  procedure pattern

  1. Select the target document relating to the task.
  2. Find out **the section** relating to the task.
  3. Examine the content in these sections whether the contents is sufficient or necessary or possible to occur misunderstanding for this ST according to the provided explanations and tips.

  For example, "The evaluator shall examine the operational user guidance to determine that it is reasonable." This task need the evaluator to check the rationality of the target document's contents. The 'operational user guidance' usually means user manuals.

- **Sufficiency and Necessity of Inside Relationship**

  The tasks in this group is about examining whether the relationship between different parts in single document relating to the evaluation.

  procedure pattern

  1. Select the tasks about the relationship between two parts in the single document.
  2. Find out **these sections** , that reflect the relationship.
  3. Examine the sufficiency and necessity of the relationship by analysis the contents of these sections according to the provided explanations and tips.

  For Example, "The evaluator shall examine the development information to determine the correspondence, between the interfaces of the base component and the interfaces on which the dependent component relies, is accurate." This task need the evaluator to check whether it is correct about the dependency of the different parts in development information (a document, usually referring to design documents) or not.

- **Correctness of Outside Relationship**

  The tasks in this group is about examining whether claimed relationship between different documents is the same as actual relationship.

  procedure pattern

  1. Select the tasks about the relationship between different documents.
  2. Find out these **the elements** in the first document and second document relating to tasks.
  3. Examine the sufficiency and necessity of the relationship by analysis the contents of these sections according to the provided explanations and tips.

  For example, "The evaluator shall examine the test coverage analysis to determine that the correspondence between the interfaces in the functional specification and the tests in the test documentation is complete." This task need the evaluator to check whether the interfaces mentioned in test documents (usually referring to test cases document) is all appearing in the functional specification or not.

- **Sufficiency and Necessity of Outside Relationship**

  The tasks in this group is about examining whether claimed relationship between different documents is the same as actual relationship.

  procedure pattern

  1. Select the tasks about the relationship between different documents.

2. Find out these **the elements** in the first document and second document relating to tasks.
3. Examine whether the set of elements in first document has one different element from or is a subset of elements in the second document by comparing the two sets.

For example, "The evaluator shall examine the mapping between the TOE (Target of Evaluation) design description and the sample of the implementation representation to determine that it is accurate." This task need the evaluator to check whether it is correct about the mapping between the TOE design description in ST and the implementation representation (usually referring to source code) or not.

- **Production of Additional Contents Based on Single Document**

  The tasks in this group is to extract contents from a target document and produce helpful information for other evaluation tasks.

  procedure pattern

  1. Select the tasks about producing additional contents based on single document.
  2. Find out **the source document**.
  3. Find out these **the sections** in source document.
  4. Prepare the contents in a specified format and save these data.

  For example, "The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment." This task need the evaluator to record the potential vulnerabilities which could be used as test data or as an evidence to prove the failure of target system in such operational environment.

- **Production of Additional Contents Based on Multiple Documents**

  The tasks in this group is to extract contents from multiple documents and produce helpful information for other evaluation tasks.

  procedure pattern

  1. Select the tasks about production of additional contents based on multiple documents.
  2. Find out **the source documents**.
  3. Find out these **the sections** in source documents.
  4. Prepare the contents in a specified format and save the data.
  5. Compare the texts in these contents automatically and save the records.

For example, "The evaluator shall identify possible potential vulnerabilities in the TOE by searching ST, guidance documentation, functional specification, TOE design and security architecture description evidence." This task need the evaluator to try to find possible potential vulnerabilities of target system by search 4 different kinds of documents.

- **Additional Physical Confirmation on Target System**

  The tasks in this group is to perform additional physical actions (for example, installation, to confirm whether the target system can be operated properly.

  procedure pattern

  1. Select the tasks about additional physical confirmation on target system.
  2. Find out **the document** relating to additional physical confirmation.
  3. Perform **the actions** specified in these document.

  For example, "The evaluator shall conduct testing using a sample of test data found in the developer test plan and procedures." This task need the evaluators to perform another testing by themselves, where test date provided by developers should be used. In a way, this is a process of reconfirmation.

Basing on our analysis, we classified detailed tasks into 7 groups. TABLE 3.1 shows these groups and their amount.

Table 3.1: Counts of Each Classification of Detailed Evaluation Tasks

Group	**Count**
Sufficiency and Necessity of Content	403
Sufficiency and Necessity of Inside Relationship	44
Correctness of Outside Relationship	88
Sufficiency and Necessity of Outside Relationship	26
Production of Additional Contents Based on Single Document	56
Production of Additional Contents Based on Multiple Documents	5
Additional Physical Confirmation on Target System	52

3.4 Supporting Methods for Security Evaluation Process

We proposed the supporting methods under the consideration that procedures of the tasks in the same group can be supported by the the same method. The supporting method for each group is as follows:

Sufficiency and Necessity of Content: the tasks in this group are about sufficiency or necessity of the contents in the specified section of a single document. Those determinations on whether each task is performed properly can only

be made by human. Thus, the supporting method for this group is providing an environment to display only the specification of the target document and guidance or helpful explanation. It is possible to implement by tagging related documents. The environment is a convenience that the developers can focus on making the determination and have no more need of finding out the relevant sections by themselves. Figure 3.1 show what kind of convenience that this supporting method can provide.

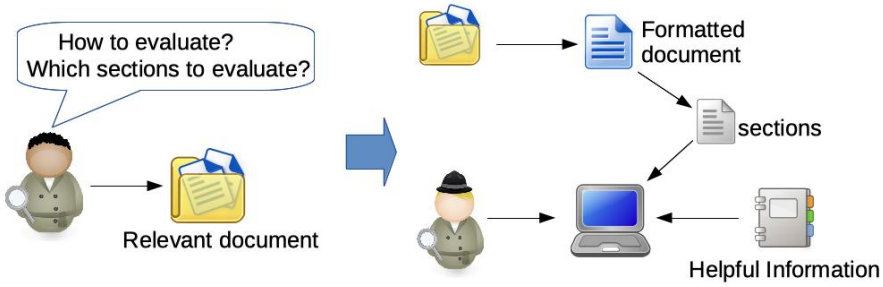


Figure 3.1: Supporting Method for Tasks of Sufficiency and Necessity of Content

Sufficiency and Necessity of Inside Relationship: the tasks in this group is about the sufficiency and necessity of the traceability between two different sections in the same document, and those determinations on whether the targets are satisfied can only be made by human. Thus, the supporting method for this group is providing an environment in which the content of trace and the two relevant sections are displayed automatically by search the tagging the document. Some prepared explanations and tips will also be displayed in the environment to help the developers to make the determination. The environment is a convenience that the developers can focus on making the determination and have no more need of finding out the relevant sections by themselves. Figure 3.2 show what kind of convenience that this supporting method can provide.

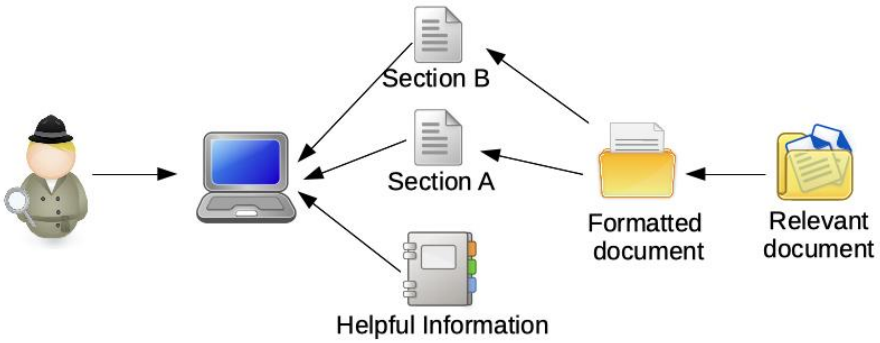


Figure 3.2: Supporting Method for Tasks of Sufficiency and Necessity of Inside Relationship

Correctness of Outside Relationship: the tasks in this group are about whether the claimed relationship is correct or not and can be checked automatically

by providing some functions. The functions can extract the relevant sections from the first document formatted in XML and relevant documents formatted in XML, and then compare these sections to confirm the relationship among these sections according to the targets. The extraction and comparison can be easily completed by the software that can save a lot of time for the evaluators. Figure 3.3 show what kind of fuctions that this supporting method can provide.

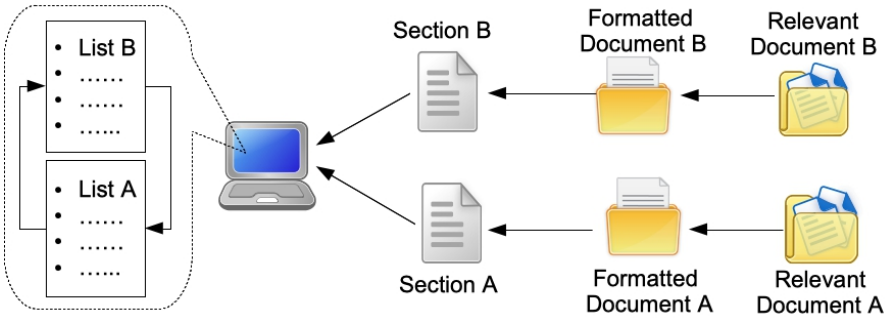


Figure 3.3: Supporting Method for Tasks of Correctness of Outside Relationship

Sufficiency and Necessity of Outside Relationship: the tasks in this group is about the sufficiency and necessity of the traceability between two different sections in the different documents, and those determinations on whether the targets are satisfied can only be made by human. Thus, the supporting method for this group is providing an environment in which the content of trace and the two relevant sections are displayed automatically by search the tagging the document. Some prepared explanations and tips will also be displayed in the environment to help the developers to make the determination. The environment is a convenience that the developers can focus on making the determination and have no more need of finding out the relevant sections by themselves. Figure 3.4 show what kind of convenience that this supporting method can provide.

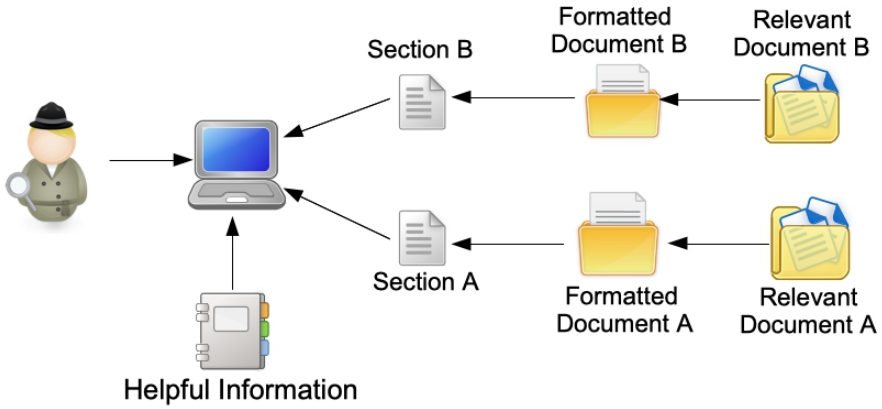


Figure 3.4: Supporting Method for Tasks of Sufficiency and Necessity of Outside Relationship

Production of Additional Contents Based on Single Document: the tasks in this group is about producing additional contents based on single document, and can be easily performed by the software tool. The software tool can extract the relevant sections from the source document, reorganize these contents in a prepared format, and save these data in prepared database. It is helpful for the evaluator to reuse the additional data and save a lot of time. Figure 3.5 show what kind of convenience that this supporting method can provide.

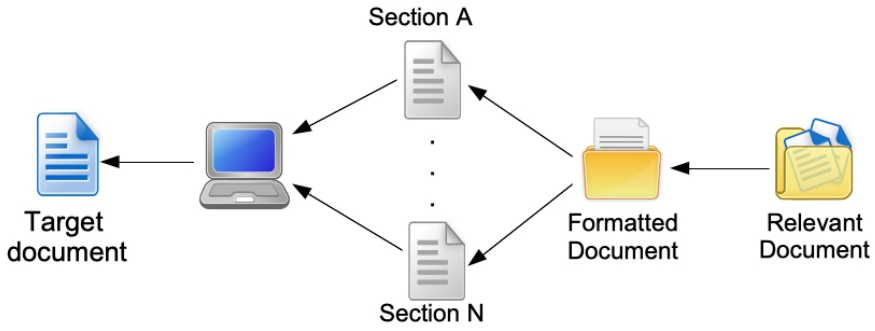


Figure 3.5: Supporting Method for Tasks of Production of Additional Contents Based on Single Document

Production of Additional Contents Based on Multiple Documents: the tasks in this group is about producing additional contents based on multiple documents, and can be easily performed by the software tool. The software tool must have the following functions: extracting the relevant sections from the source documents; reorganizing and saving these contents in prepared formats; comparing and recording the difference among these extracted contents. It is helpful for the evaluation that these data can be reused as precondition for other tasks. Figure 3.6 show what kind of convenience that this supporting method can provide.

Additional Physical Confirmation on Target System: the tasks in this group is about executing additional physical confirmation on target system, and those execution can only be performed by human. Thus, the supporting method for this group is providing an environment in which the detailed manual are displayed automatically for the evaluators. Some prepared explanations and tips will also be displayed in the environment to help the evaluators. The environment is a convenience that the developers can focus on executing the required actions to confirm the target system and have no more need of finding out the relevant documents by themselves. Figure 3.7 show what kind of convenience that this supporting method can provide.

Detailed Procedural Sequence: supporting for procedural sequence of tasks can be performed automatically according to the relationship among the tasks. To support the tasks, we built a hierarchical tree based on the procedure order. When a task is going to be executed, the relevant tasks will be confirmed according to the relationship. A list is produced to show all of the tasks whose execution must be before the selected one's. A second list is produced to show the tasks whose examination can be performed after the selected one's. It will provide a convenient

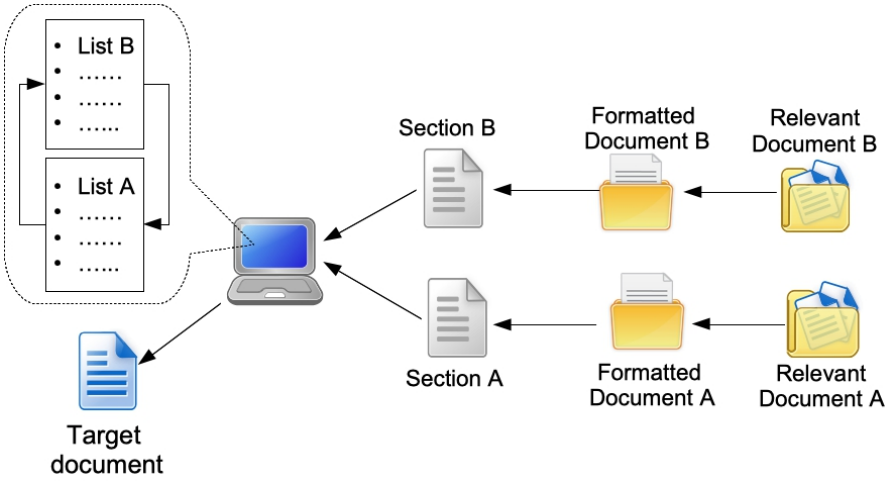


Figure 3.6: Supporting Method for Tasks of Production of Additional Contents Based on Multiple Documents

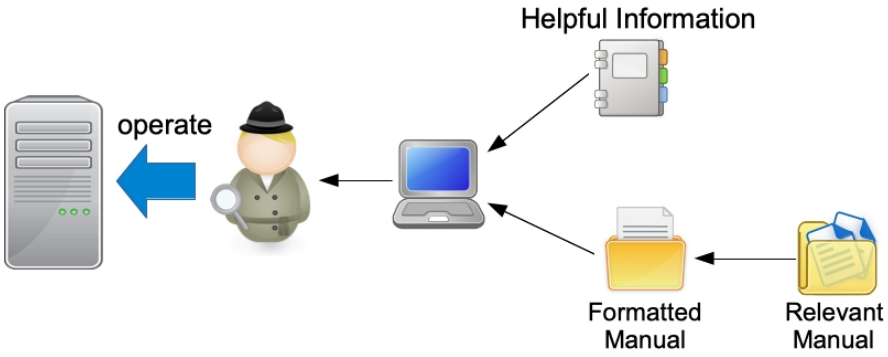


Figure 3.7: Supporting Method for Tasks of Additional Physical Confirmation on Target System

for the evaluators, because there is no need to prepare the execution order for the targets and focus on examining the targets.

3.5 Documents in Security Evaluation Process

There are over 20 kinds of documents involved in evaluation process based on ISO/IEC 15408 and ISO/IEC 18045. All the documents can be divide into 3 groups: evaluation evidences which are the input of evaluation process, intermediate documents which are produced and used during evaluation process, and finally report which is output of evaluation process. The evaluation evidences includes 19 kinds of documents [5], that were the following:

- Security Target
- Security architecture
- Functional specification
- Target of Evaluation (TOE) design
- Implementation representation
- Operational user guidance
- Preparative procedures
- Configuration Management(CM) capabilities
- CM scope
- Delivery
- Development security
- Flaw remediation
- Lifecycle definition
- Tools and techniques
- Test coverage
- Test depth
- Functional tests
- Independent tests
- Vulnerability assessment

IT systems who apply to obtain the evaluation of ISO/IEC 15408 and ISO/IEC 18045 have to develop and deliver a set of IT systems description documents called evaluation evidences. Evaluation evidence is tangible evaluation deliverable [8]. As the input of evaluation process, evaluation evidences are very important and confidential. evaluators shall perform configuration control of them in a high level security. During evaluation process, evaluators need to cheek contents of evaluation evidences according to ISO/IEC 15408 and ISO/IEC 18045, therefore evaluators should can search out specific content accurately and efficiently. Finally reports are the outputs of evaluation process which used to describe evaluation results. It is important to ensure that all those documents are with sufficient information and protected the evaluation evidences from loss and alteration, and extract the necessary information from various versions documents.

There are many difficulties and issues existing in evaluating IT systems based on ISO/IEC 15408 and ISO/IEC 18045. ISO/IEC 15408 is a set of security functions and security. However, these components and instructions are hard understood and has complex corresponding relationship between them. Moreover, there are many available versions of these two standards, and the standards are published, revised, withdrawn, and translated frequently with technology developing. Thus, in order to enable effective utilization in the environment, database can manage and protect all those documents in high security level is demanded.

3.6 XML Based Templates for Evaluation-Relative Documents

In order to manage ISO/IEC 15408 and ISO/IEC 18045 standards, and relating documents by database system, various characteristics of the standards and documents have to be taken into a careful consideration. A database system to solve these issues should satisfy following requirements according to their characteristics.

The database system should correspond with semistructured structure of the standards. The database system should manage all relating documents of evaluation process and be able to extract needed parts from the standards and documents. The database system should maintain the relationship among the standards and the documents. The database system should manage every available versions and translations of the standards and documents. The database systems should can be updated easily corresponding with ISO/IEC 15408 and ISO/IEC 18045 updating. The database system should manage progress of evaluation. The database system should manage relationship between tools composed in evaluation supporting environment.

To satisfy requirements, each relating document need a general normative template with specific unique identify informations for each specific content that need to be searched out. ISO/IEC 15408 defines what contents evaluation evidences must contain, that can be used as guidance for developers to producing an IT systems. ISO/IEC 18045 provides the criteria that the evaluation contains must satisfy. Therefore, we summarized 11 normative templates for all evaluation evidences. The following table shows all evaluation evidences and the evaluation

activities defined in ISO/IEC 18045 they corresponding with.

We used XML language to describe the templates, such that tags we defined to store specific can used as identity information, and ensure all documents produced with right structures and sufficient contents. The following Table 3.2 is an example of XML based templates we defined for describing evaluation evidences. As the document shows, we defined unique tags for each specific content and hierarchy structures of documents.

Table 3.2: List Of XML-based Templates Of Evaluation Evidences and Evaluation Activities That Each Document Corresponds With.

XML Based Templates	**Evaluation Activities ID**
Security Architecture	ADV
Functional Specifications	ADV, ATE
TOE Design	ADV, ALC
Implementation Representation	ADV, ALC
User Guidance	AGD
Test Coverage	ATE, ALC, ACO
Life-cycle Definition	ALC
High Level Design	ADV
Vulnerability Assessment	AVA, ATE
Security Target	ASE, ADV
CM Capabilities	ACO, ATE, ALC

Chapter 4

Supporting Environment for Security Evaluation

4.1 Overview

According to these supporting methods proposed in the previous section, we designed and implemented each necessary supporting tool to execute these methods. Considering the complicated relationship among various evaluation tasks, we clarified the sequence of evaluation tasks and implemented a supporting tool, called Sequence Controller, to guide evaluators perform all tasks in right order. We also designed and implemented a database for managing using all the evaluation-relevant documents.

4.2 Requirement Analysis of the Supporting Environment

It is necessary to develop supporting tools to solve the existing difficulties in current evaluation process. The supporting tools have to be connected and data exchangeable, such that we proposed the supporting tools as an information security engineering environment [2]. To support the whole evaluation process, the supporting environment must satisfy the following requirements.

R1: In order to improve the efficiency and accuracy of the results, the environment must provide support users to locate evaluation evidences easily and search target information quickly and accurately.

R2: In order to ensure the correctness of the results, the environment must support user protect evaluation evidences and intermediate products from modify and loss.

R3: In order to maintain the confidentiality of evaluation evidences, the environment must provide authentication and authorization mechanism.

R4: In order to ensure the fairness of the evaluation, the environment must ensure that evaluators perform evaluation satisfying a certain level of quality and force the activities are performed fairly.

R5: In order to maintain the confidentiality of evaluation evidences, the environment must control the disposal of evaluation evidences, intermediate products and ETR/OR according to the CEM requirement.

R5: In order to prevent evaluation results from human mistakes as possible, the environment must support performing evaluation activities as automatically as possible.

R6: In order to ensure that ETRs and ORs and other generated documents satisfy the ISO/IEC 18045 requirements for information content of report, the supporting environment must give guidance for generating qualified ETR and OR.

R7: In order to ensure that all participants of evaluation process perform their work in right order , the supporting environment must support to force users performing evaluation in sequence as the ISO/IEC 18045 defined.

4.3 Design of Supporting Environment

The supporting environment for evaluation based on ISO/IEC 15408 and ISO/IEC 18045 is an information security engineering environment [2] that consists of 11 component tools shown in Figure 4.1 which can provide comprehensive facilities to support all tasks relating to security evaluation and management of all documents and intermediate products in the whole evaluation process.

1. **Sequence Controller** is user interface of the whole evaluation environment which used to ensure all users perform evaluation tasks in right sequence and control dependence between evaluation activities. The sequence controller must control the sequence that different participants performing evaluation tasks with the supporting environment.

2. **Security Evaluation Database (ISDS)** is a central database that can store and manage relating supporting documents, user information and other evaluation information. The database is an expansion of Security Requirement Management Database Based on ISO/IEC 15408.

3. **Helper of Sufficiency and Necessity of Content** can extract the desired section from the source document, display the extracted section and helpful information for evaluators, and provide editing component to help the evaluators record their judgements or comments. The supporting method for Tasks of *Sufficiency and Necessity of Content* is providing an environment to display only the specification of the target document and guidance or helpful explanation. The environment is a convenience that the developers

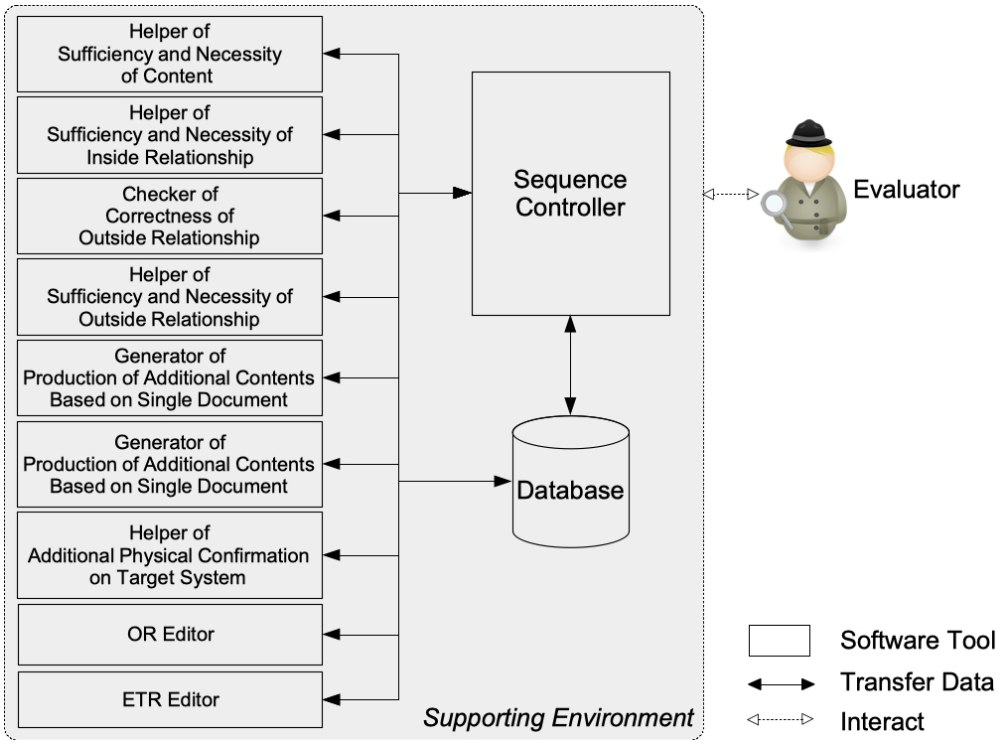


Figure 4.1: Design of The Supporting Environment

can focus on making the determination and have no more need of finding out the relevant sections by themselves.

4. **Helper of Sufficiency and Necessity of Inside Relationship** can extract two desired sections from the source document, compare these sections and save the result, display the extracted sections, the result of comparison and helpful information for evaluators, and provide editing component to help the evaluators record their judgements or comments. The supporting method for this group is providing an environment in which the content of trace and the two relevant sections are displayed automatically by search the tagging the document. The environment is a convenience that the developers can focus on making the determination and have no more need of finding out the relevant sections by themselves.

5. **Checker of Correctness of Outside Relationship** can extract two desired sections from the different source documents, compare these sections and confirm the relationship, and save their result of comparison as judgements. The functions can extract the relevant sections from the first document formatted in XML and relevant documents formatted in XML, and then compare these sections to confirm the relationship among these sections according to the targets. The extraction and comparison can be easily completed by the software that can save a lot of time for the evaluators.

6. **Helper of Sufficiency and Necessity of Outside Relationship** can extract two desired sections from the different source documents, compare these sections and save the result, display the extracted sections, the result of comparison and helpful information for evaluators, and provide editing component to help the evaluators record their judgements or comments. The supporting method for this group is providing an environment in which the content of trace and the two relevant sections are displayed automatically by search the tagging the document. The environment is a convenience that the developers can focus on making the determination and have no more need of finding out the relevant sections by themselves.

7. **Generator of Production of Additional Contents Based on Single Document** can extract the sections from the relevant document, generate the template of target document, and provide editing component to help the evaluators complete the document. This software tool can extract the relevant sections from the source document, reorganize these contents in a prepared format, and save these data in prepared database. It is helpful for the evaluator to reuse the additional data and save a lot of time.

8. **Generator of Production of Additional Contents Based on Multiple Documents** can extract the sections from relevant documents, generate the template of target document, and provide editing component to help the evaluators complete the document. This software tool must have the following functions: extracting the relevant sections from the source documents; reorganizing and saving these contents in prepared formats; comparing and recording the difference among these extracted contents. It is helpful for the evaluation that these data can be reused as precondition for other tasks.

9. **Helper of Additional Physical Confirmation on Target System** can display relevant manual for evaluators and show relevant guidance or helpful explanation to guide evaluators. The supporting method for this group is providing an environment in which the detailed manual are displayed automatically for the evaluators. The environment is a convenience that the developers can focus on executing the required actions to confirm the target system and have no more need of finding out the relevant documents by themselves.

10. **OR Editor** is a tool for users to compose standard OR.In the case of a fail verdict, the evaluator shall provide an OR to reflect the evaluation result. To make evaluation results can be easily understand and re-used, CEM defines a general structure and necessary content for OR. OR Editor is a supporting tool providing template and detail guidance for evaluator to force them produce quality OR.

11. **ETR Editor** is a tool for users to compose standard ETR by providing template and detail guidance. The evaluator shall provide an ETR to present technical justification of the verdicts. To make evaluation results can be

easily understand and re-used, CEM defines a general structure and necessary content for ETR. Same as OR Editor, ETR Editor is a supporting tool providing template and detail guidance for evaluator to force them produce quality ETR.

4.4 Development of Security Evaluation Database

4.4.1 The Data Model for Evaluation-Relative Documents

We herein explain the database model diagrams and implementation. First, based on the characteristics analysis of evaluation, we identified the following data that should be managed: C1: To satisfy R2 and R3, the database should manage all evaluation relating documents; C2: To satisfy R1 and R4, the database should manage all available versions of ISO/IEC 15408 and ISO/IEC 18045; C3: To satisfy R5, the database should manage component of ISO/IEC 15408 and instructions of ISO/IEC 18045; C4: To satisfy R6, the database should manage the relationships between all evaluation related documents and the standards; C5: To satisfy R7, the database should manage all re intermediate products of evaluation process.

Then, we design a data model for the security management based on a combine of XML data model and relational model to manage various versions of ISO/IEC 15408 and ISO/IEC 18045 series and relating documents. XML data model is used to store and manage all evaluation relating documents in pre-defined XML templates. And we used relational data model to manage ISO/IEC 15408 and ISO/IEC 18045 series and dependencies among them.

To satisfy all requirements of evaluation management database, we designed to use database system managing all tasks of evaluation process. In corresponding with structures of ISO/IEC 15408 and ISO/IEC 18045, we summarized all tasks of evaluation process. Each tasks contains minimum evaluator action defined in ISO/IEC 15408 and ISO/IEC 18045 and identify information of evaluation document contents (tags from pre-defined xml based templates). Such that our database can easily management relationship between ISO/IEC standards and the document.

4.4.2 The Implementation of Security Evaluation Database

As the Figure 2 shows, we choose to implement our database based on a combine of XML data model and relational model. And the Figure 4.2 shows the structure of our database. We chose to implement the evaluation management database by using IBM DB2 Express-C. Because data model of evaluation management database is based on a combine of XML data model and relational model. IBM DB2 Express-C is a free hybrid type database management system with strong functions to support such data models.

We have designed XML templates for evaluation relating documents, summarized all tasks of evaluation process based on Version 3.1 of ISO/IEC 15408 and ISO/IEC 18405. We implemented a prototype of database with all the tables we

designed by using IBM DB2 Express-C Database Management System [9]. The next step, we are going to put all available version and translations of ISO/IEC 15408 and ISO/IEC 18045.

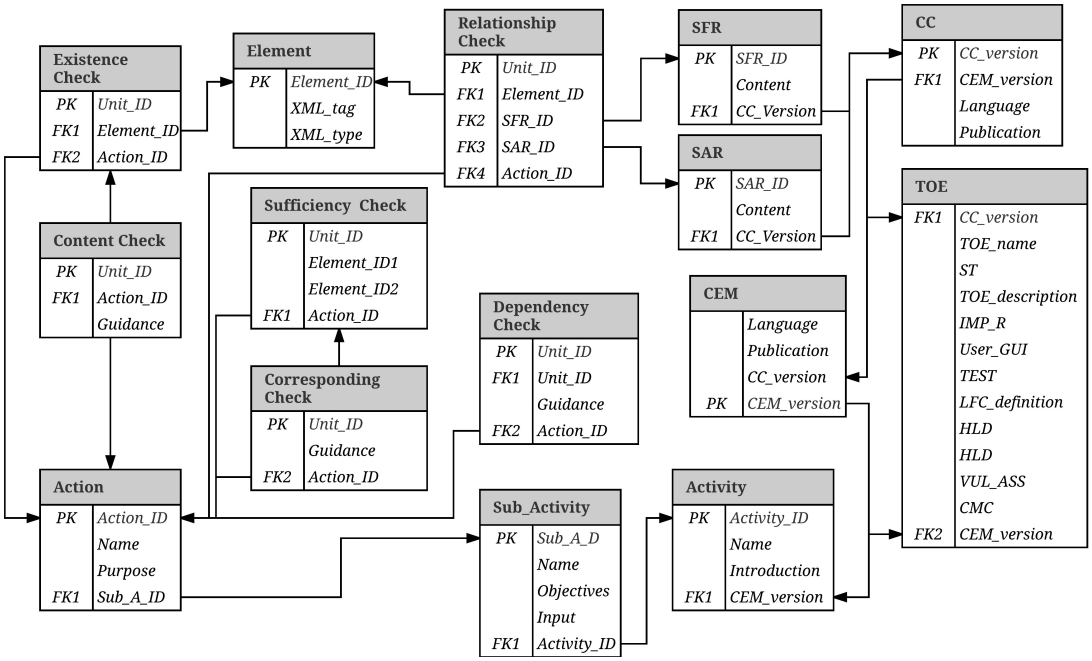


Figure 4.2: Data Model in Security Evaluation Database

4.5 Development of Supporting Tools

From view point of implementation, all supporting tools can be classified into 4 types: controller, document editor, supporter and database.

Sequence Controller is the main user interface and central tool of the whole environment it controls the sequence that user performing evaluation by using our environment. To implement the Sequence Controller, we summarized the sequence of different kinds of participants performing evaluation tasks, Sequence Controller shall ensure all users perform evaluation tasks in right sequence and control dependences between evaluation activities. We implement the control of sequence we let the controller support to transfer information between different user by sending emails; support to call other supporting tools by displaying links of other supporting tools; support to monitor current progress by monitoring the documents generating. Figure 4.3 is some screenshots when the Sequence Controller works.

ETR Editor, OR Editor belong to document editor. Most basic facilities of document editor are facilities of structured editor for XML-based format and instructor of how to describe documents. We defined the XML-based format templates which describe the general structure of target documents, the give detail guidance for user to guide them input necessary and correct. Most basic facilities of two editors are facilities of structured editor for XML-based format and

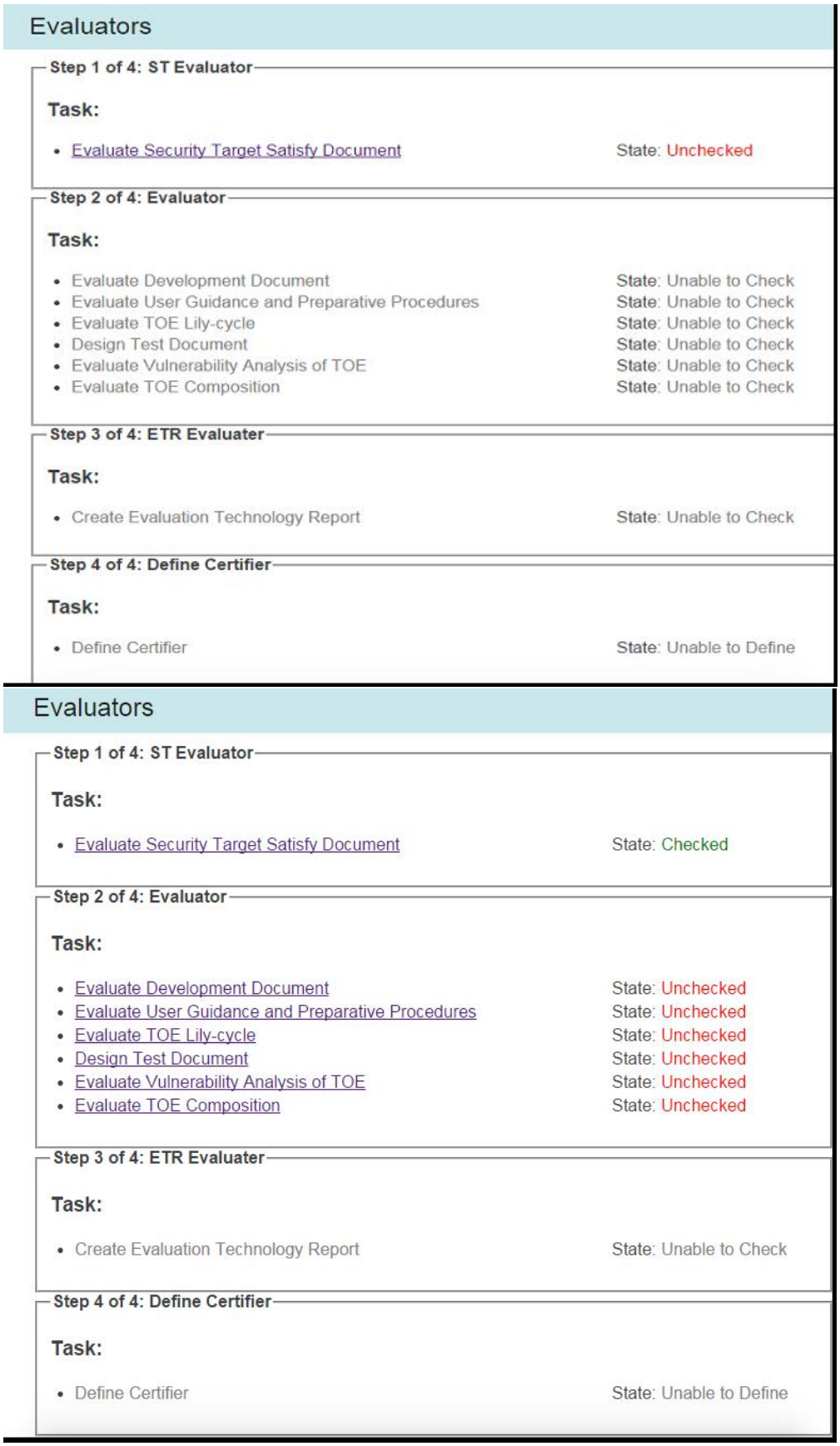


Figure 4.3: Sequence Controller

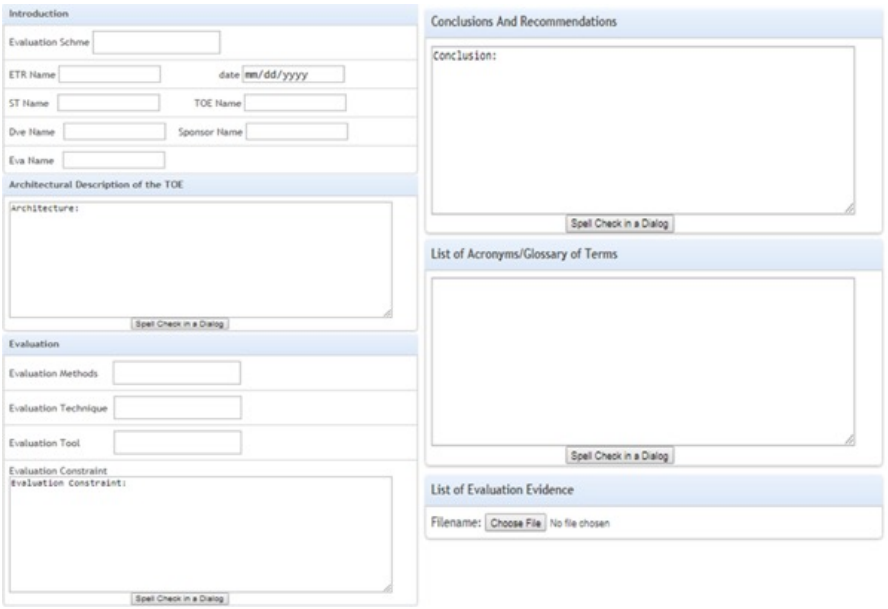
instructor of how to describe documents. We implement them by defining the XML format templates for the each kind of reports, and implementing customized XML editing component, when the editor loads target template it will become target kind document Editor. Figure 4.4 shows the user interface for managing and editing ETRs or ORs.

Helper of Sufficiency and Necessity of Outside Relationship, Helper of Sufficiency and Necessity of Content, Helper of Sufficiency and Necessity of Inside Relationship and Helper of Additional Physical Confirmation on Target System belong to evaluation supporter. The evaluation supporter is a tool consists of several simple functions to check whether content existing in specific XML-tags, find out specific content from EEs by XML-tags then display the content for evaluator with guidance and record evaluators input, provide functions to relevant specific contents from EEs and confirm relationship by comparing content XML tags, relevant and display relating contents with guidance for evaluator then record their input, relevant specific contents by using XML-tags and confirm the mapping relationship between them to confirm correspondence, provide functions to confirm whether the dependency are satisfied by searching relating contents with XML-tags.

Generator of Production of Additional Contents Based on Single Document and Generator of Production of Additional Contents Based on Multiple Documents are two kinds of supporting tools which can providing template and detail guidance for evaluator to force them produce quality temporary document date. Most basic facilities of two tools are facilities of structured editor for XML-based format and instructor of how to describe documents. We implement these three tools, by defining the XML format templates for the each kind of temporary documents, and implementing customized XML editing component, when the editor loads target template it will become target kind document Editor.

Checker of Correctness of Outside Relationship is a automatic tool that provides functions to extract two desired sections from the different XML-formatted documents, compare these sections and confirm the relationship, and save their result of comparison as judgements. The functions can extract the relevant sections from the first document formatted in XML and relevant documents formatted in XML, and then compare these sections to confirm the relationship among these sections according to the targets.

Figure 4.5 shows some user interface for evaluating Security Target by combined several supporting together.



OR_id	OR_name	Date	Toe_name	Evaluator	Standard	Organization
10017	or-title3	2017-08-17	toename	Evaluator3	OK	22
10056	222222222	2017-09-25	system1	Evaluator	OK	sadasd
10057	title	2017-09-26	system1	Evaluator	NG	organisation1
10060	asdlk	2017-11-02	system1	asdsadasd	NG	asdasad
10062	111	2017-11-02	222	2121321	OK	sad
10063	qweqw	2017-12-04	system1	asda	NG	asda
10064	qweqw	2017-12-04	system1	asda	OK	asda

OR_id search

OR_id delete

Figure 4.4: Sequence Controller

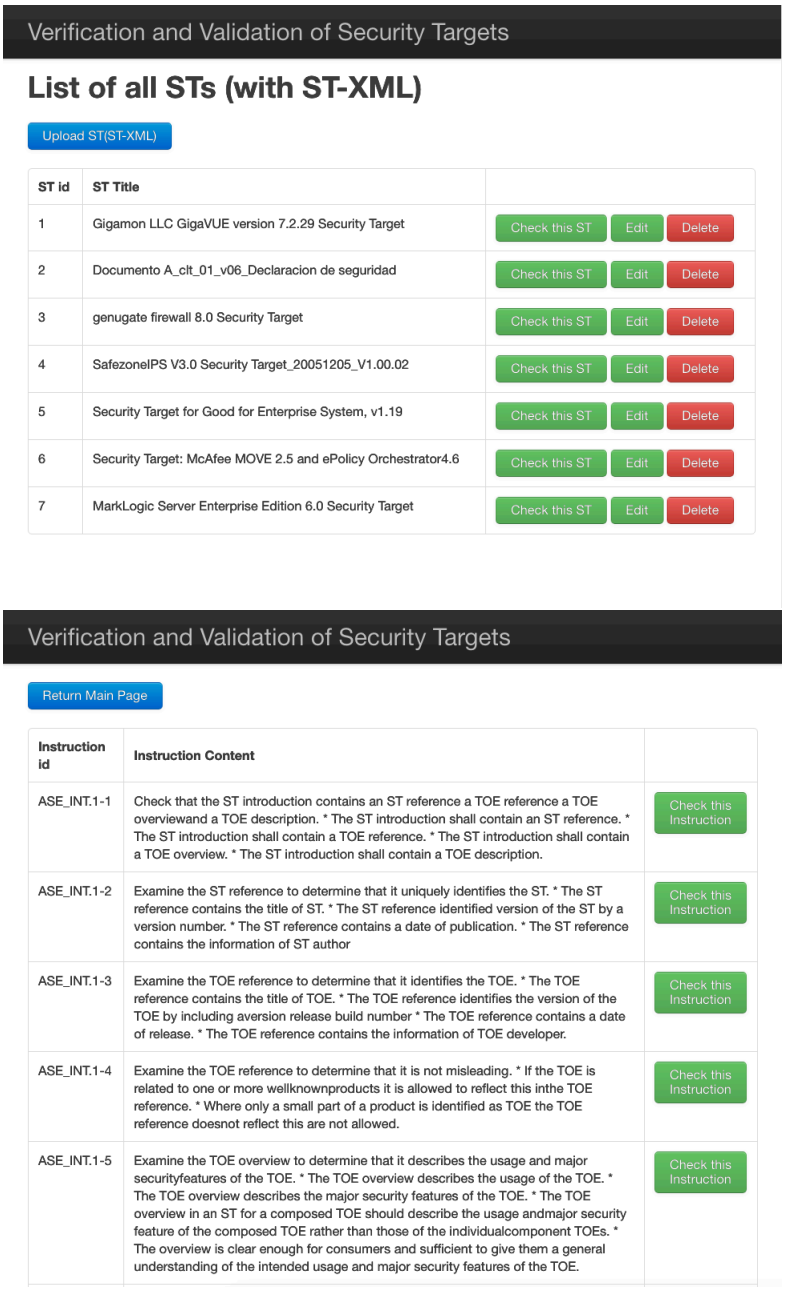


Figure 4.5: User Interfaces for Tasks of Evaluating Security Targets.

Chapter 5

Evaluation

5.1 Overview

This section explains an evaluation method we have proposed to evaluate the usefulness of the supporting environment and shows how we evaluated the supporting environment based on the method. We, then, discusses how the supporting environment is capable and useful to provide comprehensive facilities to perform all tasks in security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045.

Until now, there is no evaluation of the supporting environment to show that the environment is useful to support all participants to perform all tasks in security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045. At present, the basic idea of the supporting environment has been proposed, its requirements and necessary functions has been analyzed, its architecture has been designed, and a prototype has been implemented.

Furthermore, at present, there is no evaluation method to show the usefulness of the supporting environment. There is no suitable method to evaluate the usefulness of the supporting environment to show that the environment is useful to support organizations with security evaluation process at the moment. Therefore, we proposed an evaluation method to show usefulness of the supporting environment and evaluate the supporting environment from its design and implementation level.

5.2 Evaluation Methods

Usefulness of this supporting environment depends on the following characteristics: completeness, efficiency because these characteristics are important for evaluators to perform all evaluation tasks properly based on ISO/IEC 15408 and ISO/IEC 18045. Evaluation of usefulness of ISMEE focuses on two points:

- The completeness: whether this supporting environment can support all evaluation tasks in security evaluation process
- The efficiency: whether this supporting environment can reduce the complex of evaluation work and save time for evaluators.

Completeness of the supporting environment depends on whether its functions provide enough components to support all the evaluation activities in ISO/IEC 15408 and ISO/IEC 18045. To evaluate the completeness of STE, we need to investigate functionality of the supporting environment with authoritative evaluation guideline. The authoritative evaluation guidelines are provided by authority who is in charge of maintaining the certification of ISO/IEC 15408 and ISO/IEC 18045.

To evaluate the completeness, we need to judge whether the supporting environment cover all the software supportable tasks in evaluation process. As the Figure 7.1 shows, we summarized 42 tasks for the evaluation process need to be performed in specific sequence, and an ideal implementation of the supporting environment shall can support all these tasks. To evaluate the compliance, we need to check whether or not components of the supporting environment comply with best practices related with environmental aspects. To evaluate the usability, we need to check the check correctness of TOE evaluation results generated by using the supporting environment. Like we will use the Format translator to translate STs, then judge whether the content of it is loss or modification; Use our evaluators to evaluate documents, and judge whether the

Efficiency of the supporting environment depends on whether the tool can help users to save time in evaluation process. Two experienced evaluators performed evaluation tasks on the same Security Target. One used our supporting tool, and another did not. Though comparing the total time of two evaluators, we can estimate the efficiency of STE.

5.3 Evaluation Results

At current stage, we evaluated completeness of the supporting environment. As the result, the supporting environment matches evaluation guideline for completeness at the design level. All evaluation tasks, which we analyzed carefully, can cover all requirement in the authoritative evaluation guidelines. The supporting methods and corresponding software components keep the consistency when we designed the supporting tool. From the view of implementation level, this supporting environment has not enough function to cover all detailed evaluation tasks. Until now, the tasks about evaluating Security Target can be performed well, that is 168 of 674 tasks can be supported very well.

For evaluation of efficiency, we can only compare the time of evaluating Security Target. the evaluation with the supporting environment costs 279 minutes, and the evaluation without the supporting environment costs 435 minutes. It shows that the supporting environment has an advantage in efficiency . However, there are still some point of the supporting environment that can be improved or revised. The supporting environment now need the input evaluation-relevant documents to be transferred into a specified format and This would waste a lot of time. We will provide a format-transferring tool as next step. Moreover, there are not full facilities for evaluators to promote the security evaluation process. The full capability of this supporting environment can not be totally proved.

Chapter 6

Conclusion

6.1 Contributions

We firstly analyzed and clarified 674 necessary evaluation tasks in security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045. We also clarified the procedure and detailed actions for each task. We then classified the detailed evaluation tasks into 7 groups according to the pattern in the procedures and proposed appropriate supporting methods for each group of evaluation tasks. According to these supporting methods, we designed and implemented necessary supporting tools that can help evaluators to perform all detailed task the evaluation process. We clarified the sequence of detailed evaluation tasks and implement a supporting tool, as central core of the supporting environment, which can guide evaluators perform all tasks in right order. We analyzed all evaluation-relevant documents, intermediate information and evaluators' reviews, and then designed matched formats to transfer these information into structured data. A database for security evaluation was implemented to manage and use these structured data in the evaluation process. Currently, partial facilities can be provides for evaluating security targets. We also show the limited advantage of using this supporting environment over the evaluators who is not use it.

6.2 FutureWorks

The final goal of this research is to prepare the supporting environment with capability of supporting all detailed evaluation tasks in the security evaluation process based on ISO/IEC 15408 and ISO/IEC 18045. Although we have implemented a partial facilities that consists of functions to support evaluation on security target, which is the most important and basic tasks in the whole process. We must develop and implement other functions of this supporting environment to provide full facilities to help evaluator to promote the security evaluation process. This supporting environment can no only provide evaluators with a high time efficiency, but also can provide more fairness, more correctness and more accuracy of evaluation results.

Approaches and tools for transferring unstructured information into structured

data can improve this supporting environment additionally. This supporting environment includes a lot unified formats for various evaluation relevant documents. To use this supporting environment, it would waste a lot of time for transferring formats manually. To achieve more efficiency, such kind of tools is necessary for this supporting environment. In the future, we will develop or integrate format-transferring tools into this supporting environment.

Publications

Refereed Papers for Doctoral Dissertation

- Da Bao, Junichi Miura, Ning Zhang, Yuichi Goto, and Jingde Cheng: Supporting Verification and Validation of Security Targets with ISO/IEC 15408, Proceedings of the 2nd International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC 2013), Shenyang, China, pp. 2621-2628, IEEE Press, December 2013.
- Da Bao, Yuichi Goto, and Jingde Cheng: Predicting New Attacks for Information Security, in J. J. Park, et al. (Eds.), "Computer Science and its Applications, Ubiquitous Information Technologies," Lecture Notes in Electrical Engineering, Vol. 330, pp. 1353-1358, Springer, Heidelberg, December 2014.
- Huilin Chen, Da Bao, Yuichi Goto, and Jingde Cheng: A Supporting Environment for IT System Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045, in J. J. Park, et al. (Eds.), "Computer Science and its Applications, Ubiquitous Information Technologies," Lecture Notes in Electrical Engineering, Vol. 330, pp. 1359-1366, Springer, Heidelberg, December 2014.
- Da Bao, Kazunori Wagatsuma, Hongbiao Gao, and Jingde Cheng: Predicting New Attacks: A Case Study in Security Analysis of Cryptographic Protocols, in J. J. Park, H. Jin, Y. Jeong and M. K. Khan (Eds.), "Advanced Multimedia and Ubiquitous Engineering - FutureTech & MUE," Lecture Notes in Electrical Engineering, Vol. 393, pp. 263-270, Springer, Singapore, August 2016.
- Huilin Chen, Da Bao, Hongbiao Gao, and Jingde Cheng: A Security Evaluation and Certification Management Database Based on ISO/IEC Standards, Proceedings of the 12th International Conference on Computational Intelligence and Security (CIS 2016), pp. 249- 253, Wuxi, China, IEEE Computer Society Press, December 2016.
- Da Bao, Wen Sun, Yuichi Goto, and Jingde Cheng: Development of Supporting Environment for IT System Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045, Proceedings of 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovations (Smart-

World/UIC/ATC/ScalCom/CBDCom/IOP/SCI 2018), pp. 204-209, Guangzhou, China, IEEE Computer Society Press, October 2018.

- Da Bao, Yuichi Goto and Jingde Cheng: A Supporting Tool for IT System Security Specification Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045, "Intelligence and Security Informatics, Pacific Asia Workshop, PAISI 2019, Macau, April 14, 2019. Proceedings," Lecture Notes in Computer Science, Springer, Heidelberg, 2019. (accepted)

Other Refereed papers

- Ning Zhang, Da Bao, Liqing Xu, Ahmad Iqbal Hakim Suhaimi, Junichi Miura, Yuichi Goto, and Jingde Cheng: Supporting Tools for Software Supportable Tasks Related with ISO/IEC 15408, Proceedings of the 2nd International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC 2013), Shenyang, China, pp. 2002-2006, IEEE Press, December 2013.
- Yuichi Goto, Huilin Chen, and Da Bao: Aspect-Oriented Reuse Mechanism for Security Targets and Protection Profiles, Proceedings of the 5th IEEE International Conference on Software Engineering and Service Science (ICSESS 2014), pp. 161-164, Beijing, China, IEEE press, June 2014.
- Ahmad Iqbal Hakim Suhaimi, Da Bao, Yuichi Goto, and Jingde Cheng: Development of An Information Security Management Engineering Environment ISMEE, in J. J. Park, et al. (Eds.), "Computer Science and its Applications, Ubiquitous Information Technologies," Lecture Notes in Electrical Engineering, Vol. 330, pp. 1325-1330, Springer, Heidelberg, December 2014.
- Ahmad Iqbal Hakim Suhaimi, Da Bao, Huilin Chen, and Jingde Cheng: Usefulness of ISMEE for Supporting Organizations with ISMSs, in J. J. Park, et al. (Eds.), "Computer Science and its Applications, Ubiquitous Information Technologies," Lecture Notes in Electrical Engineering, Vol. 330, pp. 1331-1336, Springer, Heidelberg, December 2014.
- Da Bao, Huilin Chen, Sun Wen, and Jingde Cheng: A Supporting Environment for IT System Security Evaluation Based on CC and CEM, in Journal of Information Security Research, Vol.3, No.7 pp. 638-646, Beijing, China, Journal of Information Security Research, July 2017 (In Chinese).
- Da Bao and Jingde Cheng: Information Security Engineering Databases Based on ISO/IEC Standards and Their Applications, in Journal of Information Security Research, Vol.3, No.8 pp. 701-709, Beijing, China, Journal of Information Security Research, August 2017 (In Chinese).

Bibliography

[1] International Organization for Standardization. ISO/IEC 15408-1:2009, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model, 2009.

[2] International Organization for Standardization. ISO/IEC 15408-2:2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security– Part 2: Security Functional Components. 2008

[3] International Organization for Standardization. ISO/IEC 15408-3:2008, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 3: Security Assurance Components. 2008

[4] International Organization for Standardization. ISO/IEC 18045:2008, Information Technology – Security Techniques – Methodology for IT Security Evaluation. 2008.

[5] D.S. Herrmann. *Using the Common Criteria for IT Security Evaluation.* New York, iCRC Press, 2002

[6] W.H. Higaki. *Successful Common Criteria Evaluations: A Practical Guide for Vendors.* Lexington, KY: CreateSpace, USA, 2010

[7] Members of the Common Criteria Recognition: CEM v3.1, https://www.commoncriteriaportal.org/ccra/members/ (accessed November 20, 2018)

[8] National Information Assurance Partnership: Common Criteria Evaluation Validation Scheme, https://www.niap-ccevs.org/ (accessed November 20, 2018)

[9] IBM DB2 Express-C, https://www.ibm.com/analytics/jp/ja/technology/db2/db2-trials.html (accessed November 20, 2018)

[10] International Organization for Standardization. ISO/IEC 21827, Information Technology – Systems Security Engineering Capability maturity Model (SSE-CMM). 2008

[11] Cybersecurity in company - Systems Security Engineering Capability Maturity Model (SSE-CMM), http://www.sse-cmm.org (accessed November 20, 2018)

[12] Y.G. Kim, S. Cha. Security engineering methodology for developing secure enterprise information systems: An overview. In Embedded and Multimedia Computing Technology and Service (pp. 393-400). Springer, Dordrecht.

[13] J. Jurjens. Sound Methods and Effective Tools for Model-based Security Engineering with UML. In: *Proc. of the 27th International Conference on Software Engineering, ICSE 2005,* 2005, pp. 322331

[14] D. Hatebur, M. Heisel, H. Schmidt. A Security Engineering Process based on Patterns. In: *Proc. of the International Workshop on Secure Systems Methodologies using Patterns (SPatterns),* 2007. pp. 734738

[15] J. Cheng, Y. Goto, S. Morimoto, and D. Horie. "A Security Engineering Environment Based on ISO/IEC Standards: Providing Standard, Formal, and Consistent Supports for Design Development, Operation, and Maintenance of Secure Information Systems," in *Proc. of the 2nd International Conference on Information Security and Assurance ,* 2008, pp. 350-354.

[16] J. Cheng, Y. Goto, and D. Horie. "ISEE: An Information Security Engineering Environment," in *Proc. International Conference on Security and Cryptography ,* 2009, pp. 395-400.

[17] J. Cheng, Y. Goto, D. Horie, J. Miura, T. Kasahara, and A.I.H. Suhaimi. "Development of ISEE: An Information Security Engineering Environment." in *Proc. the 7th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA '09) ,* August 2009, pp. 505-510.

[18] D. Horie, S. Morimoto, N. Azimah, Y. Goto, and J. Cheng. "ISEDS: An Information Security Engineering Database System Based on ISO Standards." in *Proc. the 3rd International Conference on Availability, Reliability and Security (ARES '08) ,* March 2008, pp. 1219-1225.

[19] D. Horie, T. Kasahara, Y. Goto, and J. Cheng. "A New Model of Software Life Cycle Processes for Consistent Design, Development, Management, and Maintenance of Secure Information Systems." in *Proc. the 8th IEEE/ACIS International Conference on Computer and Information Science (ICIS '09) ,* June 2009, pp. 897-902.

[20] D. Horie, K. Yajima, N. Azimah, Y. Goto, and J. Cheng. "GEST: A Generator of ISO/IEC 15408 Security Target Templates." in *Computer and Information Science 2009, Studies in Computational Intelligence,* Vol. 208, pp. 149-158, May 2009.

[21] K. Yajima, S. Morimoto, D. Horie, N.S. Azreen, Y. Goto, and J. Cheng. "FORVEST: A Support Tool for Formal Verification of Security Specifications with ISO/IEC 15408." in *Proc. the 4th International Conference on Availability, Reliability and Security (ARES '09) ,* March 2009, pp. 624-629.

[22] A.I.H. Suhaimi, D. Horie, Y. Goto, and J. Cheng. "A Database System for Effective Utilization of ISO/IEC 27002." in *Proc. the 4th International Conference on Frontier of Computer Science and Technology (FCST '09),* December 2009, pp. 607-612.

[23] A.I.H. Suhaimi, T. Manji, Y. Goto and J. Cheng. "A Systematic Management Method of ISO Information Security Standards for Information Security Engineering Environments." *Communications in Computer and Information Science,* Vol. 251, pp. 370-384, November 2011.

[24] A.I.H. Suhaimi, Y. Goto, and J. Cheng. "An Analysis of Software Supportable Tasks in Information Security Management System Life Cycle Processes." in *Proc. International Conference on Information and Social Science (ISS 2013),* September 2013, pp. 29-58.

[25] N. Zhang, A.I.H. Suhaimi, Y. Goto, and J. Cheng. "An Analysis of Software Supportable Tasks Related with ISO/IEC 15408." in *Proc. the 9th International Conference on Computational Intelligence and Security (CIS 2013),* December 2013, pp. 601-606.

[26] N. Zhang, D. Bao, L. Xu, A.I.H Suhaimi, J. Miura, Y. Goto, and J. Cheng. " Supporting Tools for Software Supportable Tasks Related with ISO/IEC 15408." in *Proc. the 2nd International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC 2013),* December 2013, pp. 2002-2006.

[27] H. Chen, D. Bao, Y. Goto, J. Cheng. "A Supporting Environment for IT System Security Evaluation Based on ISO/IEC 15408 and ISO/IEC 18045." *LNEE,* Vol. 330, pp. 1359-1366, 2014.

[28] D. Bao, J. Miura, N. Zhang, Y. Goto, and J. Cheng. "Supporting Verification and Validation of Security Targets with ISO/IEC 15408." in *Proc. 2nd International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC 2013),* December 2013, pp. 2621-2628.

[29] G. Sun, K. Yajima, J. Miura, K. Shi, Y. Goto, and J. Cheng. "A Supporting Tool for Creating and Maintaining Security Targets According to ISO/IEC 15408," in *Proc. the 3rd IEEE International Conference on Software Engineering and Service Science (ICSESS 2012),* June 2012, pp. 745-749.

Appendix A

All Detailed Evaluation Tasks

We has clarified the original evaluation tasks and found 674 detailed evaluation tasks: 168 detailed tasks about evaluation on Security Targets, 129 detailed tasks about evaluation on development process, 11 detailed tasks about evaluation on the guidance document process, 133 detailed tasks about evaluation on life-cycle support process, 70 detailed tasks about evaluation on test process, 86 detailed tasks about evaluation on vulnerability assessment process, and 77 detailed tasks about evaluation on composition process.

A.1 168 Detailed Tasks about Evaluation on Security Targets

Table A.1: 168 Detailed Evaluation Tasks for Evaluating Secrity Targets

Task ID	Description of Evaluation Tasks
ASE-INT1-1-1	The evaluator shall examine the existence of ST reference
ASE-INT1-1-2	The evaluator shall examine the existence of TOE reference
ASE-INT1-1-3	The evaluator shall examine the existence of TOE overview
ASE-INT1-1-4	The evaluator shall examine the existence of TOE description
ASE-INT1-2-1	The evaluator shall examine the existence of the title of ST
ASE-INT1-2-2	The evaluator shall examine the existence of version of the ST
ASE-INT1-2-3	The evaluator shall examine the existence of a date of publication
ASE-INT1-2-4	The evaluator shall examine the existence of the information of ST author
ASE-INT1-3-1	The evaluator shall examine the existence of the title of TOE
ASE-INT1-3-2	The evaluator shall examine the existence of the version of the TOE
ASE-INT1-3-3	The evaluator shall examine the existence of a date of TOE release
ASE-INT1-3-4	The evaluator shall examine the existence of the information of TOE developer

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ASE-INT1-4-1	The evaluator shall examine the existence of description about the relationship between TOE and well-known products
ASE-INT1-4-2	The evaluator shall examine no misunderstanding that only a small part of a product is identified as TOE
ASE-INT1-5-1	The evaluator shall examine the existence of description of the usage of the TOE
ASE-INT1-5-2	The evaluator shall examine the existence of description of the major security features of the TOE
ASE-INT1-5-3	The evaluator shall examine no misunderstanding of description of the usage and major security feature of the composed TOE
ASE-INT1-5-4	The evaluator shall examine sufficiency of the TOE overview
ASE-INT1-6-1	The evaluator shall examine the existence of identifying the TOE type
ASE-INT1-7-1	The evaluator shall examine no absence of the expected functionality based on a certain type TOE
ASE-INT1-7-2	The evaluator shall examine the rationality of TOE's ability to operate in a certain operational environment
ASE-INT1-8-1	The evaluator shall examine the existence of description that run stand-alone, or need additional hardware, software or firmware
ASE-INT1-8-2	The evaluator shall examine the existence of additional hardware or not
ASE-INT1-8-3	The evaluator shall examine the existence of additional software or not
ASE-INT1-8-4	The evaluator shall examine the existence of additional firmware or not
ASE-INT1-9-1	The evaluator shall examine the existence of describes the physical scope of the TOE
ASE-INT1-9-2	The evaluator shall examine the existence of description of the hardware
ASE-INT1-9-3	The evaluator shall examine the existence of description of firmware
ASE-INT1-9-4	The evaluator shall examine the existence of description of software and
ASE-INT1-9-5	The evaluator shall examine the existence of description of guidance parts that constitute the TOE
ASE-INT1-9-6	The evaluator shall examine no misunderstanding to any hardware, firmware, software
ASE-INT1-10-1	The evaluator shall examine the existence of description of the logical scope of the TOE
ASE-INT1-10-2	The evaluator shall examine the existence of description of major security feature of TOE
ASE-INT1-10-3	The evaluator shall examine no misunderstanding to any logical security feature

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ASE-INT1-11-1	The evaluator shall examine consistency among TOE reference, TOE overview and TOE description
ASE-CCL1-1-1	The evaluator shall examine the existence of the version of the CC that was used to develop this ST
ASE-CCL1-1-2	The evaluator shall examine the existence of description about the usage of non english version of the CC
ASE-CCL1-1-3	The evaluator shall examine the existence of description about the CC versions differ between a component and the composed TOE
ASE-CCL1-2-1	The evaluator shall examine the existence of CC Part 2 conformance claim (CC Part 2 conformant or CC Part 2 extended)
ASE-CCL.1-2-2	The evaluator shall examine the rationality of CC Part 2 conformant, that is, all SFRs in ST are based only upon CC Part 2
ASE-CCL.1-2-3	The evaluator shall examine the rationality of CC Part 2 extended, that is, at least one SFR in that ST is not based upon CC Part 2
ASE-CCL.1-2-4	The evaluator shall examine the rationality of CC Part 2 extended that the component TOEs are Part 2 conformant, the composed TOE may be CC Part 2 extended
ASE-CCL.1-2-5	The evaluator shall examine the rationality of CC Part 2 conformant that the component TOEs are Part 2 conformant, the composed TOE may be CC Part 2 extended
ASE-CCL.1-3-1	The evaluator shall examine the existence of CC Part 3 conformance claim
ASE-CCL.1-3-2	The evaluator shall examine the rationality of CC Part 3 conformant that if all SARs in that ST are based only upon CC Part 3
ASE-CCL.1-3-3	The evaluator shall examine the rationality of CC Part 3 extended that if all SARs in that ST are based only upon CC Part 3
ASE-CCL.1-4-1	The evaluator shall examine the rationality of CC Part 2 conformant that ST does not define extended functional components
ASE-CCL.1-4-2	The evaluator shall examine the rationality of CC Part 2 extended that defines at least one extended functional component
ASE-CCL.1-5-1	The evaluator shall examine the rationality of CC Part 3 conformant that ST does not define extended assurance components
ASE-CCL.1-5-2	The evaluator shall examine the rationality of CC Part 3 extended that defines at least one extended assurance component
ASE-CCL.1-6-1	The evaluator shall examine the existence of PP claim
ASE-CCL.1-6-2	The evaluator shall examine the existence of PP claim type
ASE-CCL.1-6-3	The evaluator shall examine the rationality of PP claim about the composed TOE
ASE-CCL.1-7-1	The evaluator shall examine the existence of packages claim
ASE-CCL.1-7-2	The evaluator shall examine the rationality of packages claim
ASE-CCL.1-8-1	The evaluator shall examine the existence of package claim type

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ASE-CCL.1-8-2	The evaluator shall examine rationality of SFR package-name conformant that the ST contains all SFRs included in the package, but no additional SFRs
ASE-CCL.1-8-3	The evaluator shall examine rationality of SAR package-name conformant that the ST contains all SARs included in the package, but no additional SARs
ASE-CCL.1-8-4	The evaluator shall examine the rationality of SFR package-name augmented that ST contains all SFRs included in the package, and at least one additional SFR or at least one SFR that is hierarchical to a SFR in the package
ASE-CCL.1-8-5	The evaluator shall examine the rationality of SAR package-name augmented that ST contains all SARs included in the package, and at least one additional SAR or at least one SAR that is hierarchical to a SAR in the package
ASE-CCL.1-9-1	The evaluator shall examine the consistency of the TOE type between this ST and the claimed PPs
ASE-CCL.1-10-1	The evaluator shall examine the rationality of PP strict conformance that threats in ST are a superset of ones in PP;OSPs in ST are a superset of ones in PP;assumptions in ST are identical to ones in PP;
ASE-CCL.1-10-2	The evaluator shall examine the rationality of PP demonstrable conformance that security problem definition in ST is subset of ones in PP;
ASE-CCL.1-11-1	The evaluator shall examine the rationality of PP strict conformance that security objectives in ST is superset of ones in PP;
ASE-CCL.1-11-2	The evaluator shall examine the rationality of PP demonstrable conformance that security objectives in ST are subset of ones in PP;
ASE-CCL.1-12-1	The evaluator shall examine the rationality of PP strict conformance that SFRs in the ST are superset of SFRs in the PP; SARs in the ST are superset of SARs in the PP
ASE-CCL.1-12-2	The evaluator shall examine the rationality of PP demonstrable conformance that SFRs in the ST are subset of SFRs in the PP; SARs in the ST are superset of SARs in the PP; The completion of operations in the ST must be consistent with that in the PP;
ASE-SPD.1-1-1	The evaluator shall examine rationality (1) of the existence of Threats
ASE-SPD.1-1-2	The evaluator shall examine the existence of description the threats
ASE-SPD.1-1-3	The evaluator shall examine rationality that the threats must be countered by the TOE and/or operational environment.
ASE-SPD.1-2-1	The evaluator shall examine rationality (2) of the existence of Threats
ASE-SPD.1-2-2	The evaluator shall examine the rationality of description of all threats that all threats shall be described in terms of a threat agent, an asset, and an adverse action

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ASE-SPD.1-2-3	The evaluator shall examine the existence of further description of threat agents
ASE-SPD.1-3-1	The evaluator shall examine the rationality of no OSPs
ASE-SPD.1-3-2	The evaluator shall examine the existence of OSP
ASE-SPD.1-3-3	The evaluator shall examine sufficient detail of each OSP
ASE-SPD.1-3-4	The evaluator shall examine necessity of policy statements
ASE-SPD.1-4-1	The evaluator shall examine the existence of assumptions
ASE-SPD.1-4-2	The evaluator shall examine sufficient detail of each assumption
ASE-SPD.1-4-3	The evaluator shall examine no misunderstanding of the assumptions
ASE-OBJ.1-1-1	The evaluator shall examine the existence of Security Objectives.
ASE-OBJ.2-1-1	The evaluator shall examine the existence of Security Objectives for the TOE
ASE-OBJ.2-1-2	The evaluator shall examine the existence of the Security Objectives For the Environment
ASE-OBJ.2-2-1	The evaluator shall examine the existence of traces between each security objective and threats or OSPs, or a combination of threats and OSPs.
ASE-OBJ.2-2-2	The evaluator shall examine the existence of traces between each security objective and at least one threat or OSP.
ASE-OBJ.2-3-1	The evaluator shall examine the existence of traces between each security objective and threats, OSPs, assumptions, or a combination of threats, OSPs and/or assumptions
ASE-OBJ.2-3-2	The evaluator shall examine the existence of at least one trace between each security objective and threat, OSP or assumption.
ASE-OBJ.2-4-1	The evaluator shall examine rationality about that the security objectives rationale demonstrate that the security objectives are suitable to counter that threat.
ASE-OBJ.2-4-2	The evaluator shall examine sufficiency about taces between all security objectives and threats
ASE-OBJ.2-4-3	The evaluator shall examine necessity sufficiency about traces between all security objectives and threats
ASE-OBJ.2-4-4	The evaluator shall examine the justification for a threat demonstrates from the three element of threats
ASE-OBJ.2-5-1	The evaluator shall examine the rationality of demonstration that the security objectives are suitable to enforce that OSP.
ASE-OBJ.2-5-2	The evaluator shall examine sufficiency about all security objective that trace back to an OSP
ASE-OBJ.2-5-3	The evaluator shall examine necessity about each security objective that traces back to an OSP
ASE-OBJ.2-6-1	The evaluator shall examine rationality if demonstration that the security objectives are suitable to uphold that assumption

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ASE-OBJ.2-6-2	The evaluator shall examine sufficiency about all of security objectives trace back to an assumption
ASE-OBJ.2-6-3	The evaluator shall examine necessity about each security objective traces back to an assumption
ASE-ECD.1-0-1	The evaluator shall examine the existence of extended security requirements
ASE-ECD.1-1-1	The evaluator shall examine the rationality of the existence of SRs that all security requirements (not extended requirements) are present in CC Part 2 or in CC Part 3.
ASE-ECD.1-2-1	The evaluator shall examine the rationality of definition of extended component that A single extended component can be used to define multiple iterations of an extended security requirement
ASE-ECD.1-3-1	The evaluator shall examine the rationality of of definition of each extended component that it is either: a member of an existing CC Part 2 or CC Part 3 family, or a member of a new family defined in the ST.
ASE-ECD.1-3-2	The evaluator shall examine the rationality of definition of each extended component that it is a member of an existing CC Part 2 or CC Part 3 family
ASE-ECD.1-3-3	The evaluator shall examine the rationality of definition of each extended component that it is a member of a new family, is not appropriate for an existing family.
ASE-ECD.1-3-4	The evaluator shall examine the rationality of definition of new families that each new family is either: a member of an existing CC Part 2 or CC Part 3 class, or a member of a new class defined in the ST.
ASE-ECD.1-3-5	The evaluator shall examine the rationality of definition of the family that it is a member of an existing CC Part 2 or CC Part 3 class
ASE-ECD.1-3-6	The evaluator shall examine the rationality of definition of the family that it is not appropriate for an existing class.
ASE-ECD.1-4-1	The evaluator shall examine the rationality of definition of the family that no applicable dependencies have been overlooked
ASE-ECD.1-5-1	The evaluator shall examine the requirement of definition of extended functional component that its structure is consistent with CC Part 2 Section 7.1.3, Component structure.
ASE-ECD.1-5-2	The evaluator shall examine the consistency of the extended functional component that the extended functional component is consistent with CC Part 1 Annex C.4, Operations
ASE-ECD.1-5-3	The evaluator shall examine the consistency of the extended functional component that the extended functional component is consistent with CC Part 2 Section 7.2.1, Component changes highlighting
ASE-ECD.1-6-1	The evaluator shall examine consistency between all new functional families and CC Part 2 Section 7.1.2, Family structure

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ASE-ECD.1-7-1	The evaluator shall examine consistency between all new functional classes and CC Part 2 Section 7.1.1, Class structure
ASE-ECD.1-8-1	The evaluator shall examine consistency between the extended assurance and CC Part 3 Section 7.1.3, Assurance component structure
ASE-ECD.1-8-2	The evaluator shall examine the consistency of the extended assurance component that the extended assurance component is consistent with CC Part 1 Section Annex C.4, Operations
ASE-ECD.1-8-3	The evaluator shall examine the consistency of the extended assurance component that the extended assurance component is consistent with CC Part 3 Section 7.1.3, Assurance component structure
ASE-ECD.1-9-1	The evaluator shall examine the rationality of definition of each extended SAR that every elements of each extended SAR is a given element will demonstrate that the element has been achieved
ASE-ECD.1-10-1	The evaluator shall examine consistency between all new assurance families and CC Part 3 Section 7.1.2, Assurance family structure
ASE-ECD.1-11-1	The evaluator shall examine consistency between all new assurance classes and CC Part 3 Section 7.1.1, Assurance class structure
ASE-ECD.1-12-1	The evaluator shall examine the rationality of definition of extended functional components that their elements are stated in such a way that they are testable, and traceable through the appropriate TSF representations
ASE-ECD.1-12-2	The evaluator shall examine the rationality of definition of extended assurance components that their elements avoid the need for subjective judgment.
ASE-ECD.1-12-3	The evaluator shall examine the rationality of determination about the conformance between the extended component and the existing SFRs and SARs
ASE-ECD.1-13-1	The evaluator shall examine no misunderstanding of each extended component
ASE-REQ.1-1-1	The evaluator shall examine the existence of identification of each SFR
ASE-REQ.1-2-1	The evaluator shall examine the existence of identification of each SAR
ASE-REQ.1-3-1	The evaluator shall examine the existence of (types of) subjects and objects
ASE-REQ.1-3-2	The evaluator shall examine the existence of (types of) security attributes of subjects
ASE-REQ.1-3-3	The evaluator shall examine the existence of (types of) operations
ASE-REQ.1-3-4	The evaluator shall examine the existence of (types of) external entities
ASE-REQ.1-3-5	The evaluator shall examine the existence of other terms
ASE-REQ.1-3-6	The evaluator shall examine no misunderstanding of the description of the SFRs and SARs

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ASE-REQ.1-4-1	The evaluator shall examine the existence of identification of the operation type
ASE-REQ.1-5-1	The evaluator shall examine the rationality of the completion of SFR assignment operations
ASE-REQ.1-6-1	The evaluator shall examine the first the rationality of the completion of SFR iteration operations
ASE-REQ.1-6-2	The evaluator shall examine the second the rationality of the completion of iteration operations
ASE-REQ.1-7-1	The evaluator shall examine the rationality of the completion of SFR selection operations
ASE-REQ.1-8-1	The evaluator shall examine the first the rationality of the completion of SFR refinement operations
ASE-REQ.1-8-2	The evaluator shall examine the second the rationality of the completion of SFR refinement operations
ASE-REQ.1-9-1	The evaluator shall examine dependency of SFR that is satisfied by the inclusion of the relevant component (or one that is hierarchical to it) within the statement of security requirements
ASE-REQ.1-9-2	The evaluator shall examine the existence of a justification why a dependency is not met
ASE-REQ.1-10-1	The evaluator shall examine consistency in the combined set of all SFRs and SARs
ASE-REQ.2-1-1	The evaluator shall examine the existence of identification of each SFR
ASE-REQ.2-2-1	The evaluator shall examine the existence of identification of each SAR
ASE-REQ.2-3-1	The evaluator shall examine the existence of(types of) subjects and objects
ASE-REQ.2-4-1	The evaluator shall examine the existence of identification of the operation type.
ASE-REQ.2-5-1	The evaluator shall examine rule for SAR assignment operations
ASE-REQ.2-6-1	The evaluator shall examine rule for SAR an iteration operations
ASE-REQ.2-7-1	The evaluator shall examine rule for SAR selection operations
ASE-REQ.2-8-1	The evaluator shall examine rule for SAR refinement operations
ASE-REQ.2-9-1	The evaluator shall examine dependency that SAR should be satisfied
ASE-REQ.2-10-1	The evaluator shall examine the existence of traces between each SFR back to the security objectives
ASE-REQ.2-11-1	The evaluator shall examine sufficiency of the SFRs that trace back to security objectives
ASE-REQ.2-11-2	The evaluator shall examine necessity of each SFR that trace back to security objectives
ASE-REQ.2-12-1	The evaluator shall examine correctness of explanation of the traces that it is coherent and neither the SARs nor the explanation have obvious inconsistencies with the remainder of the PP.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ASE-REQ.2-13-1	The evaluator shall examine consistency in the combined set of all SFRs and SARs
ASE-TSS.1-1-1	The evaluator shall examine the existence of a description on how that SFR is met.
ASE-TSS.1-1-2	The evaluator shall examine the existence of description of a high-level view of how the developer intends to satisfy each SFR
ASE-TSS.1-1-3	The evaluator shall examine no misunderstanding of description for each SFR in the composed TOE
ASE-TSS.1-2-1	The evaluator shall examine consistency among TOE overview, TOE description, and TOE summary specification
ASE-TSS.2-1-1	The evaluator shall examine the existence of a description on how that SFR is met.
ASE-TSS.2-1-2	The evaluator shall examine the existence of a high-level view of how the developer intends to satisfy each SFR
ASE-TSS.2-1-3	The evaluator shall examine no misunderstanding of description for each SAR in the composed TOE
ASE-TSS.2-2-1	The evaluator shall examine the existence of a high-level view of how the developer intends to provide protection against interference and logical tampering.
ASE-TSS.2-2-2	The evaluator shall examine no misunderstanding of description for component that provides protection in the composed TOE
ASE-TSS.2-3-1	The evaluator shall examine the existence of a high-level view of how the developer intends to provide protection against bypass.
ASE-TSS.2-3-2	The evaluator shall examine no misunderstanding of description of how the components combine to provide protection
ASE-TSS.2-4-1	The evaluator shall examine no misunderstanding in TOE overview, TOE description, and TOE summary specification
ASE-TSS.2-4-2	The evaluator shall examine consistent among TOE overview, TOE description, and TOE summary specification
ASE-TSS.2-4-3	The evaluator shall examine the rationality of traces between TOE summary specification and the TOE overview

END

A.2 129 Detailed Tasks about Evaluation on Development Process

Table A.2: 129 Detailed Tasks about Evaluation on Development Process

Task ID	Description of Evaluation Tasks

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ADV-ARC.1-1-1	The evaluator shall examine the security architecture description to determine that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design document.
ADV-ARC.1-2-1	The evaluator shall examine the security architecture description to determine that it describes the security domains maintained by the TSF.
ADV-ARC.1-3-1	The evaluator shall examine the security architecture description to determine that the initialisation process preserves security.
ADV-ARC.1-4-1	The evaluator shall examine the security architecture description to determine that it contains information sufficient to support a determination that the TSF is able to protect itself from tampering by untrusted active entities.
ADV-ARC.1-5-1	The evaluator shall examine the security architecture description to determine that it presents an analysis that adequately describes how the SFR- enforcing mechanisms cannot be bypassed.
ADV-FSP.1-1-1	The evaluator shall examine the functional specification to determine that it states the purpose of each SFR-supporting and SFR-enforcing TSFI.
ADV-FSP.1-2-1	The evaluator shall examine the functional specification to determine that the method of use for each SFR-supporting and SFR-enforcing TSFI is given.
ADV-FSP.1-3-1	The evaluator shall examine the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing and SFR- supporting TSFI.
ADV-FSP.1-4-1	The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.
ADV-FSP.1-5-1	The evaluator shall list all TSFIs.
ADV-FSP.1-5-2	The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs.
ADV-FSP.1-6-1	The evaluator shall list all SFRs.
ADV-FSP.1-6-2	The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.
ADV-FSP.1-7-1	The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.
ADV-FSP.2-1-1	The evaluator shall examine the functional specification to determine that the TSF is fully represented.
ADV-FSP.2-10-1	The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.
ADV-FSP.2-2-1	The evaluator shall examine the functional specification to determine that it states the purpose of each TSFI.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ADV-FSP.2-3-1	The evaluator shall examine the functional specification to determine that the method of use for each TSFI is given.
ADV-FSP.2-4-1	The evaluator shall examine the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.
ADV-FSP.2-5-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.
ADV-FSP.2-6-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.
ADV-FSP.2-7-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes error messages that may result from SFR-enforcing actions associated with each SFR-enforcing TSFI.
ADV-FSP.2-8-1	The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs.
ADV-FSP.2-9-1	The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.
ADV-FSP.3-1-1	The evaluator shall examine the functional specification to determine that the TSF is fully represented.
ADV-FSP.3-10-1	The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.
ADV-FSP.3-11-1	The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.
ADV-FSP.3-2-1	The evaluator shall examine the functional specification to determine that it states the purpose of each TSFI.
ADV-FSP.3-3-1	The evaluator shall examine the functional specification to determine that the method of use for each TSFI is given.
ADV-FSP.3-4-1	The evaluator shall examine the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.
ADV-FSP.3-5-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.
ADV-FSP.3-6-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes the SFR-enforcing actions associated with the SFR-enforcing TSFIs.
ADV-FSP.3-7-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes error messages that may result from an invocation of each SFR-enforcing TSFI.
ADV-FSP.3-8-1	The evaluator shall examine the presentation of the TSFI to determine that it summarises the SFR-supporting and SFR-non-interfering actions associated with each TSFI.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ADV-FSP.3-9-1	The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs.
ADV-FSP.3-9-1	The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs.
ADV-FSP.4-1-1	The evaluator shall examine the functional specification to determine that the TSF is fully represented.
ADV-FSP.4-10-1	The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs.
ADV-FSP.4-11-1	The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.
ADV-FSP.4-12-1	The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.
ADV-FSP.4-2-1	The evaluator shall examine the functional specification to determine that it states the purpose of each TSFI.
ADV-FSP.4-3-1	The evaluator shall examine the functional specification to determine that the method of use for each TSFI is given.
ADV-FSP.4-4-1	The evaluator shall examine the functional specification to determine the completeness of the TSFI
ADV-FSP.4-5-1	The evaluator shall examine the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.
ADV-FSP.4-6-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all parameters associated with every TSFI.
ADV-FSP.4-7-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all actions associated with every TSFI.
ADV-FSP.4-8-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all errors messages resulting from an invocation of each TSFI.
ADV-FSP.4-9-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes the meaning of all error messages resulting from an invocation of each TSFI.
ADV-FSP.5-1-1	The evaluator shall examine the functional specification to determine that the TSF is fully represented.
ADV-FSP.5-10-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes the meaning of all error messages resulting from an invocation of each TSFI.
ADV-FSP.5-11-1	The evaluator shall examine the functional specification to determine that it completely and accurately describes all errors messages that do not result from an invocation of any TSFI.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ADV-FSP.5-12-1	The evaluator shall examine the functional specification to determine that it provides a rationale for each error message contained in the TSF implementation yet does not result from an invocation of a TSFI.
ADV-FSP.5-13-1	The evaluator shall check that the tracing links the SFRs to the corresponding TSFIs.
ADV-FSP.5-14-1	The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.
ADV-FSP.5-15-1	The evaluator shall examine the functional specification to determine that it is an accurate instantiation of the SFRs.
ADV-FSP.5-2-1	The evaluator shall examine the functional specification to determine that it is presented using a semiformal style.
ADV-FSP.5-3-1	The evaluator shall examine the functional specification to determine that it states the purpose of each TSFI.
ADV-FSP.5-5-1	The evaluator shall examine the functional specification to determine the completeness of the TSFI
ADV-FSP.5-6-1	The evaluator shall examine the presentation of the TSFI to determine that it completely identifies all parameters associated with every TSFI.
ADV-FSP.5-8-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all actions associated with every TSFI.
ADV-FSP.5-9-1	The evaluator shall examine the presentation of the TSFI to determine that it completely and accurately describes all errors messages resulting from an invocation of each TSFI.
ADV-IMP.1-1-1	The evaluator shall check that the implementation representation defines the TSF to a level of detail such that the TSF can be generated without further design decisions.
ADV-IMP.1-2-1	The evaluator shall check that the implementation representation is in the form used by development personnel.
ADV-IMP.1-3-1	The evaluator shall examine the mapping between the TOE design description and the sample of the implementation representation to determine that it is accurate.
ADV-INT.1-1-1	The evaluator shall examine the justification to determine that it identifies the basis for determining whether the TSF is well-structured.
ADV-INT.1-2-1	The evaluator shall check the TSF internals description to determine that it identifies the Assigned subset of the TSF.
ADV-INT.1-3-1	The evaluator shall examine the TSF internals description to determine that it demonstrates that the assigned TSF subset is well-structured.
ADV-INT.1-4-1	The evaluator shall determine that the TOE design for the assigned TSF subset is well-structured.
ADV-INT.1-5-1	The evaluator shall determine that the assigned TSF subset is well-structured.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ADV-INT.2-1-1	The evaluator shall examine the justification to determine that it identifies the basis for determining whether the TSF is well-structured.
ADV-INT.2-2-1	The evaluator shall examine the TSF internals description to determine that it demonstrates that the TSF is well-structured.
ADV-INT.2-3-1	The evaluator shall determine that the TOE design is well-structured.
ADV-INT.2-4-1	The evaluator shall determine that the TSF is well-structured.
ADV-TDS.1-1-1	The evaluator shall examine the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.
ADV-TDS.1-2-1	The evaluator shall examine the TOE design to determine that all subsystems of the TSF are identified.
ADV-TDS.1-3-1	The evaluator shall examine the TOE design to determine that each SFRsupporting or SFR-non-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-supporting or SFR-non-interfering.
ADV-TDS.1-4-1	The evaluator shall examine the TOE design to determine that it provides a complete; accurate; and high-level summary of the SFR-enforcing behaviourof the SFR-enforcing subsystems.
ADV-TDS.1-5-1	The evaluator shall examine the TOE design to determine that interactions between the subsystems of the TSF are described.
ADV-TDS.1-6-1	The evaluator shall examine the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.
ADV-TDS.1-7-1	The evaluator shall examine the TOE security functional requirements and the TOE design; to determine that all ST security functional requirements are covered by the TOE design.
ADV-TDS.1-7-2	The evaluator shall list all ST security functional requirements.
ADV-TDS.1-8-1	The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all security functional requirements.
ADV-TDS.2-1-1	The evaluator shall examine the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.
ADV-TDS.2-10-1	The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all security functional requirements.
ADV-TDS.2-2-1	The evaluator shall examine the TOE design to determine that all subsystems of the TSF are identified.
ADV-TDS.2-3-1	The evaluator shall examine the TOE design to determine that each SFRnon-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-non-interfering.
ADV-TDS.2-4-1	The evaluator shall examine the TOE design to determine that it provides a complete; accurate; and detailed description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ADV-TDS.2-5-1	The evaluator shall examine the TOE design to determine that it provides a complete and accurate high-level summary of the SFR-supporting and SFRnon-interfering behaviour of the SFR-enforcing subsystems.
ADV-TDS.2-6-1	The evaluator shall examine the TOE design to determine that it provides a complete and accurate high-level summary of the behaviour of the SFRsupporting subsystems.
ADV-TDS.2-7-1	The evaluator shall examine the TOE design to determine that interactions between the subsystems of the TSF are described.
ADV-TDS.2-8-1	The evaluator shall examine the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the subsystems of the TSF described in the TOE design.
ADV-TDS.2-9-1	The evaluator shall examine the TOE security functional requirements and the TOE design; to determine that all ST security functional requirements are covered by the TOE design.
ADV-TDS.3-1-1	The evaluator shall examine the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.
ADV-TDS.3-10-1	The evaluator shall examine the TOE design to determine that the description of the interfaces presented by each SFR-enforcing module contain an accurate and complete description of the SFR-related parameters; the invocation conventions for each interface; and any values returned directly by the interface.
ADV-TDS.3-10-2	The evaluator shall list all SFR-enforcing module contain.
ADV-TDS.3-11-1	The evaluator shall examine the TOE design to determine that SFR-supporting and SFR-non-interfering modules are correctly categorised.
ADV-TDS.3-12-1	The evaluator shall examine the TOE design to determine that the description of the purpose of each SFR-supporting or SFR-non-interfering module is complete and accurate.
ADV-TDS.3-12-2	The evaluator shall list all SFR-supporting or SFR-non-interfering modules.
ADV-TDS.3-13-1	The evaluator shall examine the TOE design to determine that the description of a SFR-supporting or SFR-non-interfering module's interaction with other modules is complete and accurate.
ADV-TDS.3-14-1	The evaluator shall examine the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the modules of the TSF described in the TOE design.
ADV-TDS.3-15-1	The evaluator shall examine the TOE security functional requirements and the TOE design; to determine that all ST security functional requirements are covered by the TOE design.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ADV-TDS.3-16-1	The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all security functional requirements.
ADV-TDS.3-2-1	The evaluator shall examine the TOE design to determine that the entire TSF is described in terms of modules.
ADV-TDS.3-3-1	The evaluator shall examine the TOE design to determine that all subsystems of the TSF are identified.
ADV-TDS.3-4-1	The evaluator shall examine the TOE design to determine that each subsystem of the TSF describes its role in the enforcement of SFRs described in the ST.
ADV-TDS.3-5-1	The evaluator shall examine the TOE design to determine that each SFRnon-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-non-interfering.
ADV-TDS.3-6-1	The evaluator shall examine the TOE design to determine that interactions between the subsystems of the TSF are described.
ADV-TDS.3-7-1	The evaluator shall examine the TOE design to determine that the mapping between the subsystems of the TSF and the modules of the TSF is complete.
ADV-TDS.3-8-1	The evaluator shall examine the TOE design to determine that the mapping between the subsystems of the TSF and the modules of the TSF is accurate.
ADV-TDS.3-9-1	The evaluator shall examine the TOE design to determine that the description of the purpose of each SFR-enforcing module and relationship with other modules is complete and accurate.
ADV-TDS.3-9-2	The evaluator shall list all SFR-enforcing modules and relationship with other modules.
ADV-TDS.4-1-1	The evaluator shall examine the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.
ADV-TDS.4-10-1	The evaluator shall examine the TOE design to determine that the mapping between the subsystems of the TSF to the modules of the TSF is accurate.
ADV-TDS.4-11-1	The evaluator shall examine the TOE design to determine that the description of the purpose of each SFR-enforcing and SFR-supporting module; and relationship with other modules is complete and accurate.
ADV-TDS.4-12-1	The evaluator shall examine the TOE design to determine that the description of the interfaces presented by each SFR-enforcing and SFR-supporting module contain an accurate and complete description of the SFRrelated parameters; the invocation conventions for each interface; and any values returned directly by the interface.
ADV-TDS.4-13-1	The evaluator shall examine the TOE design to determine that SFR-noninterfering modules are correctly categorised.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ADV-TDS.4-14-1	The evaluator shall examine the TOE design to determine that the description of the purpose of each SFR-non-interfering module is complete and accurate.
ADV-TDS.4-15-1	The evaluator shall examine the TOE design to determine that the description of a SFR-non-interfering module's interaction with other modules is complete and accurate.
ADV-TDS.4-16-1	The evaluator shall examine the TOE design to determine that it contains a complete and accurate mapping from the TSFI described in the functional specification to the modules of the TSF described in the TOE design.
ADV-TDS.4-17-1	The evaluator shall examine the TOE security functional requirements and the TOE design; to determine that all ST security functional requirements are covered by the TOE design.
ADV-TDS.4-18-1	The evaluator shall examine the TOE design to determine that it is an accurate instantiation of all security functional requirements.
ADV-TDS.4-2-1	The evaluator shall examine the TOE design to determine that the entire TSF is described in terms of modules.
ADV-TDS.4-3-1	The evaluator shall check the TOE design to determine that the TSF modules are identified as either SFR-enforcing; SFR-supporting; or SFRnon-interfering.
ADV-TDS.4-4-1	The evaluator shall examine the TOE design to determine that all subsystems of the TSF are identified.
ADV-TDS.4-5-1	The evaluator shall examine the TDS documentation to determine that the semiformal notation used for describing the subsystems; modules and their interfaces is defined or referenced.
ADV-TDS.4-6-1	The evaluator shall examine the TOE design to determine that each subsystem of the TSF describes its role in the enforcement of SFRs described in the ST.
ADV-TDS.4-7-1	The evaluator shall examine the TOE design to determine that each SFRnon-interfering subsystem of the TSF is described such that the evaluator can determine that the subsystem is SFR-non-interfering.
ADV-TDS.4-8-1	The evaluator shall examine the TOE design to determine that interactions between the subsystems of the TSF are described.
ADV-TDS.4-9-1	The evaluator shall examine the TOE design to determine that the mapping between the subsystems of the TSF and the modules of the TSF is complete.

END

A.3 11 Detailed Tasks about Evaluation on Guidance Document Process

Table A.3: 11 Detailed Tasks about
Evaluation on Guidance Document Process

Task ID	**Description of Evaluation Tasks**
AGD-OPE.1-1-1	The evaluator shall examine the operational user guidance to determine that it describes (for each user role) the user-accessible functions and privileges that should be controlled in a secure processing environment; including appropriate warnings.
AGD-OPE.1-2-1	The evaluator shall examine the operational user guidance to determine that it describes;; for each user role;; the secure use of the available interfaces provided by the TOE.
AGD-OPE.1-3-1	The evaluator shall examine the operational user guidance to determine that it describes;; for each user role;; the available security functionality and interfaces;; in particular all security parameters under the control of the user;; indicating secure values as appropriate.
AGD-OPE.1-4-1	The evaluator shall examine the operational user guidance to determine that it describes;; for each user role;; each type of security-relevant event relative to the user functions that need to be performed;; including changing the security characteristics of entities under the control of the TSF and operation following failure or operational error.
AGD-OPE.1-5-1	The evaluator shall examine the operational user guidance and other evaluation evidence to determine that the guidance identifies all possible modes of operation of the TOE (including;; if applicable;; operation following failure or operational error);; their consequences and implications for maintaining secure operation.
AGD-OPE.1-6-1	The evaluator shall examine the operational user guidance to determine that it describes;; for each user role;; the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD-OPE.1-7-1	The evaluator shall examine the operational user guidance to determine that it is clear.
AGD-OPE.1-8-1	The evaluator shall examine the operational user guidance to determine that it is reasonable.
AGD-PRE.1-1-1	The evaluator shall examine the provided acceptance procedures to determine that they describe the steps necessary for secure acceptance of the TOE in accordance with the developer's delivery procedures.
AGD-PRE.1-2-1	The evaluator shall examine the provided installation procedures to determine that they describe the steps necessary for secure installation of the TOE and the secure preparation of the operational environment in accordance with the security objectives in the ST.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AGD-PRE.1-3-1	The evaluator shall perform all user procedures necessary to prepare the TOE to determine that the TOE and its operational environment can be prepared securely using only the supplied preparative procedures.

END

A.4 133 Detailed Tasks about Evaluation on Life-cycle Support Process

Table A.4: 133 Detailed Tasks about Evaluation on Life-cycle Support Process

Task ID	Description of Evaluation Tasks
ALC-CMC.1-1	The evaluator shall check that the TOE provided for evaluation is labelled with its reference.
ALC-CMC.1-2	The evaluator shall check that the TOE references used are consistent.
ALC-CMC.2-1	The evaluator shall check that the TOE provided for evaluation is labelled with its reference.
ALC-CMC.2-2	The evaluator shall check that the TOE references used are consistent.
ALC-CMC.2-3	The evaluator shall examine the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.
ALC-CMC.2-4	The evaluator shall examine the configuration items to determine that they are identified in a way that is consistent with the CM documentation.
ALC-CMC.3-1	The evaluator shall check that the TOE provided for evaluation is labelled with its reference.
ALC-CMC.3-2	The evaluator shall check that the TOE references used are consistent.
ALC-CMC.3-3	The evaluator shall examine the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.
ALC-CMC.3-4	The evaluator shall examine the configuration items to determine that they are identified in a way that is consistent with the CM documentation.
ALC-CMC.3-5	The evaluator shall examine the CM access control measures described in the CM plan to determine that they are effective in preventing unauthorised access to the configuration items.
ALC-CMC.3-6	The evaluator shall check that the CM documentation provided includes a CM plan.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ALC-CMC.3-7	The evaluator shall examine the CM plan to determine that it describes how the CM system is used for the development of the TOE.
ALC-CMC.3-8	The evaluator shall check that the configuration items identified in the configuration list are being maintained by the CM system.
ALC-CMC.3-9	The evaluator shall check the CM documentation to ascertain that it includes the CM system records identified by the CM plan.
ALC-CMC.3-10	The evaluator shall examine the evidence to determine that the CM system is being operated in accordance with the CM plan.
ALC-CMC.4-1	The evaluator shall check that the TOE provided for evaluation is labelled with its reference.
ALC-CMC.4-2	The evaluator shall check that the TOE references used are consistent.
ALC-CMC.4-3	The evaluator shall examine the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.
ALC-CMC.4-4	The evaluator shall examine the configuration items to determine that they are identified in a way that is consistent with the CM documentation.
ALC-CMC.4-5	The evaluator shall examine the CM access control measures described in the CM plan (cf. ALC-CMC.4.6C) to determine that they are automated and effective in preventing unauthorised access to the configuration items.
ALC-CMC.4-6	The evaluator shall check the CM plan (cf. ALC-CMC.4.6C) for automated procedures for supporting the production of the TOE.
ALC-CMC.4-7	The evaluator shall examine the TOE production support procedures to determine that they are effective in ensuring that a TOE is generated that reflects its implementation representation.
ALC-CMC.4-8	The evaluator shall check that the CM documentation provided includes a CM plan.
ALC-CMC.4-9	The evaluator shall examine the CM plan to determine that it describes how the CM system is used for the development of the TOE.
ALC-CMC.4-10	The evaluator shall examine the CM plan to determine that it describes the procedures used to accept modified or newly created configuration items as parts of the TOE.
ALC-CMC.4-11	The evaluator shall check that the configuration items identified in the configuration list are being maintained by the CM system.
ALC-CMC.4-12	The evaluator shall check the CM documentation to ascertain that it includes the CM system records identified by the CM plan.
ALC-CMC.4-13	The evaluator shall examine the evidence to determine that the CM system is being operated in accordance with the CM plan.
ALC-CMC.5-1	The evaluator shall check that the TOE provided for evaluation is labelled with its reference.
ALC-CMC.5-2	The evaluator shall check that the TOE references used are consistent.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ALC-CMC.5-3	The evaluator shall examine the method of identifying configuration items to determine that it describes how configuration items are uniquely identified.
ALC-CMC.5-4	The evaluator shall examine the CM documentation to determine that it justifies that the acceptance procedures provide for an adequate and appropriate review of changes to all configuration items.
ALC-CMC.5-5	The evaluator shall examine the configuration items to determine that they are identified in a way that is consistent with the CM documentation.
ALC-CMC.5-6	The evaluator shall examine the CM access control measures described in the CM plan (cf. ALC-CMC.5.12C) to determine that they are automated and effective in preventing unauthorised access to the configuration items.
ALC-CMC.5-7	The evaluator shall check the CM plan (cf. ALC-CMC.5.12C) for automated procedures for supporting the production of the TOE.
ALC-CMC.5-8	The evaluator shall examine the TOE production support procedures to determine that they are effective in ensuring that a TOE is generated that reflects its implementation representation.
ALC-CMC.5-9	The evaluator shall examine the CM system to determine that it ensures that the person responsible for accepting a configuration item is not the person who developed it.
ALC-CMC.5-10	The evaluator shall examine the CM system to determine that it identifies the configuration items that comprise the TSF.
ALC-CMC.5-11	The evaluator shall examine the CM system to determine that it supports the audit of all changes to the TOE by automated means;; including the originator;; date;; and time in the audit trail.
ALC-CMC.5-12	The evaluator shall examine the CM system to determine that it provides an automated means to identify all other configuration items that are affected by the change of a given configuration item.
ALC-CMC.5-13	The evaluator shall examine the CM system to determine that it is able to identify the version of the implementation representation from which the TOE is generated.
ALC-CMC.5-14	The evaluator shall check that the CM documentation provided includes a CM plan.
ALC-CMC.5-15	The evaluator shall examine the CM plan to determine that it describes how the CM system is used for the development of the TOE.
ALC-CMC.5-16	The evaluator shall examine the CM plan to determine that it describes the procedures used to accept modified or newly created configuration items as parts of the TOE.
ALC-CMC.5-17	The evaluator shall check that the configuration items identified in the configuration list are being maintained by the CM system.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ALC-CMC.5-18	The evaluator shall check the CM documentation to ascertain that it includes the CM system records identified by the CM plan.
ALC-CMC.5-19	The evaluator shall examine the evidence to determine that the CM system is being operated in accordance with the CM plan.
ALC-CMC.5-20	The evaluator shall examine the production support procedures to determine that by following these procedures a TOE would be produced like that one provided by the developer for testing activities.
ALC-CMS.1-1	The evaluator shall check that the configuration list includes the following set of items: a) the TOE itself;
ALC-CMS.1-2	The evaluator shall check that the configuration list includes the following set of items: b) the evaluation evidence required by the SARs in the ST.
ALC-CMS.1-2	The evaluator shall examine the configuration list to determine that it uniquely identifies each configuration item.
ALC-CMS.2-1	The evaluator shall check that the configuration list includes the following set of items: a) the TOE itself;
ALC-CMS.2-1	he evaluator shall check that the configuration list includes the following set of items: b) the parts that comprise the TOE;
ALC-CMS.2-1	he evaluator shall check that the configuration list includes the following set of items: c) the evaluation evidence required by the SARs.
ALC-CMS.2-2	The evaluator shall examine the configuration list to determine that it uniquely identifies each configuration item.
ALC-CMS.2-3	The evaluator shall check that the configuration list indicates the developer of each TSF relevant configuration item.
ALC-CMS.2-3	The evaluator shall list the developer of each TSF relevant configuration item.
ALC-CMS.3-1	The evaluator shall check that the configuration list includes the following set of items: a) the TOE itself;
ALC-CMS.3-2	The evaluator shall check that the configuration list includes the following set of items: b) the parts that comprise the TOE;
ALC-CMS.3-3	The evaluator shall check that the configuration list includes the following set of items: c) the TOE implementation representation;
ALC-CMS.3-4	The evaluator shall check that the configuration list includes the following set of items: d) the evaluation evidence required by the SARs in the ST.
ALC-CMS.3-2	The evaluator shall examine the configuration list to determine that it uniquely identifies each configuration item.
ALC-CMS.3-3	The evaluator shall check that the configuration list indicates the developer of each TSF relevant configuration item.
ALC-CMS.4-1	The evaluator shall check that the configuration list includes the following set of items: a) the TOE itself;

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ALC-CMS.4-2	The evaluator shall check that the configuration list includes the following set of items: b) the parts that comprise the TOE;
ALC-CMS.4-3	The evaluator shall check that the configuration list includes the following set of items: c) the TOE implementation representation;
ALC-CMS.4-4	The evaluator shall check that the configuration list includes the following set of items: d) the evaluation evidence required by the SARs in the ST;
ALC-CMS.4-5	The evaluator shall check that the configuration list includes the following set of items: e) the documentation used to record details of reported security flaws associated with the implementation (e.g. problem status reports derived from a developer's problem database).
ALC-CMS.4-2	The evaluator shall examine the configuration list to determine that it uniquely identifies each configuration item.
ALC-CMS.4-3	The evaluator shall check that the configuration list indicates the developerof each TSF relevant configuration item.
ALC-CMS.5-1	The evaluator shall check that the configuration list includes the following set of items: a) the TOE itself;
ALC-CMS.5-2	The evaluator shall check that the configuration list includes the following set of items: b) the parts that comprise the TOE;
ALC-CMS.5-3	The evaluator shall check that the configuration list includes the following set of items: c) the TOE implementation representation;
ALC-CMS.5-4	The evaluator shall check that the configuration list includes the following set of items: d) the evaluation evidence required by the SARs in the ST;
ALC-CMS.5-5	The evaluator shall check that the configuration list includes the following set of items: e) the documentation used to record details of reported security flaws associated with the implementation (e.g. problem status reports derived from a developer's problem database);
ALC-CMS.5-6	The evaluator shall check that the configuration list includes the following set of items: f) all tools (incl. test software;; if applicable) involved in the development and production of the TOE including the names;; versions;; configurations and roles of each development tool;; and related documentation.
ALC-CMS.5-2	The evaluator shall examine the configuration list to determine that it uniquely identifies each configuration item.
ALC-CMS.5-3	The evaluator shall check that the configuration list indicates the developer of each TSF relevant configuration item.
ALC-DEL.1-1	The evaluator shall examine the delivery documentation to determine that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.
ALC-DEL.1-2	The evaluator shall examine aspects of the delivery process to determine that the delivery procedures are used.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ALC-DVS.1-1	The evaluator shall examine the development security documentation to determine that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation.
ALC-DVS.1-2	The evaluator shall examine the development confidentiality and integrity policies in order to determine the sufficiency of the security measures employed.
ALC-DVS.1-3	The evaluator shall examine the development security documentation and associated evidence to determine that the security measures are being applied.
ALC-DVS.2-1	The evaluator shall examine the development security documentation to determine that it details all security measures used in the development environment that are necessary to protect the confidentiality and integrity of the TOE design and implementation.
ALC-DVS.2-2	The evaluator shall examine the development security documentation to determine that an appropriate justification is given why the security measures provide the necessary level of protection to maintain the confidentiality and integrity of the TOE.
ALC-DVS.2-3	The evaluator shall examine the development confidentiality and integrity policies in order to determine the sufficiency of the security measures employed.
ALC-DVS.2-4	The evaluator shall examine the development security documentation and associated evidence to determine that the security measures are being applied.
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.
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.
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.
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.
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.
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.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
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.
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.
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.
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.
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.
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.
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 remediation procedures for each security flaw.
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.
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.
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.
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.
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.
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.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
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.
ALC-FLR.3-6	The evaluator shall examine the flaw remediation procedures to determine that the application of these procedures would result in a means for the developer to receive from TOE user reports of suspected security flaws or requests for corrections to such flaws.
ALC-FLR.3-7	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.
ALC-FLR.3-8	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.
ALC-FLR.3-9	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.
ALC-FLR.3-10	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 remediation procedures for each 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 safeguards that the potential correction contains no adverse effects.
ALC-FLR.3-12	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.
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.
ALC-FLR.3-14	The evaluator shall examine the flaw remediation guidance to determine that it identifies specific points of contact for user reports and enquiries about security issues involving the TOE.
ALC-LCD.1-1	The evaluator shall examine the documented description of the life-cycle model used to determine that it covers the development and maintenance process.
ALC-LCD.1-2	The evaluator shall examine the life-cycle model to determine that use of the procedures;; tools and techniques described by the life-cycle model will make the necessary positive contribution to the development and maintenance of the TOE.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ALC-LCD.2-1	The evaluator shall examine the documented description of the life-cycle model used to determine that it covers the development and maintenance process;; including the details of its arithmetic parameters and/or metrics used to measure the TOE development.
ALC-LCD.2-2	The evaluator shall examine the life-cycle model to determine that use of the procedures;; tools and techniques described by the life-cycle model will make the necessary positive contribution to the development and maintenance of the TOE.
ALC-LCD.2-3	The evaluator shall examine the life-cycle output documentation to determine that it provides the results of the measurements of the TOE development using the measurable life-cycle model.
ALC-TAT.1-1	The evaluator shall examine the development tool documentation provided to determine that each development tools is well-defined.
ALC-TAT.1-2	The evaluator shall examine the documentation of each development tool to determine that it unambiguously defines the meaning of all statements as well as all conventions and directives used in the implementation.
ALC-TAT.1-3	The evaluator shall examine the development tool documentation to determine that it unambiguously defines the meaning of all implementationdependent options.
ALC-TAT.2-1	The evaluator shall examine the development tool documentation provided to determine that each development tool is well-defined.
ALC-TAT.2-2	The evaluator shall examine the documentation of each development tool to determine that it unambiguously defines the meaning of all statements as well as all conventions and directives used in the implementation.
ALC-TAT.2-3	The evaluator shall examine the development tool documentation to determine that it unambiguously defines the meaning of all implementationdependent options.
ALC-TAT.2-4	The evaluator shall examine aspects of the implementation process to determine that documented implementation standards have been applied.
ALC-TAT.3-1	The evaluator shall examine the development tool documentation provided to determine that each development tool is well-defined.
ALC-TAT.3-2	The evaluator shall examine the documentation of each development tool to determine that it unambiguously defines the meaning of all statements as well as all conventions and directives used in the implementation.
ALC-TAT.3-3	The evaluator shall examine the development tool documentation to determine that it unambiguously defines the meaning of all implementationdependent options.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ALC-TAT.3-4	The evaluator shall examine aspects of the implementation process to determine that documented implementation standards have been applied.

END

A.5 70 Detailed Tasks about Evaluation on Test Process

Table A.5: 70 Detailed Tasks about Evaluation on Test Process

Task ID-1	Description of Evaluation Tasks
ATE-COV.1-1-1	The evaluator shall examine the test coverage evidence to determine that the correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification is accurate.
ATE-COV.2-1-1	The evaluator shall examine the test coverage analysis to determine that the correspondence between the tests in the test documentation and the interfaces in the functional specification is accurate.
ATE-COV.2-2-1	The evaluator shall list all interfaces.
ATE-COV.2-2-2	The evaluator shall examine the test plan to determine that the testing approach for each interface demonstrates the expected behaviour of that interface.
ATE-COV.2-3-1	The evaluator shall examine the test procedures to determine that the test prerequisites;; test steps and expected result(s) adequately test each interface.
ATE-COV.2-4-1	The evaluator shall examine the test coverage analysis to determine that the correspondence between the interfaces in the functional specification and the tests in the test documentation is complete.
ATE-DPT.1-1-1	The evaluator shall examine the depth of testing analysis to determine that the descriptions of the behaviour of TSF subsystems and of their interactions is included within the test documentation.
ATE-DPT.1-2-1	The evaluator shall examine the test plan;; test prerequisites;; test steps and expected result(s) to determine that the testing approach for the behaviour description demonstrates the behaviour of that subsystem as described in the TOE design.
ATE-DPT.1-3-1	The evaluator shall examine the test plan;; test prerequisites;; test steps and expected result(s) to determine that the testing approach for the behaviour description demonstrates the interactions among subsystems as described in the TOE design.

Continued on next page

Continued from previous page

Task ID-1	**Description of Evaluation Tasks**
ATE-DPT.1-4-1	The evaluator shall list all descriptions of TSF subsystem behaviour and interaction.
ATE-DPT.1-4-2	The evaluator shall examine the test procedures to determine that all descriptions of TSF subsystem behaviour and interaction are tested.
ATE-DPT.2-1-1	The evaluator shall examine the depth of testing analysis to determine that descriptions of the behaviour of TSF subsystems and of their interactions are included within the test documentation.
ATE-DPT.2-2-1	The evaluator shall examine the test plan;; test prerequisites;; test steps and expected result(s) to determine that the testing approach for the behaviour description demonstrates the behaviour of that subsystem as described in the TOE design.
ATE-DPT.2-3-1	The evaluator shall examine the test plan;; test prerequisites;; test steps and expected result(s) to determine that the testing approach for the behaviour description demonstrates the interactions among subsystems as described in the TOE design.
ATE-DPT.2-4-1	The evaluator shall examine the depth of testing analysis to determine that the interfaces of SFR-enforcing modules are included within the test documentation.
ATE-DPT.2-5-1	The evaluator shall examine the test plan;; test prerequisites;; test steps and expected result(s) to determine that the testing approach for each SFRenforcing module interface demonstrates the expected behaviour of that interface.
ATE-DPT.2-6-1	The evaluator shall examine the test procedures to determine that all descriptions of TSF subsystem behaviour and interaction are tested.
ATE-DPT.2-7-1	The evaluator shall list all interfaces of SFR-enforcing modules.
ATE-DPT.2-7-2	The evaluator shall examine the test procedures to determine that all interfaces of SFR-enforcing modules are tested.
ATE-DPT.3-1-1	The evaluator shall examine the depth of testing analysis to determine that descriptions of the behaviour of TSF subsystems and of their interactions are included within the test documentation.
ATE-DPT.3-2-1	The evaluator shall examine the test plan;; test prerequisites;; test steps and expected result(s) to determine that the testing approach for the behaviour description demonstrates the behaviour of that subsystem as described in the TOE design.
ATE-DPT.3-3-1	The evaluator shall examine the test plan;; test prerequisites;; test steps and expected result(s) to determine that the testing approach for the behaviour description demonstrates the interactions among subsystems as described in the TOE design.
ATE-DPT.3-4-1	The evaluator shall examine the depth of testing analysis to determine that the interfaces of TSF modules are included within the test documentation.

Continued on next page

Continued from previous page

Task ID-1	**Description of Evaluation Tasks**
ATE-DPT.3-5-1	The evaluator shall examine the test plan;; test prerequisites;; test steps and expected result(s) to determine that the testing approach for each TSF module interface demonstrates the expected behaviour of that interface.
ATE-DPT.3-6-1	The evaluator shall examine the test procedures to determine that all descriptions of TSF subsystem behaviour and interaction are tested.
ATE-DPT.3-7-1	The evaluator shall list all interfaces of all TSF modules.
ATE-DPT.3-7-2	The evaluator shall examine the test procedures to determine that all interfaces of all TSF modules are tested.
ATE-FUN.1-1-1	The evaluator shall check that the test documentation includes test plans;; expected test results and actual test results.
ATE-FUN.1-2-1	The evaluator shall examine the test plan to determine that it describes the scenarios for performing each test.
ATE-FUN.1-3-1	The evaluator shall examine the test plan to determine that the TOE test configuration is consistent with the ST.
ATE-FUN.1-4-1	The evaluator shall examine the test plans to determine that sufficient instructions are provided for any ordering dependencies.
ATE-FUN.1-5-1	The evaluator shall list all expected tests results.
ATE-FUN.1-5-2	The evaluator shall examine the test documentation to determine that all expected tests results are included.
ATE-FUN.1-6-1	The evaluator shall list the actual test results and the expected test results in the test documentation.
ATE-FUN.1-6-2	The evaluator shall check that the actual test results in the test documentation are consistent with the expected test results in the test documentation.
ATE-FUN.1-7-1	The evaluator shall report the developer testing effort;; outlining the testing approach;; configuration;; depth and results.
ATE-IND.1-1-1	The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.
ATE-IND.1-2-1	The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.
ATE-IND.1-3-1	The evaluator shall devise a test subset.
ATE-IND.1-4-1	The evaluator shall produce test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible.
ATE-IND.1-5-1	The evaluator shall conduct testing.
ATE-IND.1-6-1	The evaluator shall record the following information about the tests that compose the test subset: a) identification of the interface behaviour to be tested;
ATE-IND.1-6-2	b) instructions to connect and setup all required test equipment as required to conduct the test;

Continued on next page

Continued from previous page

Task ID-1	**Description of Evaluation Tasks**
ATE-IND.1-6-3	The evaluator shall record the following information about the tests that compose the test subset: c) instructions to establish all prerequisite test conditions;
ATE-IND.1-6-4	The evaluator shall record the following information about the tests that compose the test subset: d) instructions to stimulate the interface;
ATE-IND.1-6-5	The evaluator shall record the following information about the tests that compose the test subset: e) instructions for observing the behaviour of the interface;
ATE-IND.1-6-6	The evaluator shall record the following information about the tests that compose the test subset: f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;
ATE-IND.1-6-7	The evaluator shall record the following information about the tests that compose the test subset: g) instructions to conclude the test and establish the necessary post-test state for the TOE;
ATE-IND.1-6-8	The evaluator shall record the following information about the tests that compose the test subset: h) actual test results.
ATE-IND.1-7-1	The evaluator shall check that all actual test results are consistent with the expected test results.
ATE-IND.1-7-2	The evaluator shall list all actual test results and the expected test results.
ATE-IND.1-8-1	The evaluator shall report in the ETR the evaluator testing effort;; outlining the testing approach;; configuration;; depth and results.
ATE-IND.2-1-1	The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.
ATE-IND.2-2-1	The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.
ATE-IND.2-3-1	The evaluator shall examine the set of resources provided by the developer to determine that they are equivalent to the set of resources used by the developer to functionally test the TSF.
ATE-IND.2-4-1	The evaluator shall conduct testing using a sample of tests found in the developer test plan and procedures.
ATE-IND.2-5-1	The evaluator shall check that all the actual test results are consistent with the expected test results.
ATE-IND.2-6-1	The evaluator shall devise a test subset. The evaluator selects a test subset and testing strategy that is appropriate for the TOE.
ATE-IND.2-7-1	The evaluator shall produce test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible.
ATE-IND.2-8-1	The evaluator shall conduct testing. The evaluator uses the test documentation developed as a basis for executing tests on the TOE.

Continued on next page

Continued from previous page

Task ID-1	Description of Evaluation Tasks
ATE-IND.2-9-1	The evaluator shall record the following information about the tests that compose the test subset: a) identification of the interface behaviour to be tested;
ATE-IND.2-9-2	The evaluator shall record the following information about the tests that compose the test subset: b) instructions to connect and setup all required test equipment as required to conduct the test;
ATE-IND.2-9-3	The evaluator shall record the following information about the tests that compose the test subset: c) instructions to establish all prerequisite test conditions;
ATE-IND.2-9-4	The evaluator shall record the following information about the tests that compose the test subset: d) instructions to stimulate the interface;results.
ATE-IND.2-9-5	The evaluator shall record the following information about the tests that compose the test subset: e) instructions for observing the interface;
ATE-IND.2-9-6	The evaluator shall record the following information about the tests that compose the test subset: f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;
ATE-IND.2-9-7	The evaluator shall record the following information about the tests that compose the test subset: g) instructions to conclude the test and establish the necessary post-test state for the TOE;
ATE-IND.2-9-8	The evaluator shall record the following information about the tests that compose the test subset: h) actual test
ATE-IND.2-10-1	The evaluator shall check that all actual test results are consistent with the expected test results.
ATE-IND.2-11-1	The evaluator shall report in the ETR the evaluator testing effort;; outlining the testing approach;; configuration;; depth and results.

END

A.6 86 Detailed Tasks about Evaluation on Vulnerability Assessment Process

Table A.6: 86 Detailed Tasks about
Evaluation on Vulnerability Assessment Process

Task ID	Description of Evaluation Tasks

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AVA-VAN.1-1-1	The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.
AVA-VAN.1-2-1	The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.
AVA-VAN.1-3-1	The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.
AVA-VAN.1-4-1	The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.
AVA-VAN.1-5-1	The evaluator shall devise penetration tests;; based on the independent search for potential vulnerabilities.
AVA-VAN.1-6-1	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: a) identification of the potential vulnerability the TOE is being tested for;
AVA-VAN.1-6-2	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: b) instructions to connect and setup all required test equipment as required to conduct the penetration test;
AVA-VAN.1-6-3	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: c) instructions to establish all penetration test prerequisite initial conditions;
AVA-VAN.1-6-4	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: d) instructions to stimulate the TSF;
AVA-VAN.1-6-5	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: e) instructions for observing the behaviour of the TSF;
AVA-VAN.1-6-6	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AVA-VAN.1-6-7	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: g) instructions to conclude the test and establish the necessary post-test state for the TOE.
AVA-VAN.1-7-1	The evaluator shall conduct penetration testing. The evaluator uses the penetration test documentation resulting from work unit AVA-VAN.1-5 as a basis for executing penetration tests on the TOE;; but this does not preclude the evaluator from performing additional ad hoc penetration tests.
AVA-VAN.1-8-1	The evaluator shall record the actual results of the penetration tests
AVA-VAN.1-9-1	The evaluator shall report in the ETR the evaluator penetration testing effort;; outlining the testing approach;; configuration;; depth and results.
AVA-VAN.1-10-1	The evaluator shall examine the results of all penetration testing to determine that the TOE;; in its operational environment;; is resistant to an attacker possessing a Basic attack potential.
AVA-VAN.1-11-1	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: a) its source (e.g. CEM activity being undertaken when it was conceived;; known to the evaluator;; read in a publication);
AVA-VAN.1-11-2	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: b) the SFR(s) not met;
AVA-VAN.1-11-3	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: c) a description;
AVA-VAN.1-11-4	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual).
AVA-VAN.1-11-5	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: e) the amount of time;; level of expertise;; level of knowledge of the TOE;; level of opportunity and the equipment required to perform the identified vulnerabilities;; and the corresponding values using the tables 3 and 4 of Annex B.4.
AVA-VAN.2-1-1	The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.
AVA-VAN.2-2-1	The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state
AVA-VAN.2-3-1	The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AVA-VAN.2-4-1	The evaluator shall conduct a search of ST;; guidance documentation;; functional specification;; TOE design and security architecture description evidence to identify possible potential vulnerabilities in the TOE.
AVA-VAN.2-5-1	The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.
AVA-VAN.2-6-1	The evaluator shall devise penetration tests;; based on the independent search for potential vulnerabilities.
AVA-VAN.2-7-1	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: a) identification of the potential vulnerability the TOE is being tested for;
AVA-VAN.2-7-2	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: b) instructions to connect and setup all required test equipment as required to conduct the penetration test;
AVA-VAN.2-7-3	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: c) instructions to establish all penetration test prerequisite initial conditions;
AVA-VAN.2-7-4	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: d) instructions to stimulate the TSF;
AVA-VAN.2-7-5	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: e) instructions for observing the behaviour of the TSF;
AVA-VAN.2-7-6	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AVA-VAN.2-7-7	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: g) instructions to conclude the test and establish the necessary post-test state for the TOE.
AVA-VAN.2-8-1	The evaluator shall conduct penetration testing. The evaluator uses the penetration test documentation resulting from work unit AVA-VAN.2-6 as a basis for executing penetration tests on the TOE;; but this does not preclude the evaluator from performing additional ad hoc penetration tests.
AVA-VAN.2-9-1	The evaluator shall record the actual results of the penetration tests.
AVA-VAN.2-10-1	The evaluator shall report in the ETR the evaluator penetration testing effort;; outlining the testing approach;; configuration;; depth and results.
AVA-VAN.2-11-1	The evaluator shall examine the results of all penetration testing to determine that the TOE;; in its operational environment;; is resistant to an attacker possessing a Basic attack potential.
AVA-VAN.2-12-1	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: a) its source (e.g. CEM activity being undertaken when it was conceived;; known to the evaluator;; read in a publication);
AVA-VAN.2-12-2	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: b) the SFR(s) not met;
AVA-VAN.2-12-3	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: c) a description;
AVA-VAN.2-12-4	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each:) whether it is exploitable in its operational environment or not (i.e.exploitable or residual).
AVA-VAN.2-12-5	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: e) the amount of time;; level of expertise;; level of knowledge of the TOE;; level of opportunity and the equipment required to perform the identified vulnerabilities;; and the corresponding values using the tables 3 and 4 of Annex B.4.
AVA-VAN.3-1-1	The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.
AVA-VAN.3-2-1	The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state
AVA-VAN.3-3-1	The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AVA-VAN.3-4-1	The evaluator shall conduct a focused search of ST;; guidance documentation;; functional specification;; TOE design;; security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE.
AVA-VAN.3-6-1	The evaluator shall devise penetration tests;; based on the independent search for potential vulnerabilities.
AVA-VAN.3-7-1	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: a) identification of the potential vulnerability the TOE is being tested for;
AVA-VAN.3-7-2	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: b) instructions to connect and setup all required test equipment as required to conduct the penetration test;
AVA-VAN.3-7-3	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: c) instructions to establish all penetration test prerequisite initial conditions;
AVA-VAN.3-7-4	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: d) instructions to stimulate the TSF;
AVA-VAN.3-7-5	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include:e) instructions for observing the behaviour of the TSF;
AVA-VAN.3-7-6	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;
AVA-VAN.3-7-7	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: g) instructions to conclude the test and establish the necessary post-test state for the TOE.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AVA-VAN.3-8-1	The evaluator shall conduct penetration testing. The evaluator uses the penetration test documentation resulting from work unit AVA-VAN.3-6 as a basis for executing penetration tests on the TOE;; but this does not preclude the evaluator from performing additional ad hoc penetration tests.
AVA-VAN.3-9-1	The evaluator shall record the actual results of the penetration tests.
AVA-VAN.3-10-1	The evaluator shall report in the ETR the evaluator penetration testing effort;; outlining the testing approach;; configuration;; depth and results.
AVA-VAN.3-11-1	The evaluator shall examine the results of all penetration testing to determine that the TOE;; in its operational environment;; is resistant to an attacker possessing an Enhanced-Basic attack potential.
AVA-VAN.3-12-1	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: a) its source (e.g. CEM activity being undertaken when it was conceived;; known to the evaluator;; read in a publication);
AVA-VAN.3-12-2	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: b) the SFR(s) not met;
AVA-VAN.3-12-3	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: c) a description;
AVA-VAN.3-12-4	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual).
AVA-VAN.3-12-5	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: e) the amount of time;; level of expertise;; level of knowledge of the TOE;; level of opportunity and the equipment required to perform the identified vulnerabilities;; and the corresponding values using the tables 3 and 4 of Annex B.4.
AVA-VAN.4-1-1	The evaluator shall examine the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST.
AVA-VAN.4-2-1	The evaluator shall examine the TOE to determine that it has been installed properly and is in a known state.
AVA-VAN.4-3-1	The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.
AVA-VAN.4-4-1	The evaluator shall conduct a methodical analysis of ST;; guidance documentation;; functional specification;; TOE design;; security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AVA-VAN.4-5-1	The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.
AVA-VAN.4-6-1	The evaluator shall devise penetration tests;; based on the independent search for potential vulnerabilities.
AVA-VAN.4-7-1	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: a) identification of the potential vulnerability the TOE is being tested for;
AVA-VAN.4-7-2	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: b) instructions to connect and setup all required test equipment as required to conduct the penetration test;
AVA-VAN.4-7-3	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: c) instructions to establish all penetration test prerequisite initial conditions;
AVA-VAN.4-7-4	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: d) instructions to stimulate the TSF;
AVA-VAN.4-7-5	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: e) instructions for observing the behaviour of the TSF;
AVA-VAN.4-7-6	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: f) descriptions of all expected results and the necessary analysis to be performed on the observed behaviour for comparison against expected results;
AVA-VAN.4-7-7	The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable. The test documentation shall include: g) instructions to conclude the test and establish the necessary post-test state for the TOE.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
AVA-VAN.4-8-1	The evaluator shall conduct penetration testing. The evaluator uses the penetration test documentation resulting from work unit AVA-VAN.4-6 as a basis for executing penetration tests on the TOE;; but this does not preclude the evaluator from performing additional ad hoc penetration tests.
AVA-VAN.4-9-1	The evaluator shall record the actual results of the penetration tests.
AVA-VAN.4-10-1	The evaluator shall report in the ETR the evaluator penetration testing effort;; outlining the testing approach;; configuration;; depth and results.
AVA-VAN.4-11-1	The evaluator shall examine the results of all penetration testing to determine that the TOE;; in its operational environment;; is resistant to an attacker possessing a Moderate attack potential.
AVA-VAN.4-12-1	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: a) its source (e.g. CEM activity being undertaken when it was conceived;; known to the evaluator;; read in a publication);
AVA-VAN.4-12-2	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: b) the SFR(s) not met;
AVA-VAN.4-12-3	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: c) a description;
AVA-VAN.4-12-4	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: d) whether it is exploitable in its operational environment or not (i.e.exploitable or residual).
AVA-VAN.4-12-5	The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities;; detailing for each: e) the amount of time;; level of expertise;; level of knowledge of the TOE;; level of opportunity and the equipment required to perform the identified vulnerabilities;; and the corresponding values using the tables 3 and 4 of Annex B.4.

END

A.7 77 Detailed Tasks about Evaluation on Composition Process

Table A.7: 77 Detailed Tasks about Evaluation on Composition Process

Task ID	Description of Evaluation Tasks

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ACO-COR.1-1.1	The evaluator shall identify the interfaces that are relied upon by the dependent component which are not detailed in the development information.
ACO-COR.1-1	The evaluator shall examine the correspondence analysis with the development information and the reliance information to identify the interfaces that are relied upon by the dependent component which are not detailed in the development information.
ACO-COR.1-2	The evaluator shall examine the composition rationale to determine, for those included base component interfaces on which the dependent TSF relies, whether the interface was considered during the evaluation of the base component.
ACO-COR.1-3	The evaluator shall examine the composition rationale to determine that the necessary assurance measures have been applied to the base component.
ACO-DEV.1-1	The evaluator shall examine the development information to determine that it describes the purpose of each interface.
ACO-DEV.1-2	The evaluator shall examine the development information to determine the correspondence, between the interfaces of the base component and the interfaces on which the dependent component relies, is accurate.
ACO-DEV.1-3	The evaluator shall examine the development information and the reliance information to determine that the interfaces are described consistently.
ACO-DEV.2-1.1	
ACO-DEV.2-1	The evaluator shall examine the development information to determine that it describes the purpose of each interface.
ACO-DEV.2-2	The evaluator shall examine the development information to determine that it describes the method of use for each interface.
ACO-DEV.2-3	The evaluator shall examine the development information to determine that it describes the behaviour of the base component that supports the enforcement of the dependent component SFRs.
ACO-DEV.2-4	The evaluator shall examine the development information to determine the correspondence, between the interfaces of the base component and the interfaces on which the dependent component relies, is accurate.
ACO-DEV.2-5	The evaluator shall examine the development information and the reliance information to determine that the interfaces are described consistently.
ACO-DEV.3-1	The evaluator shall examine the development information to determine that it describes the purpose of each interface.
ACO-DEV.3-2	The evaluator shall examine the development information to determine that it describes the method of use for each interface.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ACO-DEV.3-3.1	The evaluator shall list all subsystems of the base component that provide interfaces to the dependent component are identified.
ACO-DEV.3-3	The evaluator shall examine the development information to determine that all subsystems of the base component that provide interfaces to the dependent component are identified.
ACO-DEV.3-4	The evaluator shall examine the development information to determine that it describes the behaviour of the base component subsystems that support the enforcement of the dependent component SFRs.
ACO-DEV.3-5	The evaluator shall examine the development information to determine that the correspondence between the interfaces and subsystems of the base component is accurate.
ACO-DEV.3-6	The evaluator shall examine the development information to determine the correspondence, between the interfaces of the base component and the interfaces on which the dependent component relies, is accurate.
ACO-DEV.3-7	The evaluator shall examine the development information and the reliance information to determine that the interfaces are described consistently.
ACO-REL.1-1	The evaluator shall check the reliance information to determine that it describes the functionality of the base dependent hardware, firmware and/or software that is relied upon by the dependent component TSF.
ACO-REL.1-2	The evaluator shall examine the reliance information to determine that it accurately reflects the objectives specified for the operational environment of the dependent component.
ACO-REL.1-3.1	
ACO-REL.1-3	The evaluator shall examine the reliance information to determine that it describes all interactions between the dependent component and the base component, through which the dependent component TSF requests services from the base component.
ACO-REL.1-4	The evaluator shall examine the reliance information to determine that it describes how the dependent TSF protects itself from interference and tampering by the base component.
ACO-REL.2-1	The evaluator shall check the reliance information to determine that it describes the functionality of the base dependent hardware, firmware and/or software that is relied upon by the dependent component TSF.
ACO-REL.2-2	The evaluator shall examine the reliance information to determine that it accurately reflects the objectives specified for the operational environment of the dependent component.
ACO-REL.2-3.1	

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ACO-REL.2-3	The evaluator shall examine the reliance information to determine that it describes all interactions between the dependent component and the base component, through which the dependent component TSF requests services from the base component.
ACO-REL.2-4	The reliance information shall describe each interaction in terms of the interface used and the return values from those interfaces.
ACO-REL.2-5	The evaluator shall examine the reliance information to determine that it describes how the dependent TSF protects itself from interference and tampering by the base component.
ACO-CTT.1-1	The evaluator shall examine the composed TOE test documentation to determine that it consists of test plans, expected test results and actual test results
ACO-CTT.1-2	The evaluator shall examine the base component interface test documentation to determine that it consists of test plans, expected test results and actual test results.
ACO-CTT.1-3	The evaluator shall examine the test documentation to determine that the developer execution of the composed TOE tests shall demonstrate that the TSF behaves as specified.
ACO-CTT.1-4	The evaluator shall examine the test documentation to determine that the developer execution of the base component interface tests shall demonstrate that the base component interfaces relied upon by the dependent component behave as specified.
ACO-CTT.1-5	The evaluator shall examine the composed TOE to determine that it has been installed properly and is in a known state.
ACO-CTT.1-6	The evaluator shall examine the set of resources provided by the developer to determine that they are equivalent to the set of resources used by the base component developer to functionally test the base component.
ACO-CTT.1-7	The evaluator shall perform testing in accordance with ATE-IND.2.2E, for a subset of the SFRs specified in the composed security target, to verify the developer test results.
ACO-CTT.1-8	The evaluator shall perform testing in accordance with ATE-IND.2.3E, for a subset of the SFRs specified in the composed security target, to confirm that the TSF operates as specified.
ACO-CTT.2-1	The evaluator shall examine the composed TOE test documentation to determine that it consists of test plans, expected test results and actual test results.
ACO-CTT.2-2	The evaluator shall examine the base component interface test documentation to determine that it consists of test plans, expected test results and actual test results.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ACO-CTT.2-3	The evaluator shall examine the test documentation to determine that it provides accurate correspondence between the tests in the test documentation relating to the testing of the composed TOE and the composed TOE SFRs in the composed TOE security target.
ACO-CTT.2-4	The evaluator shall examine the test documentation to determine that the developer execution of the composed TOE tests shall demonstrate that the TSF behaves as specified.
ACO-CTT.2-5	The evaluator shall examine the test documentation to determine that it provides accurate correspondence between the tests in the test documentation relating to the testing of the base component interfaces relied upon by the dependent component and the interfaces specified in the reliance information.
ACO-CTT.2-6	The evaluator shall examine the test documentation to determine that the developer execution of the base component interface tests shall demonstrate that the base component interfaces relied upon by the dependent component behave as specified.
ACO-CTT.2-7	The evaluator shall examine the composed TOE to determine that it hasbeen installed properly and is in a known state.
ACO-CTT.2-8	The evaluator shall examine the set of resources provided by the developer to determine that they are equivalent to the set of resources used by the base component developer to functionally test the base component.
ACO-CTT.2-9	The tests are to be selected and executed in accordance with ATE-IND.2.2E, to demonstrate the correct behaviour of the SFRs specified in the composed TOE security target.
ACO-CTT.2-10	The evaluator shall perform testing in accordance with ATE-IND.2.3E, for a subset of the SFRs specified in the composed security target, to confirm that the TSF operates as specified.
ACO-CTT.2-11	The evaluator shall perform testing, in accordance with Evaluation of subactivity (ATE-IND.2), for a subset of the interfaces to the base component to confirm they operate as specified.
ACO-VUL.1-1	The evaluator shall examine the composed TOE to determine that it has been installed properly and is in a known state.
ACO-VUL.1-2	The evaluator shall examine the composed TOE configuration to determine that any assumptions and objectives in the STs the components relating to IT entities for are fulfilled by the other components.
ACO-VUL.1-3	The evaluator shall examine the residual vulnerabilities from the base component evaluation to determine that they are not exploitable in the composed TOE in its operational environment.
ACO-VUL.1-4	The evaluator shall examine the residual vulnerabilities from the dependent component evaluation to determine that they are not exploitable in the composed TOE in its operational environment.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ACO-VUL.1-5	The evaluator shall examine the sources of information publicly available to support the identification of possible security vulnerabilities in the base component that have become known since the completion of evaluation of the base component.
ACO-VUL.1-6	The evaluator shall examine the sources of information publicly available to support the identification of possible security vulnerabilities in the dependent component that have become known since the completion of the dependent component evaluation.
ACO-VUL.1-7	The evaluator shall record in the ETR the identified potential security vulnerabilities that are candidates for testing and applicable to the composed TOE in its operational environmen.
ACO-VUL.1-8	The evaluator shall conduct penetration testing as detailed for AVA-VAN.1.3E.
ACO-VUL.2-1	The evaluator shall examine the composed TOE to determine that it has been installed properly and is in a known state.
ACO-VUL.2-2	The evaluator shall examine the composed TOE configuration to determine that any assumptions and objectives in the STs the components relating to IT entities for are fulfilled by the other components.
ACO-VUL.2-3	The evaluator shall examine the residual vulnerabilities from the base component evaluation to determine that they are not exploitable in the composed TOE in its operational environment.
ACO-VUL.2-4	The evaluator shall examine the residual vulnerabilities from the dependent component evaluation to determine that they are not exploitable in the composed TOE in its operational environment.
ACO-VUL.2-5	The evaluator shall examine the sources of information publicly available to support the identification of possible security vulnerabilities in the base component that have become known since the completion of the base component evaluation.
ACO-VUL.2-6	The evaluator shall examine the sources of information publicly available to support the identification of possible security vulnerabilities in the dependent component that have become known since the completion of the dependent component evaluation.
ACO-VUL.2-7	The evaluator shall record in the ETR the identified potential security vulnerabilities that are candidates for testing and applicable to the composed TOE in its operational environment.
ACO-VUL.2-8	The evaluator shall conduct a search of the composed TOE ST, guidance documentation, reliance information and composition rationale to identify possible security vulnerabilities in the composed TOE.
ACO-VUL.2-9	The evaluator shall conduct penetration testing as detailed for AVA-VAN.2.4E.
ACO-VUL.3-1	The evaluator shall examine the composed TOE to determine that it has been installed properly and is in a known state.

Continued on next page

Continued from previous page

Task ID	Description of Evaluation Tasks
ACO-VUL.3-2	The evaluator shall examine the composed TOE configuration to determine that any assumptions and objectives in the STs the components relating to IT entities for are fulfilled by the other components.
ACO-VUL.3-3	The evaluator shall examine the residual vulnerabilities from the base component evaluation to determine that they are not exploitable in the composed TOE in its operational environment.
ACO-VUL.3-4	The evaluator shall examine the residual vulnerabilities from the dependent component evaluation to determine that they are not exploitable in the composed TOE in its operational environment.
ACO-VUL.3-5	The evaluator shall examine the sources of information publicly available to support the identification of possible security vulnerabilities in the base component that have become known since the completion of the base component evaluation.
ACO-VUL.3-6	The evaluator shall examine the sources of information publicly available to support the identification of possible security vulnerabilities in the dependent component that have become known since completion of the dependent component evaluation.
ACO-VUL.3-7	The evaluator shall record in the ETR the identified potential security vulnerabilities that are candidates for testing and applicable to the composed TOE in its operational environment.
ACO-VUL.3-8	The evaluator shall conduct a search of the composed TOE ST, guidance documentation, reliance information and composition rationale to identify possible security vulnerabilities in the composed TOE.
ACO-VUL.3-9	The evaluator shall conduct penetration testing as detailed for AVA-VAN.3.4E.

END