Federal Office
for Information Security

Guidelines for Evaluation Reports according to CC 3.1

Christian Krause
Bundesamt für Sicherheit in der Informationstechnik

Dr. Igor Furgel
T-Systems GEI GmbH

9ICCC / 25 September, 2008

9th ICCC
9th International Common Criteria Conference

Comprehensive
Evaluation Reports required

- One of the main tasks of a CB is
  - Ensuring that different evaluations will be conducted at a comparable level of quality
- Comprehensive evaluation reports are an important contribution to this

Comprehensive Evaluation Reports required

- ❒ A comprehensive evaluation report
  - ❒ helps the reader to understand
    - ❒ the technical scope of the evaluation activities,
    - ❒ how the evaluator has interpreted and applied the CC/CEM requirements
  - ❒ and facilitates reuse of evaluation results

Difficulties when writing Evaluation Reports

- ❐ CEM defines the minimum actions to be performed by an evaluator in detail,
- ❐ but contains only general requirements for the *documentation* of the evaluation activities

Difficulties when writing Evaluation Reports

- ❒ Therefore it is difficult for evaluators to anticipate <u>what the required content of an evaluation report exactly is</u>

- ❒ This often leads to time consuming iterations between the evaluation facilities (ITSEF) and the certification bodies (CB) until the report can be approved by the CB

Guidelines for Evaluation Reports

- To support the certification and evaluation process, BSI has issued

**Guidelines for Evaluation Reports
according to Common Criteria Version 3.1**

Guidelines for Evaluation Reports

- The objectives are
  - less review cycles for evaluation reports
  - better planning reliability
  - higher comparability of different evaluations

Guidelines for Evaluation Reports

- The guidelines
  - assume that the evaluation activity is perfectly done
  - are focused on the *documentation* of the evaluation activity

Guidelines for Evaluation Reports

- The guidelines offer assistance to evaluators by
  - Advises and recommendations
    - on the structure of evaluation reports and
    - on the information to be provided in the evaluation reports for each work unit of the CEM up to EAL5
  - Examples giving an impression about the required level of detail
  - Hints about the context and how evaluation activities can be economized
  - General structure of evaluation reports that can be used as template

Structure of Evaluation Reports

- For each work unit, the evaluation report shall contain the following sections
  - The main body of the work unit (for a better readability)
  - Evaluator's summary of the developer's evidence
  - Justified analysis of the developer's contribution(s)
  - Justified evaluator's assessment and verdict

Information to be provided in Evaluation Reports

- The evaluator's summary shall contain
  - a summary of the relevant information with the own words of the evaluator
  - and precise references to the developer evidence
- It gives the reader of the report an opportunity to check, whether the evaluator has
  - considered all relevant facts
  - understood the product correctly

Information to be provided in Evaluation Reports

- The justified analysis shall show how
  - the evaluator has used the relevant information
  - the evaluation evidence fulfils the requirements of the work unit
- The analysis shall be documented in such a way that the evaluator's verdict is comprehensible without additional evaluations by the reader of the report

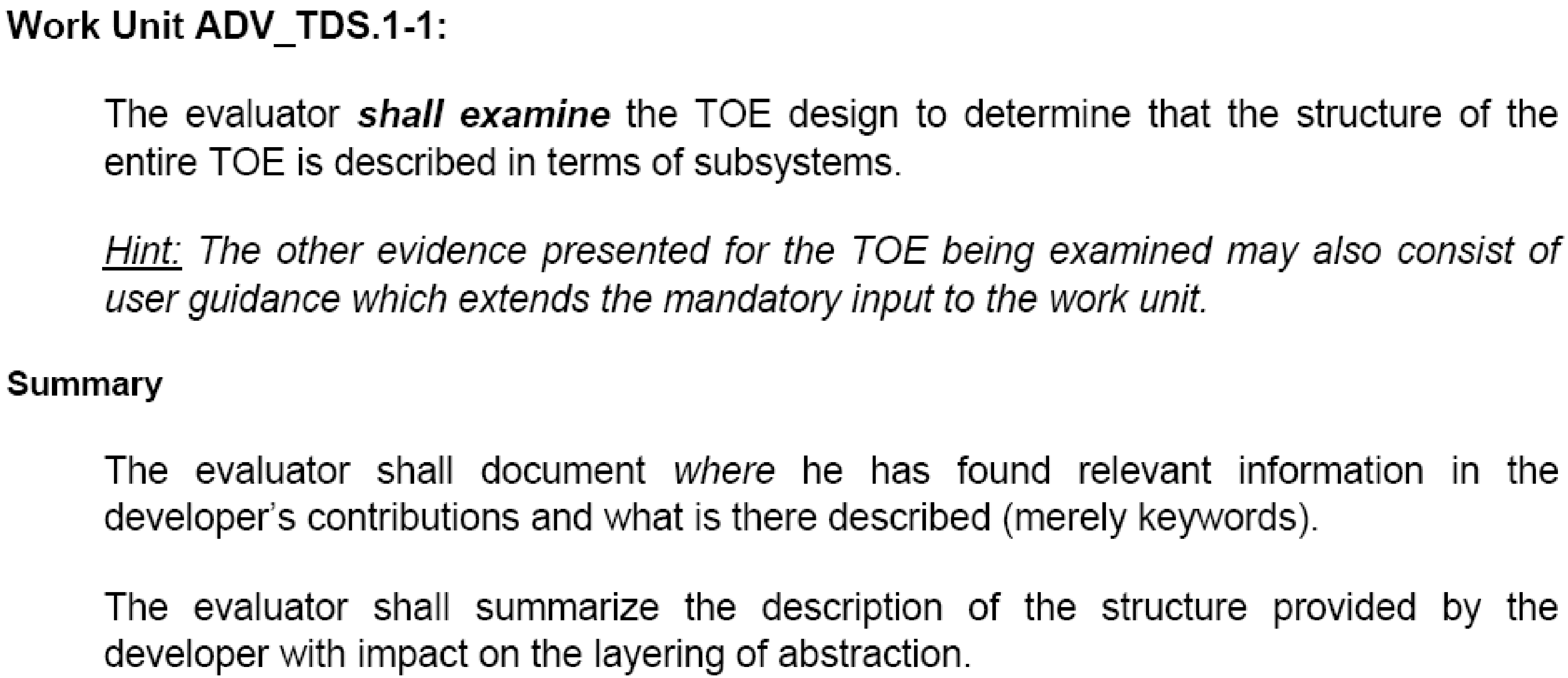
Information to be provided in Evaluation Reports

- The justified evaluator's assessment and verdict shall contain, for each question of a work unit, a clear statement, whether the requirements are fulfilled or not

- For each work unit, the evaluator shall state, whether all requirements of a work unit are fulfilled or not

Guidelines for Evaluation Reports

Example 1:



Work Unit ADV_TDS.1-1:

The evaluator ***shall examine*** the TOE design to determine that the structure of the entire TOE is described in terms of subsystems.

Hint: The other evidence presented for the TOE being examined may also consist of user guidance which extends the mandatory input to the work unit.

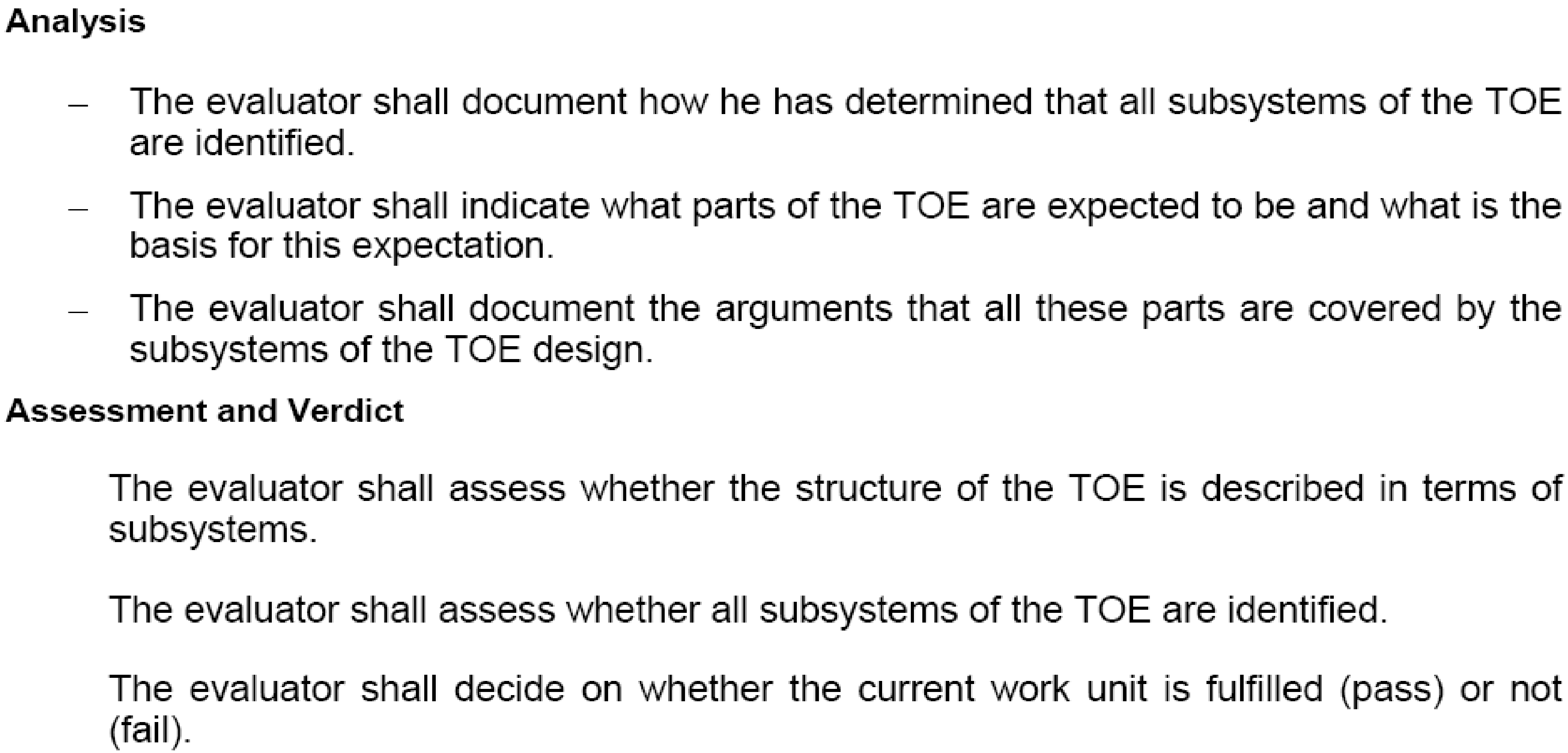
Summary

The evaluator shall document *where* he has found relevant information in the developer's contributions and what is there described (merely keywords).

The evaluator shall summarize the description of the structure provided by the developer with impact on the layering of abstraction.

Guidelines for Evaluation Reports

Example 1 (continuation):



Analysis

- The evaluator shall document how he has determined that all subsystems of the TOE are identified.
- The evaluator shall indicate what parts of the TOE are expected to be and what is the basis for this expectation.
- The evaluator shall document the arguments that all these parts are covered by the subsystems of the TOE design.

Assessment and Verdict

The evaluator shall assess whether the structure of the TOE is described in terms of subsystems.

The evaluator shall assess whether all subsystems of the TOE are identified.

The evaluator shall decide on whether the current work unit is fulfilled (pass) or not (fail).

Guidelines for Evaluation Reports

Example 2:

Example for an analysis

work units

ASE_REQ.1.5

ASE_REQ.1.6

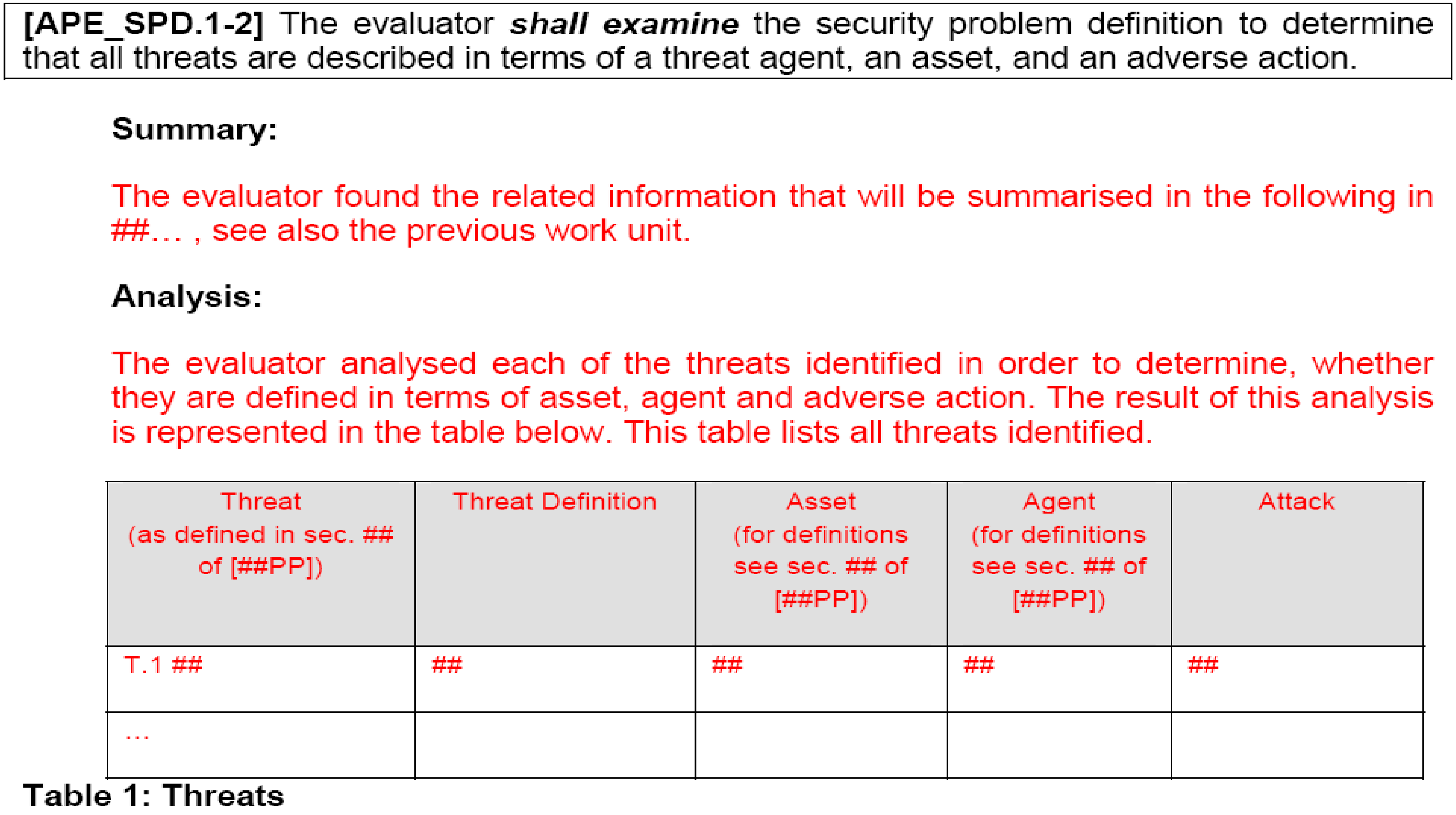
ASE_REQ.1.7

ASE_REQ.1.8

#	Functional elements (identifiers) used in [ST], sec. 5.1	Original definition of functional elements, CC Part 2 or ASE_ECD	Functional elements as used in [ST], sec. 5.1	Operation required by CC Part 2 or ASE_ECD	Operation performed in the ST	Evaluator's comments
1	FDP_ETC.1.1	The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] when exporting user data, controlled under the SFP(s), outside of the TOE.	The TSF shall enforce the Data Separation SFP when exporting user data, controlled under the SFP(s), outside of the TOE.	[assignment: *access control SFP(s) and/or information flow control SFP(s)*]	Data Separation SFP	in accordance with Annex C.4
2	FDP_ETC.1.2	The TSF shall export the user data without the user data's associated security attributes.	The TSF shall export the user data without the user data's associated security attributes.	none	none	-
3	FIA_UID.2.1/UpdateAgent	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.	The TSF shall require each ~~user~~ Update_Agent to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.	refinement	~~user~~ -> Update_Agent	in accordance with Annex C.4

Templates

Example 3:



[APE_SPD.1-2] The evaluator ***shall examine*** the security problem definition to determine that all threats are described in terms of a threat agent, an asset, and an adverse action.

Summary:

The evaluator found the related information that will be summarised in the following in ##… , see also the previous work unit.

Analysis:

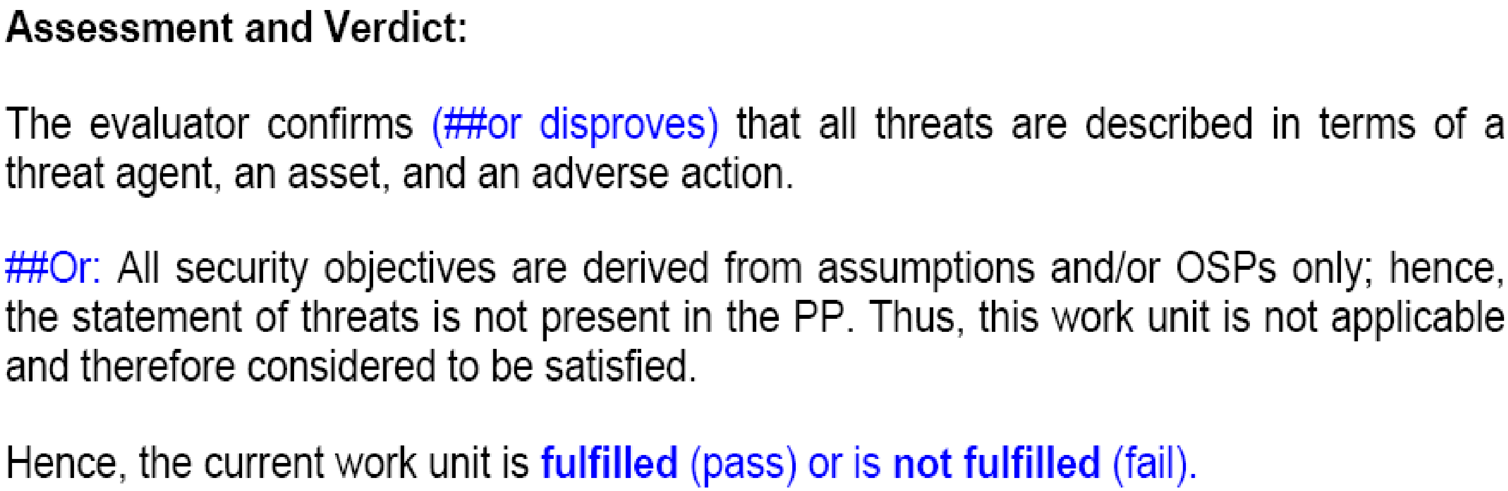
The evaluator analysed each of the threats identified in order to determine, whether they are defined in terms of asset, agent and adverse action. The result of this analysis is represented in the table below. This table lists all threats identified.

Threat (as defined in sec. ## of [##PP])	Threat Definition	Asset (for definitions see sec. ## of [##PP])	Agent (for definitions see sec. ## of [##PP])	Attack
T.1 ##	##	##	##	##
…				

Table 1: Threats

Templates

Example 3 (continuation):



Assessment and Verdict:

The evaluator confirms (##or disproves) that all threats are described in terms of a threat agent, an asset, and an adverse action.

##Or: All security objectives are derived from assumptions and/or OSPs only; hence, the statement of threats is not present in the PP. Thus, this work unit is not applicable and therefore considered to be satisfied.

Hence, the current work unit is **fulfilled** (pass) or is **not fulfilled** (fail).

Guidelines for Evaluation Reports

- The use of the guidelines is mandatory within the BSI-Scheme and can be requested at

zerti@bsi.bund.de

Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Christian Krause
Godesberger Allee 185-189
53175 Bonn

Tel.: +49 22899 9582 5116
Fax: +49 22899 10 9582 5116

christian.krause@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de

T-Systems GEI GmbH

Dr. Igor Furgel
Rabinstrasse 8
53111 Bonn

Tel.: +49 228 98410
igor.furgel@t-systems.com