the information security provider

Introduction to Common Criteria

for developers, evaluators and certifiers

Staffan Persson, atsec information security

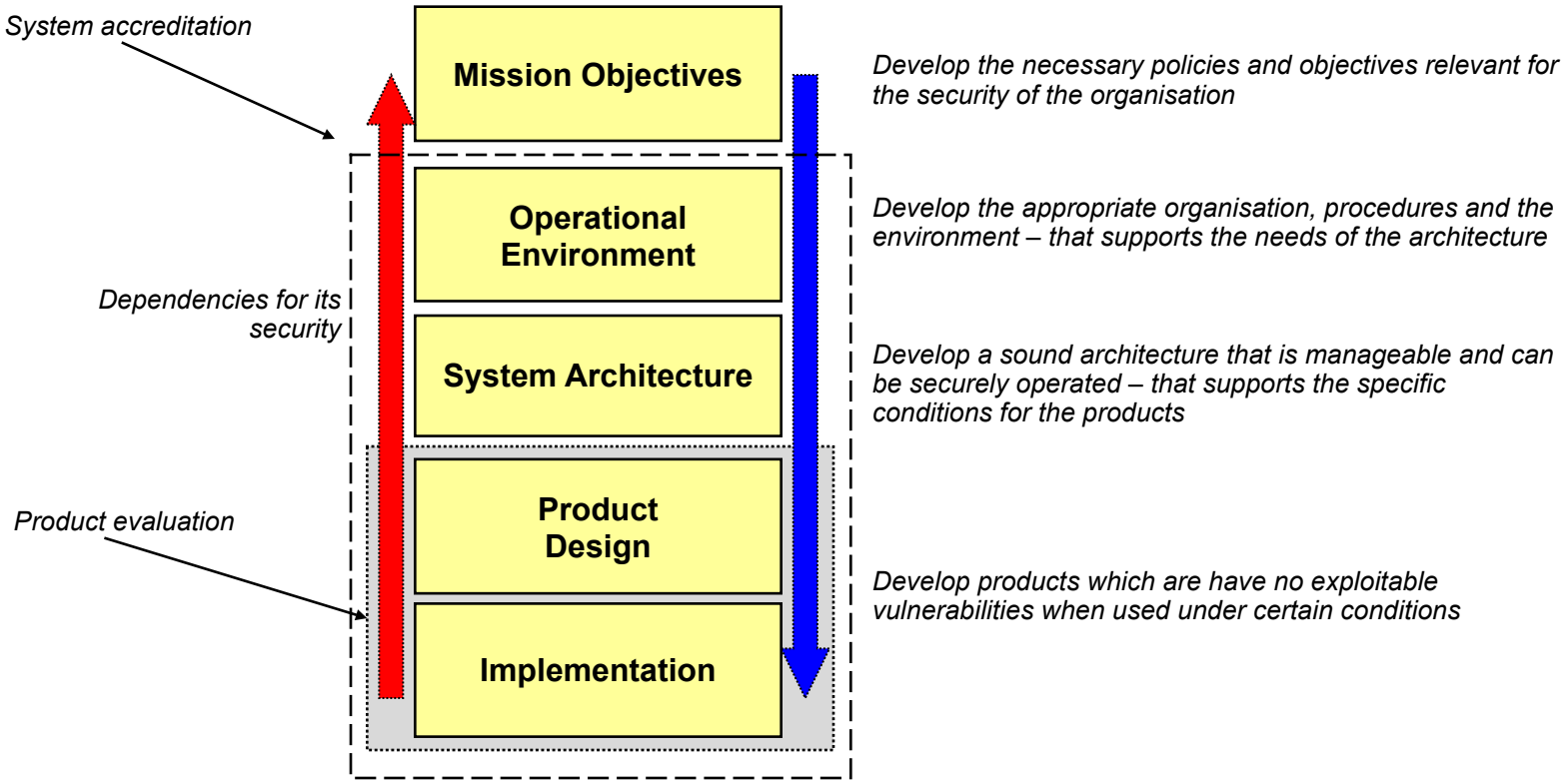
Munich, April 2024

The Common Criteria assurance model

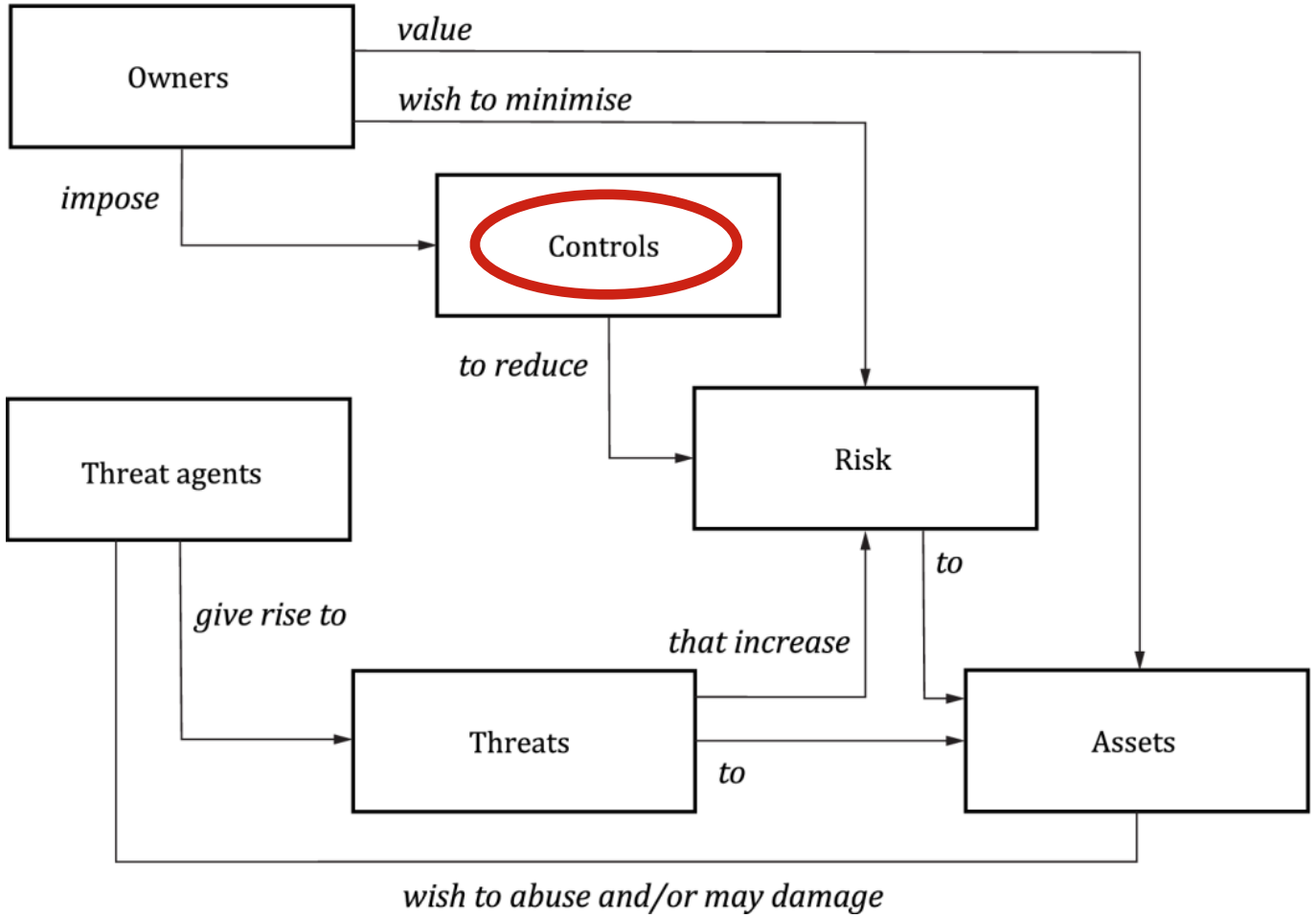
What is Common Criteria

- Common Criteria Part 1 says:
  - The CC permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation.
  - The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfill their security needs.
  - The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of the standard are cautioned to exercise care that this flexibility is not misused.

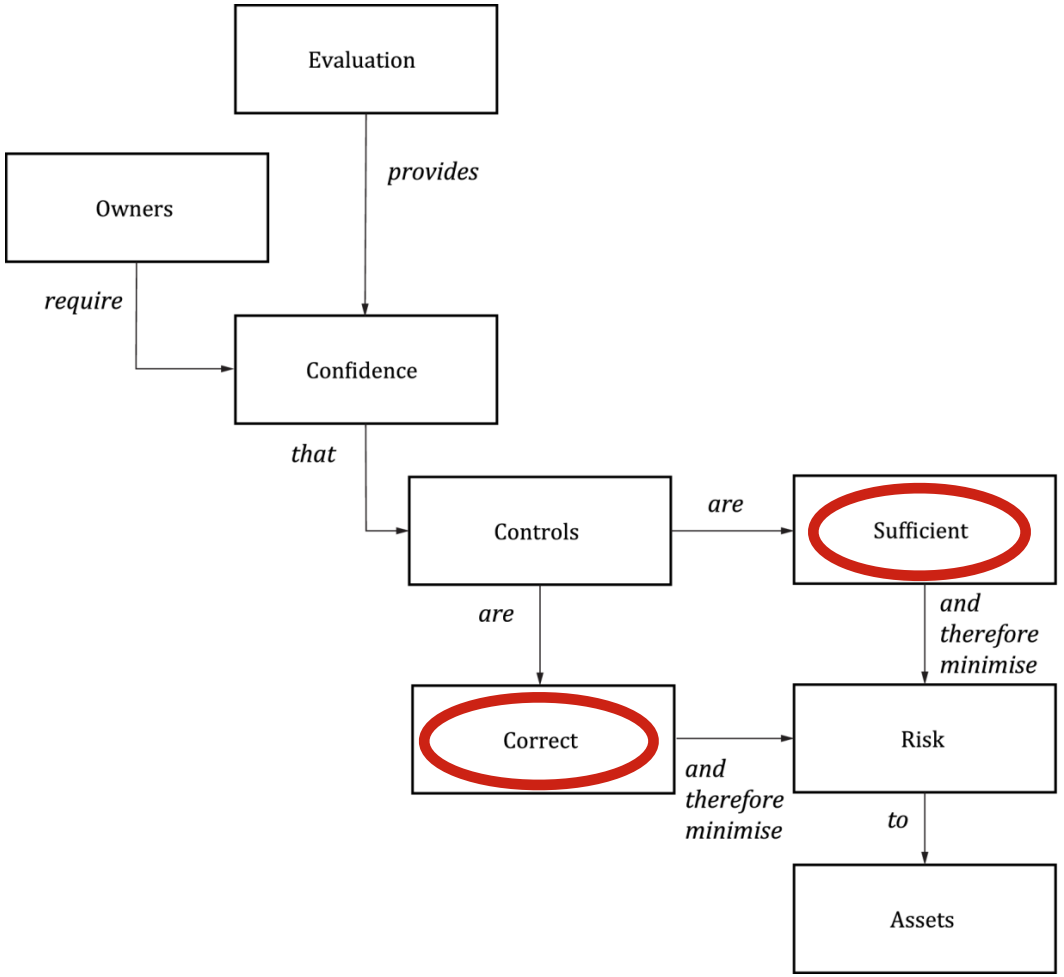
The security context



The general security model of CC



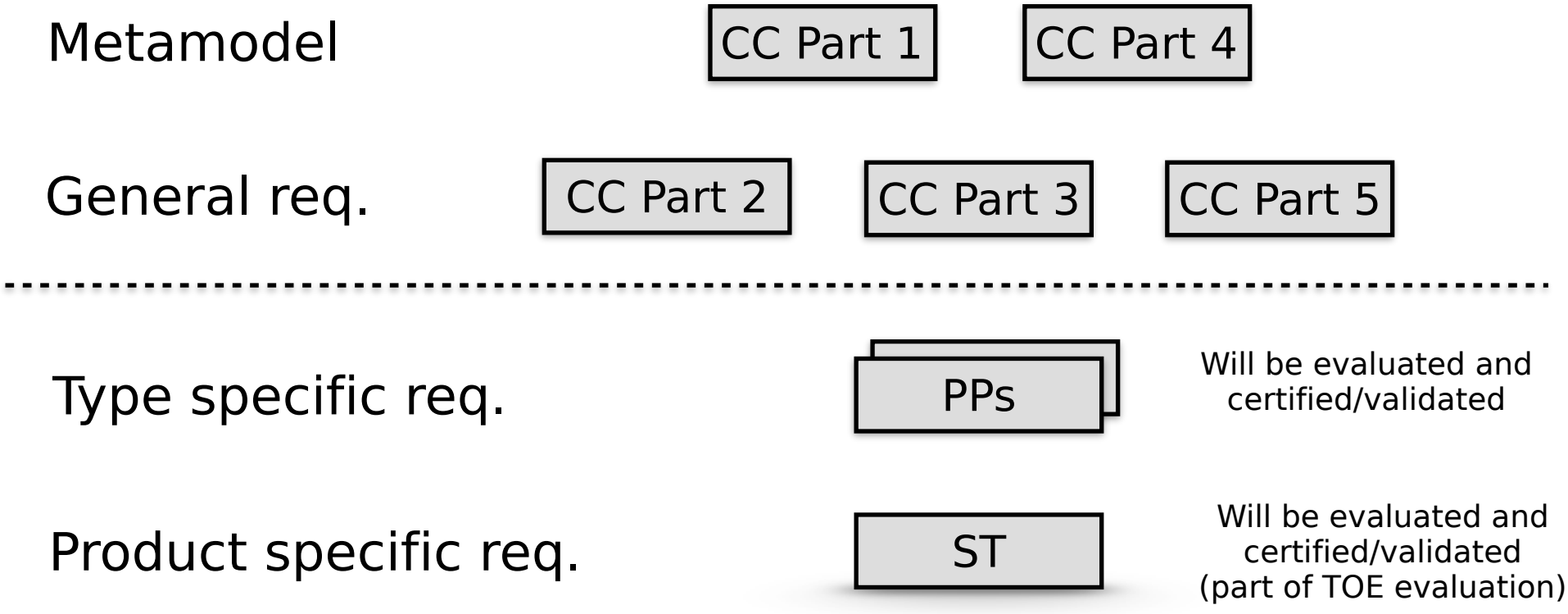
The general evaluation model of CC



Using the Common Criteria

- What the Common Criteria is
  - Common structure & language for expressing product IT security requirements (Part 1)
  - Catalogues of standardized IT security requirement components and packages (parts 2 and 3, generic part 4, predefined packages part 5)
- How the CC is used
  - Develop Protection Profiles and Security Targets – specific IT security requirements for products (there are guides for that)
  - The evaluation of products against known and understood requirements as stated in the Security Target that is specific for the Target of Evaluation (TOE) that is evaluated. There is a separate evaluation methodology CEM describing the minimum evaluator actions.
  - Consumers can then decide which level of confidence they need, using the evaluation assurance packages (EALs) or referring to specific PPs

Layers of abstractions in Common Criteria



The Security Target

- The ST serves as the basis for agreement between the developer and the evaluator on the exact security properties of the TOE and the exact scope of the evaluation.
- The ST provides a description about the TOE configuration(s) for which the evaluation is valid and makes assumptions about the environment in which the evaluation is valid.
- The ST states which threats it can counter, along with an explanation why this can be done effectively.
- The ST claims compliance to a version of CC for the functional and assurance requirements and may claim conformance to specific PPs.
- An ST should be presented as a user-oriented document that minimizes reference to other material that might not be readily available to the user.
- An ST shall conform to the content described in CC, Part 1.

The structure of the Security Target

1 ST Introduction
- 1.1 ST reference
- 1.2 TOE reference
- 1.3 TOE overview
- 1.4 TOE description

2 Conformance Claim
- 2.1 CC conformance claim
- 2.2 PP claim, package claim
- 2.3 Conformance rationale

3 Security Problem Definition
- 3.1 Threats
- 3.2 Organisational security policies
- 3.3 Assumptions

4 Security Objectives
- 4.1 Security Objectives for the TOE
- 4.2 Security objectives for the operational environment
- 4.3 Security objectives rationale

5 Extended Components Definitions

6 Security Requirements
- 6.1 Security functional requirements
- 6.2 Security assurance requirements
- 6.3 Security requirements rationale

7 TOE Summary Specification

Important decisions for the ST

- Determine the scope of the TOE
  - This must be a pragmatic decision, i.e. must be made made so the TOE is meaningful (TSF are inside the TOE) and done so that the evaluation can be performed (source code available)
- Determine the SFRs of the TOE (and of the TOE environment)
  - The SFRs and TSF must include necessary and important ones for the customer. Nice-to-have features included must be good enough to pass.
- Determine the EAL (and possible augmentations) and/or PP
  - Sufficient for the user and feasible (technically and financially). Aiming higher may be expensive, but may competitive advantage to some. Some customers may need compliance to a specific PP(s) as well.
- Determine the evaluated configuration(s) of the TOE
  - Make sure that the relevant platforms and configurations are covered. Adding more platforms or configurations means more testing.

The assurance approach of Common Criteria

- The CC philosophy is to provide assurance based upon an evaluation of the IT product that is to be trusted.
- The assurance can be described as proof of:
  - Correctness (of security function as specified)
  - Sufficiency (to meet its security objectives)
  - Absence of exploitable security vulnerabilities
- The CC proposes measuring the validity of the documentation and of the resulting IT product by expert evaluators with increasing emphasis on scope, depth, and rigour.
- Assurance is defined by the assurance requirements referenced also by predefined assurance packages, i.e. Evaluation Assurance Levels (EAL 1-7)
- Note: There are no design requirements on EAL1-4. Higher assurance levels requires e.g., domain separation and formal methods to help the analysis and to reduce the risk of critical side effects.

What the assurance requirements?

- The assurance components are confidence aspects of the TOE and they must be verified – by evaluator actions. Therefore, for the assurance components there are corresponding evaluator activities in the CEM.
- For (almost) all assurance requirements documentation is required, documentation that must be written and evaluated. The assurance requirements is what takes time and effort in evaluations!
- Assurance components are grouped together in packages to form evaluation assurance levels (EAL). These packages can be used as such or be augmented by selecting other components, such as flaw remediation.
- The components within a family are strictly hierarchical, representing increasing rigour of the confidence aspect, i.e. EAL2 is a subset of EAL4.

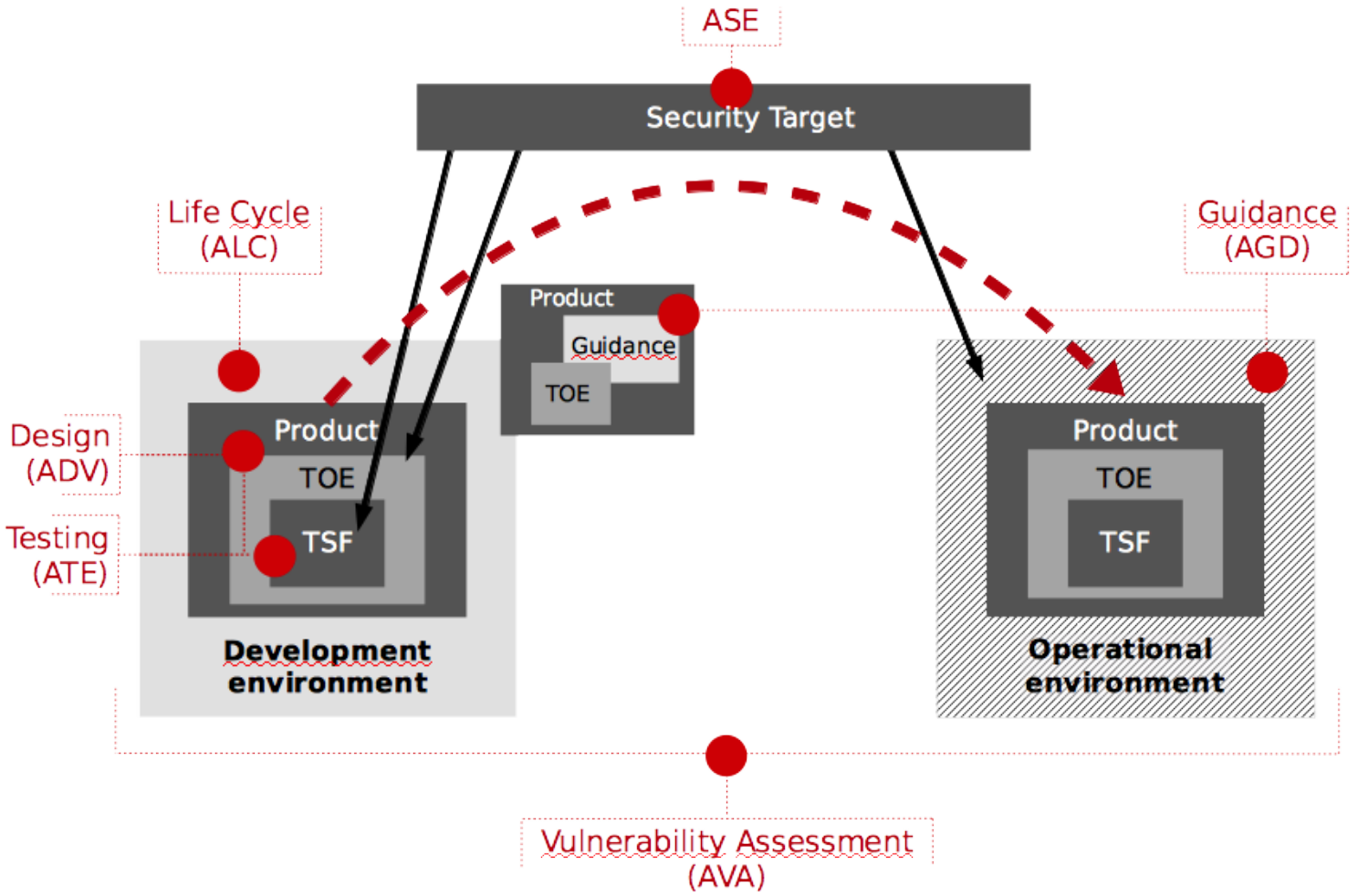
What the evidence is required?

- A Security Target, which is a unique CC document and the specification for the evaluation. The Security Target is specified in CC Part 1, Annex C.
- Documentary evidence is required by the assurance requirements. Note: not specific documentation in specific formats, but documentary evidence in more or less any type of structure or format (only exception is the ST).
  - This applies to design documentation, user guides, test plans, processes for life-cycle, etc.
  - Most documentation is (or should be) available independent of CC and not be developed as CC specific documentation. Use what you have and just add what is missing!
- Records are needed as evidence to demonstrate the application of processes related to the assurance measures, such as visitor logs or CM logs (mainly limited to life-cycle).
- Determine need of protection, version control for the evidence, etc.

The assurance classes of CC

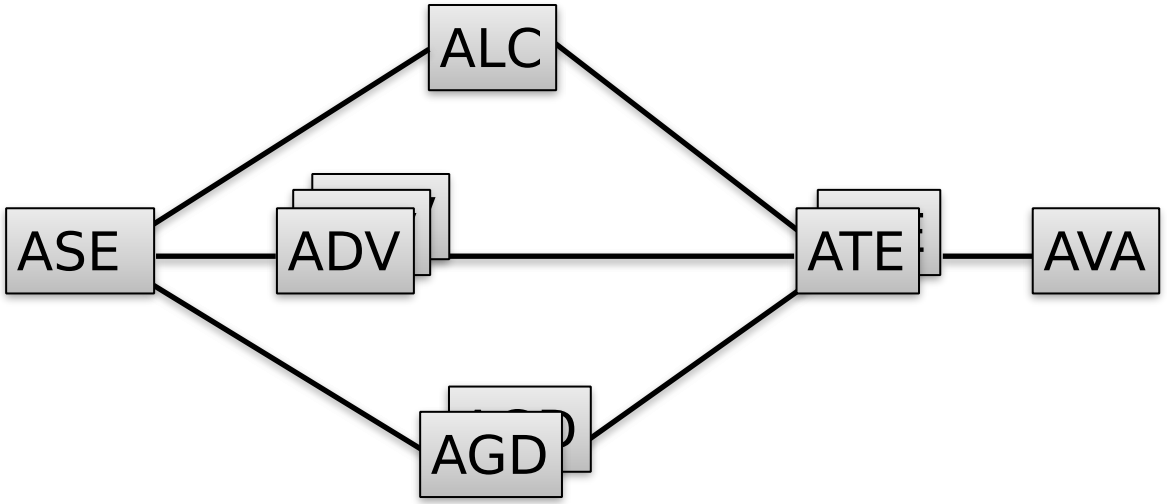
- ASE – Security Target Evaluation
  - Verifying that the security specification is suitable
- ADV – Development
  - Verifying the correctness and completeness of the design documentation and implementation
- AGD – Guidance documents
  - Verifying that the guidance is suitable for secure operation
- ALC – Life cycle support
  - Verifying that the development environment provides sufficient and effective security measures
- ATE – Tests
  - Verifying that the TOE security functions are functioning as expected
- AVA – Vulnerability assessment
  - Verifying that no exploitable vulnerabilities are found

The assurance requirements



Dependencies in the assurance activities

- All assurance activities are specified and depends on the Security Target, so unless the Security Target has been verified (evaluated as par of the ASE) we cannot rely on it.
- Many assurance activities, depends on the evidence that also must be verified, such as the testing depends on the design documentation an on the delivery process and installation guide.
- This is also the sequence when documentation has to be available!



Packages of assurance requirements (Part 5)

- Level **EAL1** – The lowest level which should be considered for purposes of evaluation
- Level **EAL2** – The best that can be achieved without imposing some additional tasks on a developer
- Level **EAL3** – Allows a conscientious developer to benefit from positive security engineering design without alteration of existing reasonably sound development practices
- Level **EAL4** – Allows a developer to gain maximum assurance from positive security engineering based on good commercial development practices. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.
- Level **EAL5** – The best achievable via pre-planned, good quality, careful security-aware development without unduly expensive practices.
- Level **EAL6** – A "high tech" level for (mainly military) use in environments with significant threats and moderately valued assets.
- Level **EAL7** – The greatest amount of evaluation assurance attainable whilst remaining in the real

The assurance packages EAL1 to EAL7

Assurance class	Assurance family	Assurance components by evaluation assurance level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
ST evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5