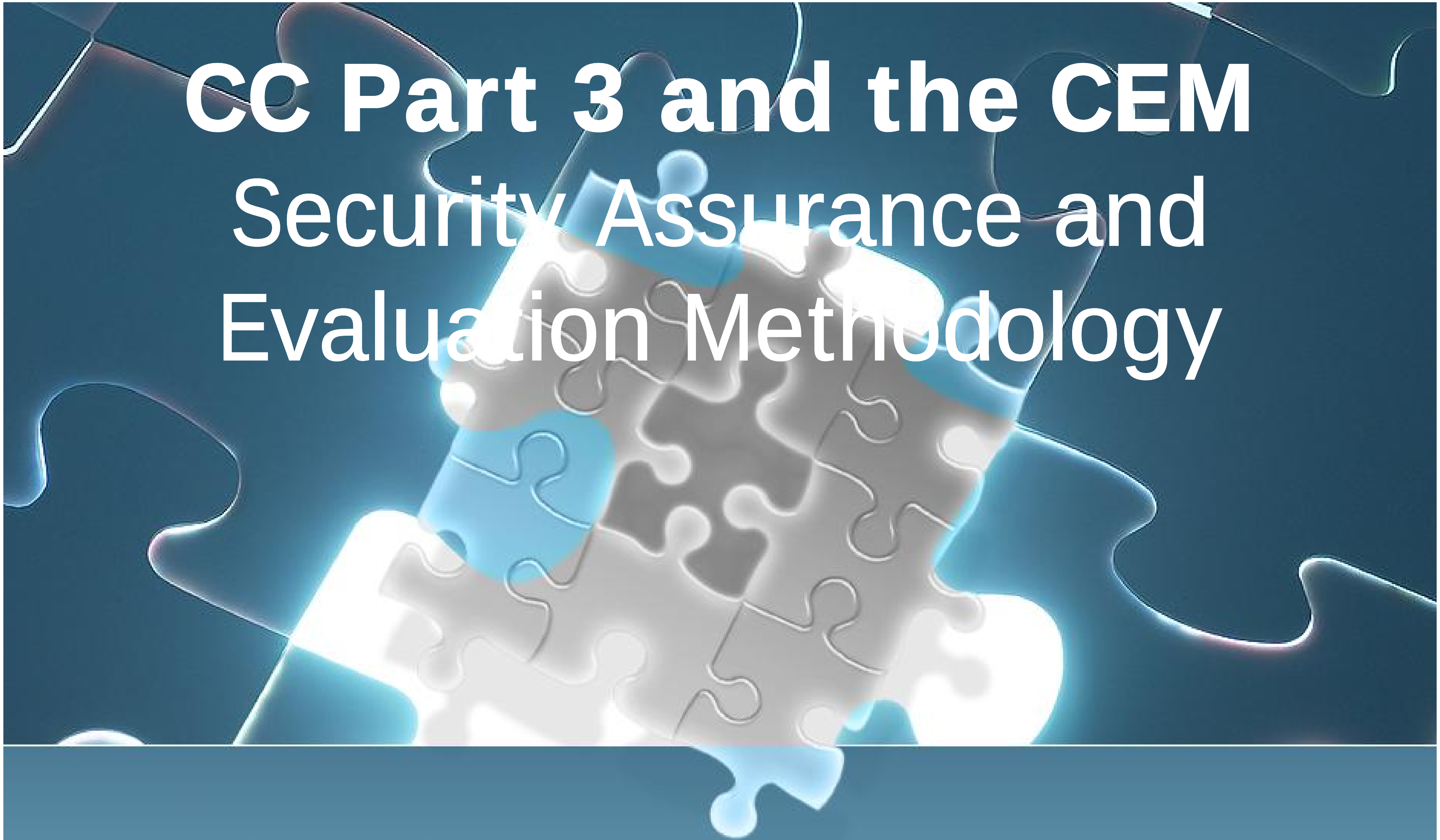
CC Part 3 and the CEM

Security Assurance and Evaluation Methodology



Su-en Yek

Australasian CC Scheme

What This Tutorial Is

An explanation of where Security Assurance Requirements fit in the CC evaluation paradigm

A tutorial about Security Assurance Requirements and the CC Evaluation Methodology that you won’t read about in CC part 3 or the CEM

What This Tutorial Will Not Focus On

- Identifying each Assurance Class, Family, Component and Element
- Explaining Assurance Classes in each Evaluation Assurance Level (EAL)
- Discussing how Evaluation Facilities, Certifying Bodies and the Common Criteria Recognition Arrangement (CCRA) interpret or apply Assurance Requirements

Definitions

- CC – Common Criteria
- CEM – Common Methodology for Information Security Evaluation, aka CC Evaluation Methodology
- EAL – Evaluation Assurance Level
- SAR – Security Assurance Requirement
- SFR – Security Functional Requirement
- ST – Security Target
- TOE – Target of Evaluation
- TSF – TOE Security Features

Order of Discussion

1. What is the CEM. What the CEM is not!
2. CC Evaluation Paradigm

What is CC Evaluation Methodology

- To evaluate is to collect, process and analyse information to determine a result

- Method is the defined as the **way** something is conducted

- Evaluation Method is the **way** information is collected, processed and analysed to determine a result

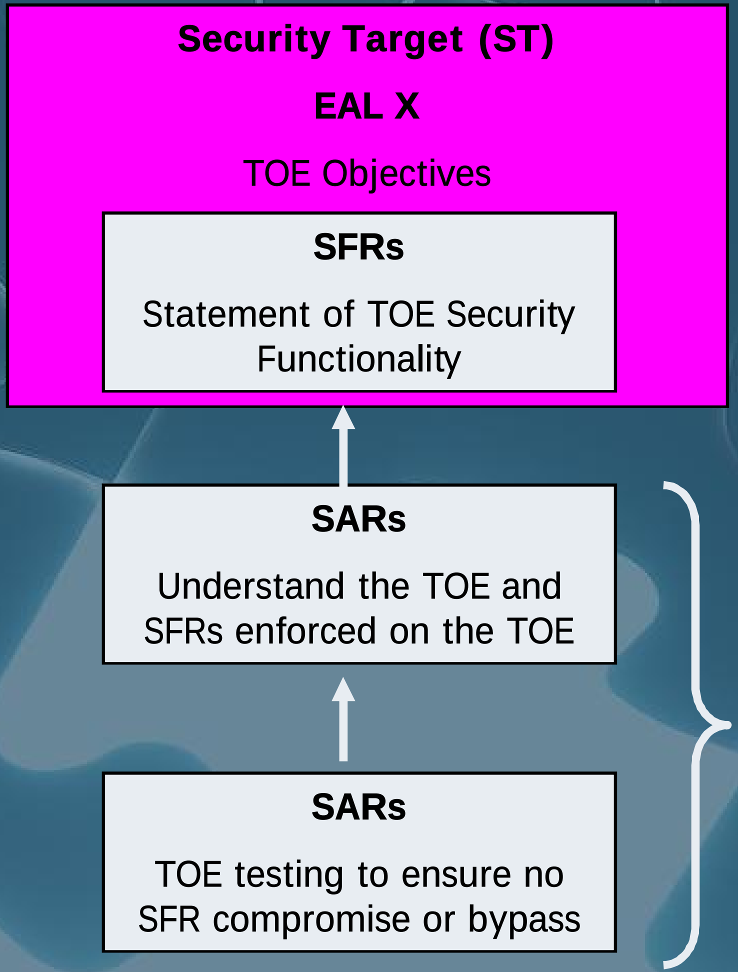
What is CC Evaluation Methodology

- Methodology defines the underlying beliefs and reasons for the way we do something
- Evaluation methodology defines the underlying beliefs and reasons for the way we conduct evaluations
- **The CEM does NOT define the underlying methodology for conducting CC evaluations**
- **Evaluators define the underlying methodology in their conduct of CC evaluations**

What is CC Evaluation Methodology

- The CC and the CEM provides a **FRAMEWORK** for Evaluators to conduct IT security evaluations using their chosen methodology
- The CC and CEM framework is designed to be hardware and software agnostic
- The CEM provides structured guidance on the methods Evaluators should adopt for evaluating
- The methodology lies in **WHY** the Evaluator chose the methods they used

Common Criteria Evaluation Paradigm



Security Target (ST)

EAL X

TOE Objectives

SFRs

Statement of TOE Security Functionality

SARs

Understand the TOE and SFRs enforced on the TOE

SARs

TOE testing to ensure no SFR compromise or bypass

GOAL

Gain assurance the SFRs enforced on the TOE are an accurate reflection of the ST and cannot be compromised or bypassed according to the attack potential associated with the EAL

Defining Functions and Assurance

- FUNCTIONS - SFRs

  A mechanism that either exists or does not exist

- ASSURANCE - SARs

  a level of confidence that can be gained

Defining SFRs and SARs in CC Context

- Security Functional Requirements are stated for an Evaluator to identify what mechanisms exist in the TOE
- Security Assurance Requirements are provided for an Evaluator to gain a level of confidence that the SFR is accurately enforced on the TOE and confidence that the SFR cannot be compromised or bypassed

Expanding on SARs

- SARs are evidence-based requisites
- SARs are **documents** eg. TOE design, **processes** eg. flaw remediation process, and **actions** eg. testing and vulnerability analysis
- The Developer provides evidence to the Evaluator for the Evaluator to understand the TOE and its security features to determine that the SFR is enforced accurately and that the SFR may not be compromised or bypassed

How Much Evaluation is Required on the Evidence?

- SAR evaluation relies on multiple evaluation methods
- The depth and rigour of SAR evaluation is determined by the EAL and subsequent attack potential of that EAL
- EAL 1 -7 is a scale of increasing assurance gained that SFR compromise and bypass cannot occur at increasing levels of attack potential (expertise, resources, motivation)

Assurance Package EAL 1

Assurance Class	Assurance Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ASE: Security Target evaluation	ASE_CCL.1 Conformance claim
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.1 Security objectives for the operational environment
	ASE_REQ.1 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Assurance Classes

Understanding the TOE and security features

- ASE – Security Target
- AGD – Guidance Documents
- ADV – Development

Determine that SFRs are enforced accurately and may not be compromised or bypassed

- ATE – Testing
- AVA – Vulnerability Assessment

Assurance Classes

- What about Life-cycle support (ALC) and Composition (ACO)?
- ALC supports Certification Continuity
- Life-cycle support is aimed at providing evidence on the Developer’s development, production and delivery processes
- ACO supports the integration of multiple evaluated TOEs
- Composition is aimed at the Developer providing evidence on composite relationships

What does Assurance and the CEM Provide?

- Strengths
  - Hardware and software agnostic evaluation criteria
  - Standardised certification result which enables mutual recognition
- Weaknesses
  - Disproportion of effort among assurance class and requirement evaluation criteria
  - EAL scale of attack potential is not commensurate to the current IT security threat environment

What’s The Way Forward?

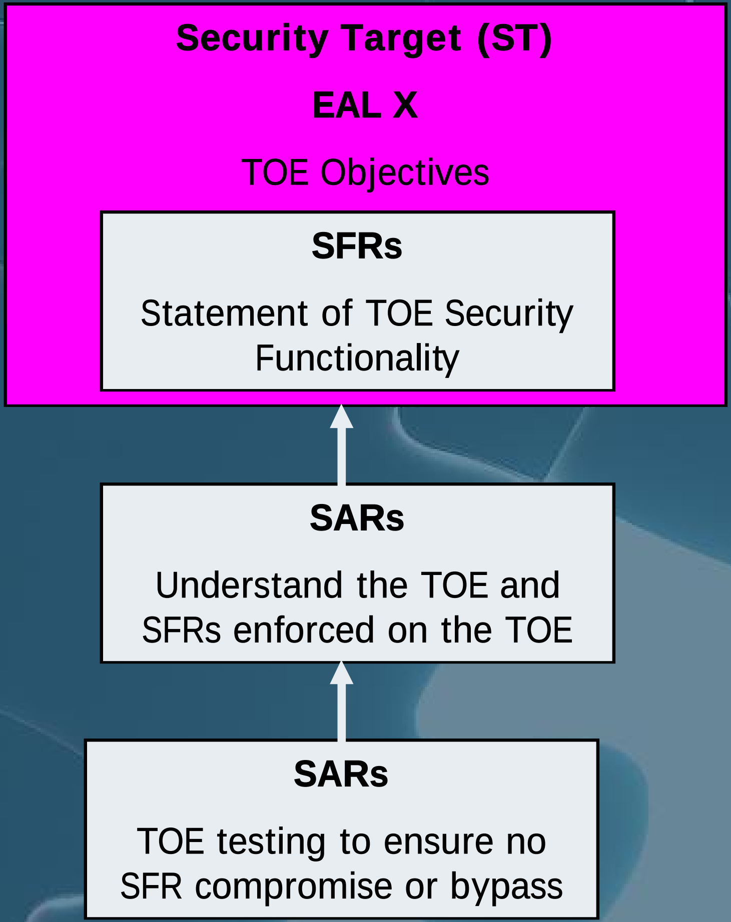
CC v 4

- CC Working Groups
  - Concentrate on improving and developing evaluations that suit **Developer**, **Consumer**, **Evaluator** and **Certifier** needs
    - Timeliness
    - Usability
    - Benefit

The CC Paradigm in Context

- The CC is an IT security evaluation criteria
- The Certifying Body (CB) ensures competence, impartiality and consistency is applied in CC evaluations by evaluation facilities
- The CC Recognition Agreement (CCRA) management bodies ensures harmony among CC schemes and mutual recognition

Common Criteria Evaluation Paradigm



Security Target (ST)

EAL X

TOE Objectives

SFRs

Statement of TOE Security Functionality

SARs

Understand the TOE and SFRs enforced on the TOE

SARs

TOE testing to ensure no SFR compromise or bypass

Understanding the CC Evaluation Paradigm enables you to apply the criteria and identify the problems for improvement

Q