



## CEM Foreword

CEM v3.1 aims to:

- eliminate redundant evaluation activities
- reduce/eliminate activities that contribute little to the final assurance of a product
- clarify CEM terminology to reduce misunderstanding
- restructure and refocus the evaluation activities to those areas where security assurance is gained
- and add new CEM requirements if needed.

# Common Evaluation Methodology (CEM)



*The governmental organisations listed below contributed to the development of this version of the Common Methodology for Information Technology Security Evaluation. As the joint holders of the copyright in the Common Methodology for Information Technology Security Evaluation, version 3.1 (called “CEM 3.1”), they hereby grant non-exclusive license to ISO/IEC to use CEM 3.1 in the continued development/maintenance of the ISO/IEC 18045 international standard. However, these governmental organisations retain the right to use, copy, distribute, translate or modify CEM 3.1 as they see fit.*

# CEM Developers



- *Australia/New Zealand: The Defence Signals Directorate and the Government Communications Security Bureau respectively;*
- *Canada: Communications Security Establishment;*
- *France: Direction Centrale de la Sécurité des Systèmes d'Information;*
- *Germany: Bundesamt für Sicherheit in der Informationstechnik;*
- *Japan: Information Technology Promotion Agency*
- *Netherlands: Netherlands National Communications Security Agency;*
- *Spain: Ministerio de Administraciones Públicas and Centro Criptológico Nacional;*
- *United Kingdom: Communications-Electronics Security Group;*
- *United States: The National Security Agency and the National Institute of Standards and Technology.*

## Relationship between CC and CEM structures



CC

Assurance Class

Assurance Component

Evaluator Action Element

Developer Action Element

Cont. & pres. Evidence

CEM

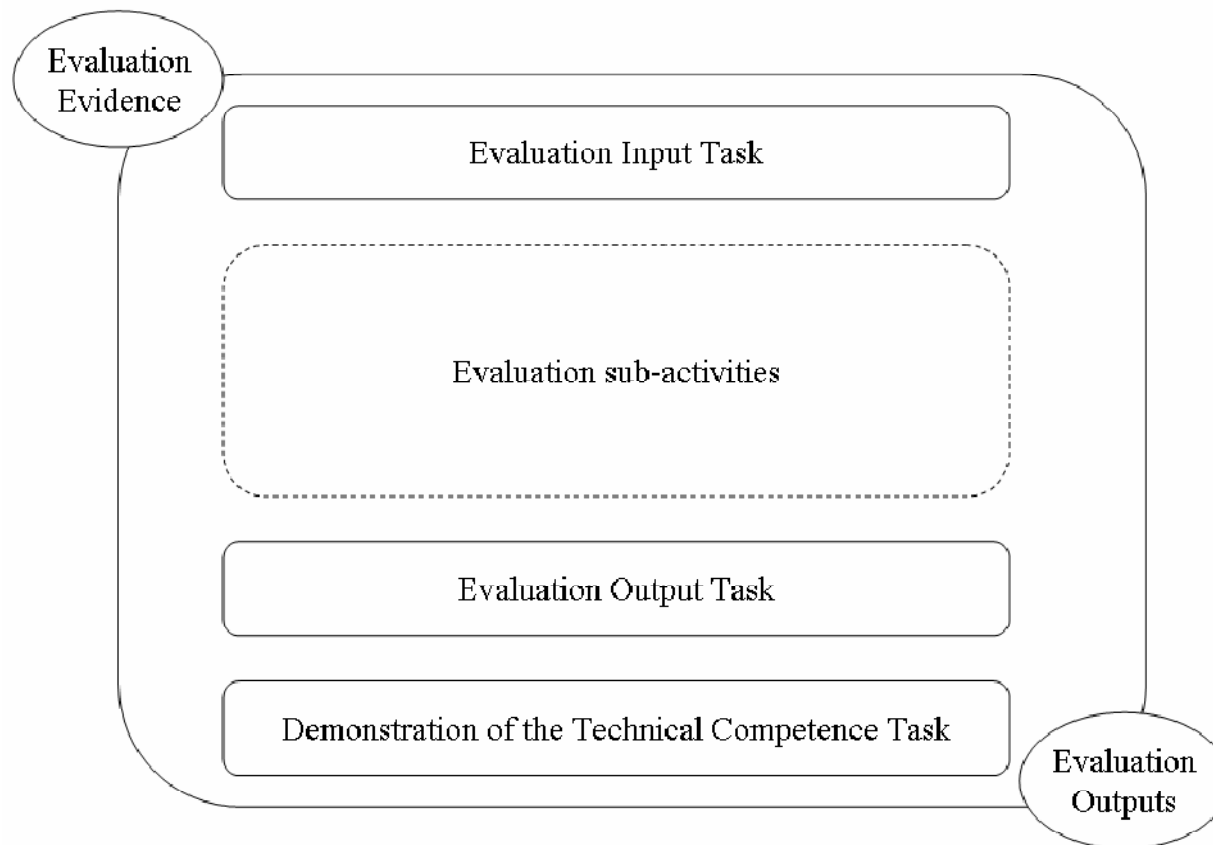
Activity

Subactivity

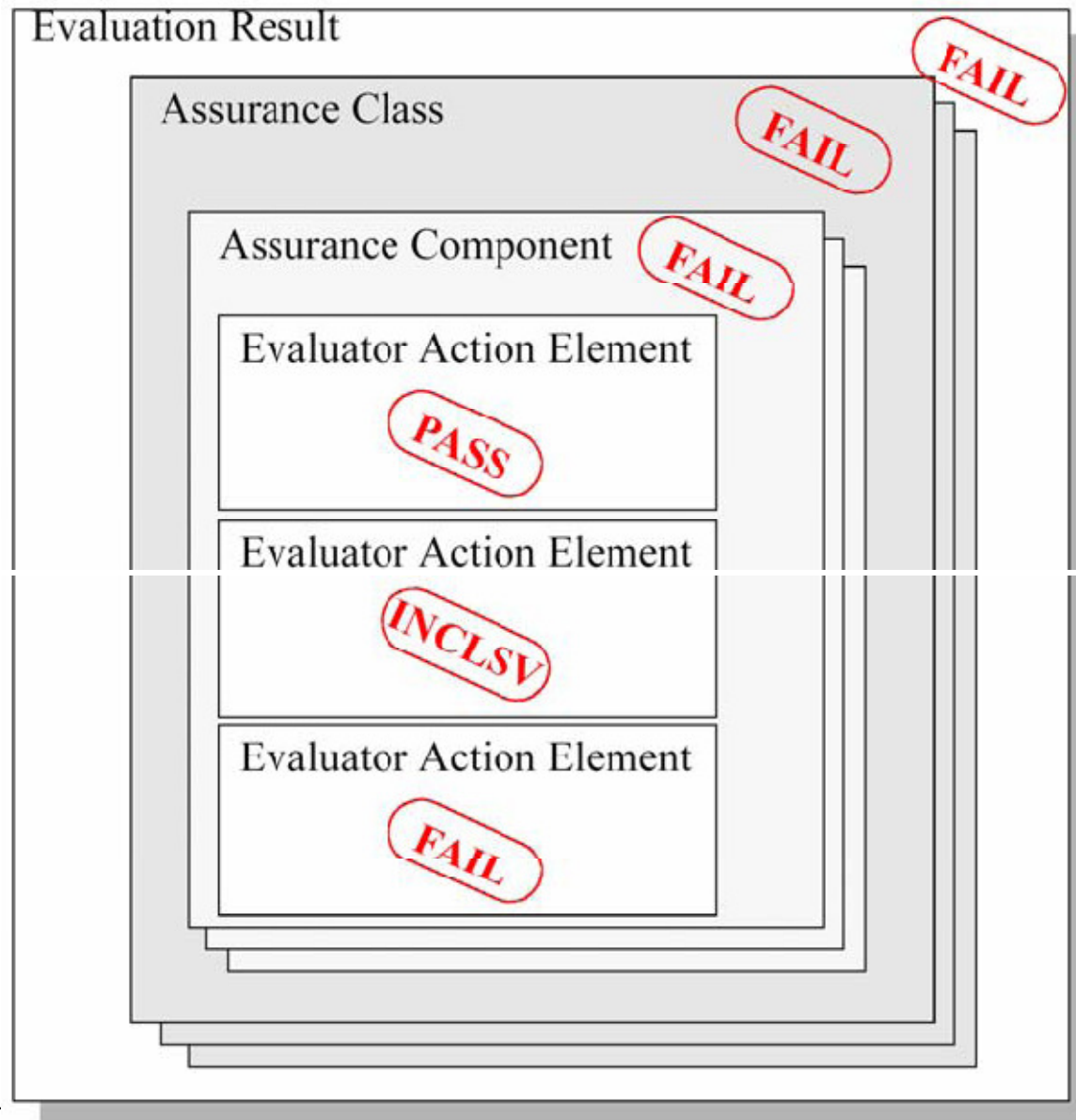
Action

Work Units

# Processes and Tasks



# Verdict Assignment





## Conditions for a Pass

- all evaluation evidence required for performing these work units is coherent, that is it can be fully and completely understood by the evaluator
- all evaluation evidence required for performing these work units does not have any obvious internal inconsistencies or inconsistencies with other evaluation evidence.



## Conditions for a Fail

- the requirements for the PP, ST, or TOE under evaluation are not met
- that the evidence is incoherent, or an obvious inconsistency in the evaluation evidence has been found



## Evaluation preparation



- test documentation, to allow the evaluator to make an early assessment of tests and test procedures;
- design documents, to provide the evaluator with background for understanding the TOE design;
- source code or hardware drawings, to allow the evaluator to assess the application of the developer's standards.



## Evaluation Output

- Observation reports (ORs)  
Evaluator -> Evaluation authority  
(sponsor, developer)
- Evaluation Technical Report (ETR)  
Evaluator -> Evaluation authority



# Observation Reports

the evaluator ***shall report*** :

- the identifier of the PP or TOE evaluated;
- the evaluation task/sub-activity during which the observation was generated;
- the observation;
- the assessment of its severity (e.g. implies a fail verdict, holds up progress on the evaluation, requires a resolution prior to evaluation being completed);
- the identification of the organisation responsible for resolving the issue;
- the recommended timetable for resolution;
- the assessment of the impact on the evaluation of failure to resolve the observation.

# Evaluation Technical Report



- Introduction
- Architectural description of the TOE
- Evaluation
- Results of the evaluation
- Conclusions and recommendations
- List of evaluation evidence
- List of acronyms and glossary of terms
- Observation reports



## Evaluation scheme

- Accreditation (NA)
  - Evaluation facilities (Secode, Norconsult)
- Certification (SERTIT)
  - Products
- Evaluation
  - Products
    - Software
    - Hardware
    - Firmware