Common Criteria Course Module

ASE/APE for CC 3.0

TNO-ITSEF BV ***IT Security Evaluation Facility***

Dirk-Jan Out
+ 31 70 374 0304
out@itsef.tno.nl
www.commoncriteria.nl / www.itsef.com

Why rewrite ASE/APE in CC 3.0?

Numerous complaints:

- **Not a good assurance/cost ratio**
- **Not easy to understand**
- **Not minimal**
- **Not consistent**

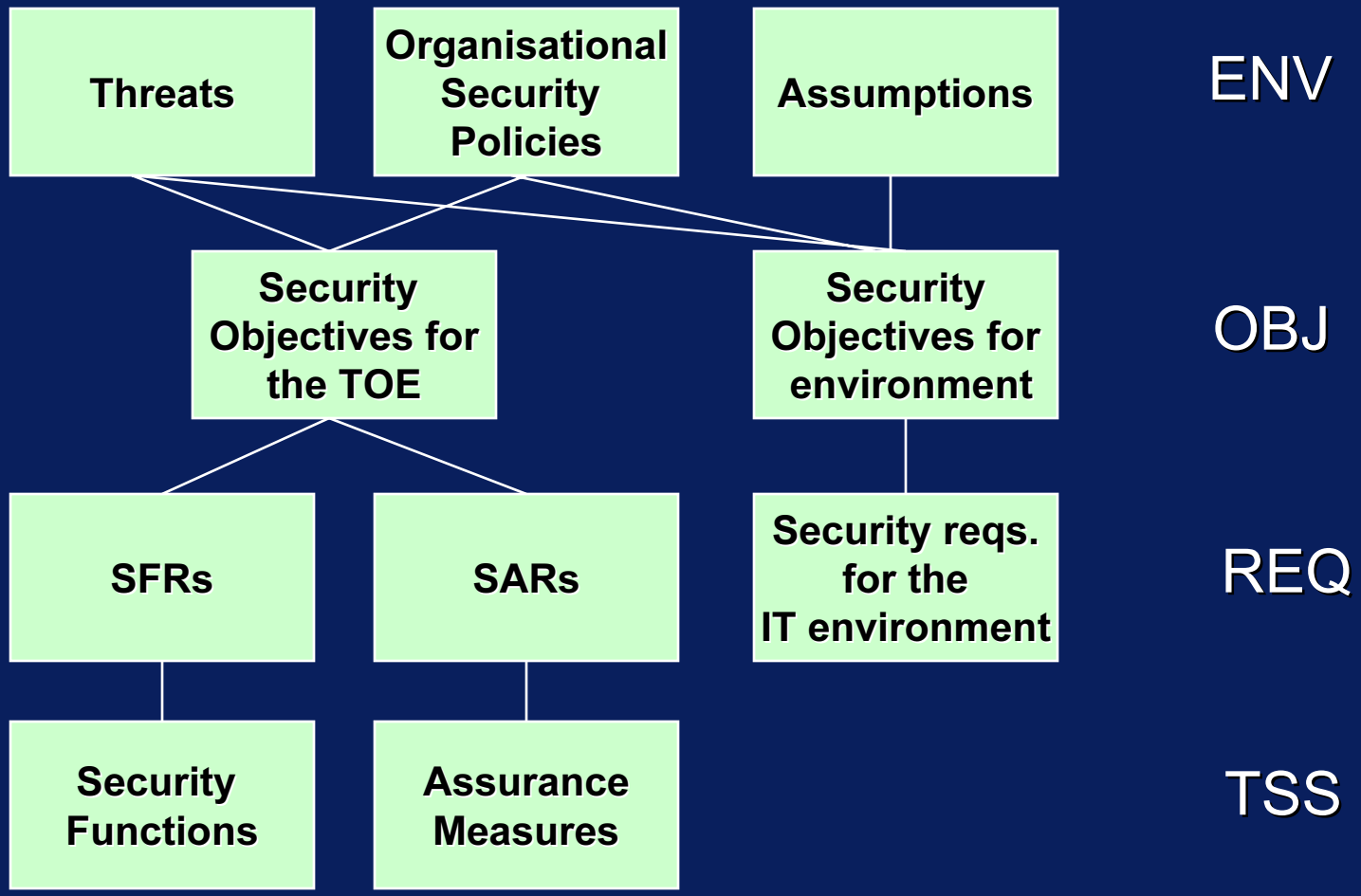
Consistent with our (TNO-ITSEF) experience

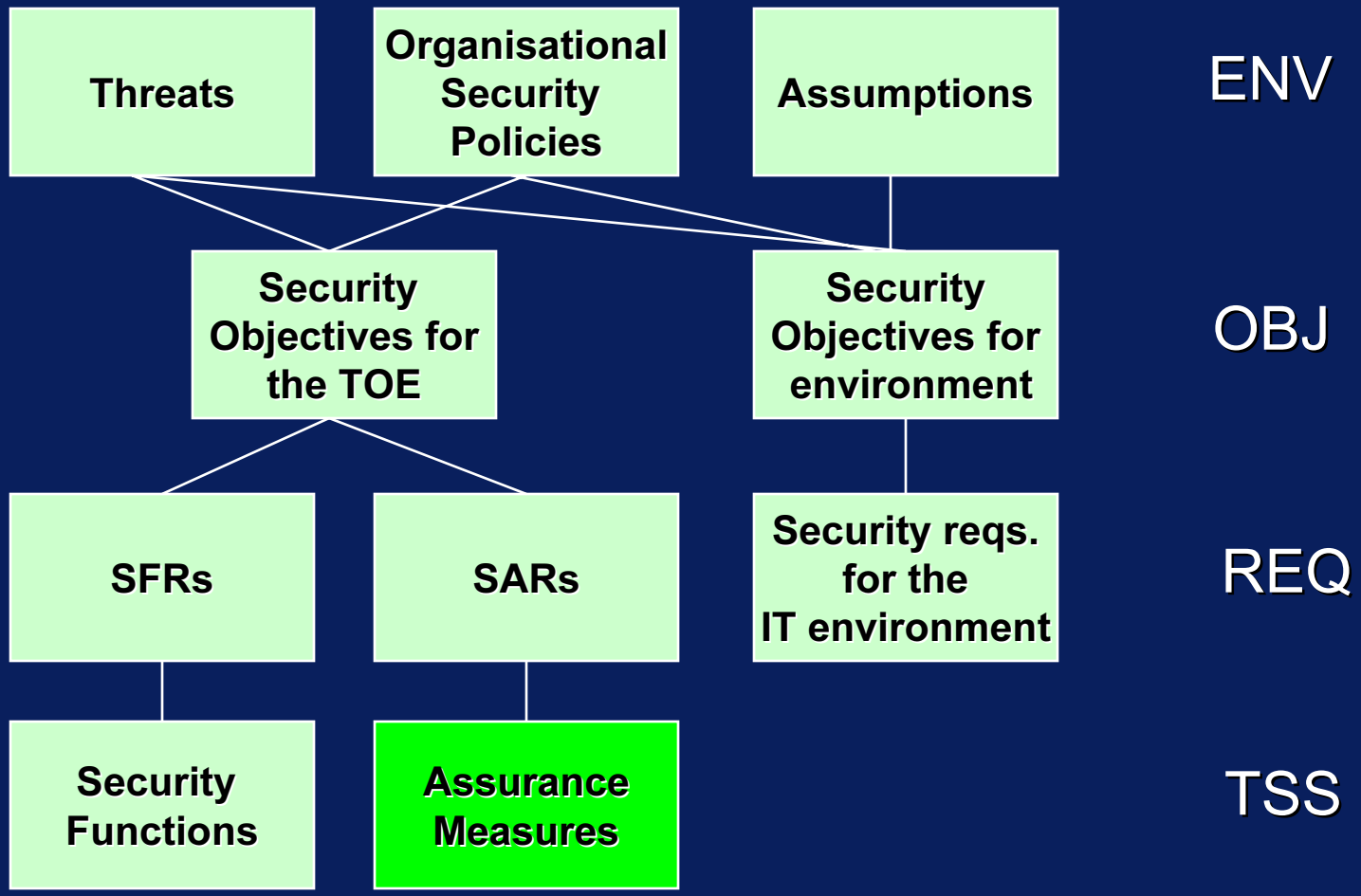
Why rewrite ASE/APE in CC 3.0?

30%-40% of comments received by CCIMB on CEM and CC are on ASE/APE

Many comments show that people lack a fundamental understanding on what is meant…..

The 2.1 ST structure




Threats
Organisational Security Policies
Assumptions
ENV
Security Objectives for the TOE
Security Objectives for environment
OBJ
SFRs
SARs
Security reqs. for the IT environment
REQ
Security Functions
Assurance Measures
TSS

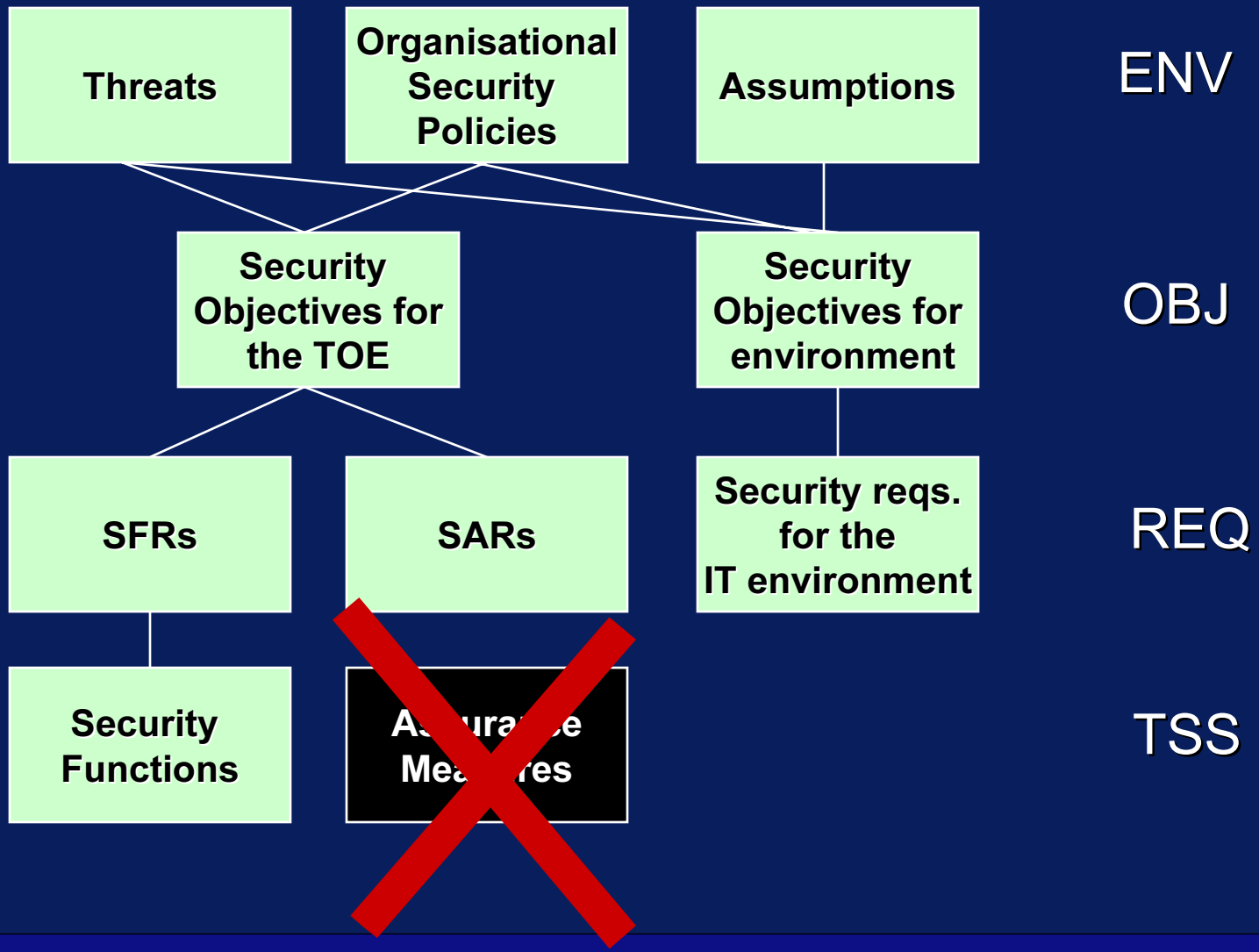
In some existing STs (e.g. ours)

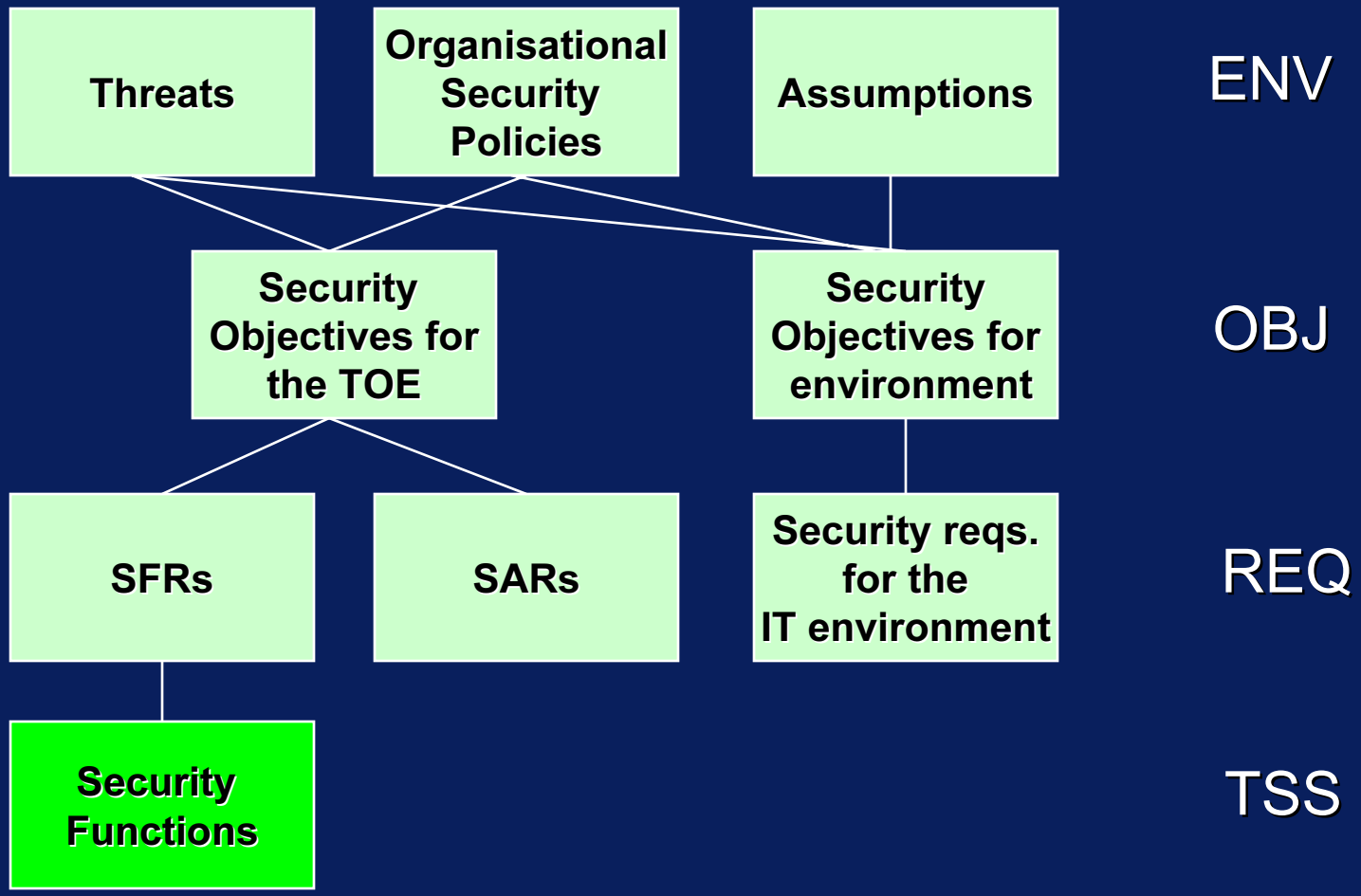
- The ADV_FSP.1 requirements are met by the document “TOE Functional Specification”
- The ADV_HLD.2 requirements are met by the document “TOE High-Level Design”
- The ADV_LLD.1 requirements are met by the document “TOE Low-Level Design”

In some other existing STs…..

- **The requirement ACM_CAP.4.6C is implemented by the following numbering scheme for configuration items:**
  - <department code><TOE code><document type code> <year><month><day> <Id of writer><id of approver>
  - Example: 43-22-HLD-2002-1-19-JF-BR

Assurance measures are gone




Threats
Organisational Security Policies
Assumptions
ENV
Security Objectives for the TOE
Security Objectives for environment
OBJ
SFRs
SARs
Security reqs. for the IT environment
REQ
Security Functions
TSS

Security functions: “to be or to do”

A security function of a TOE = “what the TOE does”

A function of a car is “moving”

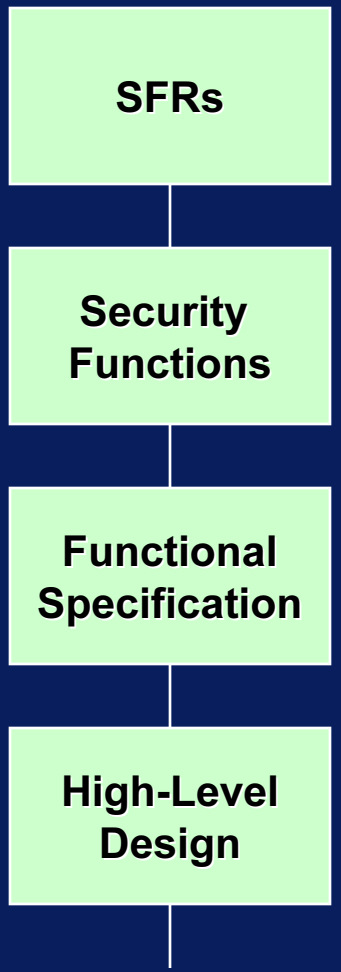
A security function of a TOE = “a part of the TOE”

A function of a car is “wheel”

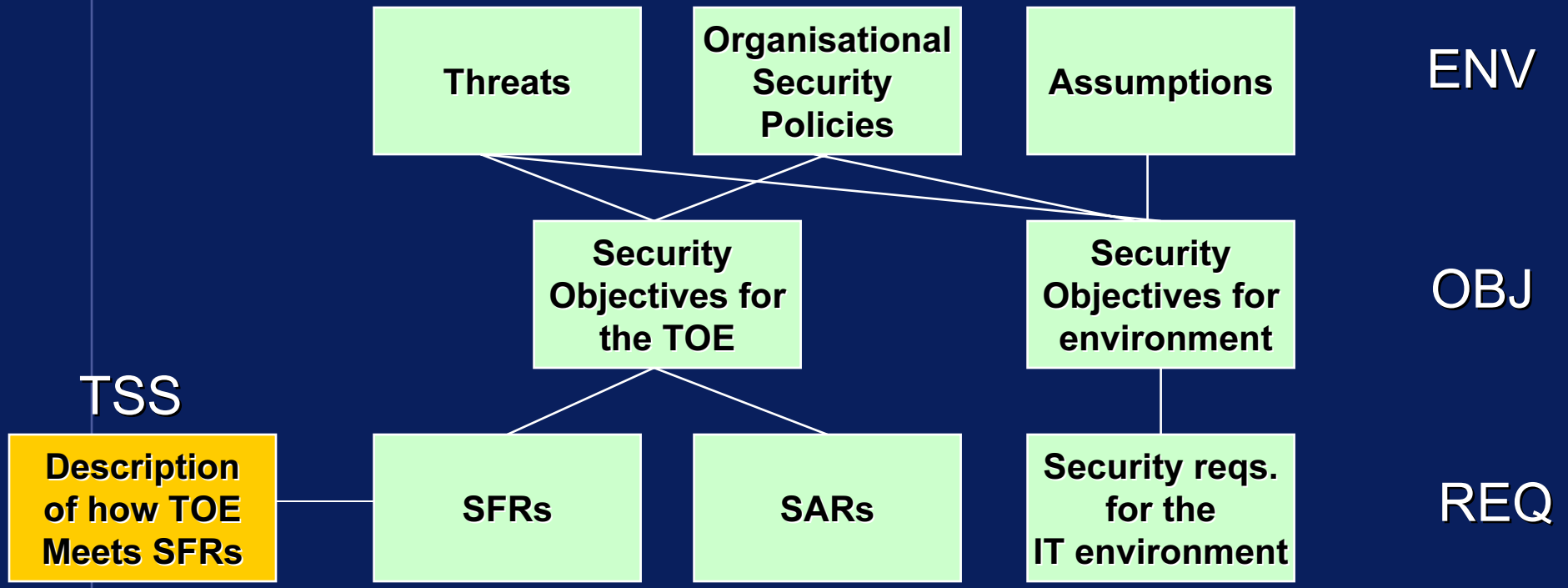
Role of Security Functions

Is it a design layer between SFRs and FSP?

Or is it a “summary” of how the TOE is Implemented?



Security Functions have changed



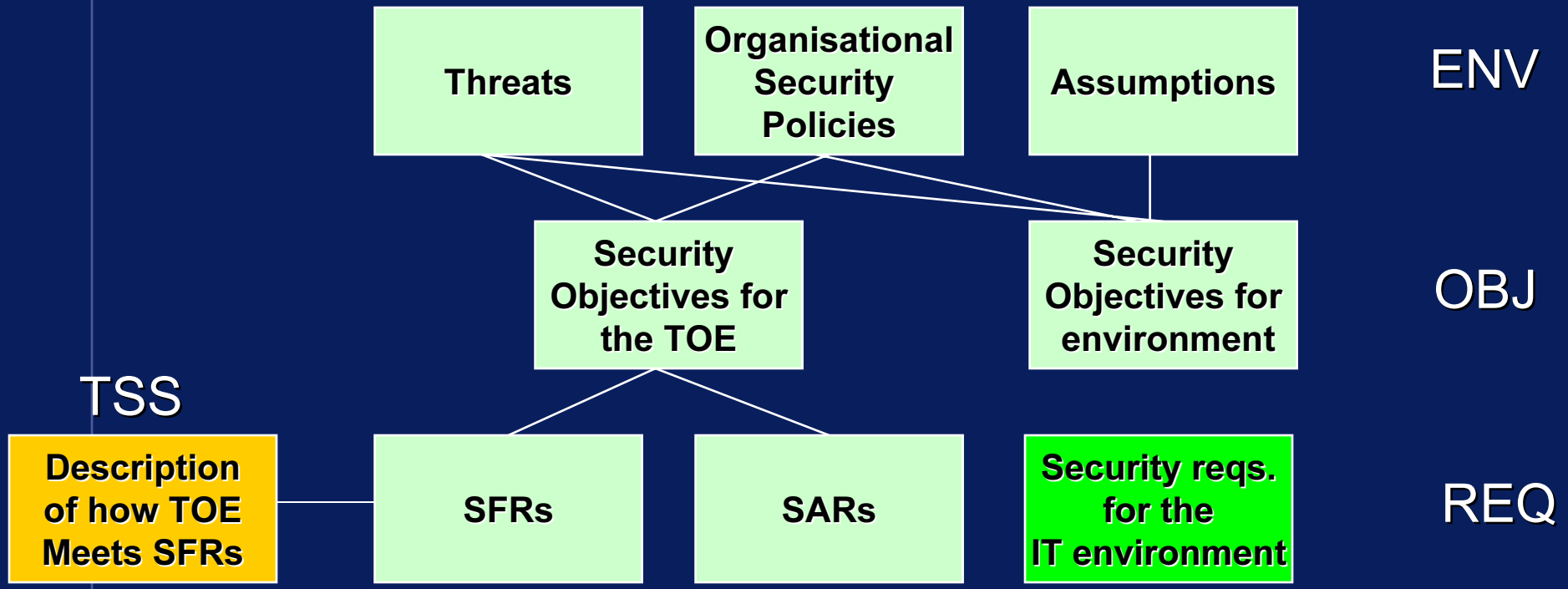
Strength-of-function

Why is it separately rated from VLA?

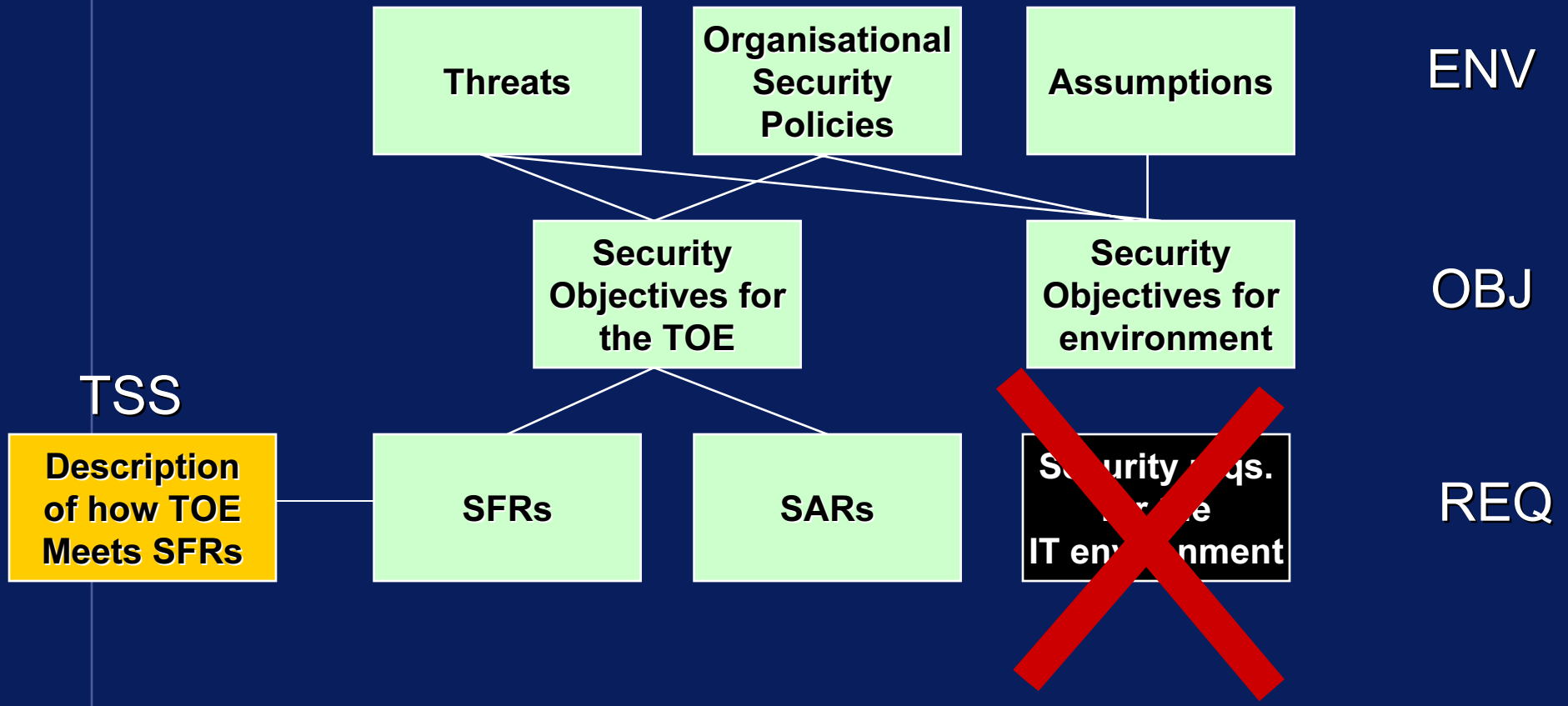
SOF-high and VLA.2 means you hack around the SOF

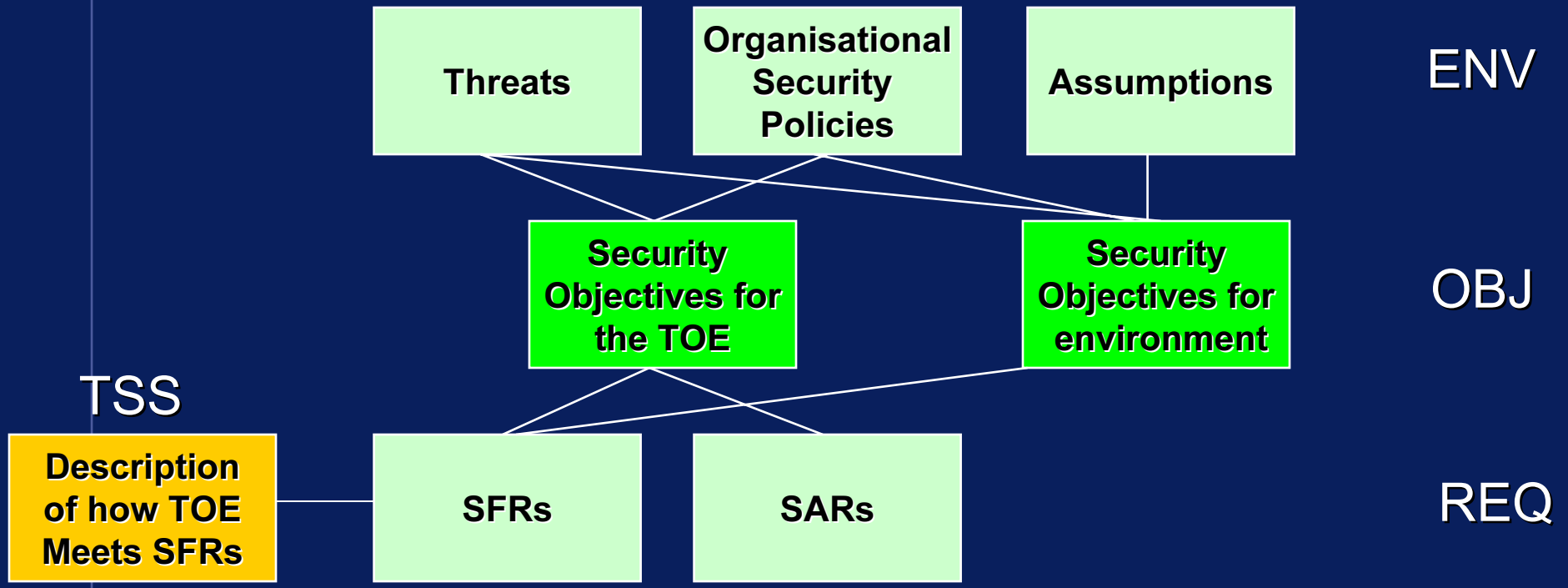
SOF-basic and VLA.4 means you guess around the VLA

SOF is merged in VLA



Nobody knew what they were for.....


Threats
Organisational Security Policies
Assumptions
ENV
Security Objectives for the TOE
Security Objectives for environment
OBJ
TSS
Description of how TOE Meets SFRs
SFRs
SARs
REQ


Threats
Organisational Security Policies
Assumptions
ENV
Security Objectives for the TOE
Security Objectives for environment
OBJ
TSS
Description of how TOE Meets SFRs
SFRs
SARs
REQ

Problems

How can assurance requirements meet security objectives for the TOE?

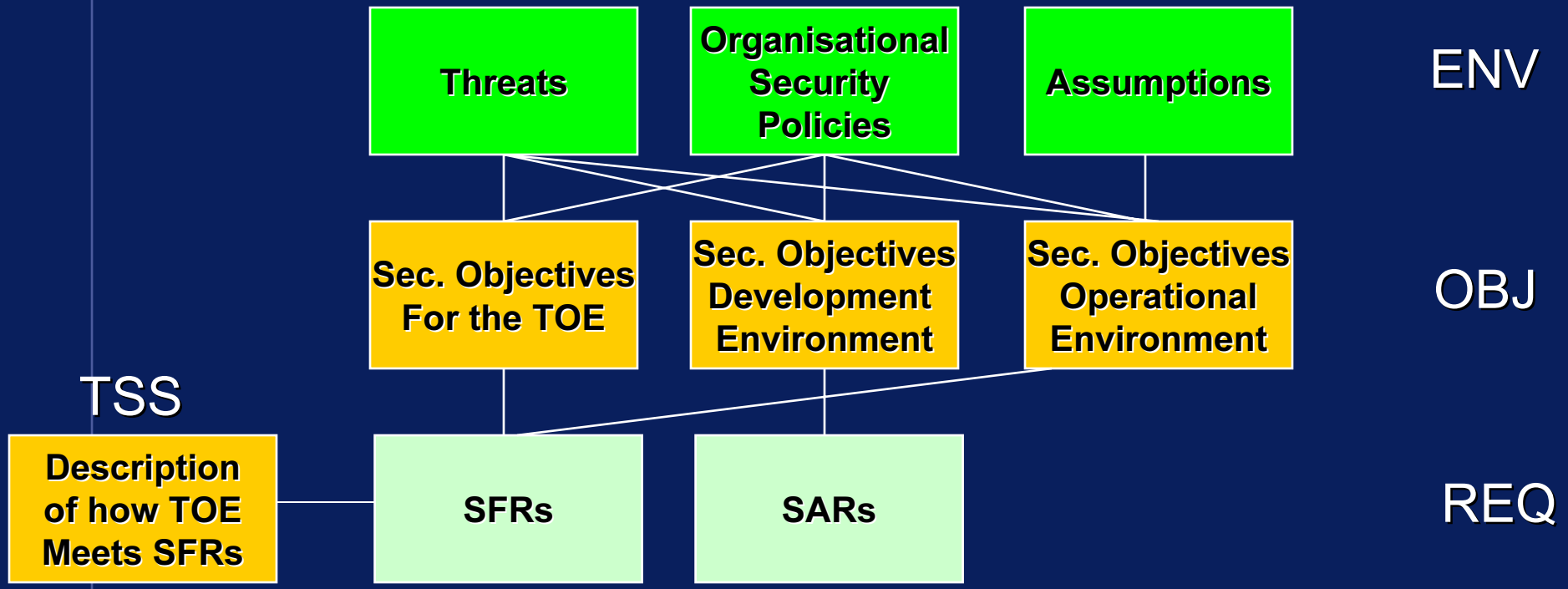
What is “the environment”?

- Operational environment?
- Development environment?

Solution (divide into three)

- **Security Objectives for the TOE** are now purely functional (and map to SFRs)
- **Security Objectives for the Development Environment** are purely assurance (and map to SARs)
- **Security Objectives for the Operational Environment** do not map to anything (they are not evaluated)

Solution (divide into three)


Threats
Organisational Security Policies
Assumptions
ENV
Sec. Objectives For the TOE
Sec. Objectives Development Environment
Sec. Objectives Operational Environment
OBJ
TSS
Description of how TOE Meets SFRs
SFRs
SARs
REQ

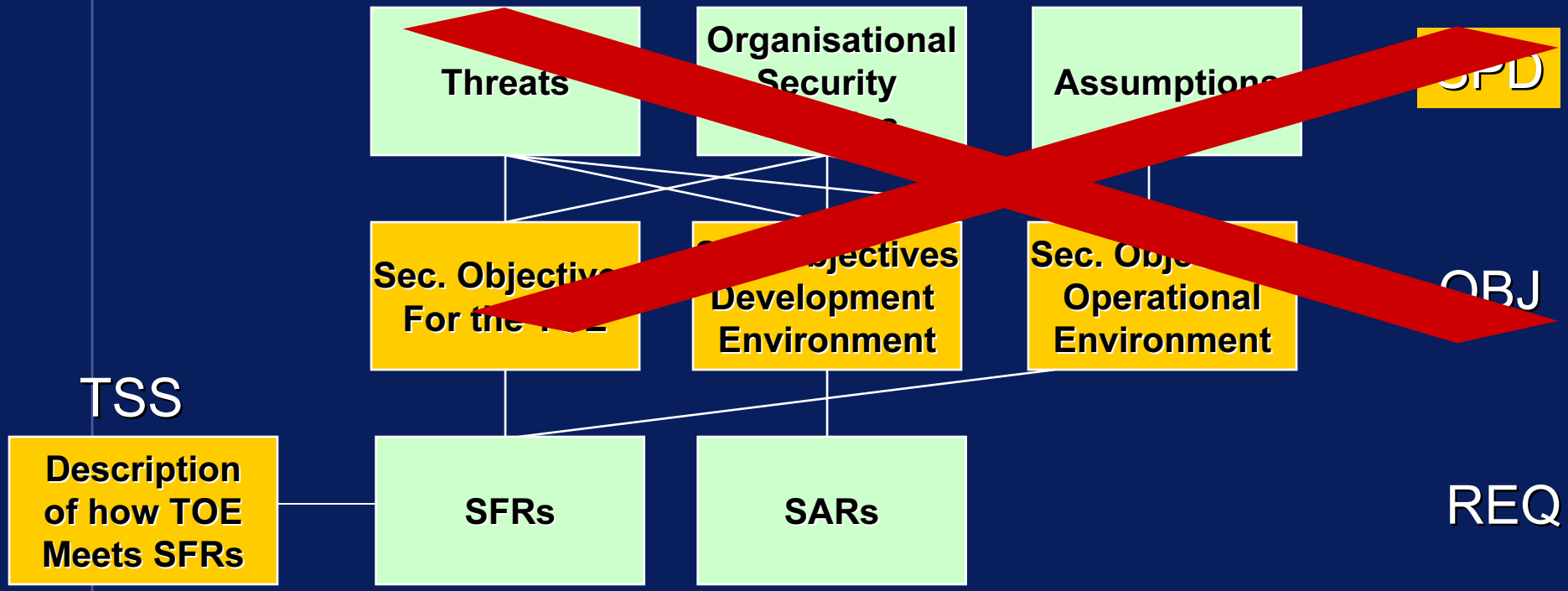
Confusing name: Environment (ENV)

- Environment (ASE_ENV)
- Operational environment
- Development environment
- IT environment
- Non-IT environment

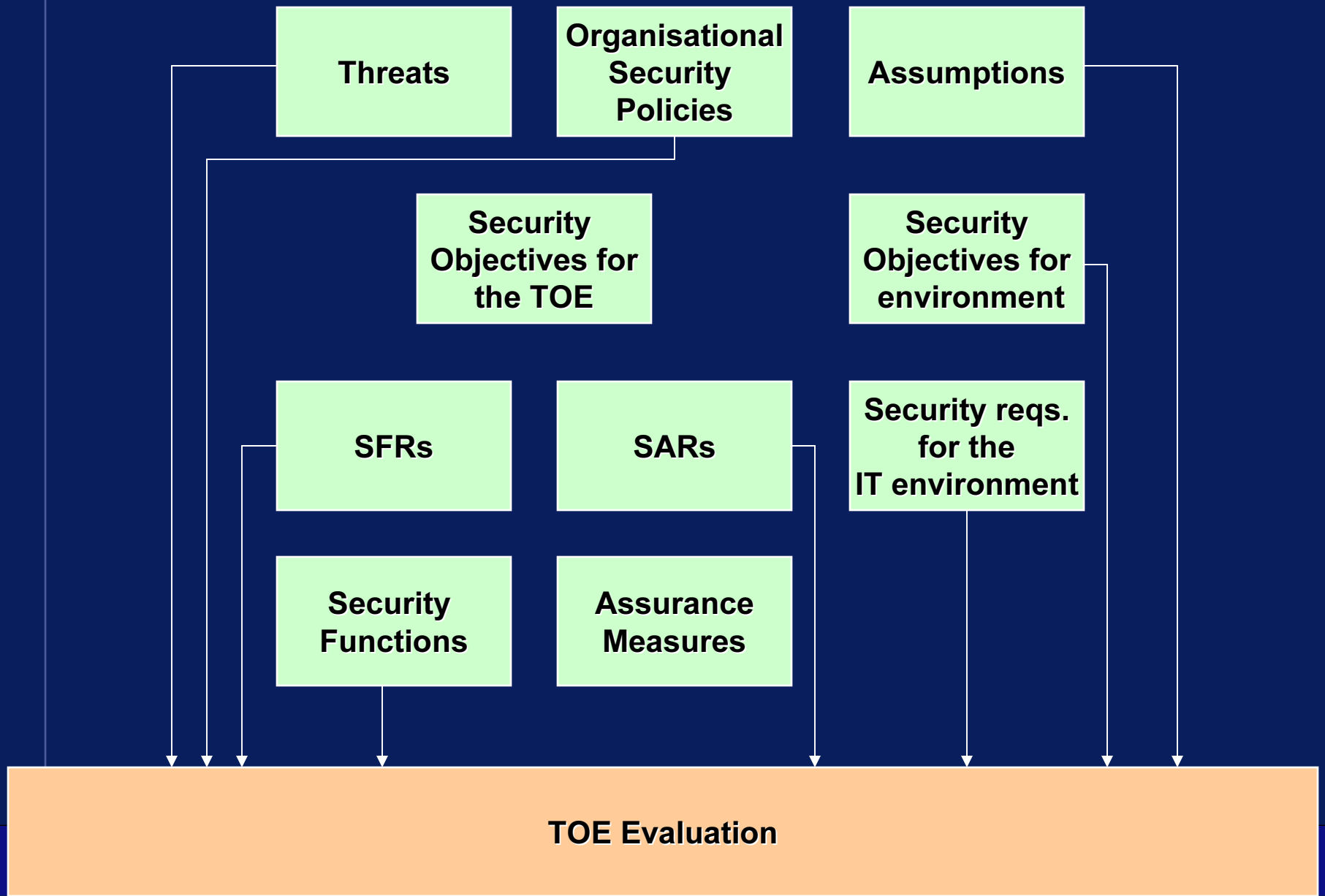
Changed to Security Problem Definition (ASE_SPD)

Renamed ENV -> SPD

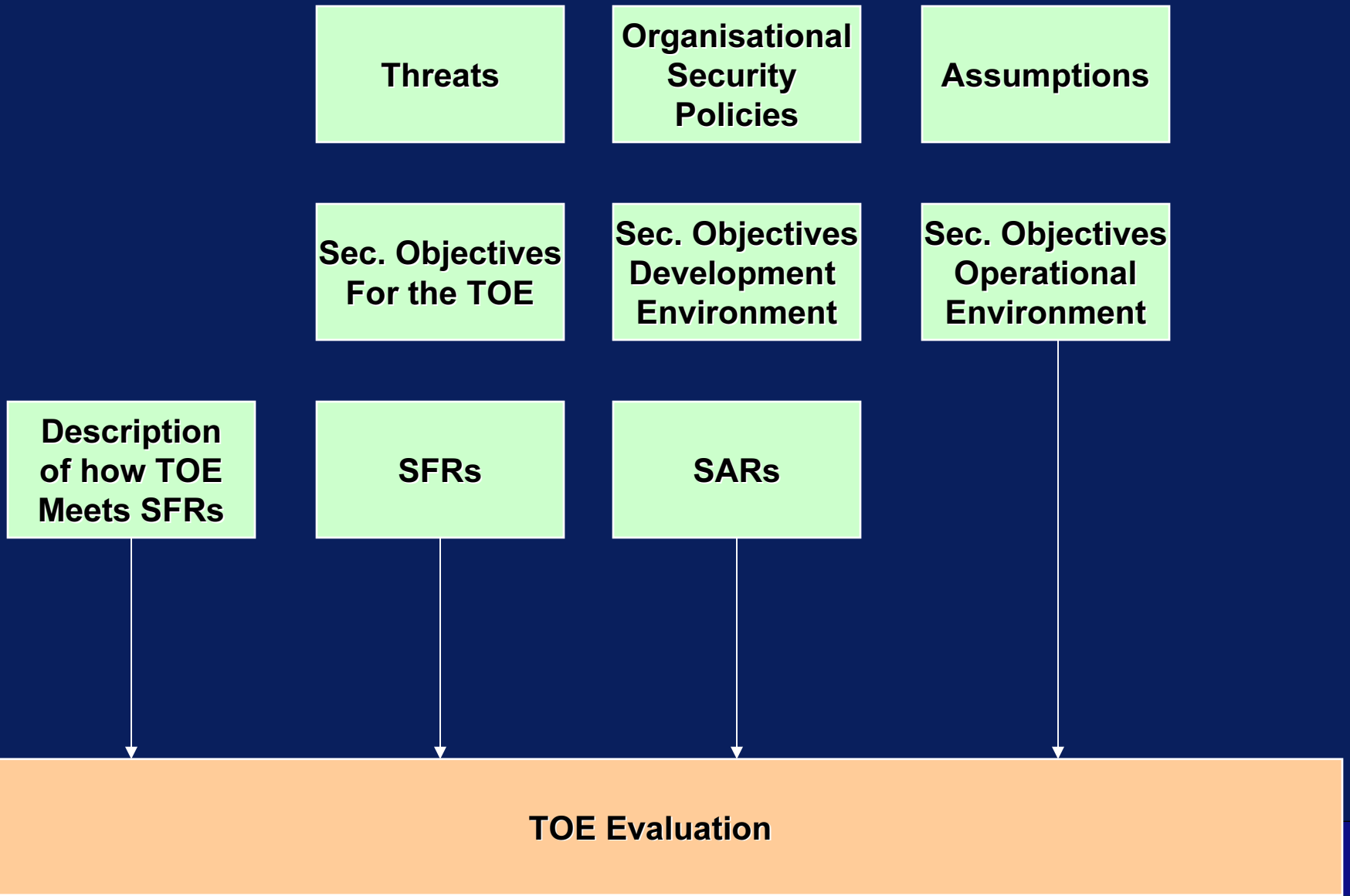
Made life a lot easier for EAL1



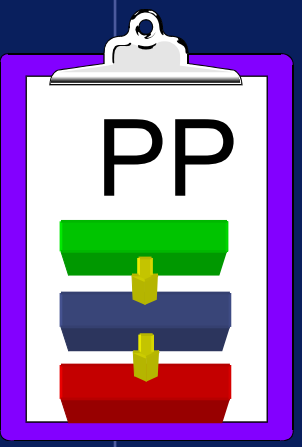
How a 2.1 ST is used



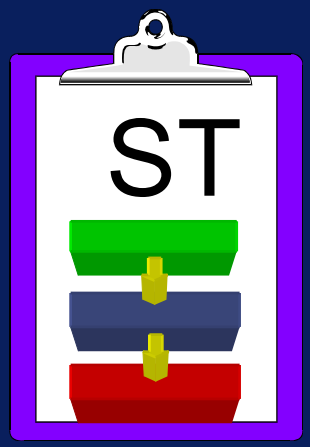
How a 3.0 ST is used



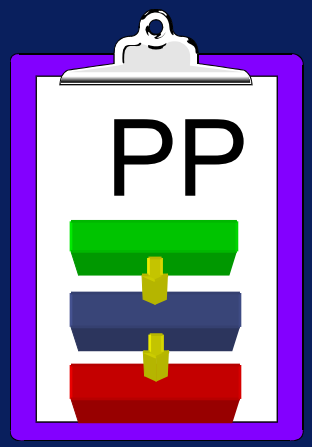
Diversified PP Compliance



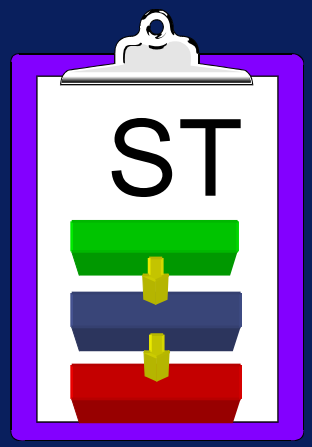
=



Exact

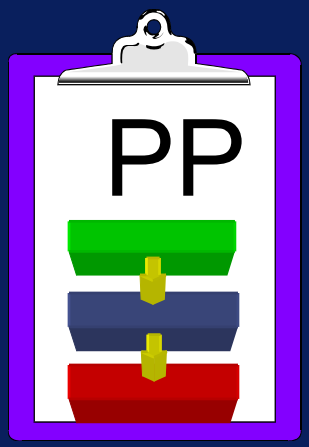


⊆

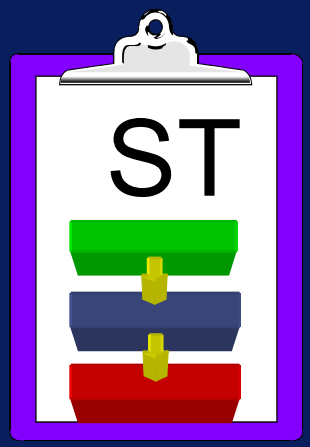


Strict

Demonstrable



≈



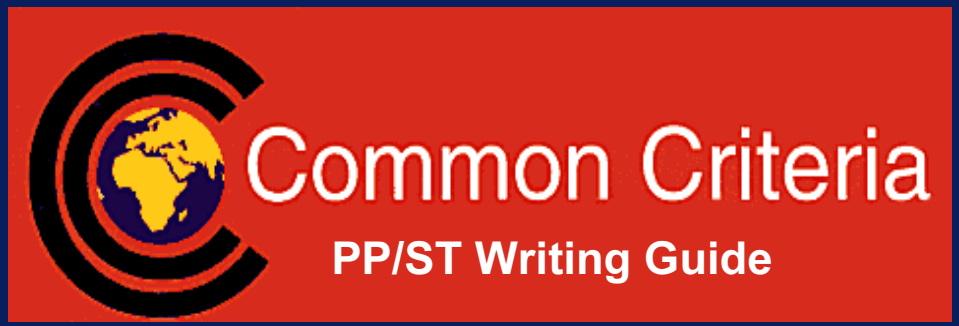
And less noticeable……

- Removed implied (double) requirements
- Removed numerous qualifications (“the threats in the ST”)
- Removed useless requirements
- Removed confusing terminology (“mutually supportive”)
- Wrote a substantive Annex for Part 1 explaining all of this

The next step

- Criteria will tell you what is allowed, not how to write a good one

- Next Step



Questions