Common Criteria Course Module

CC v3.0 The New Conceptual Framework

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

Dirk-Jan Out
+ 31 70 374 0000
out@itsef.com
www.commoncriteria.nl

This work (and the following) has been financed by:

- BSI — Germany
- CSE — Canada
- NLNCSA — Netherlands
- NSA — United States

Product of a long discussion

The CCIMB found out the we used the same words to mean different things

And of course we also used different words for the same thing.

Apparently something was wrong with the words…

If you want to clean a set of stairs

you must start at the top

bottom

Too many words

- Security functions
- TOE Security Functions
- Security functional requirements
- Security functional components
- Security functional policies
- Security attributes
- Organisational security policy
- Security environment
- Security objectives
- IT security requirements
- Security requirements for the (non)-IT environment
- TOE Security Policy
- Security Policy Model
- TSF Scope of Control
- TSF Interface

Too many undefined words…

A threat is:

An attacker gains access to confidential data?

(it threatens something the consumer holds dear)

Too many undefined words…

A threat is:

An attacker gains access to confidential data?
(it threatens something the consumer holds dear)

Or

An attacker causes a buffer overflow
(it threatens the TOE)

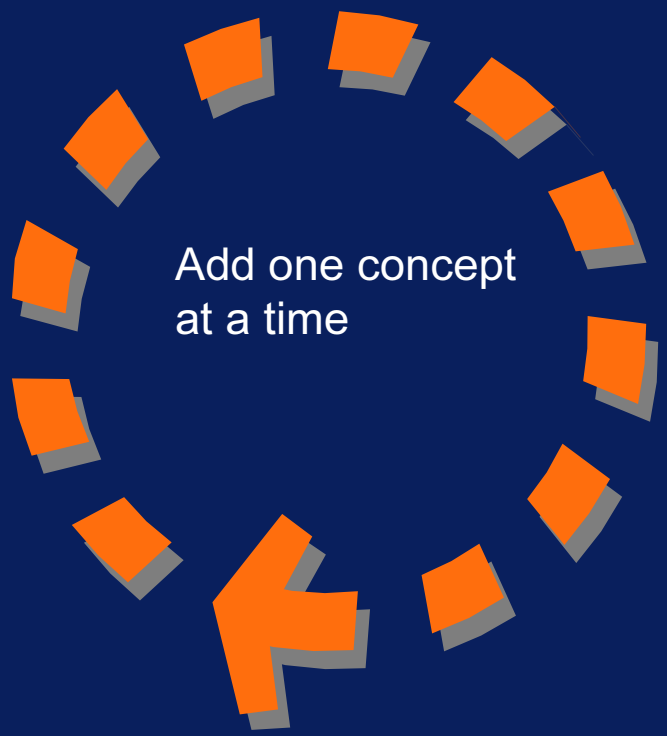
A vulnerability is something that breaks the TSP, but

Where is the TSP?

In short: it was too complex

Start from scratch

Start from a few simple concepts



Until you can model everything

Too many undefined terms…

A threat is:

An attacker gains access to confidential data

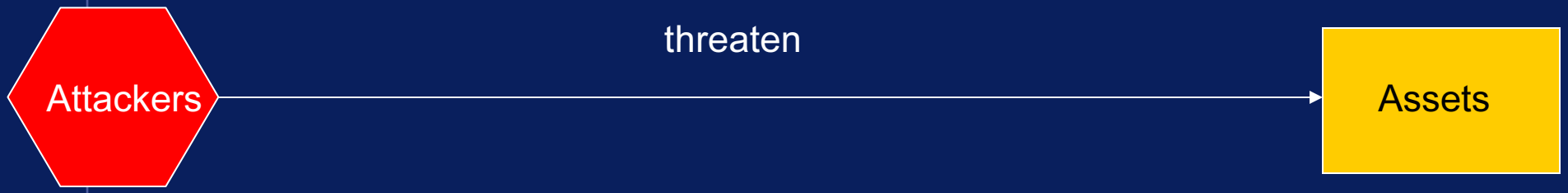
(it threatens something the consumer holds dear)

Or

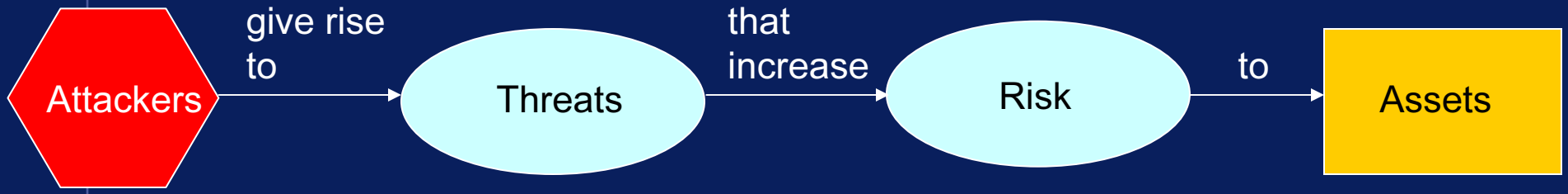
An attacker causes a buffer overflow

(it threatens the TOE)

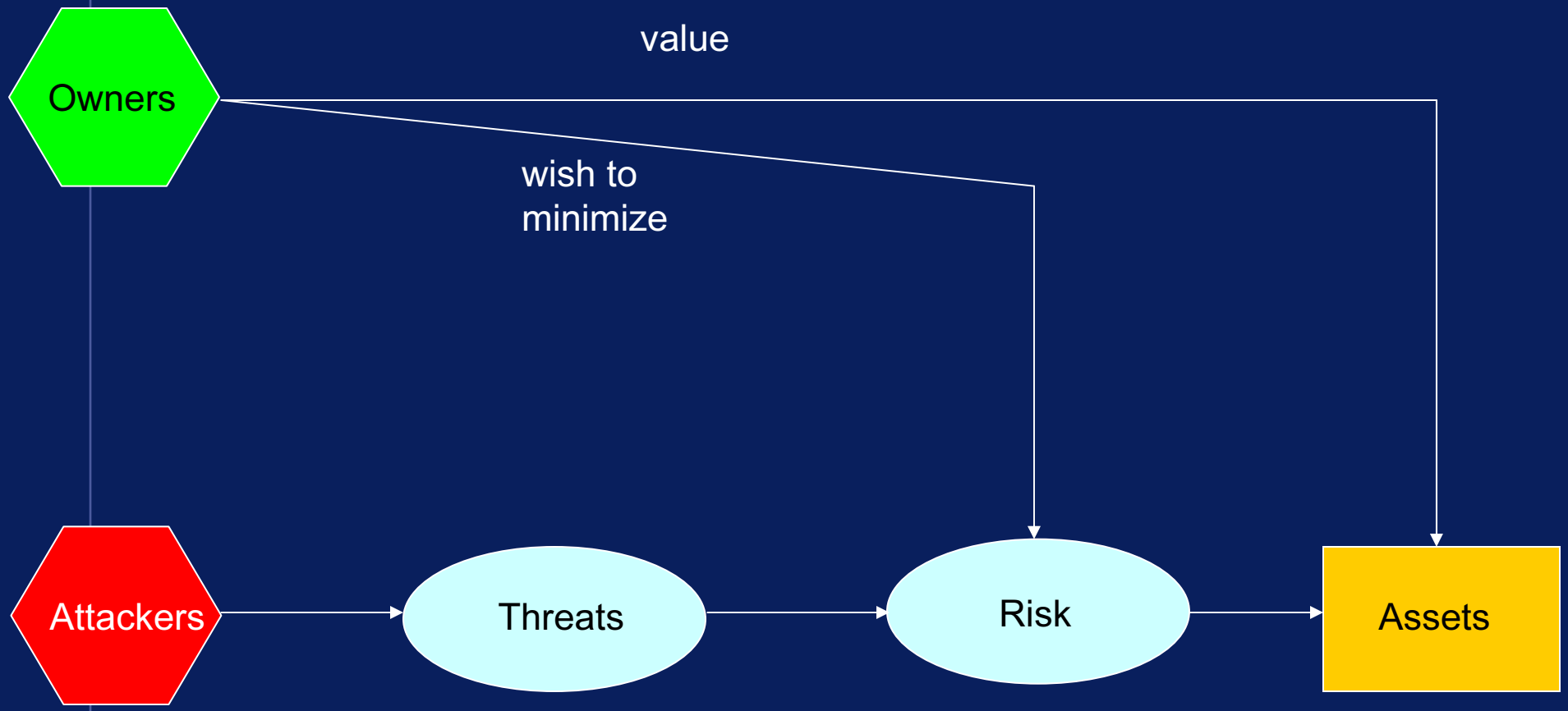
Attackers may damage assets



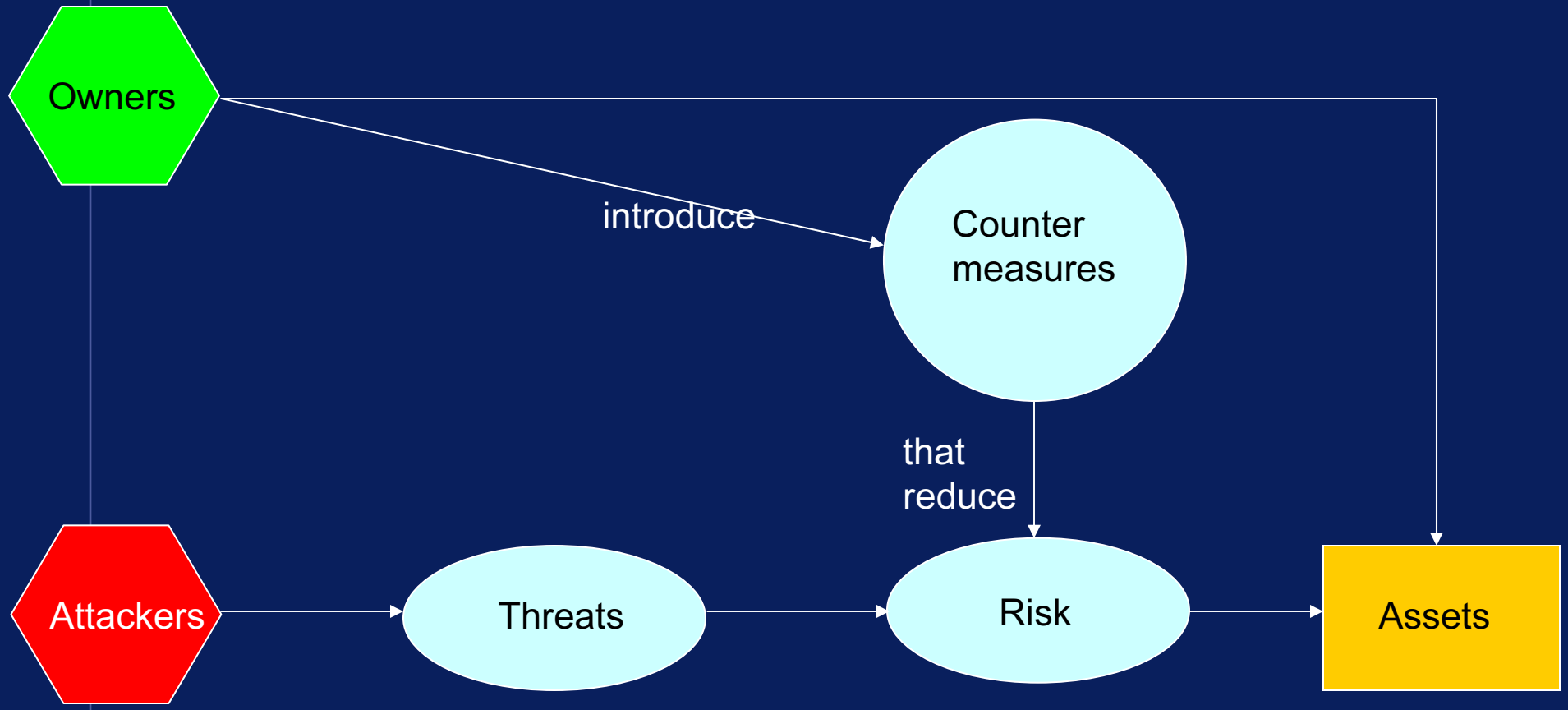
Attackers give rise to threats
Threats increase risks to assets



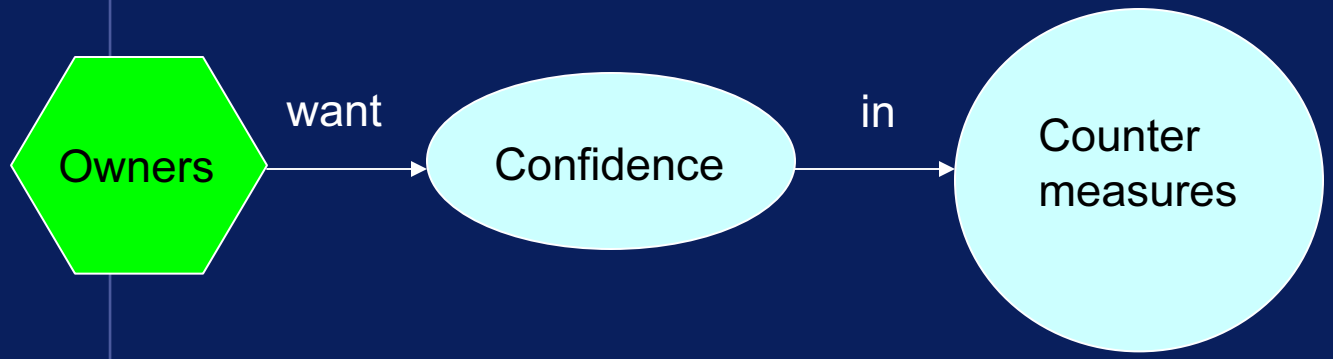
Owners value assets
Owners wish to minimize risks



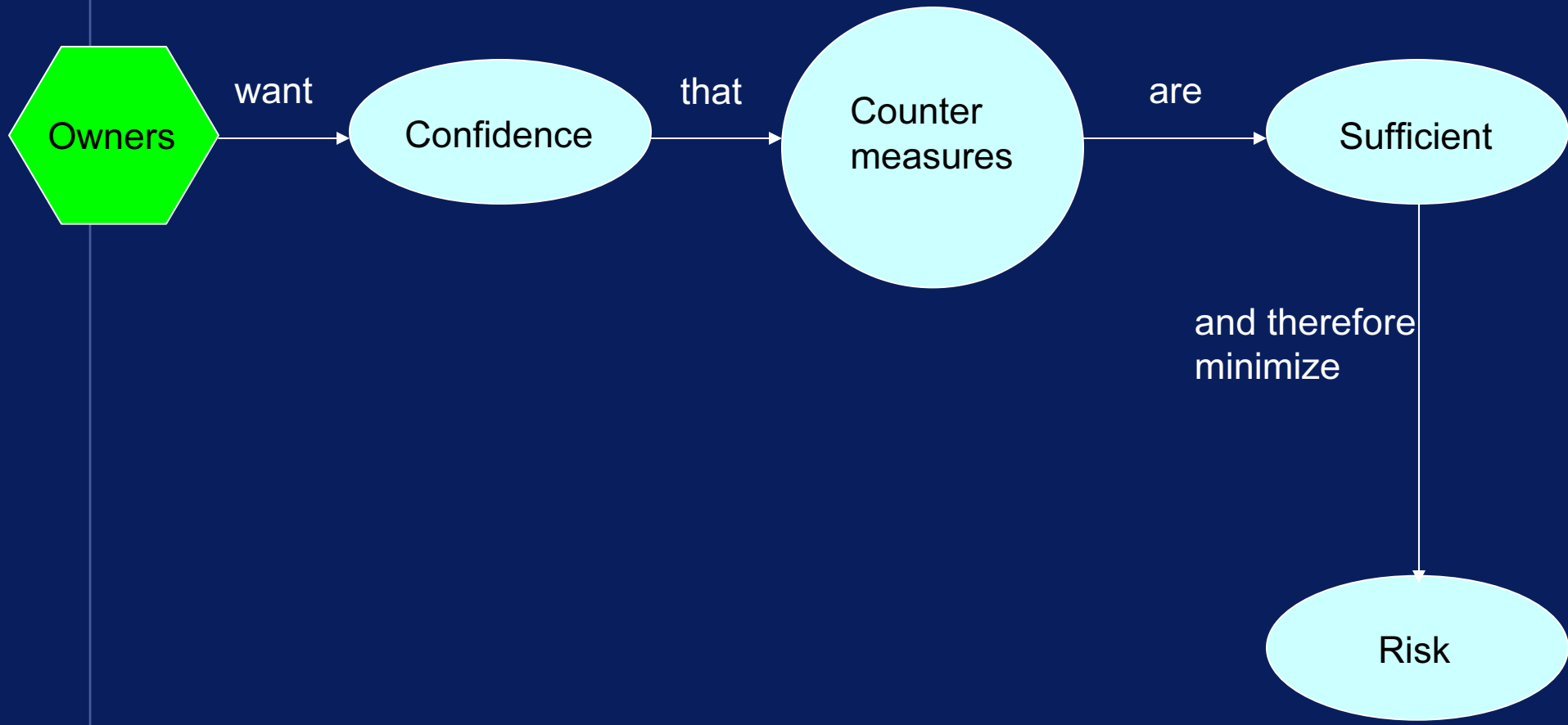
Owners introduce countermeasures
Countermeasures reduce risks



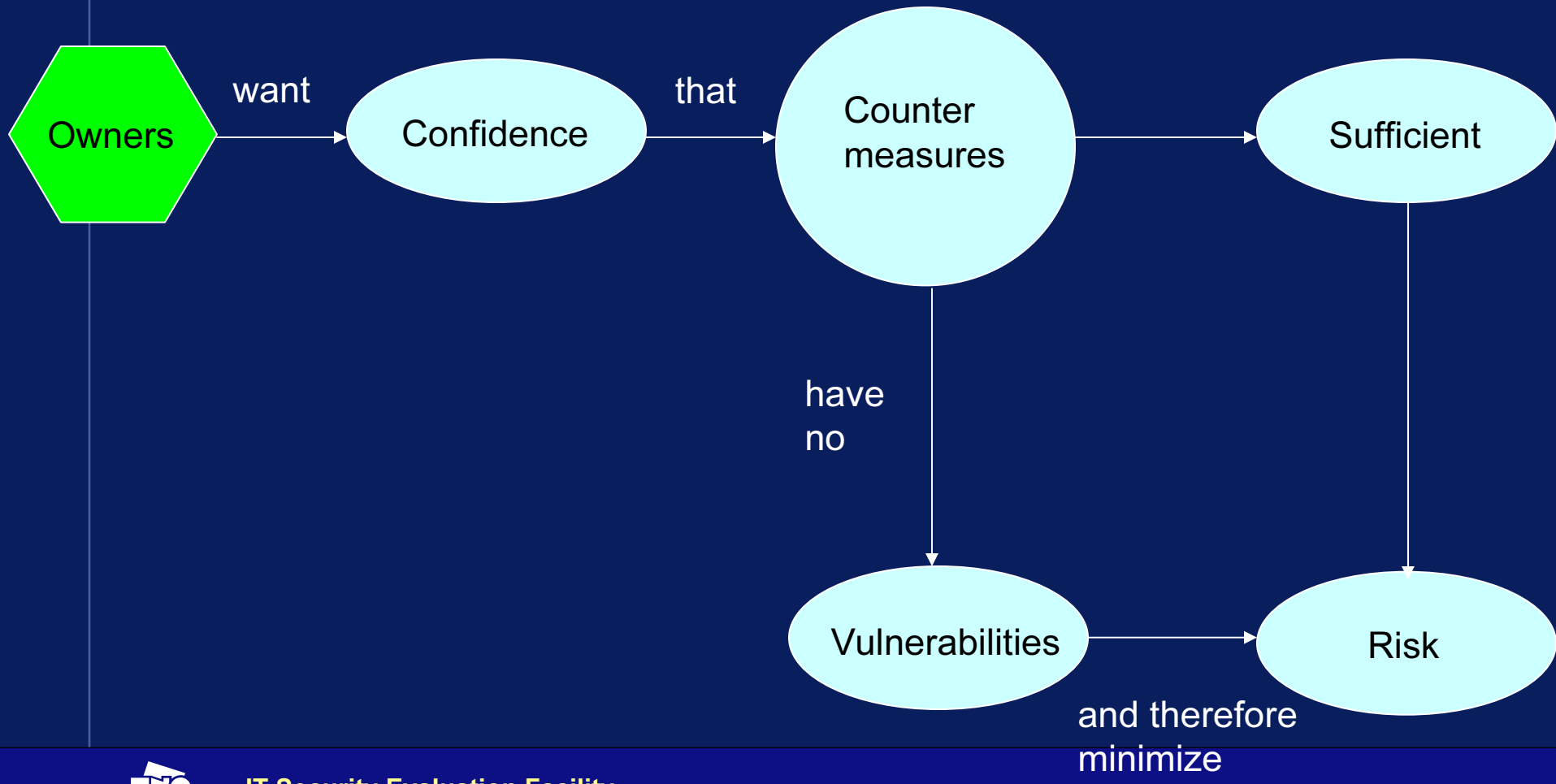
Owners want confidence in countermeasures



Countermeasures must be sufficient

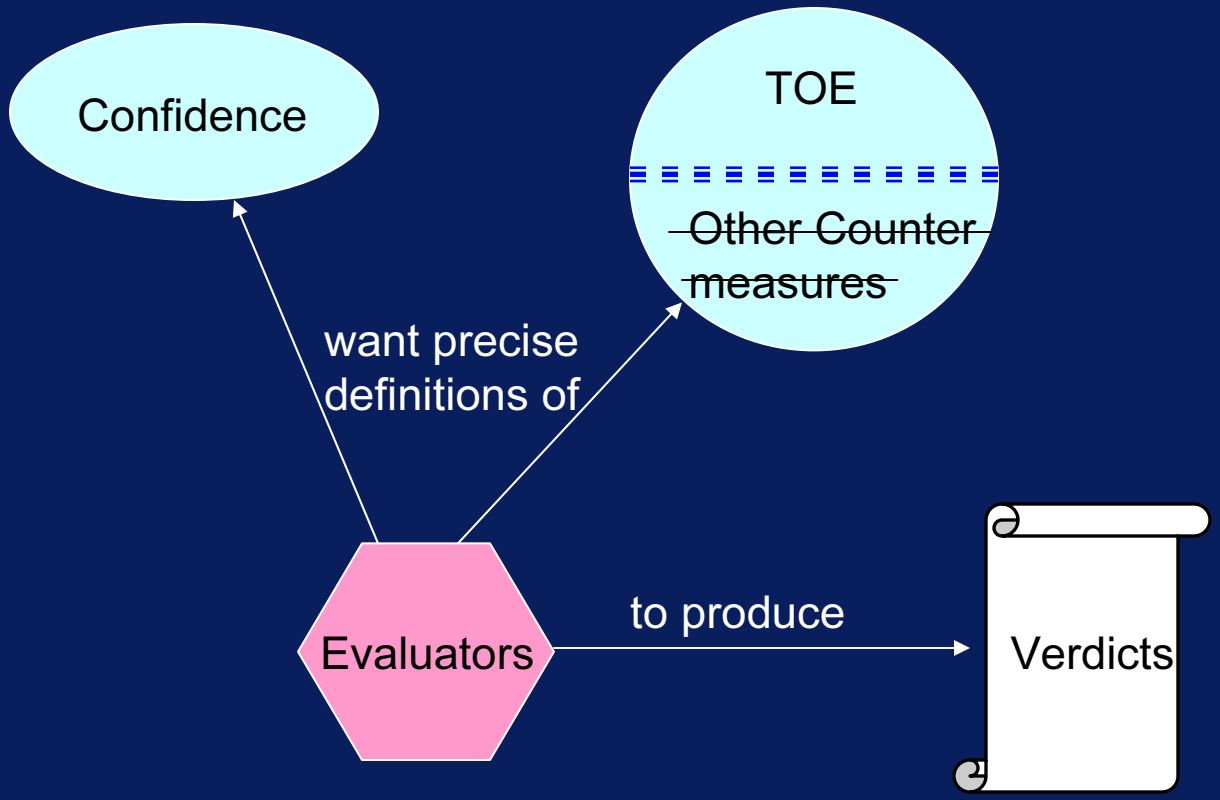


Countermeasures must have no vulnerabilities



Countermeasures consists of the TOE and other countermeasures

Evaluators need precise descriptions



The precise decriptions:

The confidence in the TOE is precisely described by the **Security Assurance Requirements**

The functionality of the TOE is precisely described by the **Security Functional Requirements**

The Security Functional Requirements are collectively referred to as "**The TOE Security Policy**"

A big OS

About 500 tools, applications, editors, applets,
Data files, user areas etc.

Kernel

TSF = TOE Security Functionality

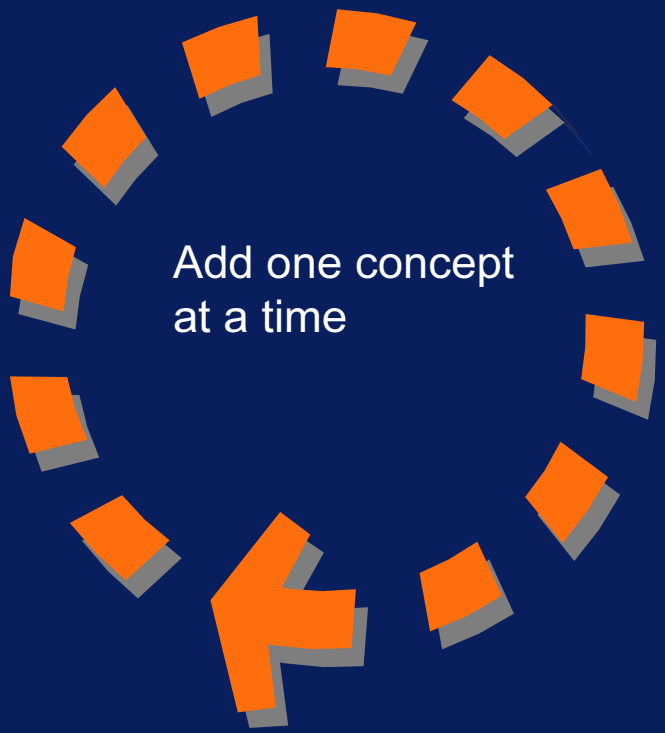
A part of the TOE that:

- implements the TSP (all SFRs)
- cannot be influenced by the rest of the TOE

Having a small TSF saves the developer work

Start from scratch

Start from a few simple concepts



Until you can model everything

Then throw away the rest

Less concepts

- ~~Security functions~~
- TOE Security Functionality
- Security functional requirements
- Security functional components
- ~~Security functional policies~~
- Security attributes
- Organisational security policy
- ~~Security environment~~
- Security objectives
- ~~IT security requirements~~
- ~~Security requirements for the (non) IT environment~~
- TOE Security Policy
- ~~Security Policy Model~~
- ~~TSF Scope of Control~~
- TSF Interface

Conclusions

It will never be easy, but now it is easier

It will never happen that everybody understands everything, but now at least a small group understands it

Hopefully, we will all understand it someday

Questions