

---

# *Common Criteria Paradigm (CC)*



*Marvella L. Towns*

*December 2000*

# Contents

- **CC Purpose and Potential Uses**
  
- **CC**
  - **Part I**
    - **Introduction & General Model**
  - **Part 2**
    - **Functional Requirements**
  - **Part 3**
    - **Assurance Requirements**

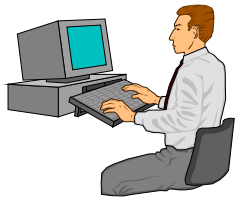
# The Common Criteria (CC)

**The CC is a collection of generic security requirements (statements) to aid in the specification of product or system security attributes (Functional and Assurance)**

# Users of the Common Criteria (CC)



**Consumers** - to support the **procurement** of products/systems with IT security features



**Product Developers and Integrators** - as a basis for the **development** of products/systems with IT security features



**Evaluators** - as the basis for the **evaluation** of IT security products/systems

**Auditors, Certifiers, Accreditors, ANYONE** - to support specific needs for security specifications

# Intended CC Application/Scope

- **A paradigm used to specify security properties of IT products and systems that address**
  - **unauthorized disclosure (confidentiality, privacy)**
  - **unauthorized modification (integrity)**
  - **loss of use (availability)**
- **The basis for comparison of the results of independent evaluations**
- **Applicable to IT security functions implemented by hardware, software, and firmware**

# Out-of-Scope for the CC

- “People-based” and physical security implementations
- CC Application Processes
  - Administrative, Legal, Procedural
  - Accreditation & Certification
  - Mutual recognition arrangements
- Evaluation methodology
  - Companion Methodology Document
    - Common Evaluation Methodology for Information Technology Security Evaluation (CEM)
- Cryptographic algorithm definition
  - CC addresses use of cryptography

# CC Documents

- **Part 1 - Introduction and General Model**
- **Part 2 - Security Functional Requirements**
- **Part 3 - Security Assurance Requirements**

# CC Part 1: Introduction & General Model

- **Scope, Glossary, Overview**
- **Security Context & CC Approach**
- **Security Concepts, Environment & Objectives**
- **Evaluation Results**
- **Appendix A: History**
- **Appendix B: Specification of Protection Profiles (PPs)**
- **Appendix C: Specification of Security Targets (STs)**

# Key Common Criteria Definitions

- **Target of Evaluation (TOE)**
  - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation
  
- **Protection Profile (PP)**
  - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs
    - “goal” specification
  
- **Security Target (ST)**
  - An implementation-dependent set of security requirements and specifications used as the basis for evaluation of the identified TOE
    - ~ as-built specification

# Protection Profiles

- **Answers the question:**  
*“What do I need in a security solution?”*
- **Implementation independent for a class of products or systems**
- **Protection Profile authors:**
  - anyone who wants to state IT security needs (e.g., commercial consumer, consumer groups)
  - anyone who supplies products which support IT security needs
  - anyone ...

# Security Targets

- Answers the question:  
*“What does a developer provide in a security solution?”*
- Implementation dependent and version specific
- Security Target authors:
  - Product vendors, developers, integrators
    - Knowledge of implementation details required

# Example of PPs and STs

- **PP makes a statement of implementation independent security needs**
  - *a generic OS with DAC, Audit, and I&A*
- **ST defines the implementation dependent capabilities of a *specific* product, e.g.**
  - **Microsoft NT 4.0.0.2 (TOE)**
  - **Sun OS 4.7.4 (TOE)**

# PP/ST Contents/Comparison

## Protection Profile

- Identification
- Overview
- TOE Description
- Security Environment
  - Assumptions, Threats, Policies
- Security Objectives
- Security Requirements
  - Functional, Assurance (EAL)
- Rationale

## Security Target

- Identification
- Overview
- TOE Description
- Security Environment
  - Assumptions, Threats, Policies
- Security Objectives
- Security Requirements
  - Functional, Assurance (EAL)
- Rationale
  
- TOE Summary Specification
- CC Conformance Claim
- PP Claims

# Security Environment

# Security Environment

- **Considerations**

- purpose and function of the TOE
- IT and Non-IT environment
- Assets to be protected

- **Assumptions**

- *The security aspects of the environment in which the TOE will be used or is intended to be used.*

- **Threats**

- *The ability to exploit a vulnerability by a threat agent.*

- **Organizational Security Policies (OSPs)**

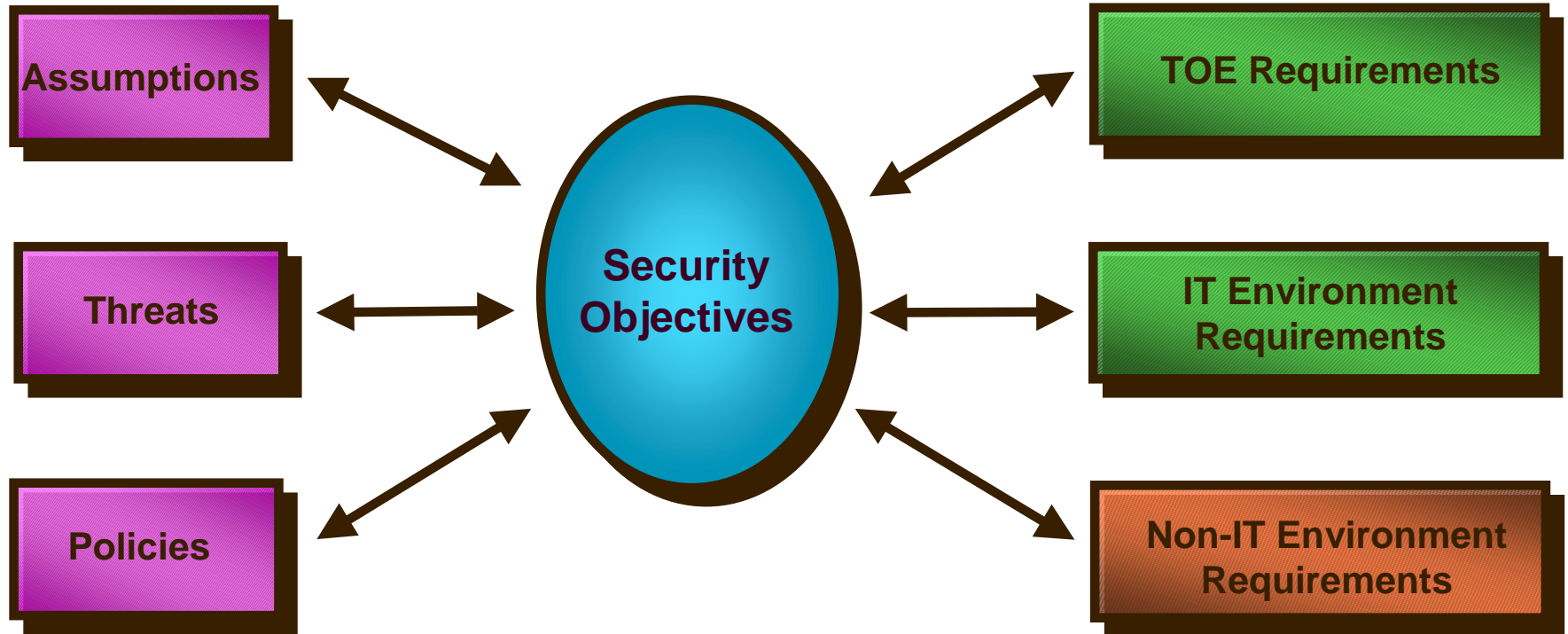
- *A set of rules, procedures, practices, or guidelines imposed by an organization upon its operations and to which the TOE may have to comply.*

# Security Objectives

# Security Objectives

- Objectives establish the basis for the selection of security requirements (functional & assurance)
- Objective are completely based upon the statement of the Security Environment
- Objectives
  - Support Assumptions
  - Counter Threats (eliminate, minimize, monitor)
  - Enforce OSPs

# Security Objectives



# Security Requirements

# CC Documents

- Part 1 - Introduction and General Model
- **Part 2 - Security Functional Requirements**
- Part 3 - Security Assurance Requirements

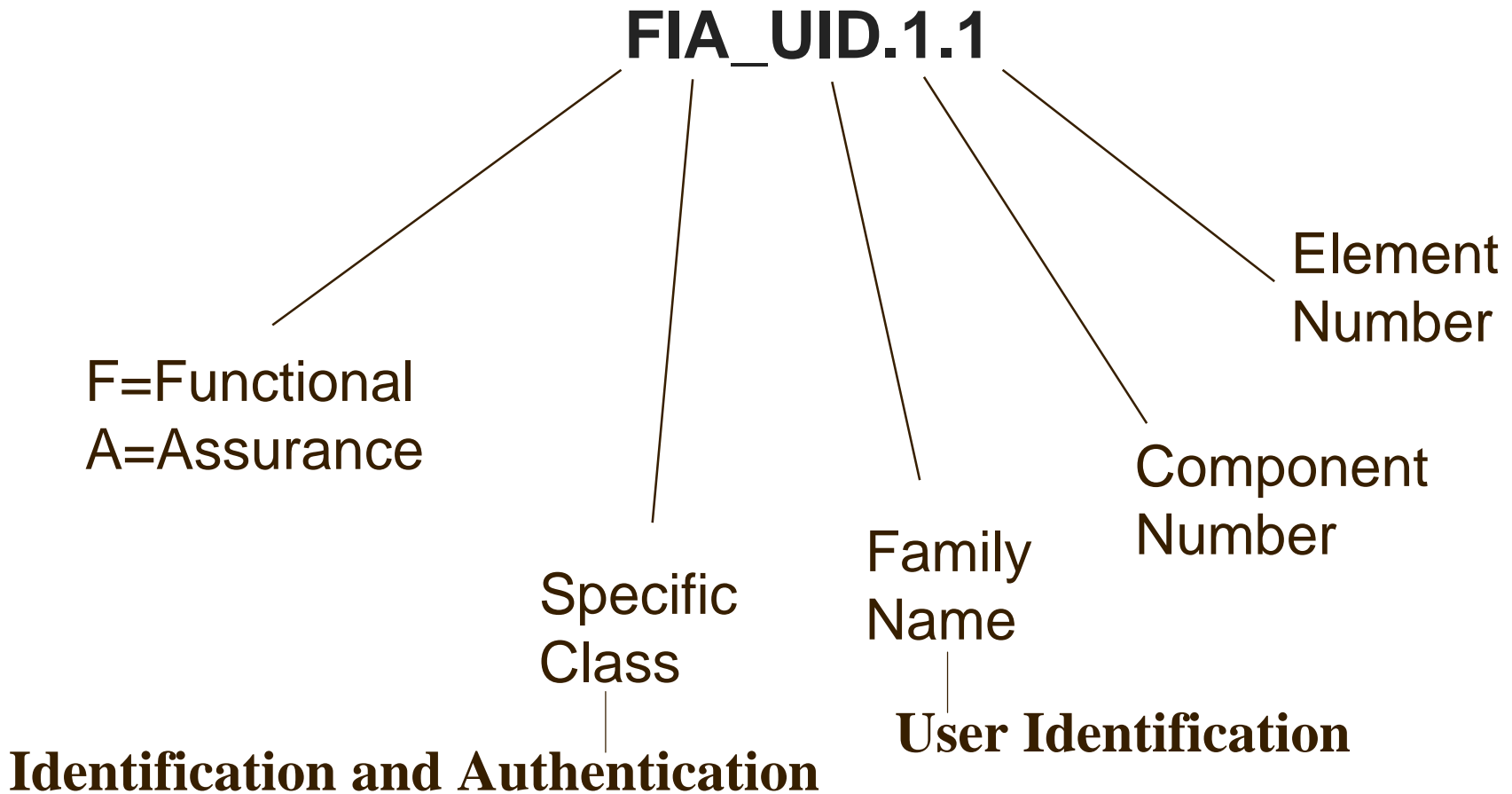
# Security Functional Requirements

*Levied upon functions of the TOE that support IT security; their behavior can generally be observed*

# Functional Requirement Classes

- **Security Audit (FAU)**
- **Communication (FCO)**
- **Cryptographic Support (FCS)**
- **User Data Protection (FDP)**
- **Identification & Authentication (FIA)**
- **Security Management (FMT)**
- **Privacy (FPR)**
- **Protection of the TOE Security Functions (FPT)**
- **Resource Utilization (FRU)**
- **TOE Access (FTA)**
- **Trusted Path/Channels (FTP)**

# Functional Requirement Names



# Using Functional Components

- **The CC defines 2 types of component relationships**
  - **Dependency relationship - other component support (functional & assurance)**
  - **Hierarchy relationship - between components within a class**
  
- **The CC provides 4 types of operations on functional components**
  - **Assignment - “fill in the blank”**
  - **Selection - “select from a list”**
  - **Iteration - “repetitive use”**
  - **Refinement - “tailor/modify”**

# CC Documents

- Part 1 - Introduction and General Model
- Part 2 - Security Functional Requirements
- **Part 3 - Security Assurance Requirements**

# What is Assurance?

## CC Definition:

*Grounds for confidence that an IT product or system meets its security objectives.*

# Assurance Classes

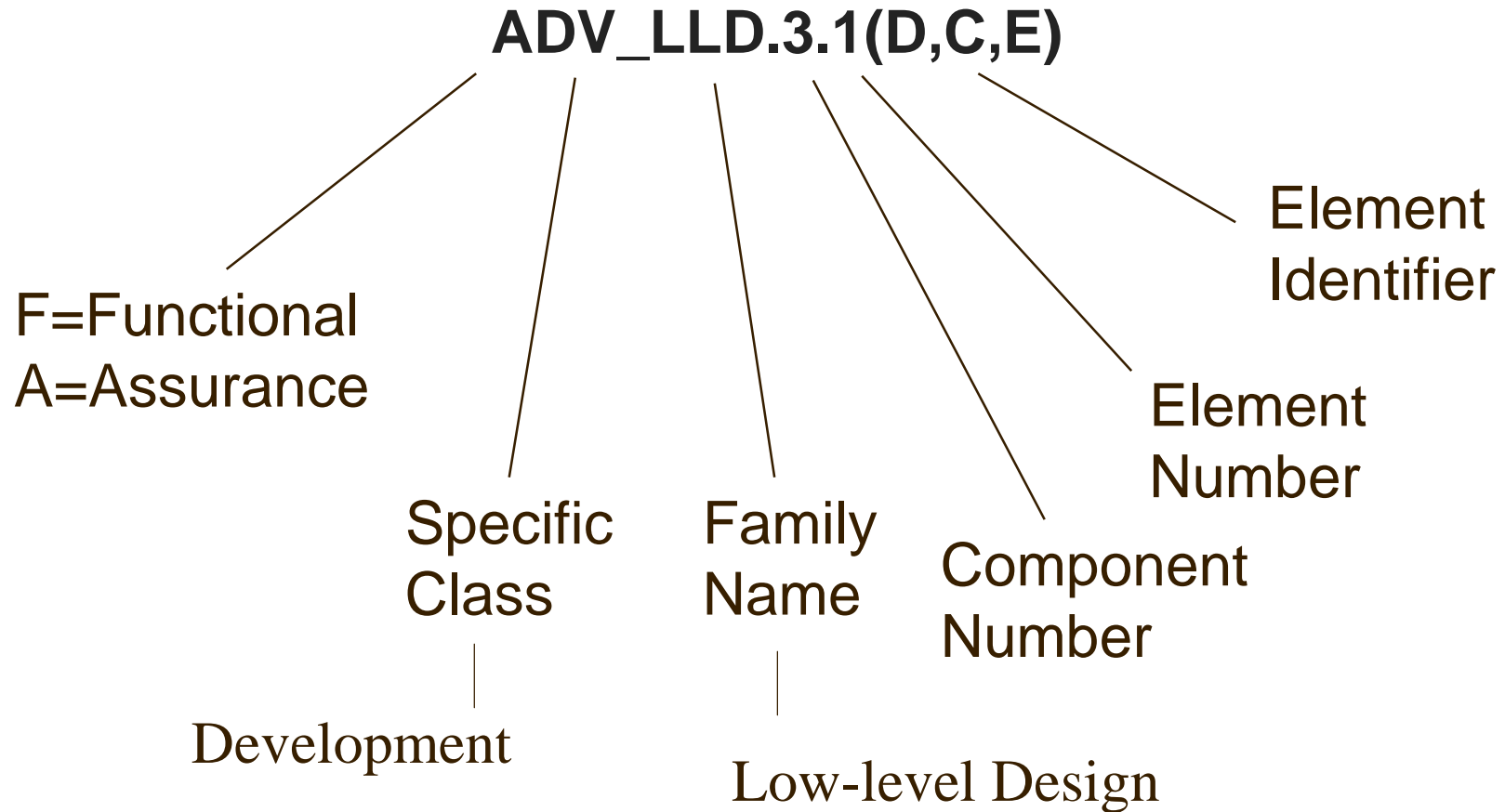
## TOE Assurance

- Configuration Management (ACM)
- Delivery and Operation (ADO)
- Development Documentation (ADV)
- Guidance Documents (AGD)
- Life-Cycle Support (ALC)
- Testing (ATE)
- Vulnerability Assessment (AVA)
  
- Maintenance of Assurance (AMA)

## Specification Assurance

- Protection Profile Evaluation (APE)
- Security Target Evaluation (ASE)

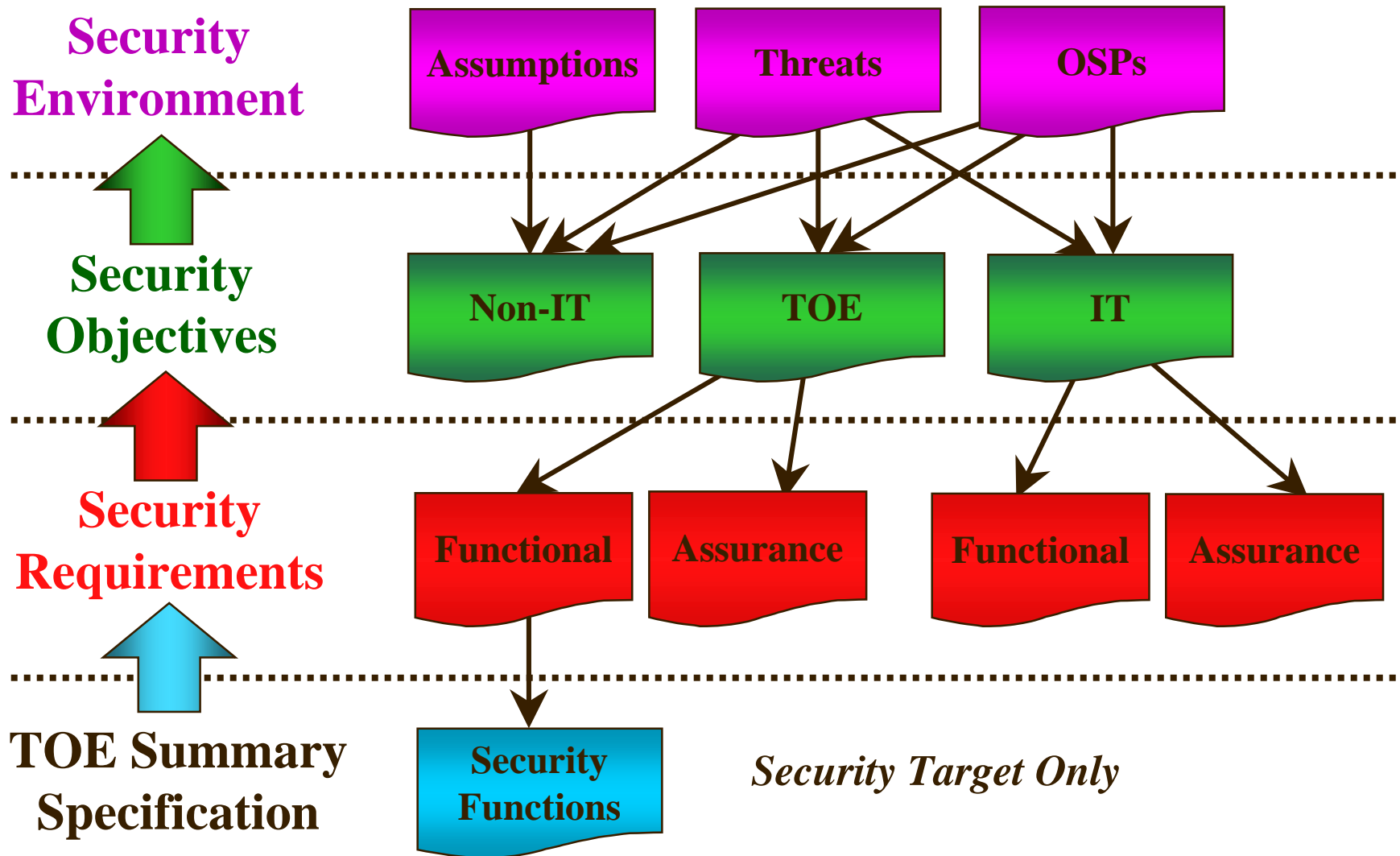
# Interpreting Assurance Requirement Names



# Assurance Packages

- **Basic Assurance Level - EAL 1 & 2**
  - Limited vendor involvement
  - Functional & independent testing
- **Medium Assurance Level - EAL 3 & 4**
  - Development environment controls
  - High-level design documentation
- **High Assurance Level - EAL 5, 6, & 7**
  - Additional CM requirements
  - Analysis based on entire TSF implementation
  - Covert channel analysis
  - Modular and layered TOE design
  - Automated CM
  - Formal methods of functional specification & high-level design

# PP/ST Framework



# CC ---> CEM Relationship

**Common  
Criteria**

**Common  
Evaluation Methodology**

**CLASS**



**ACTIVITY**

**FAMILY**



**SUB-ACTIVITY**

**EVALUATOR  
ACTION**



**WORK-UNIT**

# Automated Tool - cctoolbox

- **Questions**
  - **CC Toolbox - [cctoolbox@nist.gov](mailto:cctoolbox@nist.gov)**
  - **CC Profiling Knowledge Base - [cc-pkb@nist.gov](mailto:cc-pkb@nist.gov)**
- **Download CC Toolbox and CC Profiling Knowledge Base**
  - **<http://niap.nist.gov/tools/cctool.html>**

Visit our Internet Websites:

[\*\*http://niap.nist.gov/cc\*\*](http://niap.nist.gov/cc)

[\*\*http://niap.nist.gov/cc-scheme\*\*](http://niap.nist.gov/cc-scheme)

[\*\*http://www.radium.ncsc.mil/tpep\*\*](http://www.radium.ncsc.mil/tpep)

**CC Course Information**

**(410) 854-4458**

# Questions?