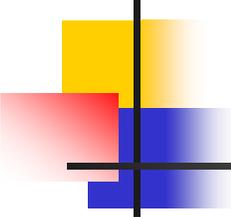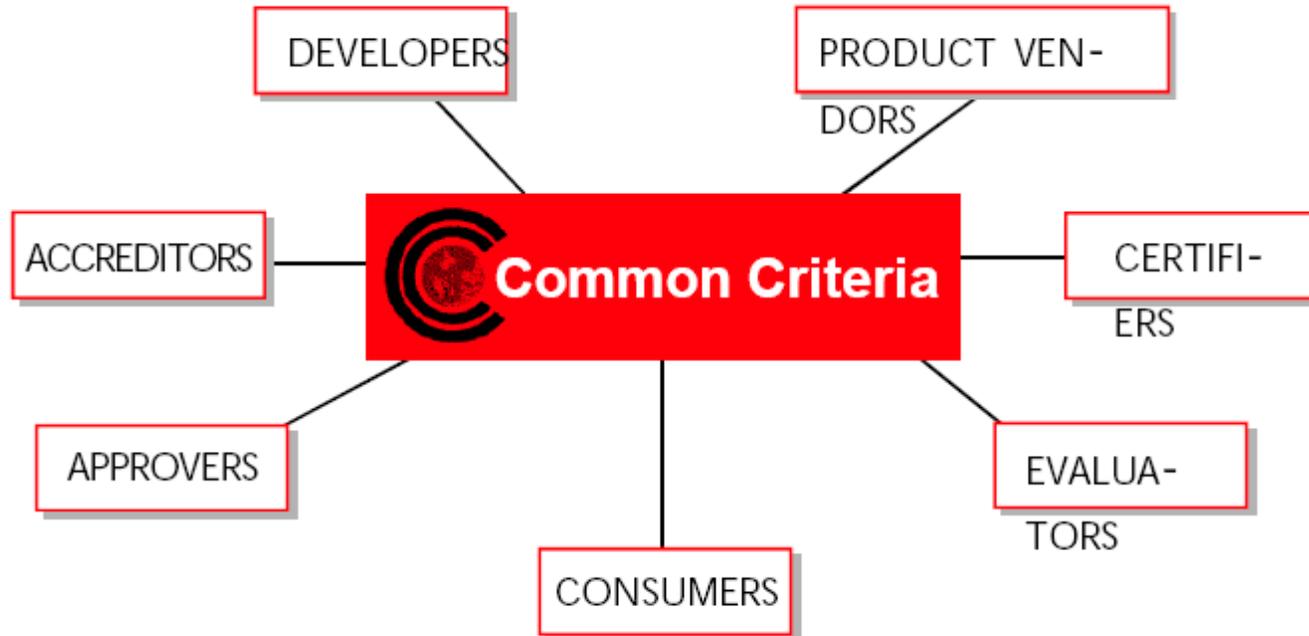# Common Criteria

Ravi Sandhu
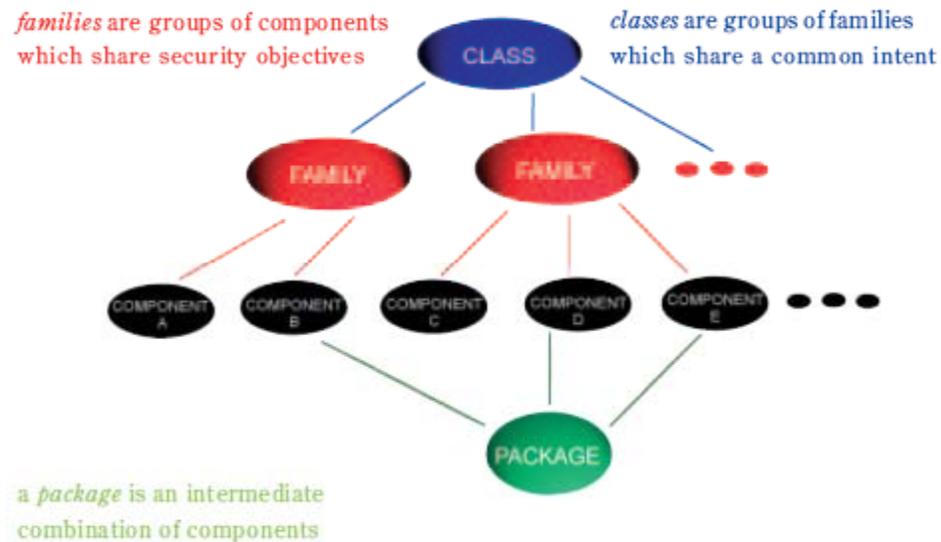
Common Criteria
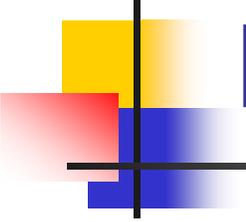
- **International unification**
  - CC v2.1 is ISO 15408
- **Flexibility**
- **Separation of**
  - Functional requirements
  - Assurance requirements
- **Marginally successful so far**
  - v1 1996, v2 1998, widespread use ???

Common Criteria

Class, Family, Component, Package

families are groups of components which share security objectives

classes are groups of families which share a common intent

a package is an intermediate combination of components

# Security Functional Requirements

- Audit
- Cryptographic Support
- Communications
- User Data Protection

- Identification and Authentication
- Security Management
- Privacy
- Protection of the TOE Security Functions

- Resource Utilisation
- TOE Access
- Trusted Path/Channels

5
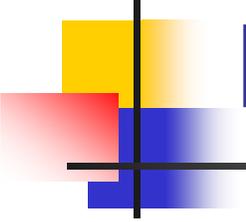
Security Assurance Requirements

- Configuration Management
- Delivery and Operation
- Development
- Guidance Documents
- Life Cycle Support
- Tests
- Vulnerability Assessment
- Assurance Maintenance

6

Evaluation Assurance Levels (EALs)
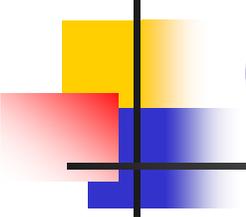
Security can be retrofitted

Security must be designed in

Impractical except for simplest systems

The seven EALs are as follows:

EAL1	-	functionally tested
EAL2	-	structurally tested
EAL3	-	methodically tested and checked
EAL4	-	methodically designed, tested and reviewed
EAL5	-	semiformally designed and tested
EAL6	-	semiformally verified design and tested
EAL7	-	formally verified design and tested

Evaluation Assurance Levels (EALs)
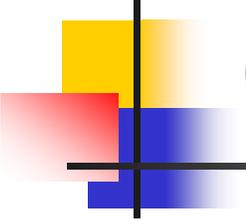
Black box evaluation
_____

Grey box evaluation

_____

White box evaluation

The seven EALs are as follows:

EAL1	-	functionally tested
EAL2	-	structurally tested
EAL3	-	methodically tested and checked
EAL4	-	methodically designed, tested and reviewed
EAL5	-	semiformally designed and tested
EAL6	-	semiformally verified design and tested
EAL7	-	formally verified design and tested

Evaluation Assurance Levels (EALs)

Common Criteria	US TCSEC	European ITSEC
EAL0	D: Minimal Protection	E0
EAL1		
EAL2	C1: Discretionary Security Protection	E1
EAL3	C2: Controlled Access Protection	E2
EAL4	B1: Labeled Security Protection	E3
EAL5	B2: Structured Protection	E4
EAL6	B3: Security Domains	E5
EAL7	A1: Verified Design	E6