Governing principles

Introduce the concept of **policy**

- It must be explicit and enforceable by a computer system
- Two kind of policies are considered DAC and MAC

Introduce the concept of **accountability**

- Users must be identified and authenticated
- Each access must be logged

TCSEC - security assurance classes (1991-2001)

Class D - minimal protection

➡ No security requirements

Class C - discretionary security protection

➡ Multi-user environment and data with different sensitivity levels

Class B - mandatory security protection

➡ Object labels, user clearance levels and multilevel security policy

Class A - verified protection

➡ Formal design and verification