

# Standards and certifications

## **How do we agree on evaluation criteria?**

- ➔ Certifications based on Standards

## **Who should run the evaluation?**

## **Who delivers the certification?**

- ➔ A certification authority (trusted third-party) called a registrar

# Outline

## **Evaluate and certify an organization**

- ISO/IEC 27000 series

## **Evaluate and certify a product or a system**

- TCSEC (“The Orange Book”) (1983-1999)  
was the American standard
- ITSEC (1991-2001)  
was the European standard
- ISO/IEC 15408 (“The Common Criteria”) (since 1998)  
is the actual international standard