



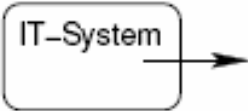
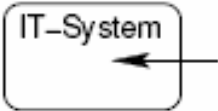
TÜV Informationstechnik GmbH

The Trust Provider

- TÜViT -

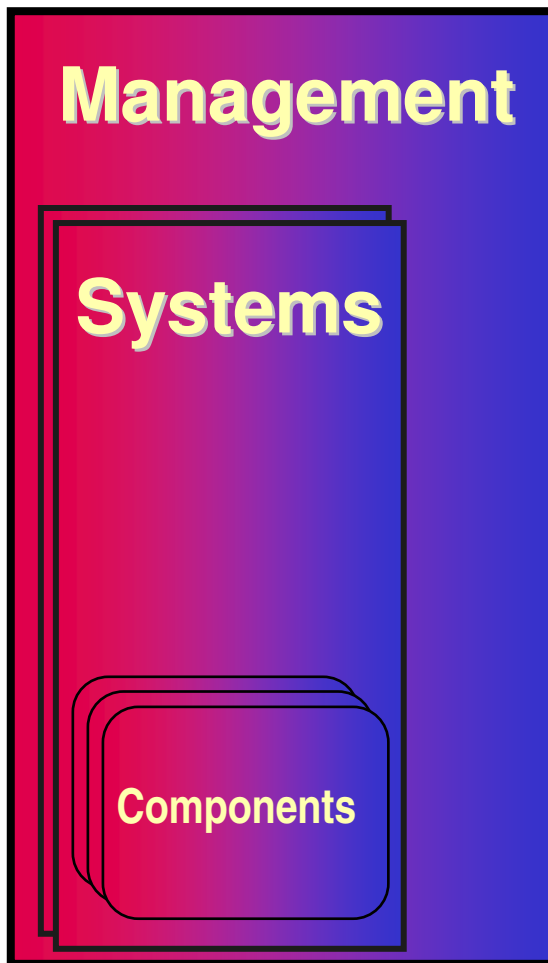
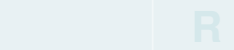


Safety and Security

Safety-critical systems	Security-critical systems
 <p>“Protect people and environment from IT-based system against accidents caused by hazards”</p>	 <p>“Protect assets (e.g. data) against threats in the environment caused by an attacker ”</p>

- Safety functionality of embedded systems often relies on stored data.
- Network connections and remote control become increasingly important.
- To achieve safety, sensitive data must be protected.

Security: Layers



Security Management

Outside Car:

Security Policy

- Security Management
- Risk Analyses
- Training

Network Security Distributed Systems Web Services

- eBilling
- Public Key Infrastructures
- Cryptography
- VPNs
- Firewall Systems

Security Products Hardware/Software

Inside Car:

- Firewall Products
- OS / Databases
- Viruses / Trojans
- digital Signatures
- Authentication Methods
- Biometrics
- Random Numbers
- Time Stamps
- Smart Cards

Security: Layers Methods



Outside Car:

ISO 27000 series

Security Management

BSI-Standards

Network Security Distributed Systems Web Services

Individual Methods
("Hacking Methods",
"Penetration Tests",
Check of Security
Concepts,..)

Inside Car:

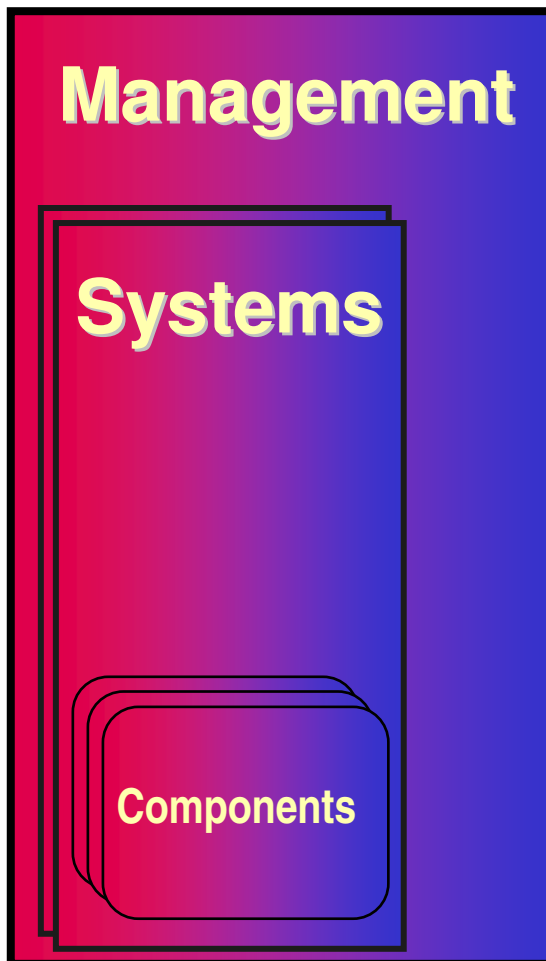
Security Products Hardware/Software

Common Criteria

ITSEC (*old Standard*)

FIPS140 (*Cryptography only*)

EMV (*Payment only*)

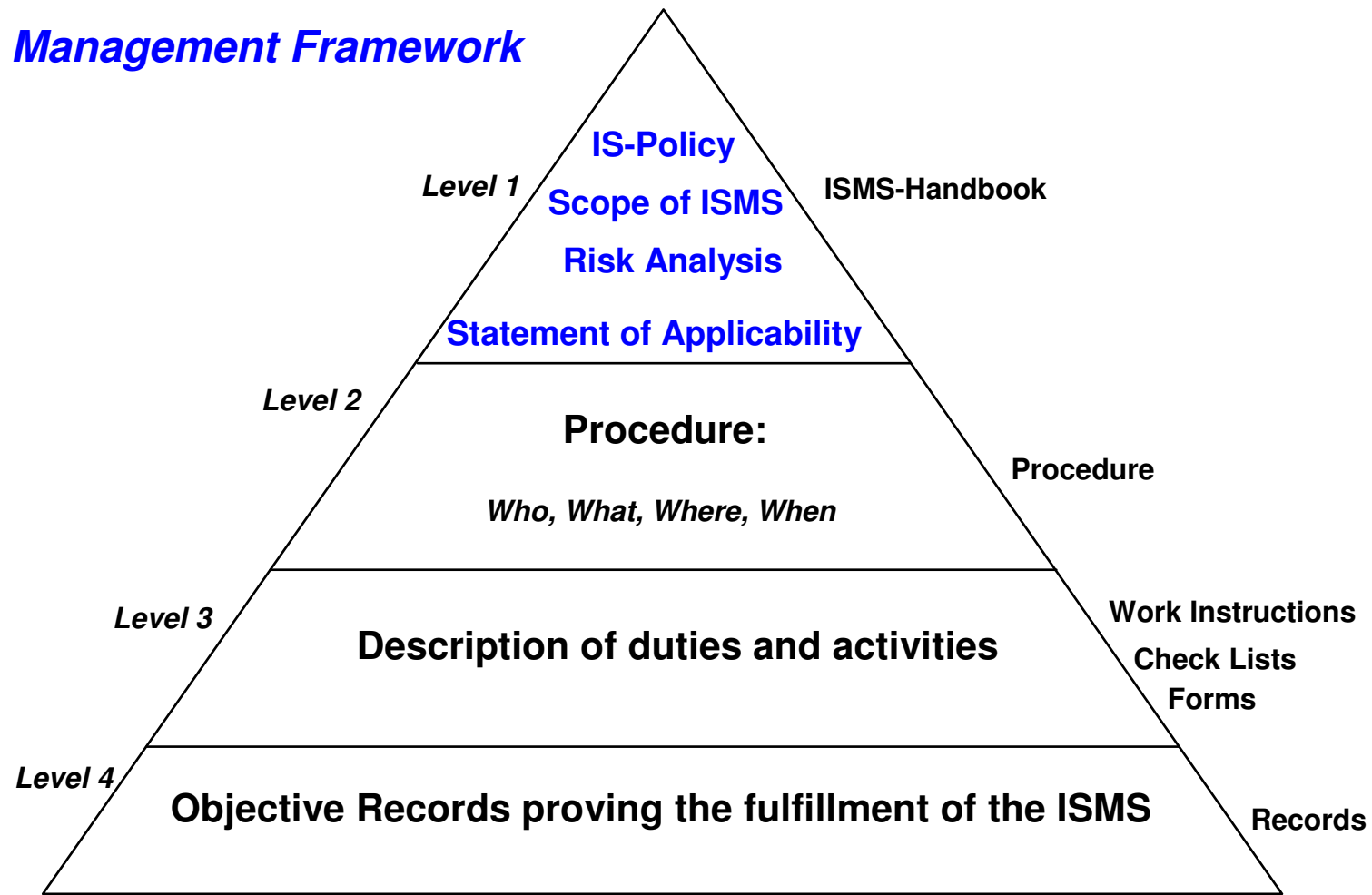


ISO 27000-series



- ISO 27000 (planned, based on ISO 13335-1): ISMS – Definition
- ISO 27001 (published, former BS 7799-2): ISMS – Requirements
- ISO 27002 (published, former ISO 17799): Guideline for ISMS
(*code of practice*)
- ISO 27003 (planned): ISMS – Implementation Guide
- ISO 27004 (planned): ISMS Measurements
- ISO 27005 (planned): Information Security Risk Management
- ISO 27006 (published): a Guide to the Certification/Registration Process
- ...

ISO 27001 – Documentation Model



ISO 27001



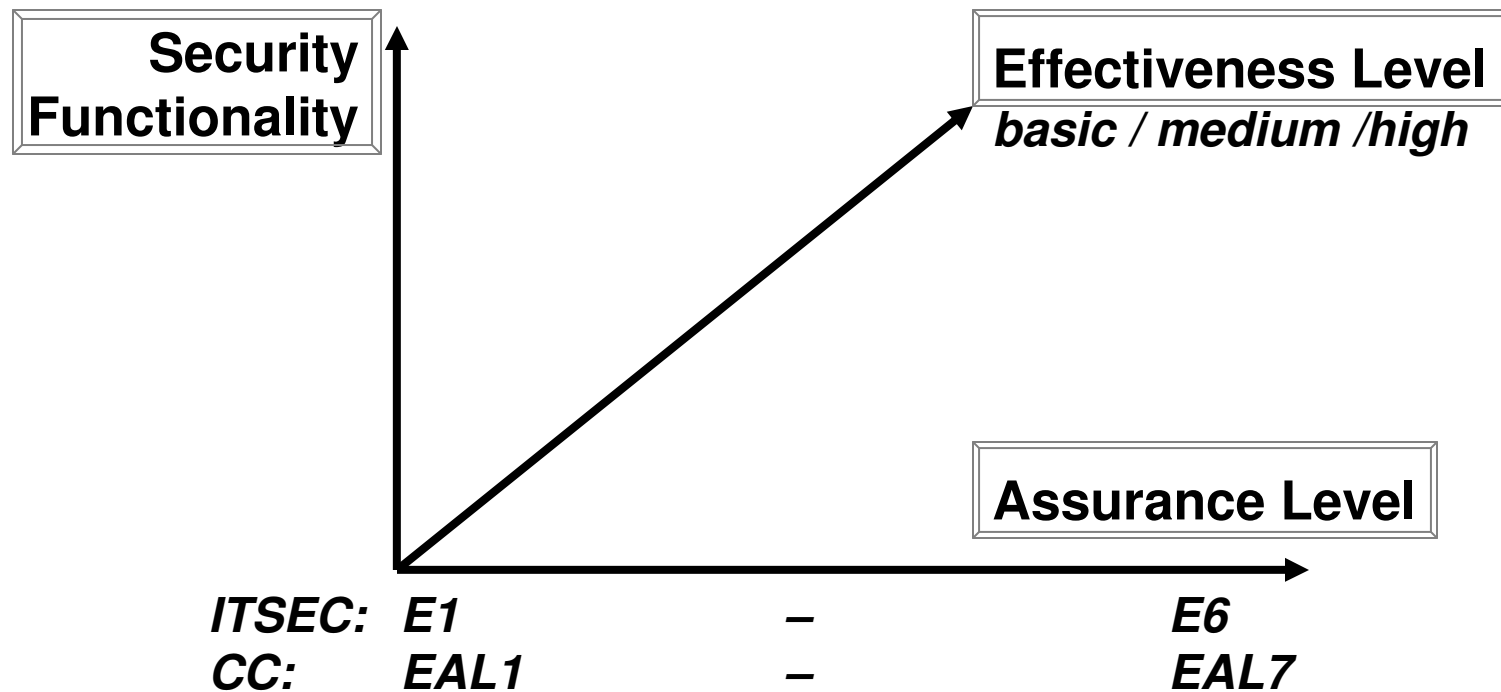
- Management Frame
- No technical Details
- Efforts to fulfill ISO 27001: >1 year
- Audit: 1 week

BSI-Standards (“IT Grundschutz”)

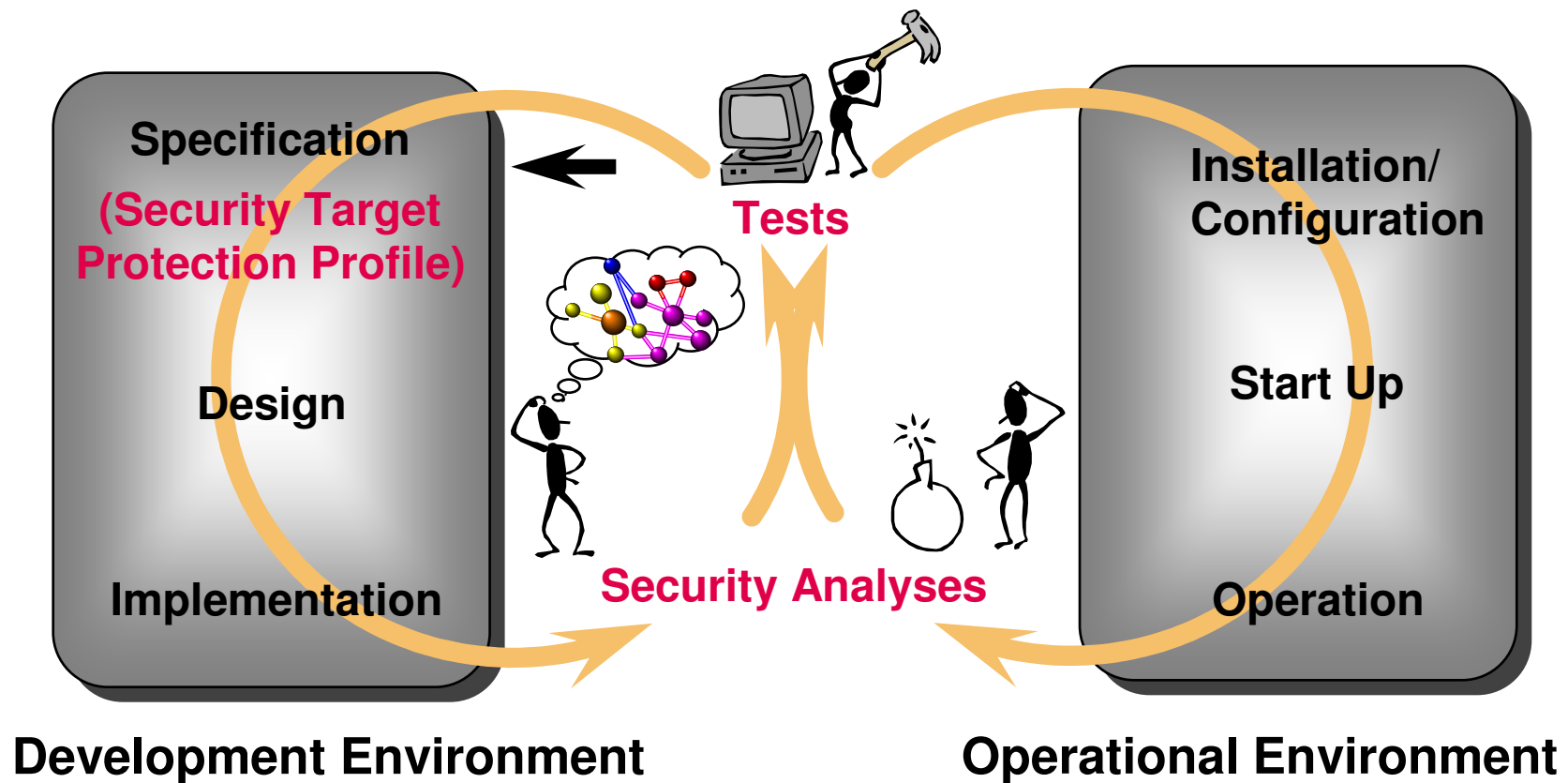


- “German Way”
- Standard IT only
 - Standard Threats
 - Standards Measures
- FOIS (BSI): Covers ISO27001
- only for medium security needs
- Efforts to fulfill IT Grundschutz: 1 year
- Audit: 1 week

Common Criteria Scaled Security



Common Criteria Evaluation Methodology



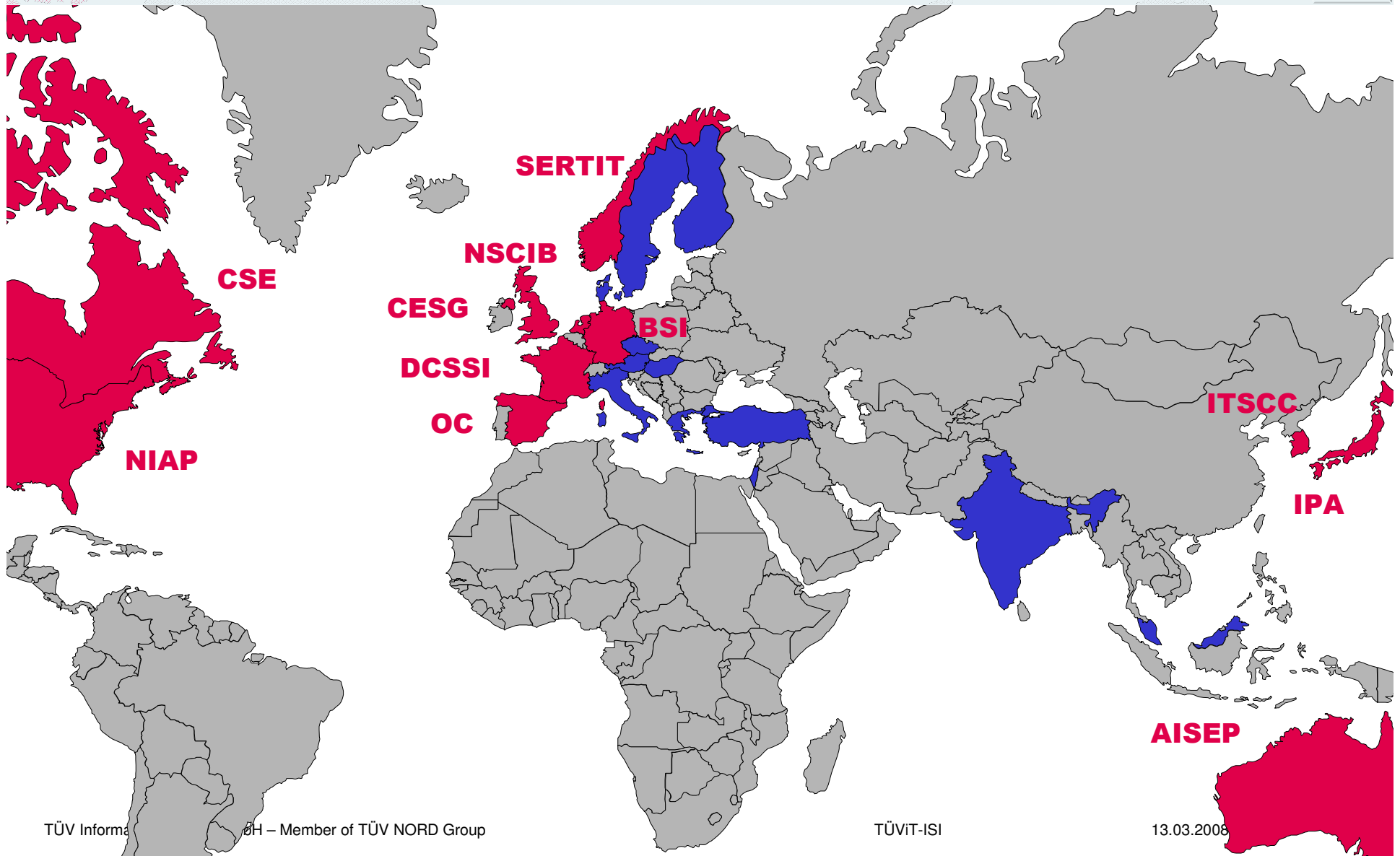
International Recognition (CC)

Certificate Issuing and Consuming Nations

Certificate Consuming Nations



R



Common Criteria



- ISO Standard (ISO 15408)
- **Internationally Accepted**
- National Schemes are already defined
- **Scalable**
 - Functionalities (any security functionality)
 - Effectiveness (*could be used for basic to very high security needs*)
 - Evaluation Assurance Level (depth of the evaluation)
- re-usable
- Efforts to fulfill CC: parallel during development depends on EAL
- Evaluation: parallel during development depends on EAL (*EAL4: 5 to 9 months*)

TÜV Informationstechnik GmbH

Member of TÜV NORD Group



Markus Bartsch

Langemarckstraße 20
45141 Essen
Germany

Telefon: +49 201 8999 – 616
Telefax: +49 201 8999 – 888
E-Mail: m.bartsch@tuvit.de
URL: www.tuvit.de