Grundzüge der Common Criteria und der Protection Profiles

Common Criteria

ISO 15408

Marcel Weinand
0228/9582-152
Marcel.Weinand@bsi.bund.de

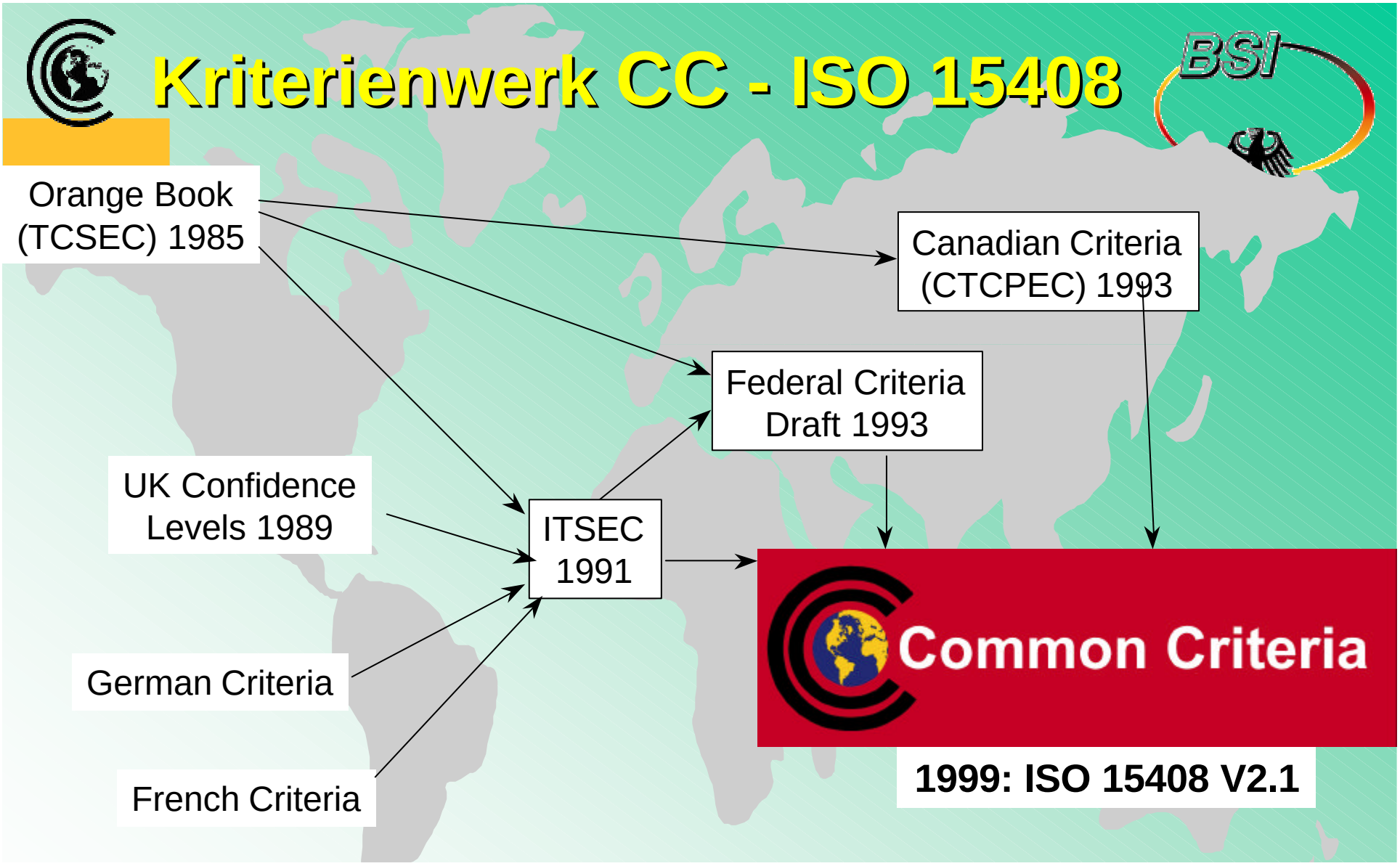
Ziele des Vortrages

Antwort auf die Frage:

Sind die Common Criteria (CC) und das Protection Profile-Konzept (PP) für mich interessant?

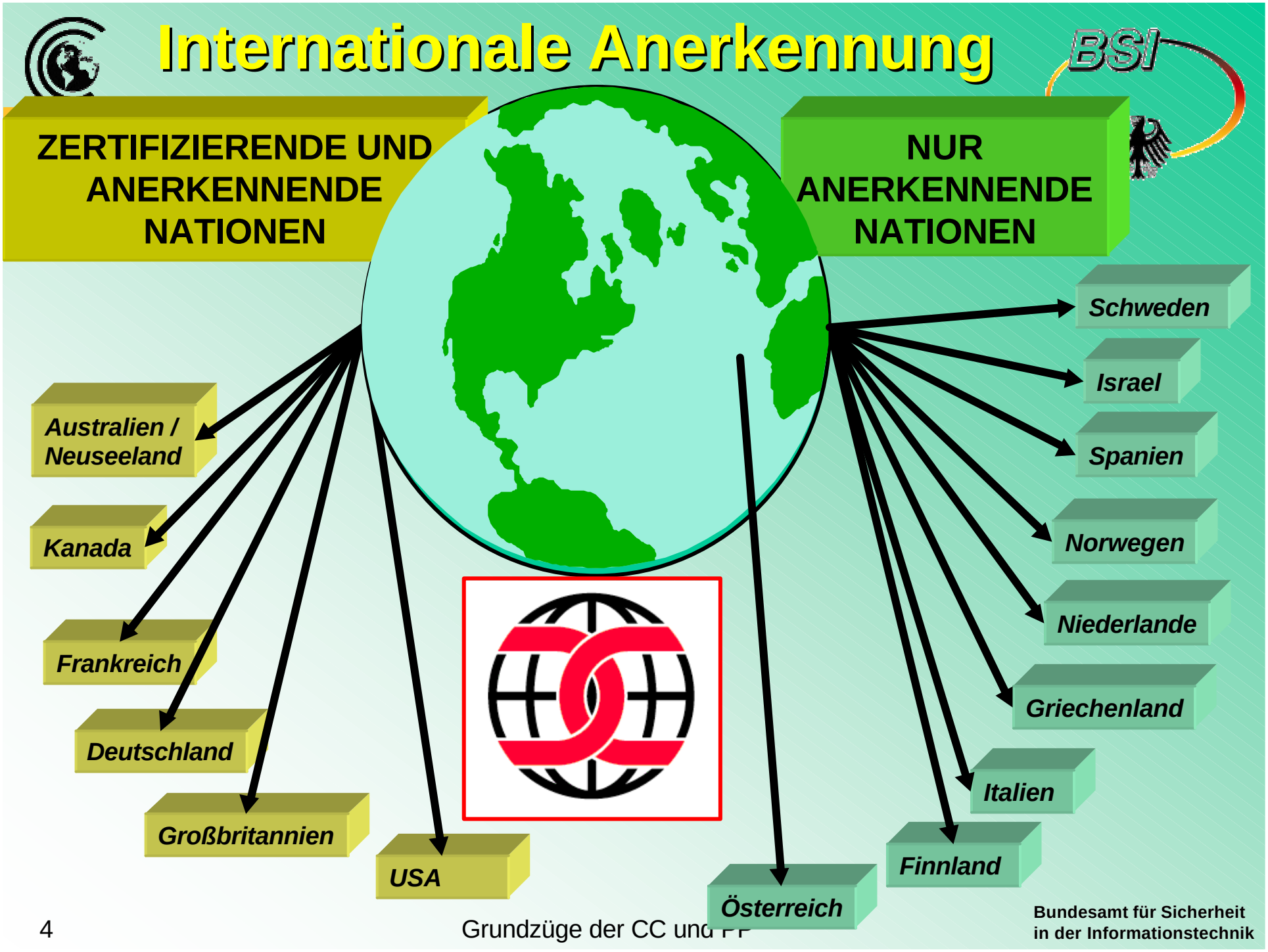
- Sie sollen wissen,
  - was sich hinter den CC verbirgt
  - welche Perspektiven das PP-Konzept anbietet

Kriterienwerk CC - ISO 15408



Common Criteria for Information Technology Security Evaluation (Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik)

Internationale Anerkennung

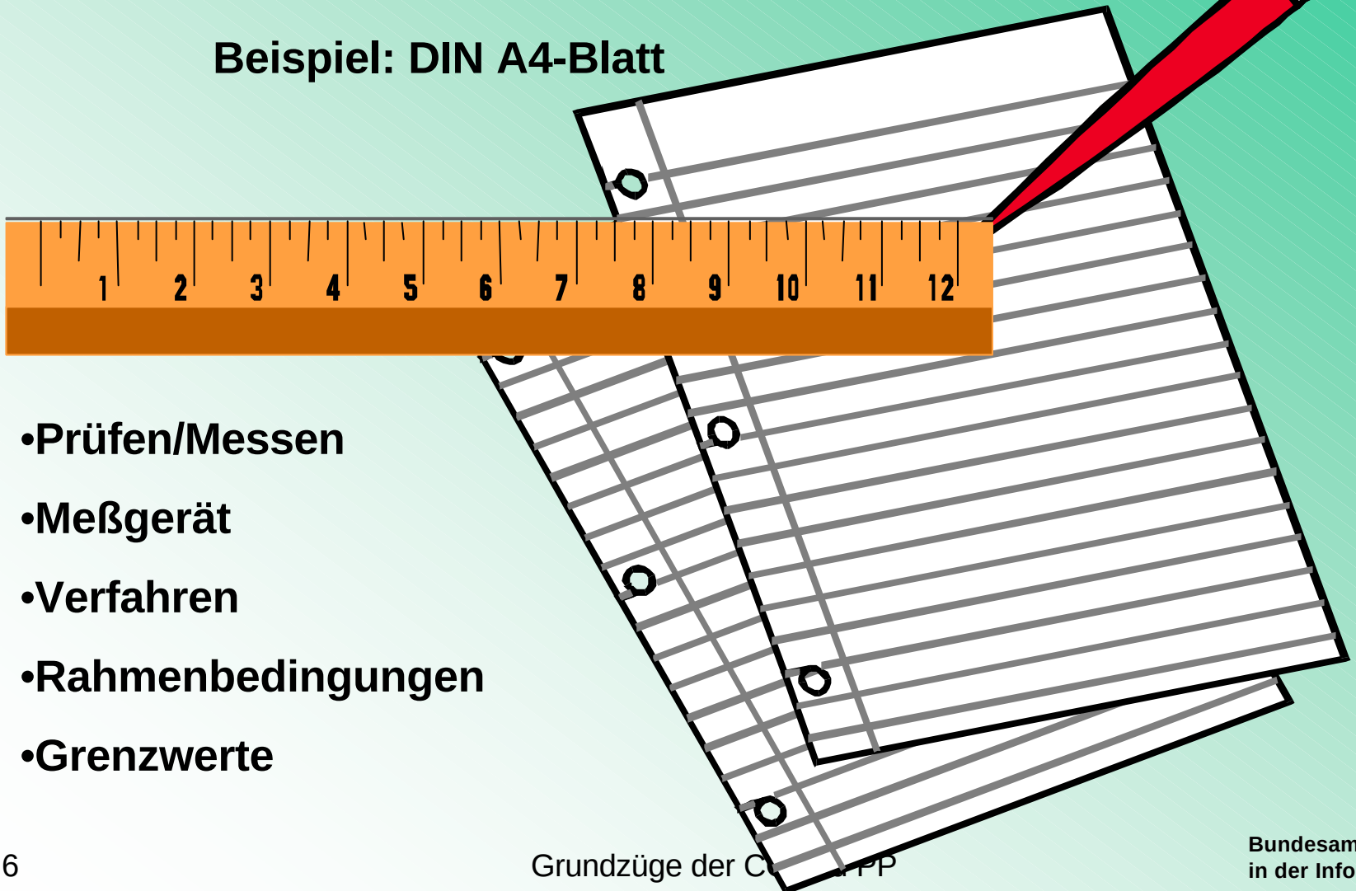


Unsere Partner -Prüfstellen

- *atsec* information security GmbH
- Competence Center Informatik GmbH *CCI*
- CSC Ploenzke AG
- Deutsches Forschungszentrum für künstliche Intelligenz GmbH *DFKI*
- Industrieanlagen-Betriebsgesellschaft mbH *IABG*
- Security Research & Consulting GmbH *SRC*
- Tele Consulting GmbH *TC*
- TNO-ITSEF BV
- T-Systems ISS GmbH
- TÜV Informationstechnik GmbH *TÜVIT*
- Wehrtechnische Dienststelle WTD 81
- BSI

Die Maßnahme

Beispiel: DIN A4-Blatt



- **Prüfen/Messen**
- **Meßgerät**
- **Verfahren**
- **Rahmenbedingungen**
- **Grenzwerte**

Was ist Vertrauen in die IT-Sicherheitsleistung?

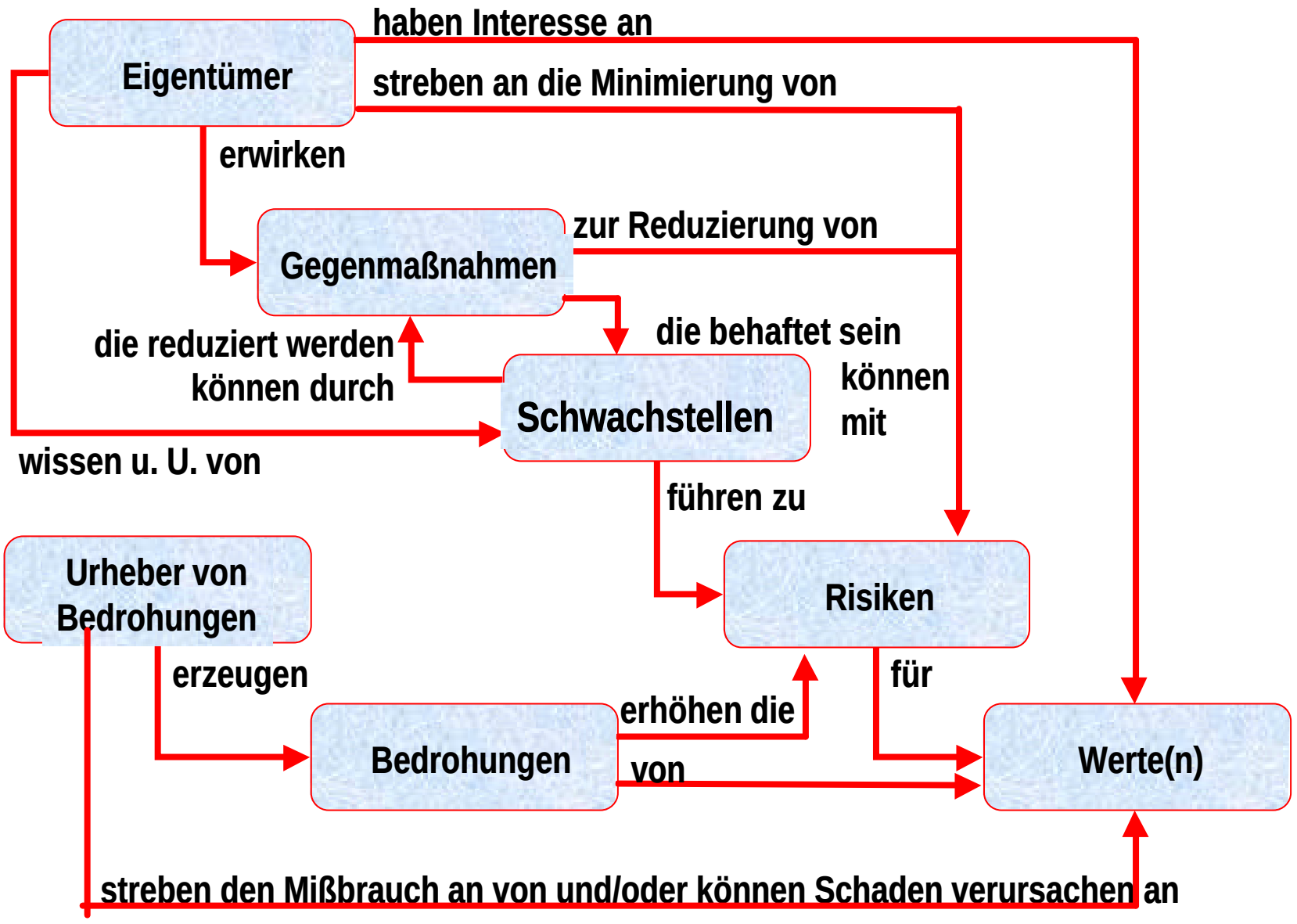
CC Definition für Vertrauen:

Begründete Überzeugung, daß der EVG seine Sicherheitsleistung erbringt.

EVG: *Evaluationsgegenstand*

TOE: *Target of Evaluation*

Ziel der CC: Vertrauen in die Wirksamkeit der IT-Sicherheitsfunktionen



Prinzipien der Kriterien

Das Vertrauen in ein Produkt steigt mit

- zunehmendem Prüfaufwand
- zunehmender Kenntnis des Produktes
- der Exaktheit der Prüfmethode

Die CC bieten:

- verschiedene Prüftiefen mit abgestuftem Prüfaufwand
- Dokumentationsanforderungen steigen mit der Prüftiefe
- steigende Anforderungen an steigende Prüfmethoden

CC Teil3 - Anforderungen an die Vertrauenswürdigkeit

Vertrauen durch

Evaluation, Tests und Schwachstellenanalysen

Klasse	Name
ACM	Konfigurationsmanagement
ADO	Delivery & Operation
ADV	Entwicklung
AGD	Handbücher
ALC	Life Cycle Support
ATE	Tests
AVA	Schwachstellenbewertung
APE	Protection Profile Evaluation
ASE	Security Target Evaluation
AMA	Maintenance of Assurance

Beispiel: die Klasse *Entwicklung*

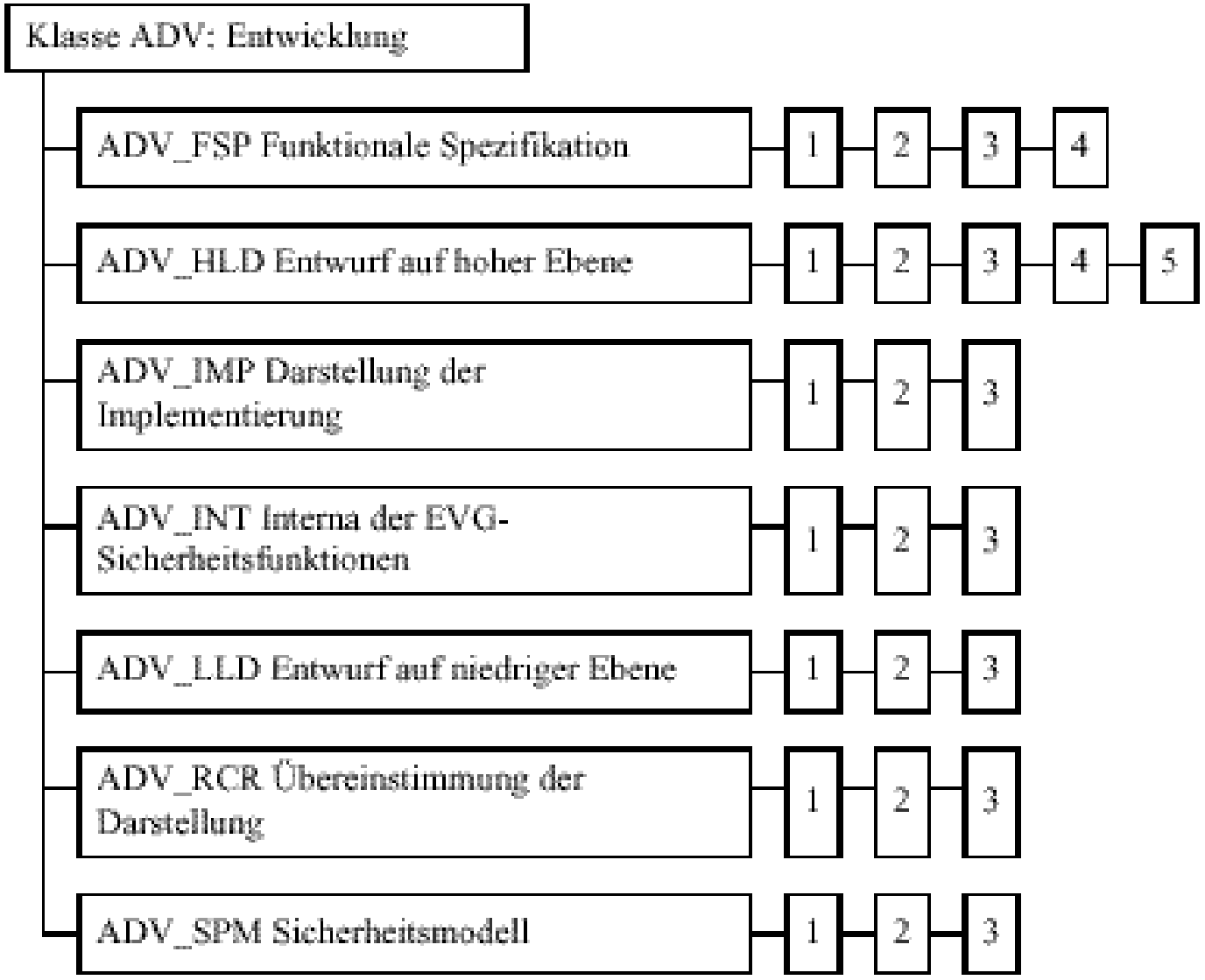
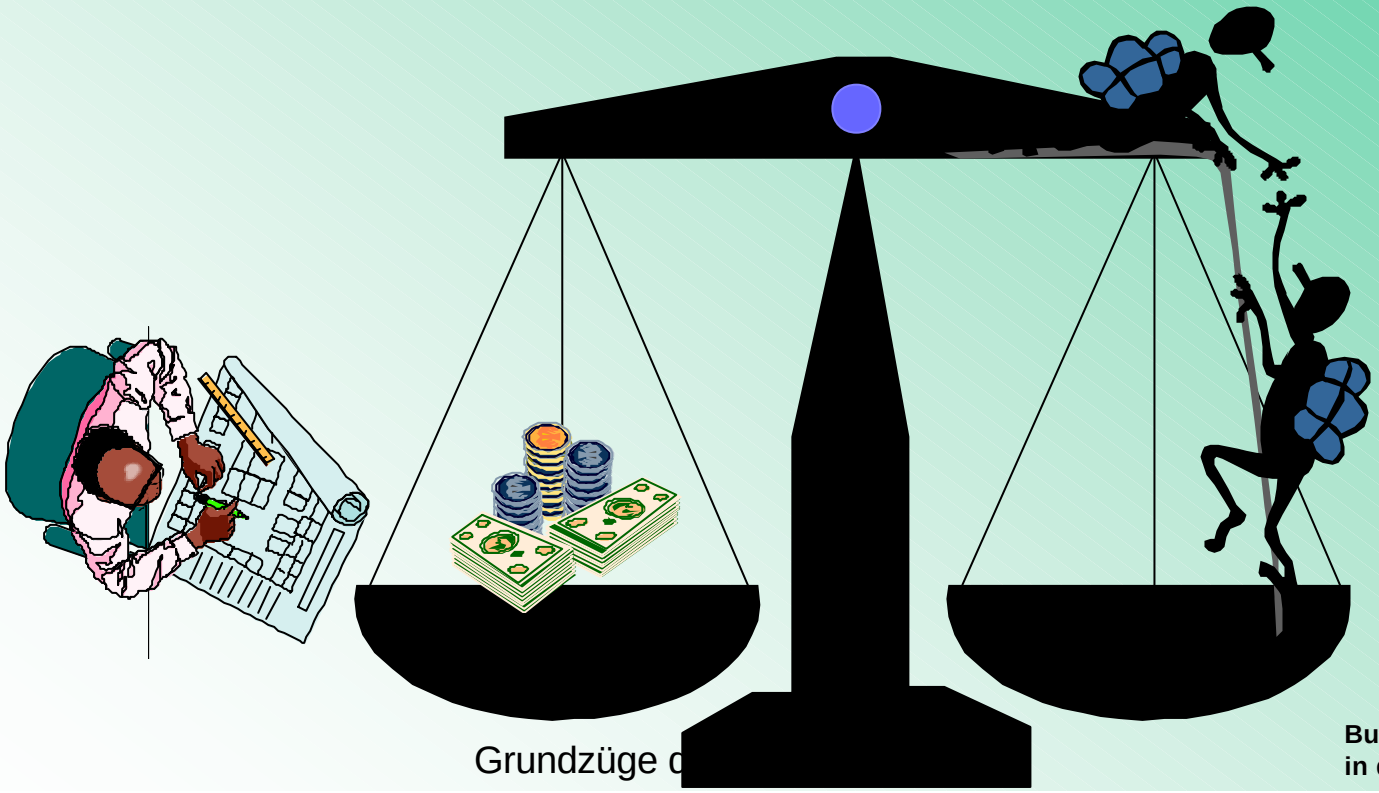


Bild 10.1 - Unterteilung der Klasse Entwicklung

Vertrauenswürdigkeitsstufen (EALs)

- Ermöglichen eine Skalierung der Vertrauenswürdigkeit
- Die Skalierung berücksichtigt die Ausgewogenheit der Vertrauensstufe mit dem Kosten- und Arbeitsaufwand



Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4
Assurance maintenance	AMA_AMP							
	AMA_CAT							
	AMA_EVD							
	AMA_SIA							

ADO_IGS.2

ADV_LLD.2

AVA_CCA.3

Bedeutung eines Schutzprofils

- Zertifizierte Schutzprofile werden national registriert und international anerkannt
- internationale Registrierung durch ISO in Vorbereitung
- Schutzprofile haben den Charakter einer *Norm* oder eines *normativen Dokuments*
- Hersteller können die Anforderungen der Schutzprofile erfüllen
  - Nachweis durch Zertifikat möglich
  - Nachweis beinhaltet Vollständigkeit, Korrektheit, Schwachstellenanalyse gemäß EAL-Stufe

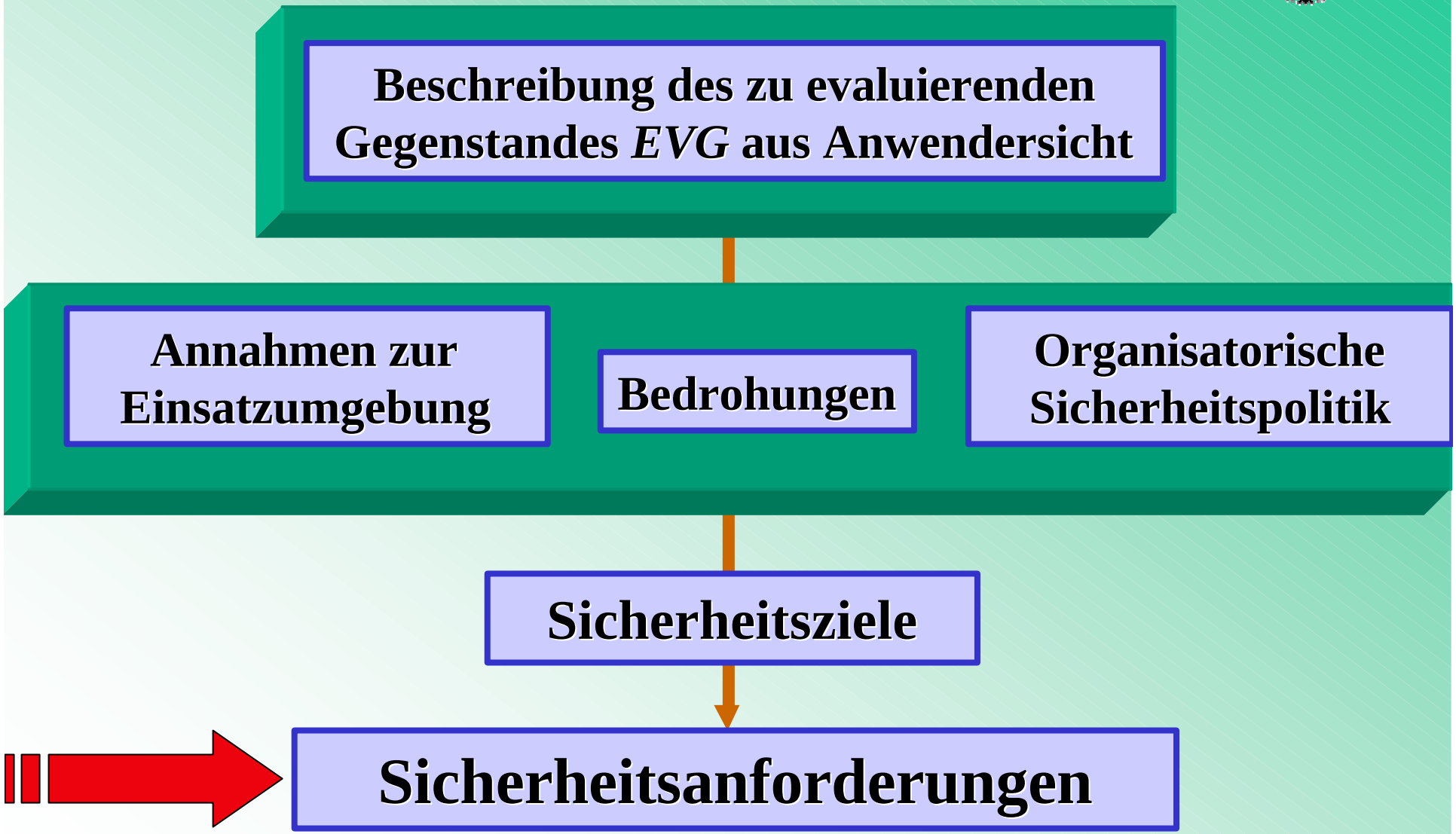
Merkmale von Protection Profiles

- PP basiert auf einem Sicherheitsbedarf (Konzept)
  - Enthält Beschreibung der angenommen Einsatzumgebung sowie die vorgesehene Nutzung
- PP deckt alle genannten Sicherheitsziele **vollständig** ab durch kompletten Satz von
  - Anforderungen an die IT-Sicherheits-Funktionalität
  - Anforderungen an die Vertrauenswürdigkeit
- Verwendbar für unterschiedliche Realisierungen
  - Abstraktionsgrad ist unabhängig von der Implementierung
  - hohe Flexibilität durch Platzhalter und Operationen

Wer benötigt Schutzprofile?

- IT-Benutzer - jeder, der Sicherheitsbedarf hat, z.B. kommerzielle Anwender, Anwendergruppen:
  - Unter der Fragestellung: “Was will ich haben oder was benötige ich!” (Vergleichbar mit Pflichtenheft)
- IT-Hersteller - für Produktklassen
  - Hersteller definieren damit IT-Sicherheitsstandards für Produktklassen
- PP ist Produktklassen-orientiert (EVG-Klasse)

Vordefiniertes Sicherheitskonzept als Bestandteil des PP



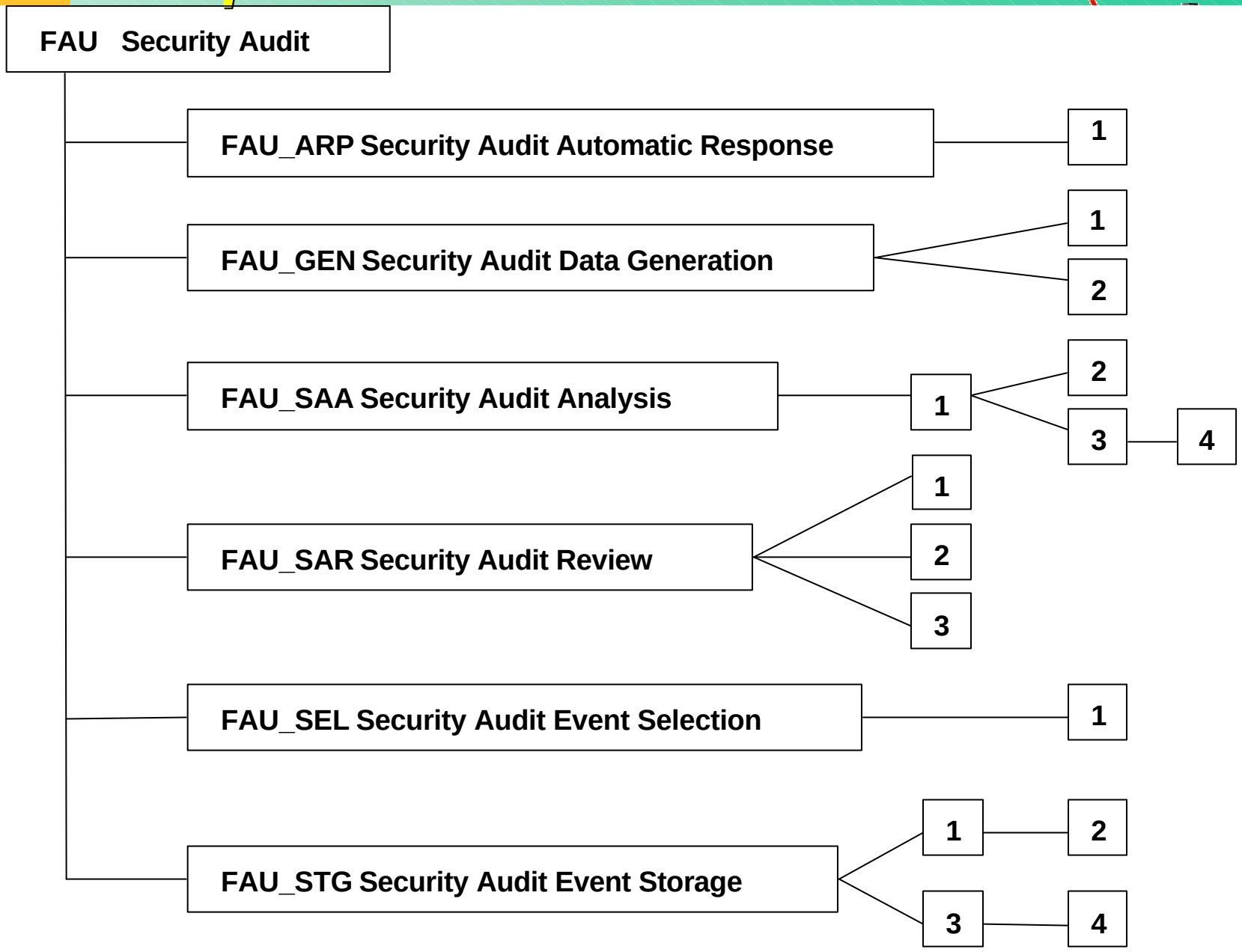
Die IT-Sicherheitsanforderungen

....schweben über den die IT-Sicherheit realisierenden Funktionen des EVG; ihr Verhalten ist kontrollierbar.

Überblick Teil 2
Die funktionalen Sicherheitsklassen

Klasse	Name
FAU	Audit
FCO	Communications
FCS	Cryptographic Support
FDP	User Data Protection
FIA	Identification & Authentication
FMT	Security Management
FPR	Privacy
FPT	Protection of TOE Security Functions
FRU	Resource Utilization
FTA	TOE Access
FTP	Trusted Path / Channels

Beispiel - Klasse FAU



CC Teil 2: Funktionaler Anforderungskatalog

- Umfassender Katalog von funktionalen Sicherheitsanforderungen, (Stand 1998)
- klare Strukturen mit hoher Flexibilität
- vollständige Liste aller Komponentenabhängigkeiten
- hohe Flexibilität durch Komponentenoperationen
- alle möglichen Administrationsfolgen sind aufgezeigt
- alle Protokollierungsmöglichkeiten sind hierarchisch dargestellt
- flexibel erweiterbar

Beispiel einer PP-Spezifikation aus Benutzersicht: Das BISS-Schutzprofil

- Einfache, robuste und gleichartige Administrationsoberfläche verschiedener Sicherheitstechniken
- Transparente Umsetzung der IT-Sicherheit⇨regelbasiert
- Betriebssystemunabhängigkeit
- Keine Beeinträchtigung vorhandener Systeme
  - Gleiches IT-Verhalten
  - keine Inkompatibilitäten mit Anwendungsprogrammen
- Externer Wartungstechniker
- Flexibilität bei Einführung
- Aufrechthaltung der Sicherheit eines Informationsflusses über unterschiedliche Sicherheitstechniken
- Zweckbindung (Workflowunterstützung)

Zusammenfassung: Das Protection Profile

- Internationale Anerkennung
- Registrierung demnächst durch ISO
- Darstellung der benötigten Sicherheitsanforderungen von IT-Benutzer, z.B. kommerzielle Anwender, Anwendergruppen
  - Unter der Fragestellung: “Was will ich haben oder was benötige ich!” (Vergleichbar mit Pflichtenheft)
- IT-Hersteller definieren IT-Sicherheitsstandards für Produktklassen
- Vergleichbarkeit der Ergebnisse von Prüfungen und Bewertungen der Sicherheit.
- PP ist verwendbar für unterschiedliche Realisierungen

Zusammenfassung: Die Common Criteria...

- sind ein Kriterienwerk zur Prüfung und Bewertung der IT-Sicherheit
- beinhalten 2 Kataloge mit CC-Komponenten zur Spezifikation
  - von Sicherheitsanforderungen für die Vertraulichkeit
  - von Sicherheitsanforderungen für die Sicherheitsfunktionalität
- bieten Strukturen und Konzepte als Hilfestellung
  - zur Erstellung angemessener Sicherheitsanforderungen
  - zur Erstellung vollständiger Sicherheitsanforderungen
  - zur Anpassung der CC-Komponenten an den individuellen Bedarf durch definierte Operationen und Ergänzungsmöglichkeiten
- sind international akzeptiert

Wo sind weitere Informationen erhältlich?

- WEB-Seiten:
  - **http://www.bsi.bund.de**
  - **http://www.commoncriteria.org**
  - **http://csrc.nist.gov/cc/pp/pplist.htm**
- Konferenzen
  - 4. Internationale Common Criteria Conference ICCC vom 07-09. Sept., Stockholm **http://www.iccconference.com**
  - BSI-Kongress (alle 2 Jahre) 13.-15. Mai 2003 in Bonn
- Schulungen
  - verschiedene CC-Schulungen nach Absprache mit dem BSI

Marcel.Weinand@bsi.bund.de
Markus.Mackenbrock@bsi.bund.de