

# Trusted Site Privacy

Zertifizierung des technisch gestützten  
Identity Managements

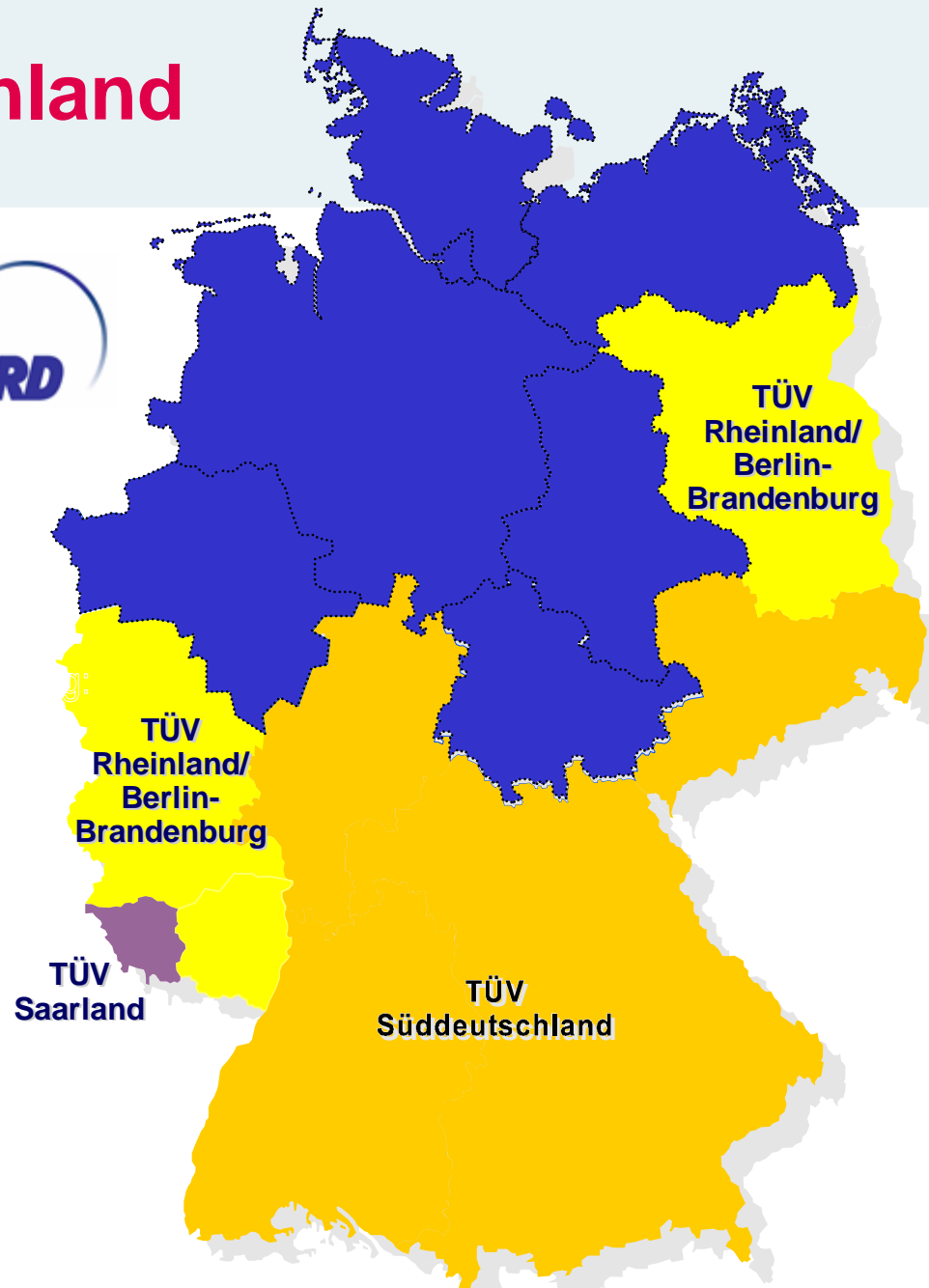
**TÜV Informationstechnik GmbH**

**The Trust Provider**

**- TÜViT -**



# TÜV's in Deutschland





∅ TÜViT – der Informatik-TÜV arbeitet

∅ neutral

∅ objektiv und

∅ unabhängig von

∅ Herstellern

∅ Distributoren

∅ Produktentwicklern

∅ Anwendern

∅ Aktionären/Mitgliedern

∅ Interessensgruppen

∅ Branchen

∅ Regierung

∅ TÜViT ist ein privat-wirtschaftliches Unternehmen, das weder Produkte entwickelt noch verkauft.

- ∅ Risikoreduzierung
- ∅ Qualitätsverbesserung von Produkten, Systemen und Prozessen

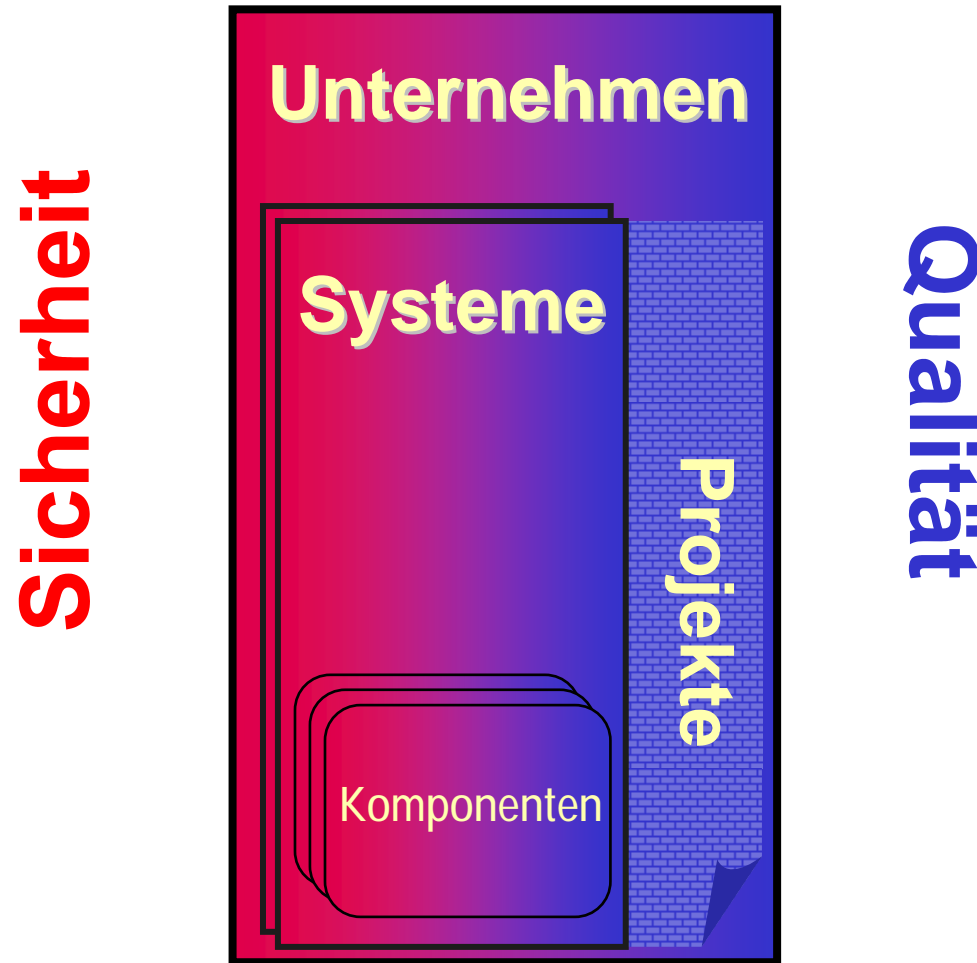


durch

- ∅ Sicherheit  
und
- ∅ Qualität

in der **Informationstechnik** und **Telekommunikation**

# Zertifizierung





## IT-Sicherheit

quid!  
ISO 17799 / BS7799-2  
GSM SAS / TU.4  
IT-Grundschutz

## IT-Qualität

ISO 9000  
ITIL

### Trusted Site

- Infrastructure
- Security
- Privacy
- Usability
- Quality

Abnahme ZDA gemäß SigG

PK-DML

CMMI

SPICE

V-Modell

RUP

ULD

IEEE 1233

Common Criteria / ITSEC

ISO 12119

FIPS 140

ISO 9241

ZKA-Kriterien

Hardware Labor

# TÜViT - Zertifizierungsstelle

## Alleinstellungsmerkmale

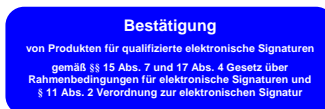


- ∅ Akkreditierungen nach ISO Guide 65 /DIN EN 45011 für ITSEC/CC -> weltweit einzigartig
- ∅ Nr. 1 in D für Bestätigungen nach Signaturgesetz für Produkte und Zertifizierungsdiensteanbieter >80 % Marktanteil in D
- ∅ Nr. 2 in D nach Bundesamt für Sicherheit in der Informationstechnik (BSI) für Zertifizierungen nach ITSEC/CC >40 % Marktanteil in D
- ∅ Eigene Zertifizierungsschemata „Trusted Site/Product“ für weitere nicht standardisierte Sicherheitskriterien PK-DML, SQ, TSI, etc.

# Zertifizierungsgebiete (Schwerpunkte)



**Deutsches IT-Sicherheitszertifikat (ITSEC/CC)**  
anerkannt durch das BSI



**Bestätigung nach Signaturgesetz (SigG/SigV)**  
anerkannt durch die BNetzA



Voluntary Validation

© 2003 TÜViT GmbH - ein Unternehmen der RWTÜV-Gruppe -

**TÜViT Trusted Product** – Zertifizierung von vertrauenswürdigen Produkten, z. B. :  
- Trusted Product Usability

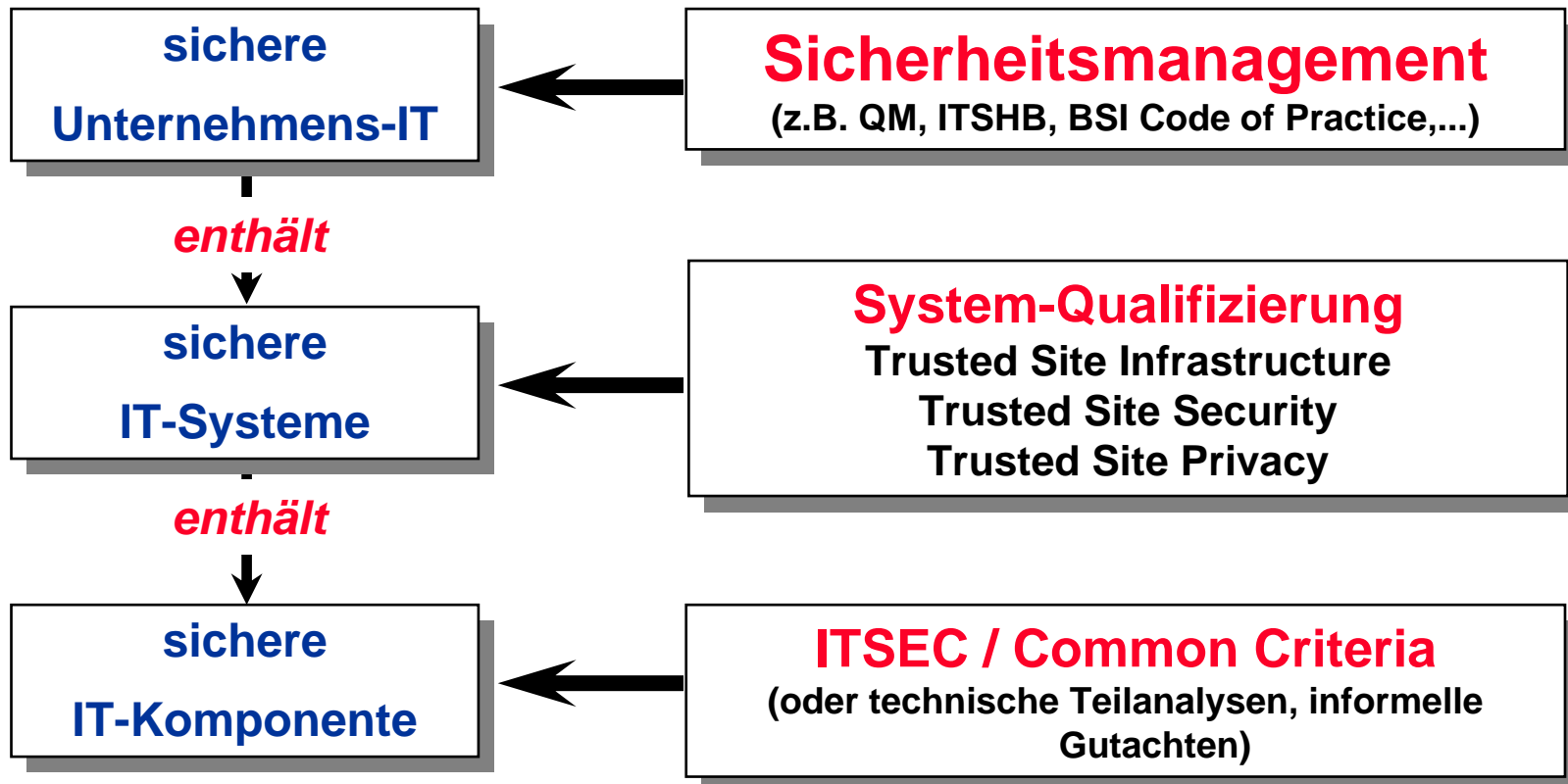


Voluntary Validation

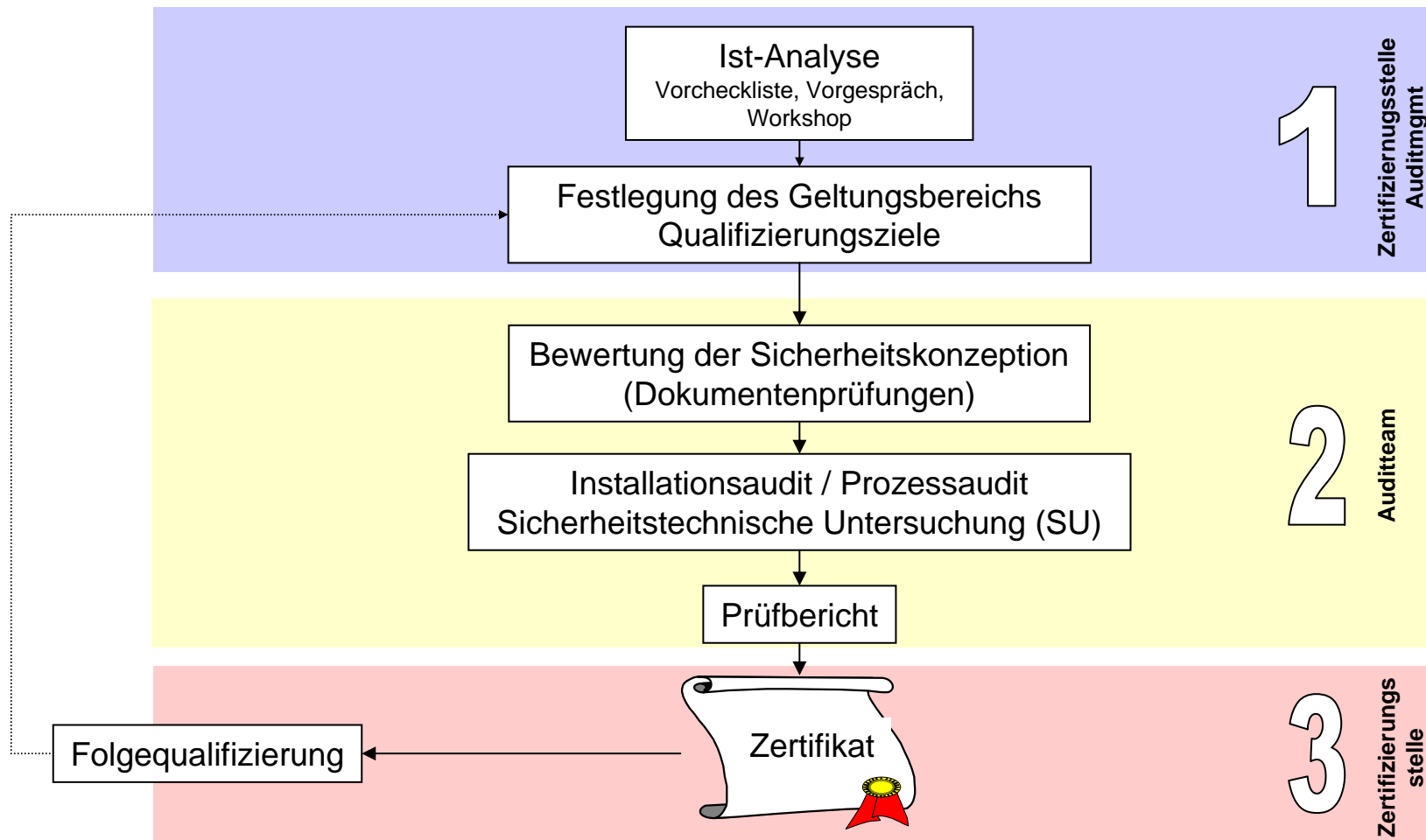
© 2003 TÜViT GmbH - ein Unternehmen der RWTÜV-Gruppe -

**TÜViT Trusted Site** – Zertifizierung von vertrauenswürdigen Installationen, z. B. :  
- Trusted Site Infrastructure  
- Trusted Site Privacy  
- Trusted Site Security

# Trusted Site - Positionierung



# Das Trusted Site - Zertifizierungsschema



## Identity

- ∅ Personenrepräsentanz (auch Objektrepräsentanz)
- ∅ Personenbeschreibende und personenbezogene Daten
- ∅ Persönliche Rechte und Rollen

## Management

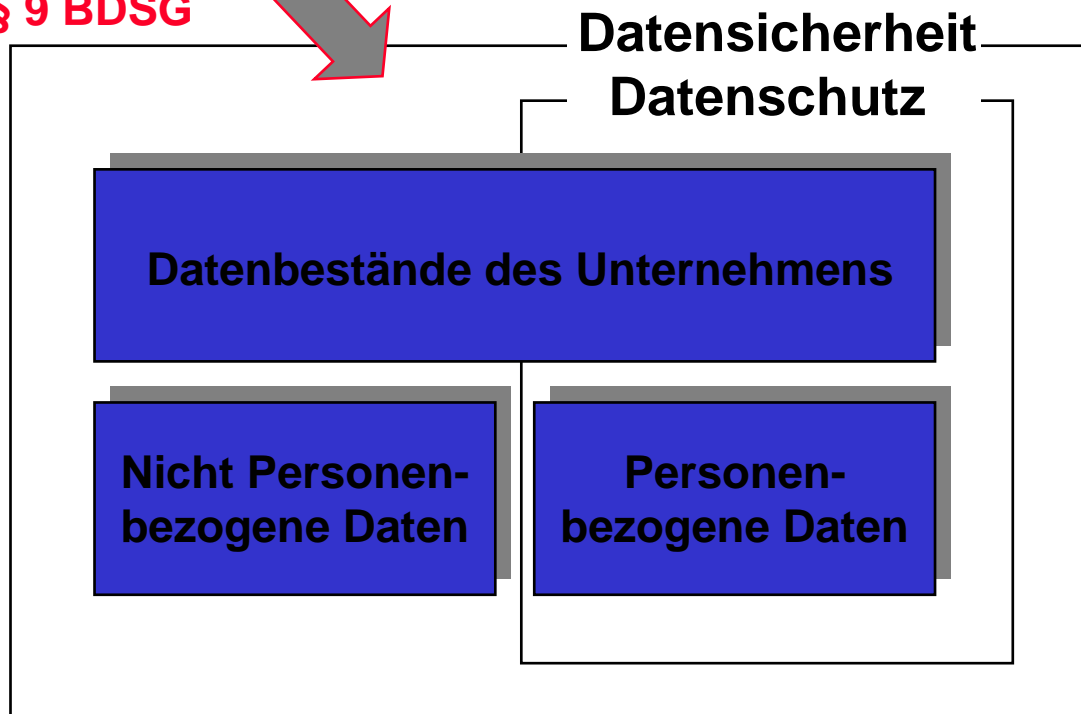
- ∅ Verwaltung der Identity-Daten
- ∅ Auswertung von Identity-Daten
  
- ∅ Verwaltung von Rollen und Berechtigungen
  
- ∅ Verknüpfung von Personen und Objekten durch Rollen- und Berechtigungszuweisungen
- ∅ Zugriffsprotokollierung und -auswertung

# Datenschutz und Datensicherheit

## Einordnung



Kontrollen  
gemäß Anlage  
zu § 9 BDSG



Bei personenbezogene Daten handelt es sich um Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbarer Person (§ 3 Abs. 1 BDSG). Diese Person wird als **Betroffener** bezeichnet.

# Datenschutz und Datensicherheit

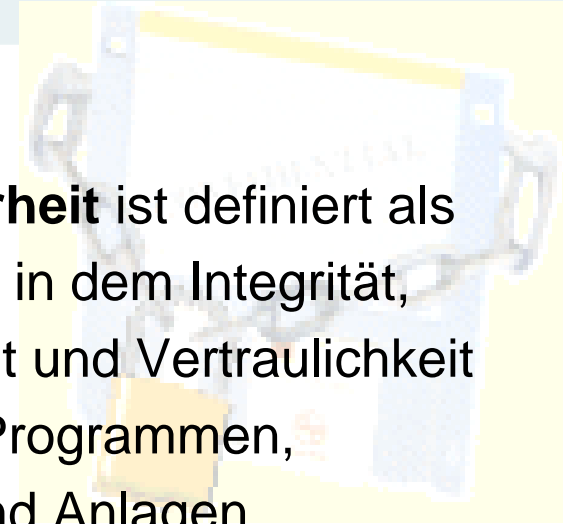
## Definition



**Datenschutz** ist definiert als alle Maßnahmen, deren Ziel es ist, das Individuum (Betroffener) vor der missbräuchlichen (z. B. rechtswidrigen, zweckfremden) Verwendung der über seine Person gespeicherten Informationen (Daten) zu schützen.

**Datensicherheit** ist definiert als der Zustand, in dem Integrität, Verfügbarkeit und Vertraulichkeit von Daten, Programmen, Verfahren und Anlagen gewährleistet wird.

**Datensicherung** meint alle Verfahren, die dazu dienen, den Zustand der Datensicherheit zu erreichen.



- Ø **Es sind technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um den gesetzlich vorgeschriebenen Datenschutz und das Persönlichkeitsrecht auf informationelle Selbstbestimmung zu gewährleisten.**
  
- Ø **Maßnahmen:**  
**Anlage zu § 9 BDSG**
  - Ø **Zugangskontrolle, Benutzerkontrolle, Eingabekontrolle, Organisationskontrolle, Datenträgerkontrolle, Zugriffskontrolle, Auftragskontrolle, Speicherkontrolle, Übermittlungskontrolle, Transportkontrolle.**

- ∅ Die Einhaltung von Datensicherheit und Datenschutz haben große Bedeutung. Für zahlreiche Gefährdungen gibt es physikalische und logische Sicherungsmechanismen, deren Implementierung und Funktionsfähigkeit in der konkreten Installation umfassend zu prüfen sind.
- ∅ Personenbezogene und betriebliche Daten sind gegen unbefugten Zugriff zu sichern; die Funktionsfähigkeit des Gesamtsystems hängt von der Integrität und Konsistenz des Datenbestandes ab.
- ∅ Insbesondere wird die Installation geprüft hinsichtlich:
  - ∅ Datenvermeidung
  - ∅ Datensparsamkeit
  - ∅ Datensicherheit der Datenverarbeitung
  - ∅ Revisionsfähigkeit der Datenverarbeitung
  - ∅ Gewährleistung der Rechte des Betroffenen

# Bewertungsaspekte



Sicherheitsanforderungen	1. Technische Sicherheitsanforderungen und Vorgaben aus dem Einsatz- und Rechtskontext
Dokumentation	2. Dokumentation der IT-Installation 3. Benutzer-, Administrations- und sonstige Betriebsdokumente
Technische Tests	4. Sicherheit der verwendeten Komponenten 5. Mittel des Systemmanagements 6. Tests und Inspektionen
Organisation	7. Änderungsmanagement 8. Operationelle Anforderungen
Sicherheitsanalysen	9. Sicherheitsanalysen gegen Sicherheitsanforderungen

Die Sicherheitsanforderungen/Datenschutzanforderungen, die der Betreiber durch seine IT-Installation realisiert haben möchte, werden konkretisiert und aufgenommen.

Diese müssen widerspruchsfrei sein und geltenden Sicherheitsstandards sowie den zu beachtenden gesetzlichen Anforderungen genügen.

Im Rahmen der SU wird nachfolgend geprüft, ob diese Sicherheitsanforderungen ohne Einschränkung erfüllt sind bzw. diese durch entsprechende Funktionalitäten fehlerfrei abgedeckt werden, so dass jegliche Restrisiken minimiert sind.

# Berücksichtigte Aspekte bei der Prozesszertifizierung



- ∅ Dem datenverarbeitende Prozess ist ein Verfahrensbeschreibung mitzugeben, in dem der Prozess, das Konzept, das Verfahren (Zweck) sowie auch die datenschutzgerechten Einsatzbedingungen und gegebenenfalls Ausschlussbereiche transparent gemacht werden.
- ∅ Technik, Organisations- und Produktbeschreibung müssen nutzeradäquat ausgestaltet sein.



# Berücksichtigte Aspekte bei der Prozesszertifizierung



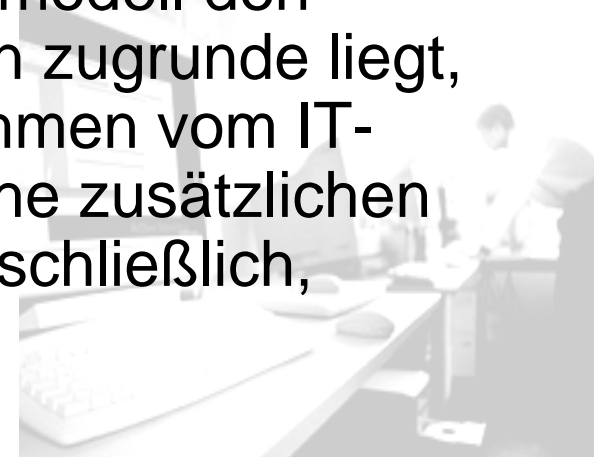
- ∅ Der datenverarbeitende Prozess darf nicht gegen datenschutzrechtliche Bestimmungen verstoßen.
- ∅ Der datenverarbeitende Prozess sollte Datenschutz- und Datensicherheitsziele durch Technikgestaltung sicherstellen.
- ∅ Verbleibende notwendige organisatorische Maßnahmen müssen verständlich beschrieben und mit angemessenem Aufwand umsetzbar sein.



# Technisch-organisatorische Maßnahmen - Begleitmaß. zum Schutz der Betroffenen



- ∅ Für Datenschutzanforderungen werden (technische) Maßnahmen diskutiert, die zur Umsetzung dieser Anforderungen führen können. Dabei wird auch der Grad der technischen Umsetzung dieser Maßnahmen durch das Produkt problematisiert und ob das Produkt selbst sicherheitszertifiziert ist. Beachtet werden muss bei der Bewertung, welches Angreifermodell den getroffenen/zu treffenden Maßnahmen zugrunde liegt, gegen welche Angriffe Schutzmaßnahmen vom IT-Produkt selbst vorgesehen sind, welche zusätzlichen Maßnahmen unterstützt werden, und schließlich, welche Restrisiken verbleiben.



## Ø Sicherheit der verwendeten Komponenten

Für alle Komponenten und Subsysteme der Zerlegung sind funktionale Spezifikationen erkennbar. Darlegungen der externen Schnittstellen der Installation liegen vor. Die Sicherheitsanforderungen von sicherheitsspezifischen Subsystemen sind erkennbar. Für wesentliche sicherheitsspezifische Subsysteme liegen Darlegungen der Sicherheitsanforderungen vor.

## Ø Mittel des Systemmanagements

Handbücher zur IT-Installation sowie zu den sicherheitsspezifischen und kritischen Subsystemen liegen vor.

## Ø Tests und Inspektionen

Im Rahmen von umfangreichen Penetrationstests und Konfigurationsanalysen werden Schwachstellen der IT-Installation festgestellt und bewertet.



Voluntary Validation

© 2005 TÜViT GmbH - ein Unternehmen der TÜV NORD Gruppe

## § Trusted Site Privacy

TÜViT hat ein Zertifizierungsverfahren entwickelt, bei dem die Bewertung des Datenschutzes eines Prozesses mit der sicherheitstechnischen Untersuchung der entsprechenden Installationen kombiniert wird.

# TÜV Informationstechnik GmbH

Unternehmensgruppe TÜV NORD



Dr. Ernst-Hermann Gruschwitz  
Bereichsleiter Zertifizierung

Langemarckstraße 20  
45141 Essen

Telefon: +49 201 8999 – 580  
Telefax: +49 201 8999 – 555  
E-Mail: [E.Gruschwitz@tuvit.de](mailto:E.Gruschwitz@tuvit.de)  
URL: [www.certuvit.de](http://www.certuvit.de)