



# Vorlesung

## VPN: Drahtgebunden und drahtlos

Fachbereich Informatik (FB 20)

Lehrstuhl Prof. J. Buchmann

WS-05/ V2 - 20.205.1

In Zusammenarbeit mit dem CAST-Forum

Dr. Wolfgang Böhmer

Skript: <http://www.cdc.informatik.tu-darmstadt.de/~wboehmer/>

Email: [wboehmer@cdc.informatik.tu-darmstadt.de](mailto:wboehmer@cdc.informatik.tu-darmstadt.de)

---





# Vorlesungsinhalte

- Informations- und Kommunikationssicherheit
  - Definition IuK-Sicherheit
  - Verfahren zur Erlangung der IuK-Sicherheit
    - Risikoanalysen
    - ITSEC und Common Criteria (CC)
    - Sicherheitsarchitektur offener Systeme
  - Evaluierung der Gesamtunternehmenssicherheit
    - Die Sicherheitshierarchie
    - Lieferantenbewertungsmethoden
    - Benchmarking der IT-Sicherheit im Unternehmen





# Informations- und Kommunikationssicherheit

- Grenzen zwischen traditionellen und modernen Kommunikationsmittel lösen sich mehr und mehr auf
- Grundsätzlich zwei verschiedene Typen von Kommunikationsnetzen
  - Verteilnetze: Alle Teilnehmer bekommen vom Netz die gleiche Information (Fernsehen, Radio). Jeder Teilnehmer wählt lokal aus was er empfangen will.
  - Vermittlungsnetze: Jede Teilnehmerstation erhält vom Netz individuell nur das was vom Teilnehmer angefordert oder geschickt wurde. Es wird generell in zwei Richtungen kommuniziert.
- Aufbau von neuen Informationssystemen bringt nicht nur Vorteile, Risiken und Gefährdungen müssen ebenso in Betracht gezogen werden.
- Zu Vertiefung dieser Frage werden Schutzziele und Mechanismen betrachtet
  - Duale IT-Sicherheit
    - Verlässlich
    - Beherrschbar





# Die fünf Hauptaspekte der IuK-Sicherheit

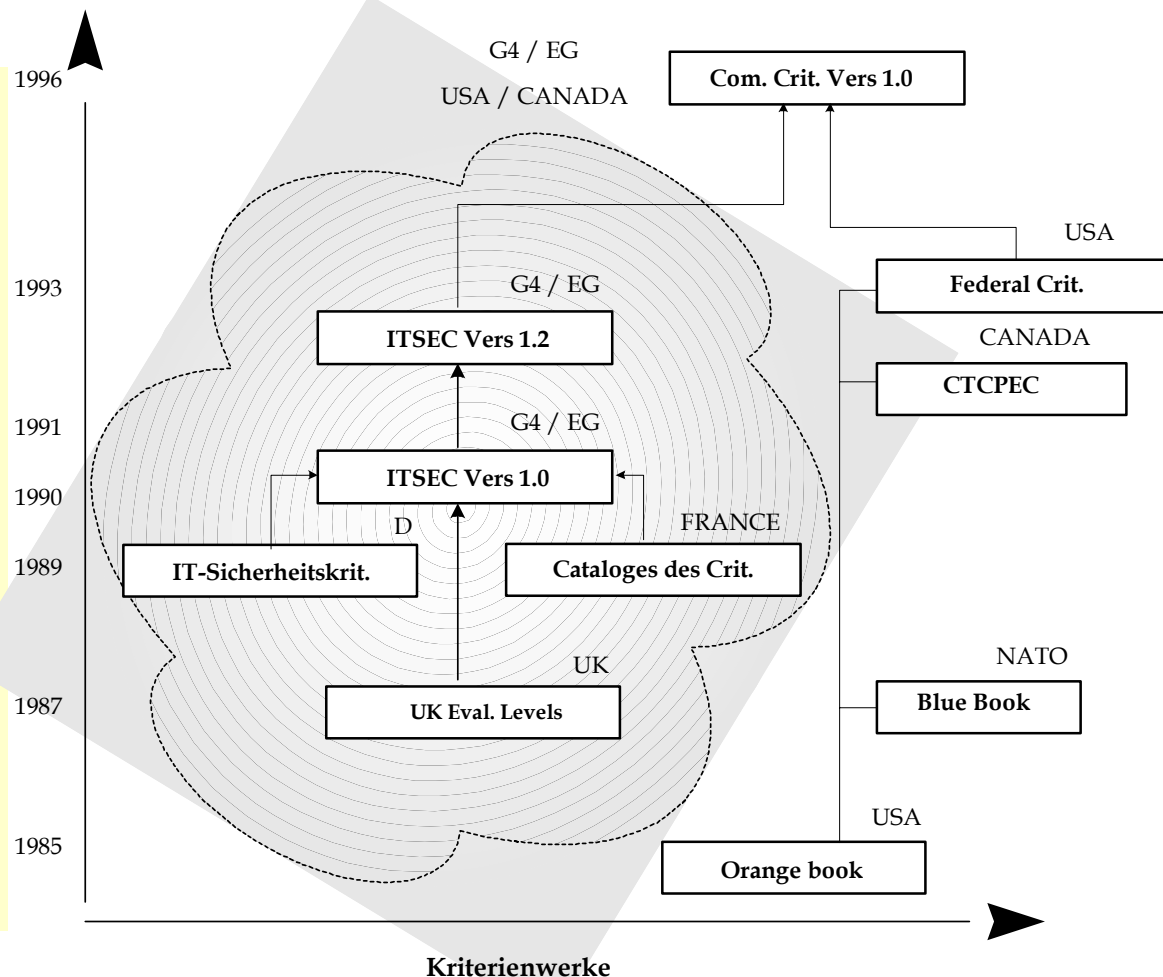
- Definition der IuK-Sicherheit gemäß BSI (neue Definition, ca. seit 2000)
  - Vertraulichkeit (*confidentiality*)
  - Integrität (*integrity*)
  - Verfügbarkeit (*availability*)
- Ergänzung Benutzersicht
  - Zurechenbarkeit (*accountability*)
  - Verbindlichkeit (*liability*)
- Hauptaspekte der IuK-Sicherheit sind Ziele eines jeden IT-Sicherheitskonzept
  - Unterbrechung, gerichtet gegen die Verfügbarkeit
  - Abhören, gerichtet gegen die Vertraulichkeit
  - Fälschung gerichtet gegen die Authentifizierung
  - Modifikation gerichtet gegen die Integrität





# Verfahren zur Erlangung der IuK-Sicherheit

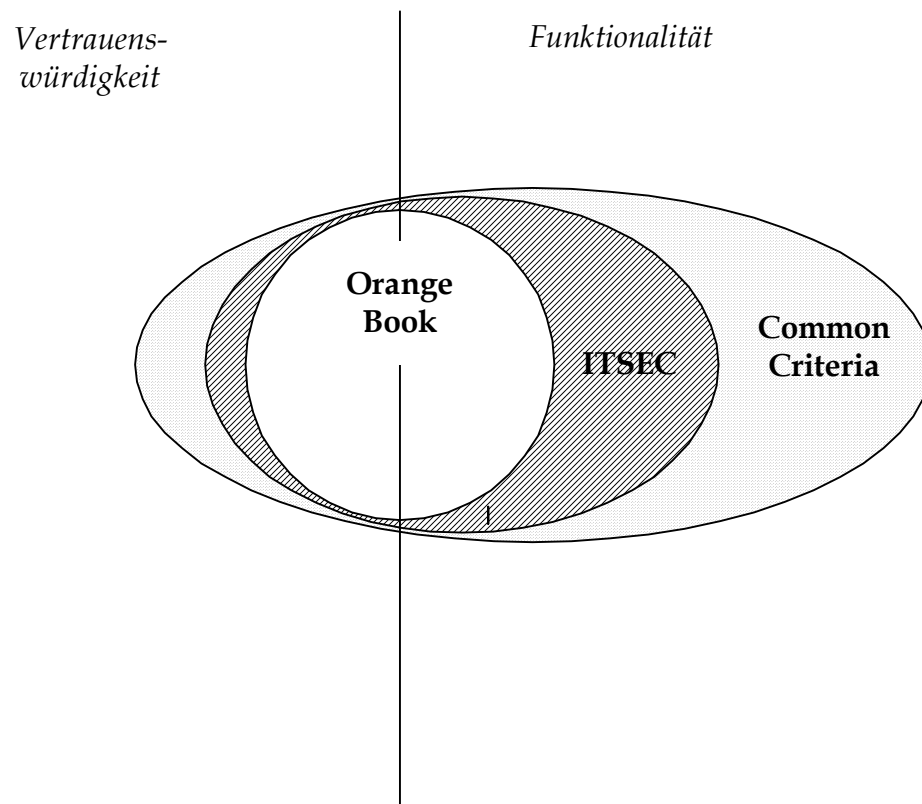
- **IuK-Sicherheit nicht nur technisch orientiert**
- **Beginn von Kriterienwerken ca. 1985 (Orange Book)**
- **Europäisches Modell ITSEC ca. 1990**
- **BSI-IT-Grundschutzhandbuch**
- **(erfreut sich großer Beliebtheit)**
- **BSI-IT-Sicherheitshandbuch**
- **(kaum angenommen)**





# Kriterienwerke im Vergleich

- Viele Gemeinsamkeiten zwischen ITSEC und CC
- Z.B. EAL2 der CC entspricht der Stufe E1 der ITSEC
- ITSEC-Funktionsklassen wird durch die CC-Schutzprofile abgelöst.
- CC deckt das größte Spektrum der Vertrauenswürdigkeit und Funktionalität ab





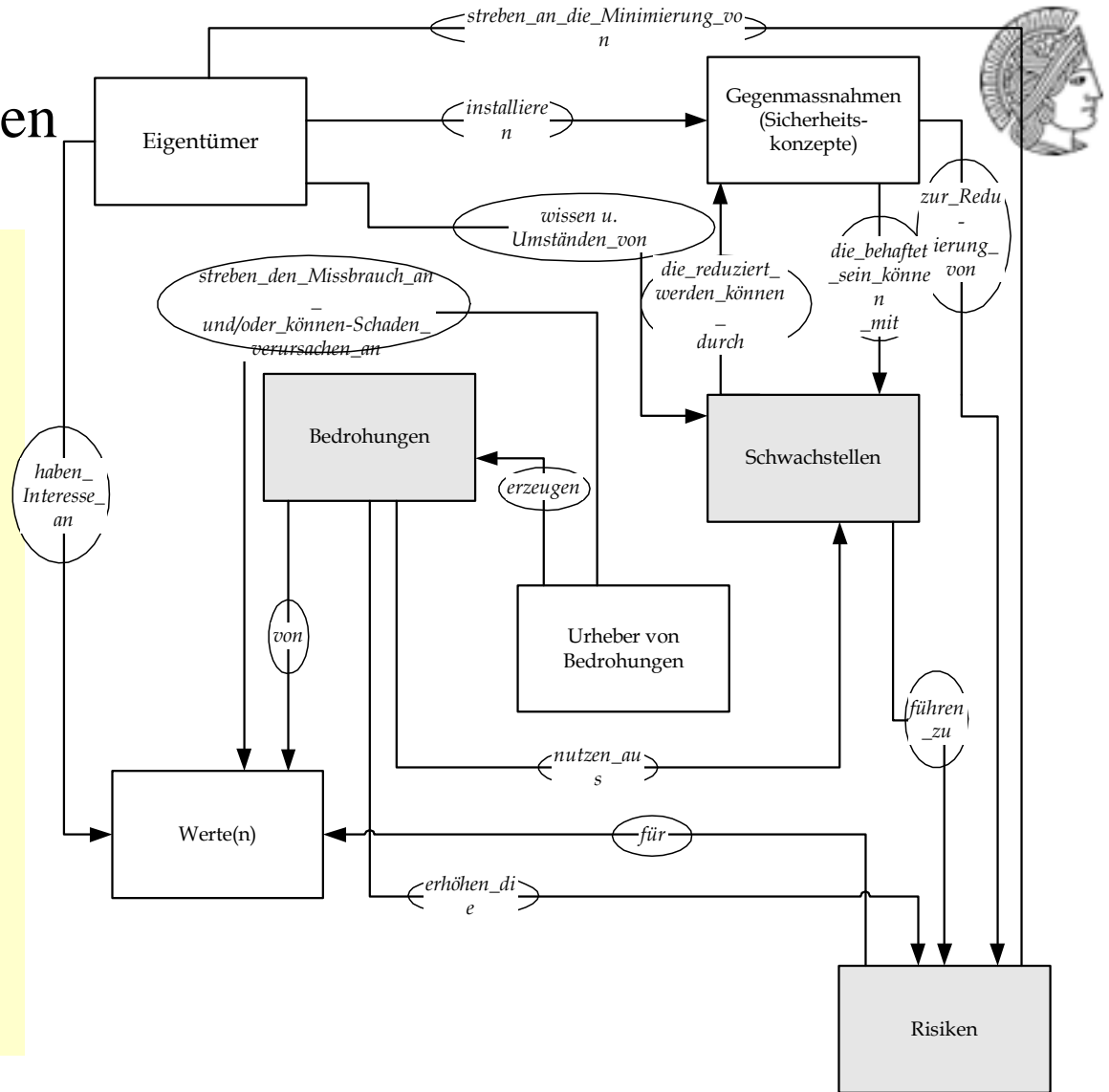
## Risikoanalyse (*Schutzbedarf hoch bis sehr hoch*)

- Versicherungsgesellschaften haben schon immer das Risiko kalkuliert
- Risiko-Definition nach DIN, VDE NORM 3100
  - **Risiko: Produkt von möglichen Eintrittswahrscheinlichkeiten und auftretenden Schäden**
- Wechselbeziehung zwischen Werten, Schwachstellen, Bedrohungen, Risiken
- Die CRAMM (CCTA Risk Analysis and Management Method) Methodik diskutiert diesen Sachverhalt. (Central Computer and Telecommunication Agency). Diese wurde im Auftrag der britischen Regierung entwickelt.
- Schutz von Werten mittels Sicherheitskonzept fällt in den Verantwortungsbereich der Eigentümer von Werten



# Wechselbeziehungen

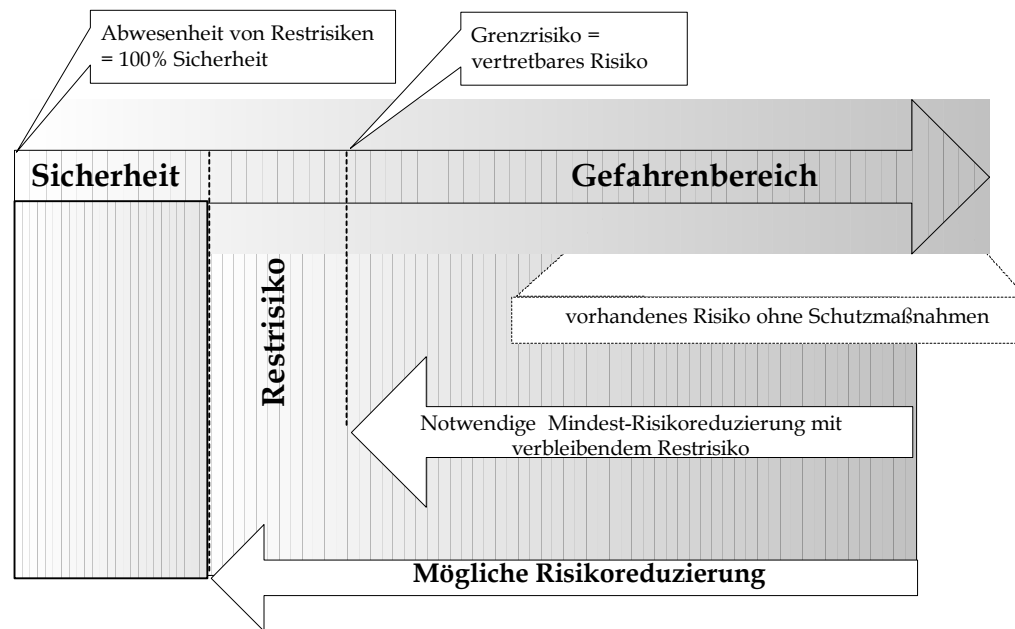
- **Bedrohungen und Schwachstellen bilden die Voraussetzung für mögliche Risiken**
- **Was ist Sicherheit?**





# Risikoachse

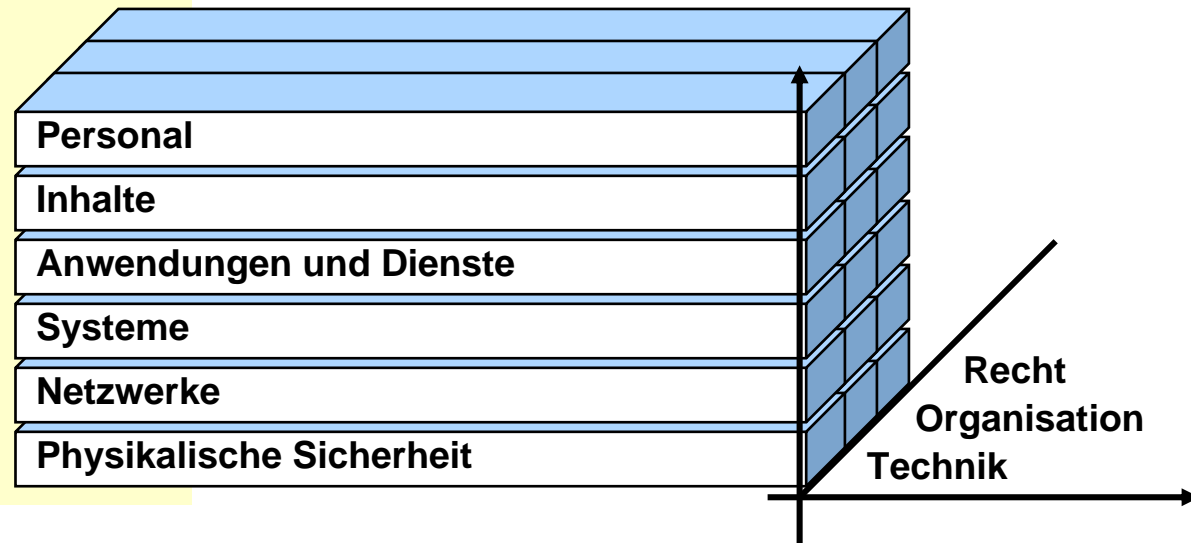
- **Sicherheit ein relativer Begriff, lässt sich nur durch die Restrisiken näher bestimmen.**
- **100% Sicherheit trifft zu, wenn keine Restrisiken mehr existieren**
- **Minimierung von Restrisiken ist das Ziel von Sicherheitskonzepten und deren Umsetzungen**





# Architekturmodell

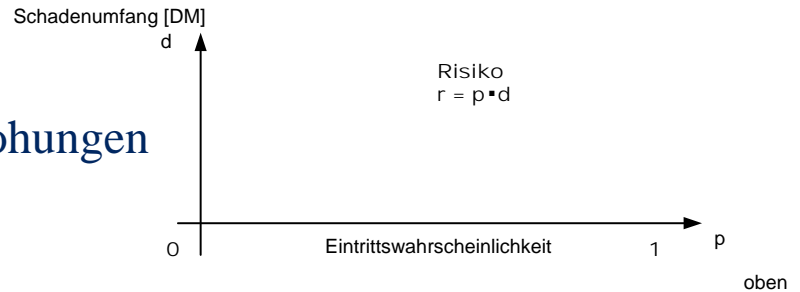
- Reduktion der Komplexität durch ein Architekturmodell
- Jede horizontale Ebene wird mit jeder vertikalen Ebene verknüpft
- Statische und dynamische Prüfung



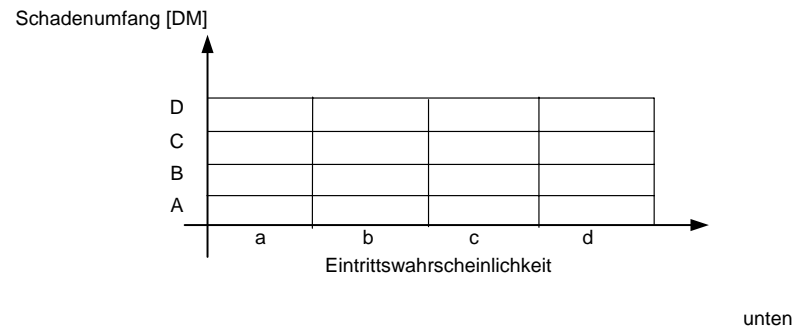


# Risikobestimmung mittels Szenarien

- Grundlage: Daten der IST-Aufnahme
- Diskussion der Schwachstellen und Bedrohungen
- Risikobetrachtung und Szenarienbildung



Risikoformel  
nach DIN 3100:



$$Rsz_i = Ep_i \left( \sum_{j=1}^l b_j \cdot \sum_{k=1}^m Schw_k \right) \bullet Scha_i$$





# Risikomatrix und Risikoentscheidung

|             |   |  |   |                                       |
|-------------|---|--|---|---------------------------------------|
| Sehr hoch   | RSz5                                    |  |   |                                       |
| Eher hoch   | RSz3/3, RSz6/3, RSz7/3, RSz9/3, RSz30/3 | RSz3/4, RSz6/4, RSz7/4, RSz9/4, RSz10, RSz11, RSz17/2, RSz22/3, RSz24/2, RSz27/2, RSz29/2, RSz37/2                                       | RSz16/3, RSz18/3, RSz20/3, RSz26, RSz30/2, RSz34  | RSz28/2, RSz31, RSz32, RSz33          |
| Eher gering | RSz13/2                                 | RSz3/1, RSz6/1, RSz7/1, RSz9/1, RSz12/1, RSz12/2, RSz14/2, RSz15/2, RSz17/1, RSz18/1, RSz19/2, RSz21/2, RSz24/1, RSz24/2, RSz29/1, RSz36 | RSz1, RSz2, RSz3/1, RSz6/2, RSz7/2, RSz8, RSz9/2, RSz13/1, RSz14/1, RSz15/1, RSz16/2, RSz18/2, RSz19/1, RSz20/1, RSz21/1, RSz22/1, RSz23/1, RSz25/1, RSz25/2, RSz34, RSz35, RSz37/1 | RSz28/1, RSz30/1, RSz31, RSz32, RSz33 |
|             | Sehr gering                             | Eher gering  | Eher hoch   | Sehr hoch                             |

Auswirkungen

Eintrittswahrscheinlichkeit

Risiken tragbar

Risiken sind zu beobachten

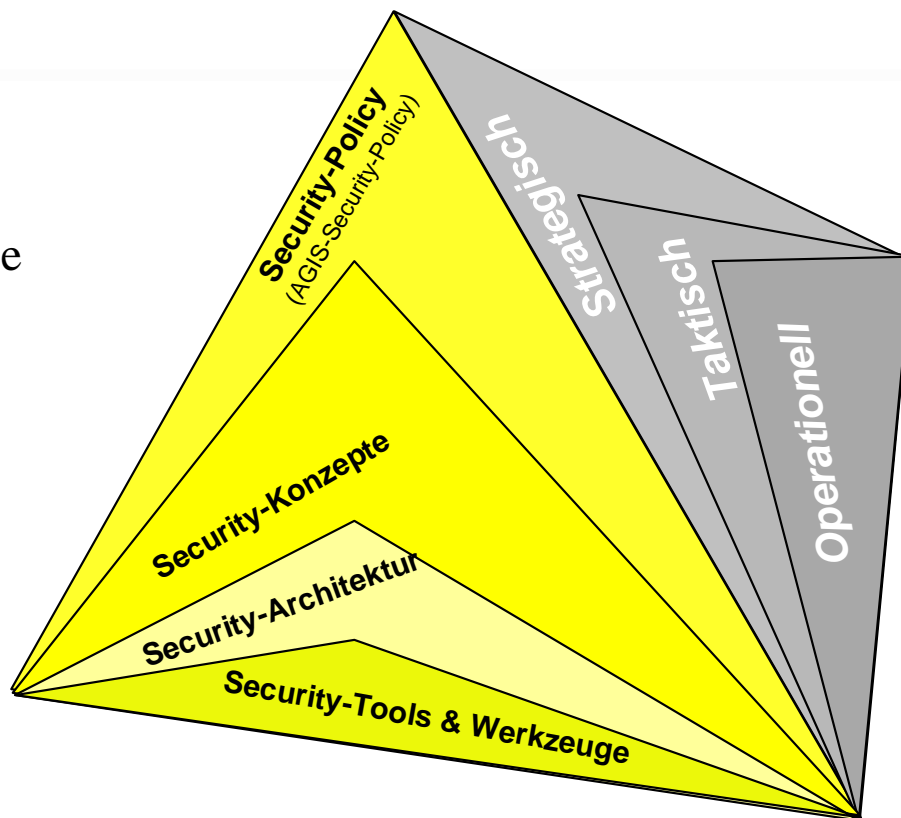
Risiken sind untragbar





# Ideale Sicherheitsstrukturen im Unternehmen

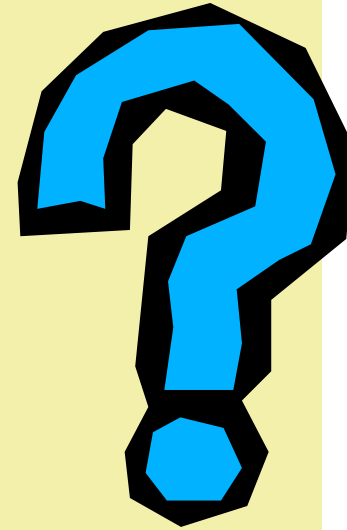
- IT-Sicherheitspolitik
- IT-Sicherheitskonzepte
- IT-Sicherheitsarchitektur
- Security-Tools & Werkzeuge





# VPN-Sicherheitspolitik

- Einzelbetrachtungen
  - BSI-Grundschutz
  - ITSec, CommonCriteria
  - BS7799 (ISO17799), BS7799-2
  - KonTraG, Artikel V, Basel II, IDW-PS-720 (§54HGrG)
  - HGB §289, §315 (Lagebericht mit Risiken)
  - Business Continuity Planning (BCP)
  - Business Impact Analysis (BIA)
  - COBRA, ITIL
  - Firewall-Systeme, IDS
  - Sniffer-Tools
  - etc,...



- Gesamtbeurteilung eines Unternehmens nicht möglich
  - Im Fall von Extranet-VPN tritt Unsicherheit ein
  - Es fehlen Verfahren die derartiges leisten

*Gibt es ähnliche Fragestellungen in der Wirtschaft?*



# Geschäftsprozessmodellierung anhand der Wertschöpfungskette des Unternehmens



- Kernprozesse werden modelliert
- Kernelemente werden identifiziert
- Kernelemente werden in die Bestandteile Organisation, Recht und Technik zerlegt.

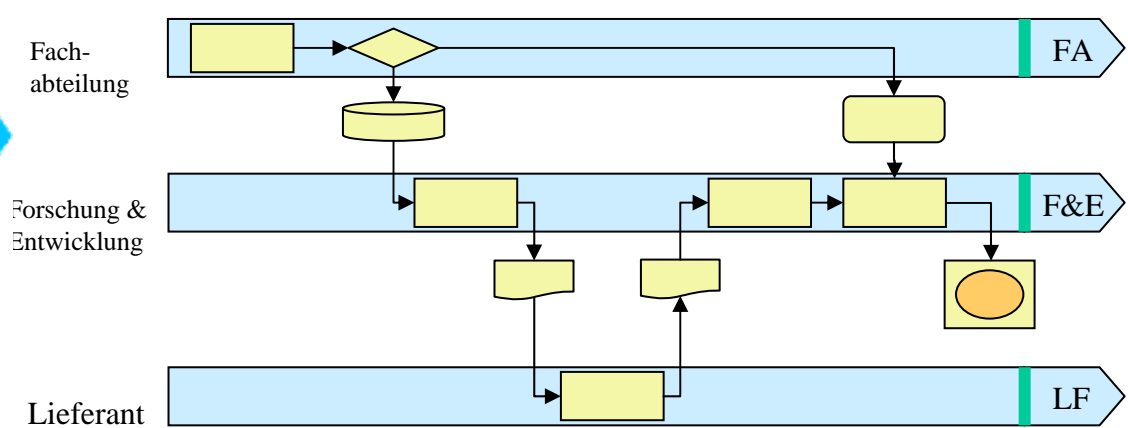
## Risikobewertung



## Risikoidentifikation



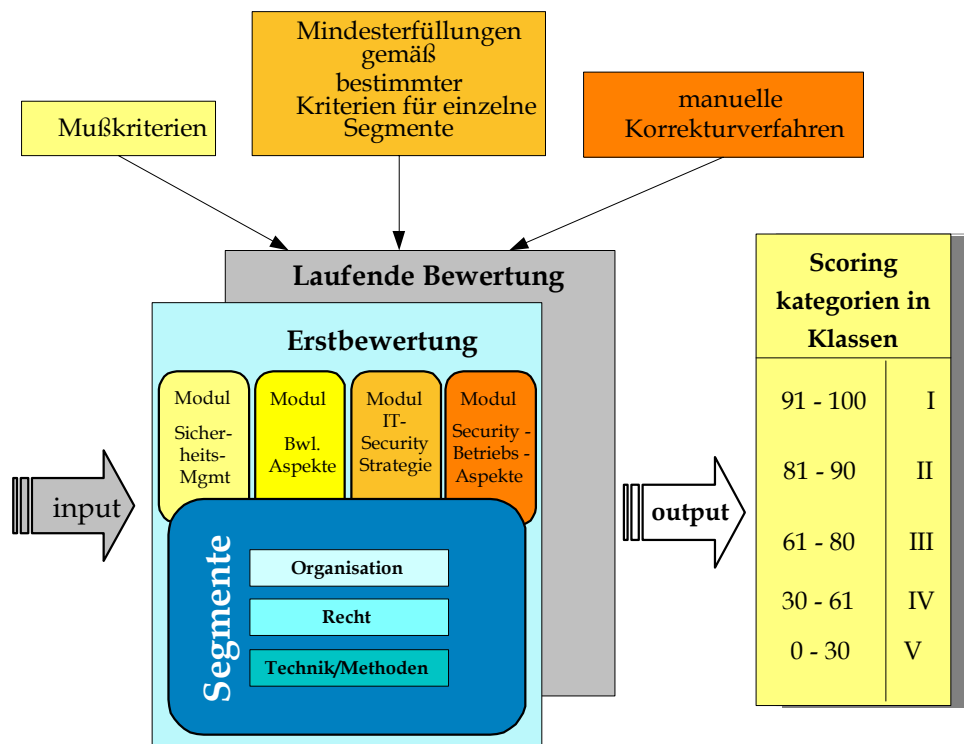
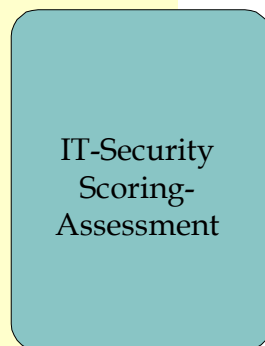
Checklisten, Interviews,  
Besichtigungen, Audits,  
Schadenanalysen,  
Prozessanalyse





# Evaluierung der Unternehmenssicherheit

- Diagnostisches Verfahren
  - Metrische Kennzahlen und
  - Empirisch Kennzahlen
- Entlehnt von der Lieferantenbewertungsmethode
- Aufteilung in Segmente / Module / Hauptkriterien
  - Sicherheitsmanagement
  - Betriebswirtschaft
  - IT-Security Strategie
  - IT-Security Betrieb





# Evaluierung der Hauptkriterien

Beispiel Modul: *Sicherheitsmanagement*

- Gewichtung der Hauptkriterien ist vorgegeben
- Struktur ist ähnlich wie ein Verzweigungsbaum

| Gewicht | Segment          | Hauptkriterium                | Nebenkriterium            | Gewichtung | Punkte (0-4) | Indexergebnis Beispiel Kunde A |
|---------|------------------|-------------------------------|---------------------------|------------|--------------|--------------------------------|
| 40 %    | Organisation     | <b>Personen / Kompetenzen</b> | Verantwortlichkeit        | 17,9%      |              |                                |
|         |                  | 30%                           | Leitung                   | 17,9%      |              |                                |
|         |                  |                               | Befugnisse                | 17,9%      |              |                                |
|         |                  |                               | Datenschutz               | 10,6%      |              |                                |
|         |                  |                               | IT-Sec.-Administration    | 10,7%      |              |                                |
|         |                  |                               | IT-Revision               | 14,3%      |              |                                |
|         |                  |                               | Notfallmanagement         | 10,7%      |              |                                |
|         |                  | <b>Dokumente / Konzepte</b>   | IT-Sicherheitspolitik     | 21,7%      |              |                                |
|         |                  | 30%                           | IT-Sicherheitskonzepte    | 21,7%      |              |                                |
|         |                  |                               | Schutzbedarf /Kategorie   | 21,7%      |              |                                |
|         |                  |                               | Dokumentenklassifizier.   | 21,7%      |              |                                |
|         |                  |                               | Notfallpläne              | 13,2%      |              |                                |
|         |                  | <b>Formale Kriterien</b>      | Bezug zum BS-7799         | 26,7%      |              |                                |
|         |                  | 10%                           | Bezug zu CoBit            | 26,7%      |              |                                |
|         |                  |                               | Bezug zum GsHB            | 20,7%      |              |                                |
|         |                  |                               | Bezug zum ISO-17799       | 26,7%      |              |                                |
|         |                  | <b>Sicherheitsprozess</b>     | Definition/Initiierung    | 18,5%      |              |                                |
|         |                  | 30%                           | Erstellung v. Richtlinien | 18,5%      |              |                                |
|         |                  |                               | Umsetzung d. Vorgaben     | 18,5%      |              |                                |
|         |                  |                               | Auditierung               | 18,5%      |              |                                |
|         |                  |                               | Sanktionen                | 14,8%      |              |                                |
|         |                  |                               | Fortschreibung            | 11,1%      |              |                                |
| 25 %    | Recht            |                               |                           |            |              |                                |
| 35 %    | Technik/Methoden |                               |                           |            |              |                                |








29.11.2005



# Nebenkriterium



- Nebenkriterien am Beispiel Personen /Kompetenzen bezogen auf eine 5 Pkt. Werteskala

| Personen / Kompetenzen   |   |   |
|--|---|---|
| <ul style="list-style-type: none"> <li>➤ Verantwortlichkeit                             <ul style="list-style-type: none"> <li>• keine vorhanden</li> <li>• einzelne Admins im Verantwortungsbereich</li> <li>• einzelne Sicherheitsverantwortliche koordinieren</li> <li>• zentraler Sicherheitsbaufr. koor.diniert</li> <li>• Ausgeprägte hierarische Strukturen vorhanden</li> </ul> </li> </ul>  | ➔ | 0  4   |
| <ul style="list-style-type: none"> <li>➤ Leitung                             <ul style="list-style-type: none"> <li>• Aufgabe wird nicht wahr genom.men</li> <li>• Aufgaben nimmt CISO wahr</li> <li>• Aufgabe nimmt Vorstand wahr</li> <li>• Aufgabe nimmt GF wahr</li> </ul> </li> </ul>   | ➔ | 0  4   |
| <ul style="list-style-type: none"> <li>➤ Befugnisse                             <ul style="list-style-type: none"> <li>• Keine Befugnisse</li> <li>• Nur empfehlender Charakter der Befugnis</li> <li>• Nur auf Abteilungsebene</li> <li>• Nur für die IT-Abtl.</li> <li>• Unternehmensweite Befugnis</li> </ul> </li> </ul>   | ➔ | 0  4   |
| <ul style="list-style-type: none"> <li>➤ Datenschutz                             <ul style="list-style-type: none"> <li>• existiert ein aktiver Datenschutz</li> <li>• Ist der Datenschutzbeauftragte ins IT-Sicherheitsmanagement eingebunden?</li> </ul> </li> </ul>   | ➔ | 0  4   |
| <ul style="list-style-type: none"> <li>➤ IT-Revision                             <ul style="list-style-type: none"> <li>• Existiert Fachpersonal für die IT-Revision?</li> <li>• Wird IT-Revision mit der reg. Revision abgedeckt?</li> </ul> </li> </ul>  | ➔ | 0  4   |
| <ul style="list-style-type: none"> <li>➤ Notfallmanagement                             <ul style="list-style-type: none"> <li>• Es ist kein Notfallmanagement vorhanden</li> <li>• Es sind einzelne isolierte Notfall-Verantw. vorhan..</li> <li>• verschiedene N-Verantwortliche arbeiten zusam.</li> <li>• Ein zentraler N-Verantwortlicher koordiniert</li> <li>• Ein komplettes Notfall-Magement ist vorhanden.</li> </ul> </li> </ul> | ➔ | 0  4 |
| <ul style="list-style-type: none"> <li>➤ IT-Sec-Administration                             <ul style="list-style-type: none"> <li>• Existieren spezielle Sicherheits-Admins?</li> <li>• Nur für bestimmte Bereiche , bzw. Betriebssysteme</li> <li>• Es existieren unternehmensweit IT-Sec-Admins?</li> </ul> </li> </ul>  | ➔ | 0  4 |



# Scoring-Ergebnisse

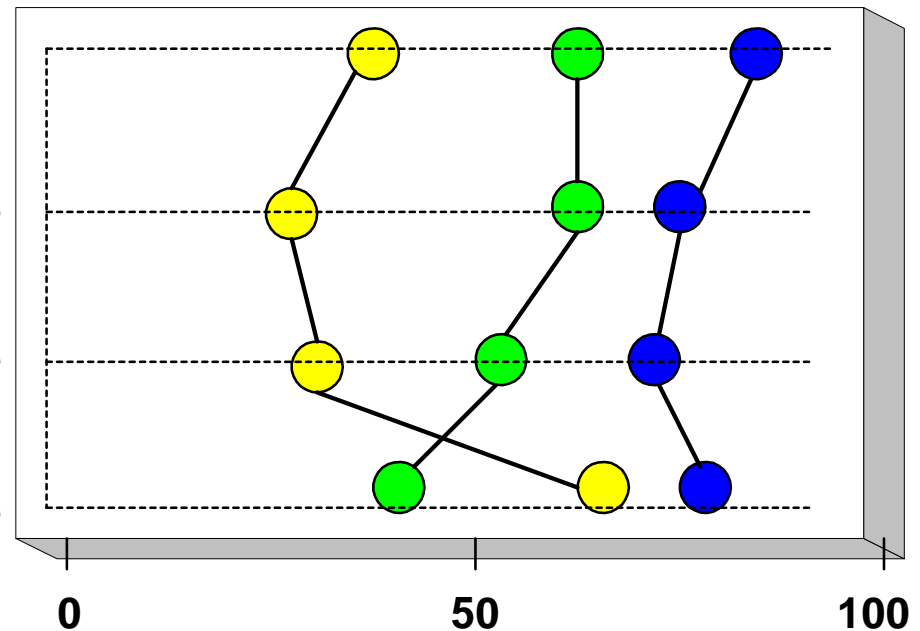


Modul: **Sicherheitsmanagement**

Modul: **Betriebswirtschaftl. Aspekte**

Modul: **IT-Sec-Strategie**

Modul: **Security-Betriebsaspekte**

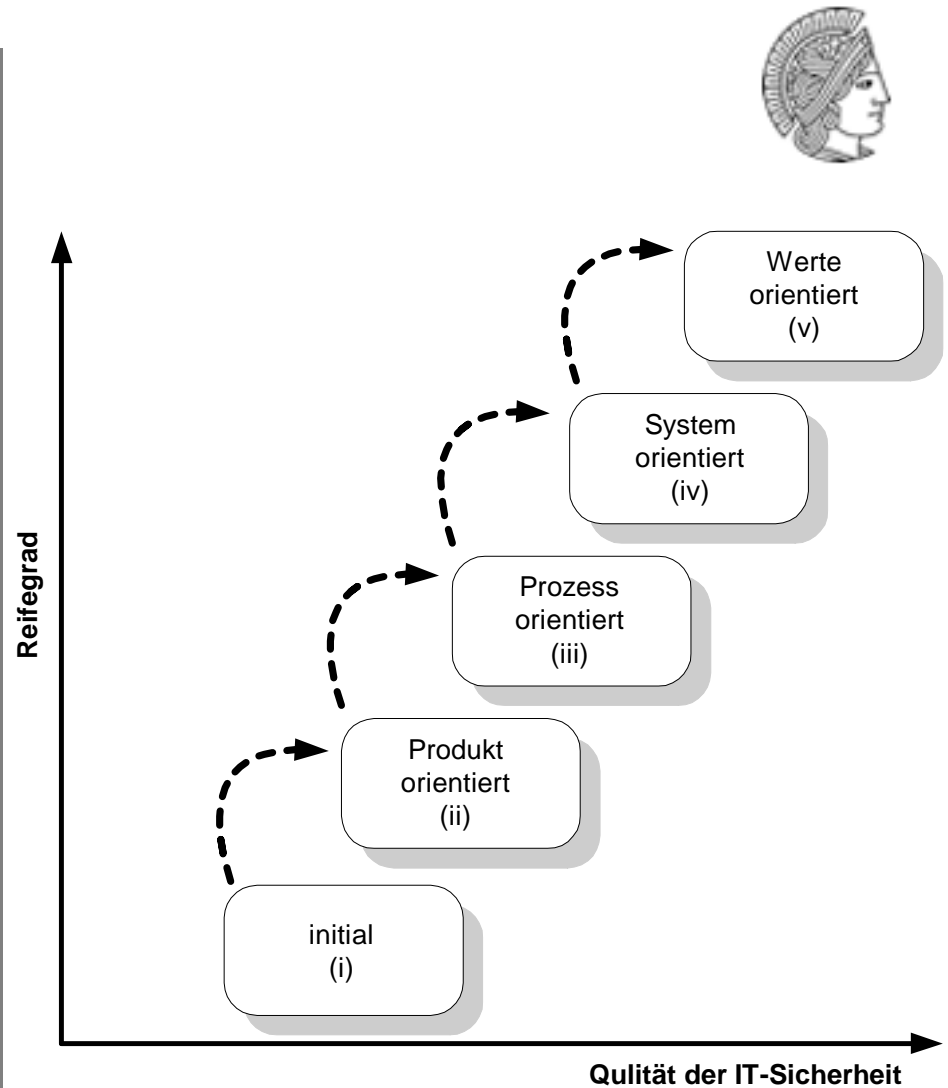


- Branchendurchschnitt
- betrachtetes Unternehmen
- Best-in-Class



# IT-Security Maturity Model

- *Klasse I* zeigt den untersten Reifegrad. Unternehmen auf diesem Niveau haben keine IT-Sicherheit bzw. beginnen erst sich damit auseinander zusetzen.
- *Klasse II* bringt einen geringen Reifegrad zum Ausdruck. Das Unternehmen hat hier seine IT-Sicherheit lediglich auf Sicherheits-Komponenten wie z.B. Firewall-Systeme und Virens Scanner beschränkt
- *Klasse III* kennzeichnet besser ausgelegte Unternehmen, in denen bereits in IT-Sicherheitsprozesse gedacht und gehandelt wird und IT-Sicherheitsprodukte als Mittel zum Zweck eingesetzt werden
- *Klasse IV* stellt systemorientierte Unternehmen dar, die z.B. abteilungsübergreifend ihre IT-Sicherheit ausgelegt und aufeinander abgestimmt haben. Weiterhin sollte bereits ein gewisses Maß an taktischen Vorgaben und Verfahren der IT-Sicherheit im Unternehmen, neben operativen IT-Sicherheitstätigkeiten, beherrscht und angewendet werden.
- *Klasse V - als höchster Reifegrad* - bezeichnet Unternehmen, das seine IT-Sicherheit an seiner Wertschöpfungskette ausrichtet und nicht nur taktische sondern auch strategische IT-Sicherheitsentwicklung, neben den operativen IT-Sicherheitstätigkeiten, beherrscht und anwendet.





# Literatur

- <http://www.tu-darmstadt.de/vvws04/comments/20.205.1>
- Heindl, E. et al.: Der IT-Sicherheitsexperte, Addison-Wesley Verlag, 2001, ISBN 3-8273-1840-8.
- Mühlenbrock, F.: IT-Sicherheit im Unternehmen, Verlag: Smart Books. Version: 1. Auflage, 2003 ISBN: 3908492440.
- CRAMM, from Insight Consulting, Feb 2004, <http://www.cramm.com>
- A Practitioner's View of CRAMM. Januar 2003-  
<http://www.gammassl.co.uk/topics/hot5.html>
- BSI.: GsHB, Grundschutzhandbuch Ausgabe 2004, [www.bsi.bund.de](http://www.bsi.bund.de)
- Hertoge-Vogt, M. Kreischatus, B.: IT-Service Management, Eine Einführung, Übersetzung aus dem Englischen, Erste Auflage, ISBN 90-806713-5-5.
- Eckert, C.: IT-Sicherheit, Konzepte-Verfahren-Protokolle, Oldenbourg Verlag, 2. Auflage, ISBN: 3486272055





# Übungsaufgabe

1. Wie könnte eine typische Richtlinie aussehen bezogen auf die Folie 13, wenn es um die Absicherung von personenbezogenen Daten außerhalb eines Unternehmen geht?
2. Wie könnte ein typisches Konzept bezogen auf die Frage 1. aussehen?
3. Wie könnte ein typische Architektur (Teilkomponente) bezogen auf die Frage 2 aussehen?
4. Wie könnte eine typische operative Umsetzung bezogen auf die Frage 3 aussehen?
5. Was steht einem Risiko gegenüber?

